

**Universidad ORT Uruguay
Facultad de Ingeniería**

Mejora de la seguridad de la información en un organismo público

Entregado como requisito para la obtención del título de Máster en Gestión de Sistemas
de Información

Luis Jaunarena - 101915

Ma. Mercedes Schicht - 316998

Katherine Venegas - 317442

Tutor: Felipe Sotuyo

2025

Declaración de autoría

Nosotros, Katherine Venegas, Ma. Mercedes Schicht y Luis Jaunarena declaramos que el trabajo que se presenta en esa obra es de nuestra propia mano. Podemos asegurar que:

- La obra fue producida en su totalidad mientras realizábamos Master en Gestión de Sistemas de Información;
- Cuando hemos consultado el trabajo publicado por otros, lo hemos atribuido con claridad;
- Cuando hemos citado obras de otros, hemos indicado las fuentes. Con excepción de estas citas, la obra es enteramente nuestra;
- En la obra, hemos acusado recibo de las ayudas recibidas;
- Cuando la obra se basa en trabajo realizado conjuntamente con otros, hemos explicado claramente qué fue contribuido por otros, y qué fue contribuido por nosotros;
- Ninguna parte de este trabajo ha sido publicada previamente a su entrega, excepto donde se han realizado las aclaraciones correspondientes.



Luis Jaunarena

24/03/2025



Ma. Mercedes Schicht

24/03/2025



Katherine Venegas

24/03/2025

Agradecimientos

Este trabajo marca el cierre de una etapa significativa en nuestras vidas. Ha sido un camino lleno de aprendizajes, desafíos y crecimiento personal y profesional. Un trayecto que, aunque no siempre fue fácil, resultó profundamente gratificante y enriquecedor. Hoy, al llegar a su fin, miramos hacia atrás con gratitud por cada paso dado y por todas las personas que caminaron a nuestro lado.

Queremos expresar nuestro más sincero agradecimiento a todas las personas que nos acompañaron y apoyaron durante la realización de esta tesis.

A nuestras familias, por su amor, comprensión y constante apoyo en cada etapa de este proceso. Su presencia y ánimo fueron fundamentales para mantenernos firmes en los momentos de mayor desafío.

A nuestros amigos y personas cercanas, gracias por su compañía, palabras de aliento y por celebrar cada avance con nosotros. Su apoyo emocional fue clave para continuar con motivación y confianza.

Agradecemos especialmente a nuestro tutor, por su guía, compromiso y disposición para acompañarnos en cada paso de este trabajo. Su experiencia y orientación fueron esenciales para dar forma a nuestro trabajo.

También queremos agradecer a las personas del organismo que nos brindaron su colaboración y apoyo durante la ejecución de la tesis. Su aporte fue invaluable para poder llevar adelante este proyecto de manera exitosa.

A todos, gracias por ser parte de este camino y de este logro.

Abstract

El presente trabajo, titulado "Mejora de la seguridad de la información en un organismo público", tiene como objetivo proponer un conjunto de recomendaciones basadas en el Marco de Ciberseguridad (MCS) de AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento), diseñado para fortalecer la seguridad de la información en un organismo público de Uruguay.

Este proyecto se centra en el área de Tecnología de la Información y Comunicaciones (TIC), evaluando su situación actual en términos de ciberseguridad y perfilando estrategias para implementar el MCS de manera efectiva. El estudio aborda cinco funciones clave del MCS de AGESIC: Identificar, Proteger, Detectar, Responder y Recuperar, analizando las brechas existentes y priorizando las acciones de mejora en función de los niveles de madurez establecidos por el modelo de AGESIC.

Los resultados obtenidos buscan no solo mitigar los riesgos inmediatos, sino también establecer una base sólida para la mejora continua de la ciberseguridad, alineando los objetivos estratégicos del organismo con las mejores prácticas recomendadas por el MCS de AGESIC. Este enfoque pretende ser escalable y adaptable, permitiendo su extensión futura a otras áreas del organismo.

Palabras clave

Seguridad de la Información, Políticas de Seguridad de la Información, Ciberseguridad, Marco de Ciberseguridad de AGESIC.

Índice

1.	Introducción.....	12
2.	El organismo.....	13
2.1.	Descripción del organismo	13
2.2.	Estructura organizacional	14
2.3.	Descripción de responsabilidades por división.....	16
2.3.1.	Comunicación Institucional	16
2.3.2.	Secretaría de Directorio	16
2.3.3.	Tecnología de la Información y Comunicaciones	16
2.3.4.	Planeamiento y Presupuesto Estratégico	16
2.3.5.	Jurídica	17
2.3.6.	Dirección General.....	17
2.3.7.	Centro de Capacitación y Formación	17
2.3.8.	Subdirección General de Administración.....	17
2.3.9.	Financiero Contable.....	17
2.3.10.	Adquisiciones.....	17
2.3.11.	Gestión y Desarrollo Humano	18
2.3.12.	Logística.....	18
2.3.13.	Áreas de Servicio	18
2.4.	Responsabilidades por departamento en la División TIC.....	18
2.4.1.	Departamento de Desarrollo.....	18
2.4.2.	Departamento de Soporte	18
2.4.3.	Departamento de Infraestructura	18
3.	Marco de Ciberseguridad de AGESIC	19
3.1.	Aplicabilidad.....	19
3.2.	Estructura	19

3.3.	Ciclo de vida de la ciberseguridad	20
3.4.	Estructura del MCS.....	20
3.4.1.	Función	21
3.4.2.	Categoría.....	21
3.4.3.	Subcategoría	21
3.4.4.	Perfil	21
3.4.5.	Prioridad	22
3.4.6.	Referencias	23
3.4.7.	Requisitos	23
3.4.8.	Niveles de Implementación	25
3.5.	Modelo de madurez	27
3.5.1.	Objetivos del modelo.....	28
3.5.2.	Niveles de madurez	28
3.5.3.	Ámbitos de evaluación	29
3.5.4.	Pasos para seguir la implementación del MCS de AGESIC	29
4.	Protección de Datos Personales.....	32
4.1.	La Ley N° 18.331 y su relevancia para el organismo	32
4.2.	Alineación de la Ley N° 18.331 con el MCS de AGESIC.....	32
4.3.	Creación de la Política de Protección y Privacidad de los Datos (PPPD) alineada con la Ley N° 18.331 y el MCS	33
5.	Aplicación del MSC de AGESIC	35
5.1.	Justificación de la utilización del MCS de AGESIC	35
5.1.1.	Recomendaciones de adopción del MCS de AGESIC	35
5.1.2.	Diferencias entre el MCS de AGESIC y el Marco ITIL	36
5.2.	Aplicación del MCS en la División TIC.....	38
5.2.1.	Tamaño del organismo	39

5.2.2.	Tiempos reducidos del proyecto.....	39
5.2.3.	Dificultades de adopción del marco	40
5.2.4.	Alineación con los riesgos y necesidades actuales.....	40
5.3.	Plan de Implementación del MCS de AGESIC	40
6.	Evaluación de la situación actual del organismo según el MCS de AGESIC	42
6.1.	El modelado del Marco para el organismo	42
6.2.	Aplicación del cuestionario para evaluar los niveles de madurez	43
6.2.1.	Entrevistas realizadas	43
6.3.	Situación actual en ciberseguridad	46
6.3.1.	Responsable en ciberseguridad.....	46
6.3.2.	Referente de Datos Personales	46
6.3.3.	Comisión de Seguridad de la Información (CSI)	46
6.3.4.	Política de Seguridad de la Información (PSI)	46
6.3.5.	Capacitación y formación en Seguridad de la Información	46
6.3.6.	Enfoque reactivo ante incidentes de seguridad.....	46
7.	Análisis de la situación actual del organismo.....	48
7.1.	Perfil Actual del Organismo	48
7.1.1.	Identificar.....	49
7.1.2.	Proteger.....	50
7.1.3.	Detectar.....	52
7.1.4.	Responder	53
7.1.5.	Recuperar.....	54
7.2.	Recomendaciones propuestas	55
8.	Mejoras introducidas en temas de Políticas de Seguridad y Capacitación.....	57
8.1.	Principales modificaciones en la PSI.....	57
8.2.	Generación de nuevas Políticas	59

8.3.	Capacitaciones	61
8.3.1.	Plan de Concientización y Sensibilización.....	61
8.3.2.	Material de Capacitaciones.....	62
9.	Resumen de actividades realizadas a la fecha de presentación de este trabajo ...	65
10.	Conclusiones.....	67
	Referencias bibliográficas	68
	ANEXO 1 - Carta de consentimiento	70
	ANEXO 2 - Entregable 1: Situación actual de la Seguridad de la Información en el organismo	71
	ANEXO 3 - Entregable 2: Políticas a medida del organismo	110
	ANEXO 4 - Entregable 3: Plan y material de capacitaciones	305
	ANEXO 5 - Listado de actividades pendientes	448
	ANEXO 6 - Listado completo de actividades	475
	ANEXO 7 - Política de Seguridad de Información vigente	540

Índice de tablas

Tabla 1: Funciones del MCS de AGESIC	24
Tabla 2: Proceso de Gestión de Riesgos.....	25
Tabla 3: Proceso de Integración de la Gestión de Riesgos.....	26
Tabla 4: Proceso de Participación Externa	26
Tabla 5: Tabla comparativa de MCS de AGESIC y el Marco de ITIL	38
Tabla 6: Tabla con distribución de cantidad de tareas por prioridad.....	41
Tabla 7: Descripción de la categoría ID.GO y subcategoría ID.GO-1.....	44
Tabla 8: Tabla de actividades para subcategoría ID.GO-1 por nivel de madurez.....	45
Tabla 9: Resultados de la Función Identificar	49
Tabla 10: Resultados de la Función Proteger	51
Tabla 11: Resultados de la Función Detectar	52
Tabla 12: Resultados de la Función Responder	53
Tabla 13: Resultados de la Función Recuperar	55
Tabla 14: Principales modificaciones de la PSI	58
Tabla 15: Detalle de cantidad de tareas por función y estado para P1	65
Tabla 16: Detalle de cantidad de tareas por función y estado para P2	66
Tabla 17: Detalle de cantidad de tareas por función y estado para P3	66

Índice de ilustraciones

Ilustración 1: Distribución de personal en OP	14
Ilustración 2: Organigrama conceptual del OP.....	15
Ilustración 3: El ciclo de vida de la ciberseguridad	20
Ilustración 4: Estructura del MCS	21
Ilustración 5: Niveles de madurez del MCS de AGESIC.....	27
Ilustración 6: Resultados de Función Identificar	49
Ilustración 7: Resultados de la Función Proteger	51
Ilustración 8: Resultados de la Función Detectar	52
Ilustración 9: Resultados de la Función Responder.....	54
Ilustración 10: Resultados de la Función Recuperar	55

1. Introducción

El presente proyecto titulado “Mejora de la seguridad de la información en un organismo público” tiene como objetivo diagnosticar la situación actual con relación a la seguridad de la información de un organismo público en Uruguay (que denominaremos con el nombre ficticio OP) y proponer un conjunto de recomendaciones de mejora.

La información que gestiona el OP, de acuerdo con la clasificación de la información promovida por la ley N° 18.331 “Protección de Datos Personales y acción de Habeas Data” [1], es considerada sensible, motivo principal por el que se desea proponer un conjunto de mejoras de la seguridad de la información a los efectos de asegurar la protección de los datos personales y la seguridad de la información.

Para este proyecto utilizamos como referencia el Marco de Ciberseguridad (en adelante MCS) [2] de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (en adelante, AGESIC) [3], asegurándonos de que nuestras recomendaciones estén alineadas con las directrices establecidas.

2. El organismo

En este capítulo se presenta una descripción del organismo público, su estructura organizacional y se describen las responsabilidades por división, en particular de la División TIC.

A los efectos de mantener la confidencialidad de la información recabada en este proyecto, se elaboró un Acuerdo de Confidencialidad (ver ANEXO 1 - Carta de consentimiento), la cual fue suscrita por la Dirección de la División de Tecnología de la Información y Comunicaciones del organismo (en adelante División TIC) y los integrantes de este proyecto. En este documento se establecen de manera clara y detallada las condiciones de confidencialidad respecto al manejo de la información proporcionada por el organismo.

Dado que mucha de la información provista por el organismo se puede clasificar como información privada y/o sensible, y considerando el manejo que el organismo hace de este tipo de información, en este acuerdo se especifica que toda la información suministrada por el organismo será utilizada exclusivamente para los fines definidos en el marco de este proyecto.

Es importante destacar, que toda la información será adecuadamente anonimizada en este documento, para que no pueda ser utilizada con otros fines diferentes a los específicos para este proyecto.

2.1. Descripción del organismo

El OP tiene su sede central en Montevideo, donde se encuentran sus oficinas principales, pero ofrece servicios en todos los departamentos del país. Cada departamento cuenta con una sede departamental que actúa como oficina principal de su región, además de otros puntos de atención distribuidos en distintas localidades del departamento para asegurar su cobertura de servicios.

El OP cuenta con aproximadamente 5.000 vínculos laborales, que podrían dividirse principalmente en dos categorías: personal de servicio y personal

administrativo. Como se presenta en la Ilustración 1, aproximadamente el 65 % es personal de servicio y el restante 35 % es personal administrativo.



Ilustración 1: Distribución de personal en OP

Cabe destacar que el OP se distingue por el profundo impacto que tiene en la sociedad, gracias a la diversidad de los servicios que ofrece. Su tamaño y alcance no solo evidencian su relevancia, sino que también lo consolidan como un actor clave en la promoción del cambio social en el país. Además, colabora de manera activa con otros organismos públicos, fortaleciendo el bienestar colectivo. Su labor está enfocada en impulsar transformaciones sostenibles, contribuyendo significativamente al desarrollo y bienestar de la sociedad uruguaya.

2.2. Estructura organizacional

La estructura organizacional se compone por un Directorio conformado por cuatro integrantes: el presidente, el vicepresidente y dos directores. Este Directorio se reúne de forma semanal, instancia en la cual se toman decisiones estratégicas sobre los temas del organismo y se hace un seguimiento de los avances de los proyectos en curso.

Por debajo del Directorio, se establece una estructura jerárquica clásica, propia de los organismos públicos en Uruguay, organizada en aproximadamente 28 divisiones. Cada división está encabezada por un Director y puede subdividirse en diferentes departamentos, sumando un total de alrededor de 70 departamentos, cada uno de los cuales también cuenta con un Director a cargo.

Según su organigrama conceptual se destacan las siguientes divisiones (ver Ilustración 2): Comunicación Institucional, Secretaría de Directorio, Dirección General, Jurídica, Planeamiento y Presupuesto Estratégico, TIC, Financiero Contable, Adquisiciones, Gestión y Desarrollo Humano, Logística, Centro de Capacitación y Formación, y Áreas de Servicio.

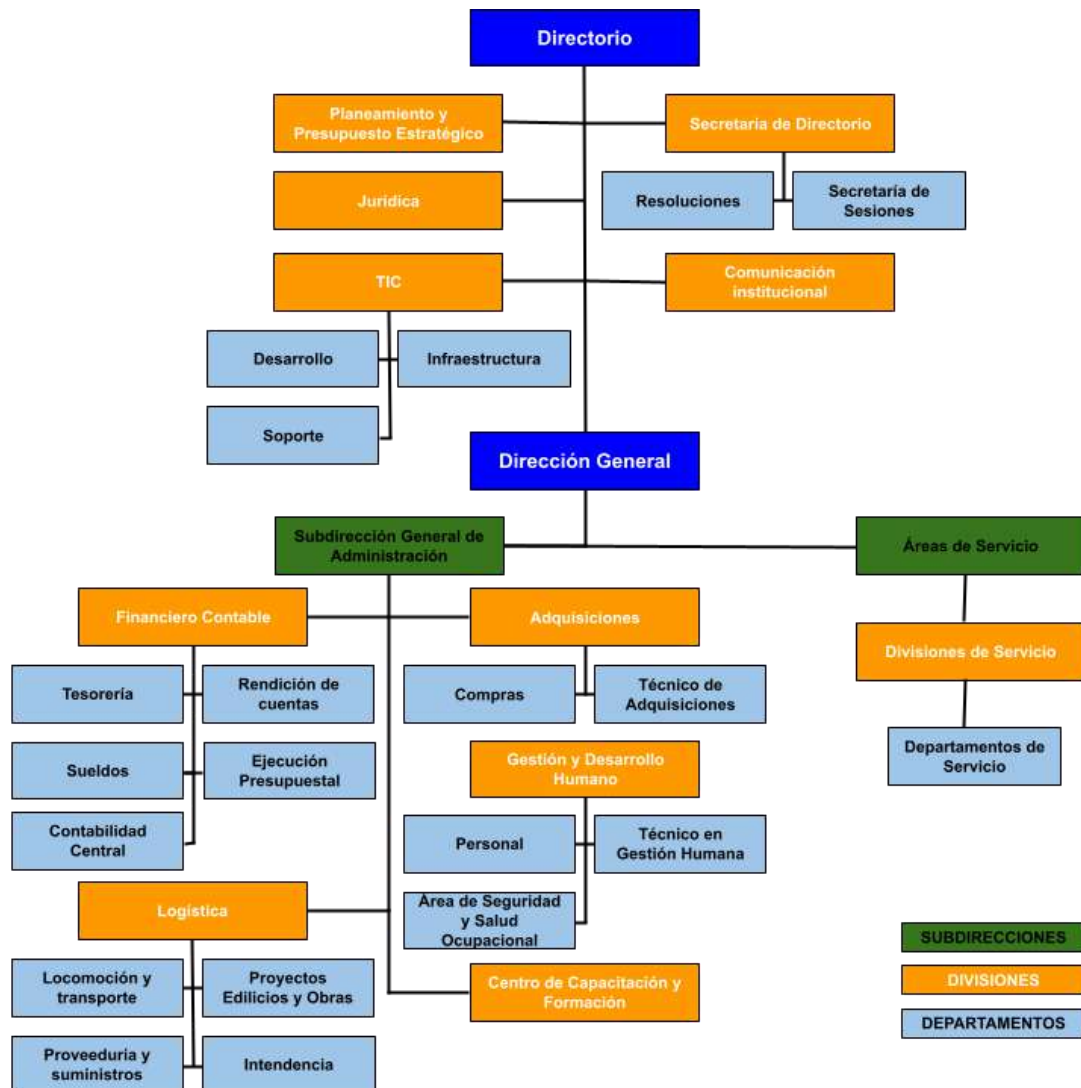


Ilustración 2: Organigrama conceptual del OP

2.3. Descripción de responsabilidades por división

2.3.1. Comunicación Institucional

Esta división es responsable de administrar los canales de comunicación de la organización, asegurando la difusión de mensajes a nivel interno para garantizar el correcto funcionamiento del organismo. Su labor permite que todos los colaboradores accedan a información actualizada, promoviendo el alineamiento del OP. En cuanto a la comunicación externa, se encarga de actualizar el contenido de su página web, asegurando que refleje de manera precisa la información relevante para el público en general.

2.3.2. Secretaría de Directorio

Esta división actúa como un puente de comunicación entre el Directorio y las áreas internas del organismo. Lleva el registro de las resoluciones adoptadas durante las sesiones del Directorio. Está compuesta por los departamentos de Secretaría de Sesiones, y de Resoluciones.

2.3.3. Tecnología de la Información y Comunicaciones

Esta división gestiona los recursos tecnológicos y de comunicación que son necesarios para llevar adelante todas las operaciones del organismo. Está compuesta por los departamentos: Desarrollo y Gestión de Sistemas (que denominaremos Desarrollo), Operaciones y Soporte de Sistemas (que denominaremos Soporte), e Infraestructura Tecnológica de Sistemas (que denominaremos Infraestructura). Cada departamento cuenta con responsabilidades específicas para garantizar el correcto funcionamiento del organismo, las cuales se describirán en detalle más adelante.

2.3.4. Planeamiento y Presupuesto Estratégico

Esta división tiene como objetivos principales coordinar y orientar los procesos de planificación estratégica y la gestión presupuestal, asegurando la alineación de recursos con los objetivos del organismo.

2.3.5. Jurídica

Esta división tiene como objetivo proporcionar asesoramiento legal y garantizar el cumplimiento de las normativas jurídicas vigentes que rigen para el funcionamiento del organismo. Está compuesta por los departamentos de Asesoría Legal, Sumarios y Notarial.

2.3.6. Dirección General

La Dirección General es responsable de liderar, coordinar y supervisar las actividades estratégicas y operativas del organismo, asegurando el cumplimiento de sus objetivos.

2.3.7. Centro de Capacitación y Formación

Esta división tiene como objetivo principal proporcionar capacitación orientada a las áreas de servicio, con el propósito de fortalecer las capacidades de sus colaboradores. Para ello realiza actividades de capacitación adaptadas a las necesidades del organismo.

2.3.8. Subdirección General de Administración

La Subdirección General de Administración tiene como misión principal supervisar los procesos administrativos y financieros del organismo. Las divisiones de Financiero Contable, Adquisiciones, Gestión y Desarrollo Humano, y Logística operan bajo la supervisión directa de esta Subdirección.

2.3.9. Financiero Contable

El cometido de esta división es asegurar la sostenibilidad económica y el uso responsable de los recursos del organismo. Está compuesta por los departamentos: Rendición de cuentas, Tesorería, Sueldos, Ejecución Presupuestal y Contabilidad Central.

2.3.10. Adquisiciones

Esta división es responsable de gestionar los procesos de compra de bienes y servicios necesarios para el funcionamiento del organismo. Está compuesta por los departamentos de Compras y de Técnico de Adquisiciones.

2.3.11. Gestión y Desarrollo Humano

Esta división tiene como misión la administración del capital humano del organismo, garantizando un entorno laboral eficiente. Está compuesta por los departamentos: Personal, Técnico en Gestión Humana y Área de Seguridad, y Salud Ocupacional.

2.3.12. Logística

Esta división tiene como objetivo principal garantizar la gestión eficiente de los recursos materiales, infraestructura y servicios logísticos necesarios para el funcionamiento del organismo. Está compuesta por los departamentos: Proyectos Edilicios y Obras, Proveeduría y suministros, Locomoción y transporte, e Intendencia.

2.3.13. Áreas de Servicio

Esta división tiene como responsabilidad llevar a cabo tareas específicas alineadas con la misión del organismo, y se organiza en diversas divisiones y departamentos que contribuyen al cumplimiento de sus objetivos.

2.4. Responsabilidades por departamento en la División TIC

2.4.1. Departamento de Desarrollo

Es responsable de la creación, implementación y mantenimiento de aplicaciones y sistemas informáticos. Se enfoca en el desarrollo de software a medida y la integración de sistemas, tanto internos como externos.

2.4.2. Departamento de Soporte

Proporciona asistencia técnica a los usuarios finales. Su principal función es resolver incidencias relacionadas con hardware y software.

2.4.3. Departamento de Infraestructura

Gestiona los recursos tecnológicos físicos y virtuales, incluyendo servidores, redes, bases de datos y sistemas de almacenamiento. Debe mantener la disponibilidad de la infraestructura tecnológica que soporta las operaciones de la organización.

3. Marco de Ciberseguridad de AGESIC

En este capítulo se presenta una descripción del Marco de Ciberseguridad de AGESIC. Este marco comprende un conjunto de requisitos normativos y de buenas prácticas que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Está basado en el marco para la mejora de la seguridad cibernética en infraestructuras críticas, mejor conocido en inglés como NIST Cyber Security Framework (CSF) versión 1.1 [4], que fue liberado en abril de 2018, como una evolución de marco inicialmente emitido en febrero de 2014 en los Estados Unidos de Norte América.

La orientación del marco es ayudar a las organizaciones de todos los tamaños a comprender, gestionar y reducir los riesgos cibernéticos y proteger sus redes y datos, proporcionando un lenguaje común y un resumen de las mejores prácticas en ciberseguridad.

3.1. Aplicabilidad

El marco es aplicable a organizaciones que dependen en la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en tecnología de la información (TI), sistemas de control industrial (ICS), sistemas ciberfísicos (CPS) o dispositivos conectados en general, incluido el Internet de las Cosas (IoT).

3.2. Estructura

El MCS consta de tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco.

El **Núcleo del Marco** es un conjunto de funciones y actividades de seguridad cibernética, resultados esperados y referencias informativas que son comunes en todos los sectores y en la infraestructura crítica. Consta de cinco funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar. Cuando se consideran juntas, estas funciones proporcionan una visión estratégica de alto nivel del ciclo de vida del proceso de gestión de riesgos de la seguridad cibernética de una organización.

Cada función está compuesta de categorías, cada categoría se divide a su vez en subcategorías y cada subcategoría viene acompañada de referencias normativas a otros marcos de buenas prácticas (*frameworks*) o estándares (ISO 27.001 [5], CobiT 5 [6], NIST SP-83, entre otros) en los cuales se encuentra mayor nivel de detalle para la implementación de los controles de seguridad cibernética referidos.

3.3. Ciclo de vida de la ciberseguridad

El ciclo de vida de la ciberseguridad (ver Ilustración 3) se compone de **funciones** que permiten abstraer los principales conceptos de la seguridad de la información, en particular de la ciberseguridad.



Ilustración 3: El ciclo de vida de la ciberseguridad

3.4. Estructura del MCS

La estructura del MCS (ver Ilustración 4) está compuesta por una matriz en la que se incluyen los diferentes componentes que hacen a la estructura de marco.

FUNCIÓN	CATEGORÍA	SUB CATEGORÍA	PRIORIDAD POR PERFIL			MADUREZ				REF.	REQUISITOS
			B	E	A	N1	N2	N3	N4		
IDENTIFICAR											
PROTEGER											
DETECTAR											
RESPONDER											
RECUPERAR											

Ilustración 4: Estructura del MCS

3.4.1. Función

Es el nivel más alto en la estructura para organizar las actividades básicas de ciberseguridad.

3.4.2. Categoría

Es la subdivisión de una función en grupos de resultados de ciberseguridad estrechamente ligados a las necesidades funcionales y actividades particulares. Algunos ejemplos son: “Gestión de activos”, “Evaluación de riesgos”, “Mantenimiento”.

3.4.3. Subcategoría

Divide una categoría en resultados concretos de las actividades técnicas y/o de gestión. Proporcionan un conjunto de resultados que, aunque no de forma exhaustiva, ayudan al logro de los resultados en cada categoría. Algunos ejemplos son: “La política de seguridad de la información se encuentra establecida”, “Gestión de acceso remoto”, “Existe un plan de gestión de vulnerabilidades”.

3.4.4. Perfil

Un perfil representa las necesidades de ciberseguridad, basadas en los objetivos de negocio, considerando el riesgo percibido y la dependencia existente de las TIC. Cada organización tendrá asignado un perfil sobre el cual trabajar. Se han definido tres perfiles

para poder priorizar y establecer el avance en ciberseguridad: básico, estándar y avanzado.

- **Básico (B):** el riesgo percibido vinculado a ciberseguridad es bajo; una falla, disrupción o incidente que pueda afectar los servicios propios, se recuperan al mejor esfuerzo, no existiendo afectación directa a los objetivos del negocio.
- **Estándar (E):** el riesgo percibido vinculado a ciberseguridad es moderado, pero existe alta dependencia de las TIC para el cumplimiento de los objetivos del negocio. La continuidad de los servicios no soporta más de 48 horas corridas de indisponibilidad.
- **Avanzado (A):** el riesgo percibido vinculado a ciberseguridad es alto; una falla, disrupción o incidente puede afectar servicios transversales y/o críticos propios o de terceros. La continuidad de los servicios no soporta más de 24 horas corridas de indisponibilidad.

3.4.5. Prioridad

Las subcategorías del Marco, dependiendo del perfil definido para el organismo (Básico - B, Estándar - E, Avanzado - A) tienen asociado un nivel de prioridad de abordaje. Las prioridades definidas son:

- P1: Subcategoría que forma parte de una línea base de ciberseguridad, de abordaje inmediato y cumplimiento en el corto plazo (hasta 1 año).
- P2: Subcategoría que se requiere implementar a mediano plazo (de 1 a 2 años).
- P3: Subcategoría que se requiere implementar a largo plazo (de 2 a 3 años).
- N/A: Para esta versión del marco, no se han identificado requisitos que se ajusten a la subcategoría.

3.4.6. Referencias

En esta columna se transcriben todas las referencias mencionadas en el MCS de NIST para cada subcategoría. Es decir, todos los vínculos a controles similares definidos en otros marcos de seguridad, como ser ISO/IEC 27001, CobiT 5, etc.

3.4.7. Requisitos

Los requisitos o conjunto de requisitos mínimos incluidos en cada subcategoría refieren a las evidencias requeridas a los efectos de poder validar la existencia del control correspondiente para minimizar los riesgos identificados. Un requisito podrá mencionarse en más de una subcategoría, dependiendo de su enfoque. El detalle de cada requisito podrá consultarse en la “Guía de implementación” [7] incluida en el marco.

A continuación, se muestra cada Función con sus respectivas categorías:

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID. AM	Gestión de activos
		ID. BE	Entorno empresarial
		ID. GV	Gobernanza
		ID. RA	Evaluación de riesgos
		ID. RM	Estrategia de gestión de riesgos
		ID. SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR. AC	Gestión de identidad y control de acceso
		PR. AT	Conciencia y capacitación
		PR. DS	Seguridad de datos
		PR. IP	Procesos y procedimientos de protección de la información
		PR. MA	Mantenimiento
		PR. PT	Tecnología productora
DE	Detectar	DE. AE	Anomalías y eventos
		DE. CM	Vigilancia continua de seguridad
		DE. DP	Procesos de detección
RS	Responder	RS. RP	Comunicaciones
		RS. CO	Análisis
		RS. AN	Análisis
		RS. MI	Mitigación
		RS. IM	Mejoras
RC	Recuperar	RC. RP	Planificación de recuperación
		RC. IM	Mejoras
		RC.CO	Comunicaciones

Tabla 1: Funciones del MCS de AGESIC

3.4.8. Niveles de Implementación

Los Niveles de Implementación del MCS de AGESIC proporcionan un mecanismo para que las organizaciones puedan ver y comprender las características de su enfoque para gestionar el riesgo de seguridad cibernética, lo que ayudará a priorizar y alcanzar los objetivos de la seguridad cibernética. El marco considera cuatro niveles desde el más débil hasta el más robusto: Parcial, Riesgo informado, Repetible y Adaptativo.

El nivel es determinado con base en tres atributos:

- Proceso de gestión de riesgos
- Proceso de integración de la gestión de riesgos
- Proceso de participación externa

En las siguientes tablas se pueden apreciar las características de cada uno de los atributos mencionados (ver Tabla 2, Tabla 3 y Tabla 4).

Parcial	Informado	Repetible	Adaptativo
No formalizado	Procesos aprobados, pero podrían no ser establecidos como políticas de toda la organización.	Procesos aprobados y se expresan como políticas.	Mejor continua que incluye lecciones aprendidas e indicadores predictivos.
Ad-hoc		Actividades de ciberseguridad se actualizan regularmente	La organización continuamente se adapta a un panorama cambiante de amenazas y tecnologías y responde de manera eficaz.
Reactivo	Actividades de ciberseguridad basadas en objetivos de riesgo.	con base en cambios en el perfil de riesgo.	

Tabla 2: Proceso de Gestión de Riesgos

Parcial	Informado	Repetible	Adaptativo
Conciencia limitada sobre riesgos. La organización implementa la gestión del riesgo de seguridad cibernética de forma irregular, caso por caso.	Existe conciencia del riesgo de seguridad cibernética a nivel organizacional. Se lleva a cabo evaluación de riesgos, pero NO es recurrente	Se han definido e implementado políticas y procedimientos. Hay un enfoque consistente para monitorear y gestionar el riesgo. Se cuenta con personal competente. La alta dirección comunica regularmente sobre ciber-riesgos.	La gestión de riesgos de ciberseguridad es parte de la cultura organizacional. Existe alineación entre riesgos de seguridad y los objetivos del negocio. El riesgo es monitoreado como cualquier otro tipo de riesgos (por ejemplo: Riesgo Operativo). El presupuesto de la organización se basa en la comprensión del entorno al riesgo actual y previsto, y su tolerancia al riesgo.

Tabla 3: Proceso de Integración de la Gestión de Riesgos

Parcial	Informado	Repetible	Adaptativo
La organización no colabora, ni recibe/comparte información con otras entidades. Se desconocen los riesgos de la CS.	La organización colabora y recibe alguna información de otras entidades, pero no comparte. Es consciente de los riesgos de la CS, pero no actúa de forma consistente sobre dichos riesgos.	La organización recibe y comparte información con otras entidades. Es consciente de los riesgos de la CS y actúa de forma consistente sobre dichos riesgos.	Utiliza información en tiempo real o casi en tiempo real para comprender y actuar de forma coherente sobre los riesgos de CS. Comunica de manera proactiva, utilizando mecanismos formales e informales para desarrollar y mantener relaciones sólidas de la CS.

Tabla 4: Proceso de Participación Externa

Por último, el Perfil representa los resultados que se basan en las necesidades empresariales que una organización ha seleccionado de las categorías y subcategorías del Marco. El Perfil se puede caracterizar como la alineación de estándares, directrices y prácticas con el Núcleo del Marco en un escenario de implementación particular.

De forma más coloquial se puede decir que el Perfil es una “foto” en el tiempo que muestra el estado actual (o el nivel de estado deseado) de ciberseguridad en una organización o unidad de negocio. La diferencia entre el perfil del estado actual y el perfil de estado deseado permitirá construir una hoja de ruta priorizada para la implementación.

3.5. Modelo de madurez

El modelo de madurez de ciberseguridad planteado por AGESIC en su MCS establece una estructura para evaluar y mejorar continuamente las capacidades de ciberseguridad en las organizaciones.

Este modelo tiene como objetivo ayudar a las entidades públicas y privadas a identificar el nivel de madurez de sus procesos y controles de seguridad, y a implementar mejoras progresivas para alcanzar un nivel más alto de protección frente a ciberamenazas.

El modelo de madurez propuesto incluye 5 niveles (del 0 al 4), donde este último es el más alto. Cada nivel superior incluye los niveles inferiores, por lo tanto, cumplir con las pautas del nivel 4 implica cumplir también con las pautas del nivel 1, 2 y 3 (ver Ilustración 6). El nivel 0 de madurez indica que las acciones vinculadas a seguridad de la información y ciberseguridad son casi o totalmente inexistentes.

Nivel 1	Nivel 2	Nivel 3	Nivel 4
Mejor esfuerzo. Centrado en el centro de datos.	Extensión al resto de la organización.	Políticas y procedimientos formales.	Mejora continua. Auditoría.

Ilustración 5: Niveles de madurez del MCS de AGESIC

3.5.1. Objetivos del modelo

Los objetivos que se establecen en el modelo de madurez son los siguientes:

- Mejorar la capacidad de ciberseguridad de las organizaciones en Uruguay de manera progresiva y sostenible.
- Facilitar la gestión de riesgos mediante un enfoque estructurado y basado en evidencias.
- Optimizar los recursos y esfuerzos dedicados a la ciberseguridad, alineándolos con las mejores prácticas internacionales.

3.5.2. Niveles de madurez

A continuación, se detallan los niveles de madurez definidos en el modelo:

- **Nivel 0:** Es el primer nivel del modelo de madurez donde las acciones vinculadas a seguridad de la información y ciberseguridad son casi o totalmente inexistentes. La organización no ha reconocido aún la necesidad de realizar esfuerzos en ciberseguridad. Este nivel no es incluido en la tabla del modelo de madurez.
- **Nivel 1:** Es el segundo nivel del modelo. Existen algunas iniciativas sobre ciberseguridad, aunque los esfuerzos se realizan en forma aislada. Se realizan implementaciones con enfoques ad-hoc y existe alta dependencia del personal que lleva a cabo las tareas que habitualmente no se encuentran documentadas. Existe una actitud reactiva ante incidentes de seguridad.
- **Nivel 2:** Es el tercer nivel del modelo de madurez. Se han establecido ciertos lineamientos o pautas para la ejecución de las tareas, pero aún existe dependencia del conocimiento individual. Se ha avanzado en el desarrollo de los procesos y existe cierta documentación para realizar las tareas.
- **Nivel 3:** Es el cuarto nivel del modelo de madurez y se caracteriza por la formalización y documentación de políticas y procedimientos, así como implementaciones de alta complejidad y/o automatizaciones que centralizan y

permiten iniciativas de gobernanza. Las políticas y procedimientos son difundidos, facilitan la gestión y posibilitan establecer controles y métricas. Los esfuerzos en ciberseguridad se enfocan en los procesos, las personas y la tecnología.

- **Nivel 4:** Es el último nivel del modelo de madurez. El Responsable de la Seguridad de la Información (RSI) tiene un rol clave en el control y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) realizando o coordinando actividades de control interno para verificar cumplimientos y desvíos. Se desarrollan las lecciones aprendidas que, junto con los controles determinan las acciones para la mejora continua. Las partes interesadas son informadas periódicamente, lo cual permite alinear los esfuerzos, estrategias y tecnologías de ciberseguridad con los objetivos y estrategias de la organización.

3.5.3. Ámbitos de evaluación

El modelo abarca varias áreas clave dentro de la ciberseguridad, tales como:

- Gestión de riesgos
- Protección de la información
- Resiliencia ante incidentes
- Cumplimiento normativo
- Capacitación y conciencia

3.5.4. Pasos para seguir la implementación del MCS de AGESIC

1. **Priorización y Alcance:** La organización identifica sus objetivos empresariales o de misión y las prioridades organizacionales de alto nivel. Con esta información, el organismo toma decisiones estratégicas con respecto a las implementaciones de seguridad cibernética y determina el alcance de los sistemas y activos que respaldan la línea o proceso comercial seleccionado.
2. **Orientación:** La organización identifica los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general. La organización luego

consulta las fuentes para identificar las amenazas y vulnerabilidades aplicables a esos sistemas y activos.

3. **Perfil Actual:** La organización desarrolla un Perfil Actual en el que indica qué resultados de categoría y subcategoría del Núcleo del Marco se están logrando actualmente. Si se logra parcialmente un resultado, tomar nota de este hecho ayudará a respaldar los pasos posteriores al proporcionar información de referencia.
4. **Evaluación de riesgos:** Esta evaluación puede estar orientada por el proceso de gestión de riesgos general de la organización o actividades previas de evaluación de riesgos. La organización analiza el entorno operativo para discernir la probabilidad de un evento de seguridad cibernética y el impacto que el evento podría tener en la organización. Es importante que las organizaciones identifiquen los riesgos emergentes y utilicen la información de amenazas de seguridad cibernética de fuentes internas y externas para obtener una mejor comprensión del riesgo asociado con los eventos de seguridad cibernética.
5. **Perfil Deseado:** La organización crea un Perfil Objetivo que se centra en la evaluación de las categorías y subcategorías del Marco que describen los resultados deseados de seguridad cibernética de la organización. La organización también puede considerar las influencias y los requisitos de las partes interesadas externas, como las entidades del sector, los clientes y los socios empresariales, al crear un Perfil deseado.
6. **Determinar, analizar y priorizar brechas:** La organización compara el Perfil Actual y el Perfil Deseado para determinar las brechas. A continuación, crea un plan de acción priorizado para abordar las brechas (que reflejan los impulsores, los costos y los beneficios, y los riesgos de la misión) para lograr los resultados en el Perfil Objetivo. Luego, el organismo determina los recursos necesarios para abordar las brechas, que incluyen los fondos y la fuerza laboral. El uso de Perfiles de esta manera alienta a el organismo a tomar decisiones informadas sobre las actividades de seguridad cibernética, respalda la gestión de riesgos y permite a el organismo realizar mejoras específicas y rentables.

7. **Implementar plan de acción:** La organización determina qué acciones tomar para abordar las brechas, si las hay, identificadas en el paso anterior y luego ajusta sus prácticas actuales de seguridad cibernética para lograr el Perfil Objetivo. Para proveer más dirección, el Marco identifica ejemplos de referencias informativas sobre las categorías y subcategorías, pero las organizaciones deben determinar qué normas, directrices y prácticas, incluidas aquellas que son específicas del sector, funcionan mejor para sus necesidades.

4. Protección de Datos Personales

En este capítulo se presenta la Ley N° 18.331 “Ley de protección de datos personales”, su relevancia para el organismo y su alineación con el MCS de AGESIC. Además, se describe la Política de Protección y Privacidad de los Datos (PPPD) elaborada, con el fin de fortalecer la protección de los datos personales.

4.1. La Ley N° 18.331 y su relevancia para el organismo

La Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data, establece el marco legal en Uruguay para regular el tratamiento de datos personales, garantizando la privacidad y seguridad de la información de los ciudadanos. Esta normativa define principios clave como la licitud, finalidad, calidad, seguridad y consentimiento informado, exigiendo a los organismos implementar medidas de protección para evitar accesos no autorizados, pérdidas o alteraciones de datos.

Además, la ley otorga derechos a los titulares de los datos, permitiéndoles acceder, rectificar, actualizar, incluir, suprimir u oponerse al tratamiento de su información personal. También impone obligaciones a quienes gestionan bases de datos, como la inscripción en la Unidad Reguladora y de Control de Datos Personales (en adelante URCDP) y la adopción de controles adecuados para garantizar el cumplimiento normativo.

El cumplimiento de esta ley es esencial para evitar riesgos legales, financieros y reputacionales en los organismos. Cualquier vulneración podría generar consecuencias graves tanto para los usuarios afectados como para la entidad responsable del tratamiento de los datos.

4.2. Alineación de la Ley N° 18.331 con el MCS de AGESIC

Como se detalló en el capítulo anterior, el MCS de AGESIC establece directrices para fortalecer la seguridad de la información en las organizaciones públicas y privadas en Uruguay. Esta estructura se basa en cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar.

La Ley N° 18.331 se alinea especialmente con las funciones de Identificar y Proteger dentro del marco de ciberseguridad:

- **Identificar:** Implica el reconocimiento y clasificación de los datos personales como activos críticos dentro de la organización, asegurando su correcto tratamiento y resguardo.
- **Proteger:** Requiere la implementación de medidas de seguridad para evitar accesos no autorizados, pérdidas de información y alteraciones en los datos. La ley refuerza la necesidad de implementar controles y auditorías que garanticen la integridad de los datos personales.

El MCS de AGESIC proporciona un enfoque estructurado para que las organizaciones cumplan con la Ley N° 18.331 y aseguren una adecuada gestión de riesgos asociados a la protección de datos personales.

4.3. Creación de la Política de Protección y Privacidad de los Datos (PPPD) alineada con la Ley N° 18.331 y el MCS

En el contexto actual, donde la protección de la información es fundamental para la confianza y operatividad del organismo, hemos desarrollado una PPPD con el objetivo de establecer un marco normativo interno que garantice la seguridad y confidencialidad de los datos personales. Esta política responde a la necesidad de cumplir con la Ley N° 18.331, así como con los lineamientos del MCS de AGESIC, asegurando que todos los procesos de tratamiento de datos se realicen de manera segura y conforme a la normativa vigente (ver más detalles en el ANEXO 3 - Entregable 2: Políticas a medida del organismo).

Dada la naturaleza del sector en el que opera el organismo, la gestión segura de los datos personales adquiere una relevancia crítica. El organismo maneja información altamente sensible de sus usuarios, cuya exposición o uso indebido podría generar impactos graves tanto en los derechos de las personas como en la reputación y legalidad de la entidad. Por ello, la PPPD busca fortalecer la seguridad de la información y minimizar los riesgos asociados al tratamiento de datos.

Entre sus principales objetivos, la política establece:

- Garantizar la confidencialidad, integridad y disponibilidad de los datos personales almacenados en los sistemas del organismo.
- Cumplir con la normativa vigente, asegurando que el tratamiento de la información se realice conforme a los principios de legalidad, finalidad, seguridad y consentimiento informado.
- Asignar roles y responsabilidades claras.
- Implementar medidas de seguridad y controles para prevenir accesos no autorizados, alteraciones o pérdidas de información.
- Organizar instancias de concientización y capacitación para todo el personal, asegurando que cada colaborador conozca sus obligaciones y buenas prácticas en materia de protección de datos.

Desde el punto de vista del MCS de AGESIC, esta política refuerza la función de "Proteger", estableciendo controles para la preservación de los datos y asegurando su tratamiento adecuado dentro de los sistemas del organismo. También contribuye a la función de "Responder", ya que prevé mecanismos para la gestión de incidentes de seguridad de la información, siguiendo los lineamientos del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (en adelante CERTuy) [8] y las normativas nacionales.

La implementación de la PPPD es un paso clave para fortalecer la seguridad del organismo, su adopción no solo permite mitigar riesgos asociados a filtraciones o usos indebidos de información, sino que también refuerza la confianza de los usuarios y colaboradores en la protección de su privacidad.

El éxito de esta política dependerá del compromiso de todo el organismo, desde los niveles directivos hasta cada colaborador que acceda a información sensible. La ciberseguridad y la protección de datos son responsabilidades compartidas, y con esta nueva política se establecen las bases para una gestión segura, eficiente y alineada con las mejores prácticas.

5. Aplicación del MCS de AGESIC

En este capítulo se presentan los motivos por los cuales se decidió utilizar el MCS de AGESIC, recomendado por esta entidad. También se consideró el marco de buenas prácticas de ITIL [9] (Biblioteca de Infraestructura de Tecnologías de la Información) que está más dirigido a la gestión de los servicios de las TIC; en este capítulo analizaremos las diferencias entre ambos marcos. Además, se explica el motivo por el cual se optó por iniciar su aplicación en la División TIC y se detalla el plan de implementación.

5.1. Justificación de la utilización del MCS de AGESIC

5.1.1. Recomendaciones de adopción del MCS de AGESIC

AGESIC recomienda la adopción del MCS como referencia para fortalecer la seguridad de la información en las entidades gubernamentales. Este marco basado en estándares internacionales como el NIST CSF, está adaptado a la realidad uruguaya y establece un conjunto de prácticas y controles, su implementación permite a las organizaciones públicas evaluar y mejorar su postura de ciberseguridad, alineando sus procesos a un modelo de madurez que facilita la gestión del riesgo digital.

AGESIC proporciona guías y herramientas para apoyar la adopción del MCS, asegurando que las entidades gubernamentales cuenten con un marco sólido para proteger la infraestructura crítica, garantizar la continuidad de los servicios y mitigar los riesgos asociados a incidentes de ciberseguridad.

Este marco está también respaldado por CERTuy, gestionado por AGESIC, el cual desempeña un papel fundamental en la aplicación del MCS dentro de las entidades gubernamentales. Su misión es coordinar la prevención, detección y respuesta a incidentes de ciberseguridad, proporcionando asistencia técnica y orientación estratégica para la gestión de riesgos digitales de los organismos públicos.

A su vez, el Poder Ejecutivo de Uruguay ha emitido un decreto [10] con el objetivo de fortalecer la ciberseguridad en el sector público, estableciendo lineamientos claros para

la protección de la información y la gestión de riesgos digitales. Esta normativa también promueve la adopción del Marco de Ciberseguridad de AGESIC.

5.1.2. Diferencias entre el MCS de AGESIC y el Marco ITIL

El MCS de AGESIC y el marco ITIL son herramientas relevantes en la gestión de Tecnologías de la Información, aunque presentan enfoques diferentes, especialmente en lo que respecta a la gestión de cambios de TI. Mientras el MCS de AGESIC está centrado en la seguridad de la información y la protección de los activos digitales, ITIL se orienta a la gestión eficiente de los servicios tecnológicos, con un fuerte énfasis en la continuidad operativa, la calidad del servicio y la mejora continua.

La elección de ITIL como marco de comparación se debe a que es uno de los más utilizados y valorados por los departamentos de TI. Esto se debe a que dichos departamentos son responsables de generar y mantener servicios tecnológicos, y ITIL ofrece un enfoque sólido para su gestión. Sin embargo, es importante destacar que, si bien ITIL incluye aspectos relacionados con la gestión de riesgos y la continuidad, la seguridad de la información no es uno de sus pilares centrales, lo que marca una diferencia clave con el enfoque del MCS de AGESIC.

A continuación, se presentan las principales diferencias entre el MCS de AGESIC y el marco ITIL en relación con la gestión de cambios en TI:

	MCS AGESIC	ITIL
Enfoque primario	Se centra en la gestión de riesgos de ciberseguridad y la protección de activos de información. Sus procesos de gestión de cambios están diseñados con la seguridad como preocupación central.	Se centra en la gestión general de servicios de TI, siendo la gestión de cambios uno de los muchos procesos destinados a mejorar la prestación y la eficiencia de los servicios de TI.

Alcance	Proporciona un marco más amplio para gestionar los riesgos de ciberseguridad en toda una organización, siendo la gestión de cambios un componente de esta estrategia de seguridad más amplia.	Ofrece un conjunto más detallado y específico de mejores prácticas para la gestión de servicios de TI, incluido un proceso integral de gestión de cambios.
Evaluación de riesgos	Enfatiza la evaluación y mitigación exhaustivas de riesgos en el proceso de gestión de cambios, centrándose en las posibles implicaciones de seguridad de los cambios.	Si bien incluye evaluación de riesgos, el enfoque de ITIL está más equilibrado entre eficiencia operativa y gestión de riesgos.
Cambiar Clasificación	Clasifica los cambios basándose principalmente en su impacto potencial en la postura de seguridad y los niveles de riesgo.	Categoriza los cambios según su escala, impacto y urgencia, con un enfoque en la prestación de servicios y la continuidad del negocio.
Proceso de aprobación	Enfatiza la aprobación del personal o comités centrados en la seguridad, garantizando que los cambios se alineen con las políticas y estándares de seguridad.	Utiliza un Consejo Asesor de Cambio (CAC) que considera varios aspectos del cambio, incluidos los impactos operativos, financieros y estratégicos.
Enfoque de implementación	Enfatiza las prácticas de implementación segura, que a menudo requieren pruebas y validación de seguridad adicionales.	Se centra en la implementación eficiente y controlada, con énfasis en minimizar las interrupciones del servicio.
Revisión posterior a la implementación	Prioriza las revisiones centradas en la seguridad, buscando posibles vulnerabilidades o brechas de seguridad introducidas por el cambio.	Realiza revisiones posteriores a la implementación más amplias, considerando la calidad del servicio, la satisfacción del usuario y el impacto general en los servicios de TI.

Mejora Continua	Se centra en mejorar la postura de seguridad y reducir los riesgos de ciberseguridad a lo largo del tiempo.	Tiene como objetivo la mejora general del servicio, incluida la eficiencia, la rentabilidad y la satisfacción del usuario.
Métricas y Medición	Hace hincapié en métricas relacionadas con la seguridad, como la reducción de vulnerabilidades o la mejora de los tiempos de respuesta a incidentes.	Utiliza una gama más amplia de métricas, incluida la disponibilidad del servicio, la satisfacción del cliente y la eficiencia operativa.

Tabla 5: Tabla comparativa de MCS de AGESIC y el Marco de ITIL

Si bien estos marcos tienen diferentes enfoques principales, no son mutuamente excluyentes. Muchas organizaciones encuentran valor en la integración de aspectos del MCS AGESIC y de ITIL para crear un enfoque integral para la gestión de cambios de TI que aborde tanto las preocupaciones de seguridad como la eficiencia de la prestación de servicios. Esta integración puede conducir a un entorno de TI más sólido y seguro manteniendo al mismo tiempo la prestación de servicios de alta calidad.

5.2. Aplicación del MCS en la División TIC

En esta tesis abordaremos el MCS de AGESIC exclusivamente en la División TIC. Esta es una decisión estratégica que responde a las limitaciones de tiempo del proyecto, la estructura organizacional, y la necesidad de enfocarse en las áreas más críticas para la seguridad.

Al aplicar el marco exclusivamente a la División TIC, es posible concentrarnos en los elementos más críticos y donde la ciberseguridad tiene un impacto más inmediato, como en los sistemas de información, la información estructural y de los usuarios, y la infraestructura tecnológica.

Por otro lado, las TIC suelen ser el área que enfrenta mayores riesgos de ciberseguridad debido a la digitalización de procesos, el uso de plataformas en línea y el

manejo de datos sensibles. Por tanto, aplicar el MCS en la División TIC se garantiza un enfoque estratégico y de protección en los puntos más vulnerables del organismo.

Un enfoque restringido en la División TIC permite abordar los aspectos más urgentes y relevantes dentro del tiempo disponible. Además, es posible mejorar la ciberseguridad en áreas clave como redes, servidores, bases de datos y comunicaciones, lo cual es esencial para la operatividad del organismo.

A continuación, se presentan los diferentes puntos evaluados que avalan esta decisión:

5.2.1. Tamaño del organismo

El organismo tiene una estructura jerárquica y una gama de funciones muy amplias. Esto dificulta la implementación de un MCS en todas las áreas de forma simultánea, por la cantidad de recursos que son necesarios, especialmente cuando se trata de áreas no relacionadas directamente con las tecnologías de la información y las comunicaciones.

5.2.2. Tiempos reducidos del proyecto

Debido a los tiempos del proyecto, también consideramos más adecuado delimitar el alcance a la aplicación del marco con alcance limitado a una división, en lugar de tratar de abarcar todo el organismo. Implementar un MCS completo, que cubra todas las áreas del organismo, requeriría más tiempo y recursos para el análisis, y la creación de políticas interdepartamentales que aseguren la protección y seguridad de los datos en todo el organismo. Este enfoque permite generar avances a corto plazo, demostrando el valor del proyecto y abriendo puertas para una futura expansión hacia otras áreas.

Somos conscientes de que la duración del proyecto no nos permitirá la implementación completa del MCS en el organismo, por lo que, como parte del proyecto, dejaremos planteadas todas las actividades que se deberían implementar una vez que este proyecto académico se concluya.

5.2.3. Dificultades de adopción del marco

La adopción de marcos de ciberseguridad en áreas no relacionadas directamente con las TIC puede encontrar resistencia debido a la falta de comprensión sobre la importancia de la ciberseguridad en sus procesos o funciones específicas. El marco de AGESIC está diseñado para ser aplicable principalmente a las áreas tecnológicas, y no todas las unidades del organismo pueden estar dispuestas o preparadas para asumir la implementación inmediata de políticas de ciberseguridad.

La implementación del marco en las TIC permite una transición hacia la ciberseguridad en la organización. A medida que los beneficios de la aplicación del marco sean visibles en las áreas tecnológicas, será más fácil convencer a otras áreas sobre la necesidad de extender la ciberseguridad a sus procesos y funciones.

5.2.4. Alineación con los riesgos y necesidades actuales

Las TIC suelen ser la principal vía de ataque en ciberseguridad, y las amenazas digitales son cada vez más complejas y frecuentes. La protección de datos, infraestructuras críticas y la gestión de accesos son desafíos inmediatos dentro de las TIC, lo que justifica su enfoque prioritario. Esto reduce el riesgo de exposición del organismo a incidentes cibernéticos, que podrían afectar tanto su operatividad como su reputación.

5.3. Plan de Implementación del MCS de AGESIC

Para la implementación del marco MCS, hemos desarrollado un listado de actividades necesarias para cumplir con cada una de las subcategorías y alcanzar el nivel de madurez máximo requerido en cada caso (ver ANEXO 6 - Listado completo de actividades).

Esta lista comprende un total de 876 actividades, cuya distribución por prioridad (basado en el perfil Básico) se detalla en la Tabla 6.

Prioridad	Cantidad de Actividades
Actividades P1	266
Actividades P2	424
Actividades P3	186
Total	876

Tabla 6: Tabla con distribución de cantidad de tareas por prioridad

Como detallará en el siguiente capítulo, por tratarse de un organismo categorizado con un perfil Básico, en una primera etapa se implementarán las actividades vinculadas con las subcategorías de nivel de prioridad P1, para las cuales se dispone de un plazo máximo de un año desde el comienzo de la implementación.

Posteriormente, se abordarán las actividades vinculadas con las subcategorías de nivel de prioridad P2, para las cuales se dispone de un plazo máximo de dos años desde el comienzo de la implementación.

Finalmente se implementarán las actividades vinculadas con las subcategorías de nivel de prioridad P3, para las cuales se dispone de un plazo máximo de tres años desde el comienzo de la implementación.

Si bien estas recomendaciones se basan en buenas prácticas reconocidas internacionalmente, cada organización tiene la flexibilidad de adelantar la ejecución de actividades en función de sus necesidades y recursos. Por ejemplo, una actividad de prioridad **P2** podría implementarse en los primeros meses del proyecto, incluso antes de completar otras actividades de prioridad **P1**.

6. Evaluación de la situación actual del organismo según el MCS de AGESIC

En este capítulo se presenta una evaluación de la situación actual del organismo según el MCS de AGESIC, a partir de la aplicación del cuestionario elaborado para evaluar el nivel de madurez del organismo.

6.1. El modelado del Marco para el organismo

Para nuestra tesis trabajaremos con el perfil Básico propuesto por el marco. La elección del perfil básico está justificada por las características propias del organismo, según la definición de AGESIC. El perfil básico se asigna a aquellas organizaciones cuyo riesgo percibido vinculado a la ciberseguridad es bajo, lo que significa que, en caso de una falla, disrupción o incidente que afecte los servicios, estos pueden recuperarse con el mejor esfuerzo, sin que haya una afectación directa a los objetivos del organismo. Este perfil se refiere a aquellos organismos con una baja dependencia de las TIC, lo que implica que las consecuencias de un incidente no pondrán en peligro los objetivos fundamentales del organismo.

En este caso, las medidas de ciberseguridad se enfocan en controles esenciales como la protección de los accesos y la gestión básica de incidentes, priorizando la recuperación de los servicios en caso de fallas, sin que se afecten gravemente los objetivos del organismo y poder fortalecer las medidas de seguridad, mejorar la gestión de incidentes y asegurar una mayor continuidad en los servicios críticos.

En el futuro, se pretende que el organismo avance hacia una mejora continua en sus capacidades de ciberseguridad. En este contexto, a medida que estas capacidades se fortalezcan, se deberán implementar progresivamente los perfiles Estándar y Avanzado definidos por AGESIC. Esta implementación se adaptará a las necesidades específicas de su infraestructura y el aumento de los riesgos percibidos, con el propósito de implementar controles más sofisticados y proactivos, garantizar la protección de los activos más sensibles y asegurar la continuidad de los servicios ante posibles amenazas.

6.2. Aplicación del cuestionario para evaluar los niveles de madurez

Se elaboró un documento estructurado para evaluar de manera sistemática el estado del organismo en términos de ciberseguridad. Este documento comprende un cuestionario de evidencias y está alineado con los lineamientos de AGESIC. La aplicación del cuestionario permitió determinar el nivel de madurez mediante la vinculación de las evidencias recolectadas con las subcategorías del marco. Como resultado, se obtuvo un diagnóstico preciso que identificó las áreas que requieren fortalecimiento.

Para completar el cuestionario, se accedió a documentación proporcionada por el organismo y se realizaron entrevistas con actores clave del OP. En el ANEXO 2 - Entregable 1: Situación actual de la Seguridad de la Información en el organismo, se encuentra detallado dicho documento y el proceso realizado para llegar al resultado.

6.2.1. Entrevistas realizadas

Las entrevistas realizadas tuvieron como objetivo recopilar información sobre la situación actual de ciberseguridad del organismo y, además, reunir los datos necesarios para completar el cuestionario del MCS, tal como se mencionó anteriormente.

Para obtener una primera aproximación a la situación actual de ciberseguridad del organismo, se realizaron entrevistas semiestructuradas. Este enfoque permitió comprender en profundidad el contexto del OP y los principales desafíos en materia de ciberseguridad. Entre los entrevistados se incluyeron la Dirección de TIC y el Director de Infraestructura (ANEXO 2 - Entregable 1: Situación actual de la Seguridad de la Información en el organismo, punto 2).

En cuanto al cuestionario del MCS, para completarlo se realizaron entrevistas estructuradas, enfocadas en determinar de manera objetiva si las actividades detalladas se estaban llevando a cabo o no.

Por ejemplo, para la función “Identificar”, en la categoría “ID.GO”, denominada “Gobernanza”, se consultó al Director de TIC para evaluar el nivel de madurez correspondiente. En particular, respecto a la subcategoría “ID.GO-1”, relacionada con la PSI, su detalle puede observarse en la Tabla 7.

Función	Cat	Cat_Descripción	Subcat	Descripción
IDENTIFICAR (ID)	ID.GO	Las políticas, procedimientos y procesos para gestionar y monitorear los requisitos regulatorios, legales, ambientales y operativos de la organización, son comprendidos y se informa a las gerencias sobre los riesgos de ciberseguridad.	ID.GO-1	La política de seguridad de la información se encuentra establecida.

Tabla 7: Descripción de la categoría ID.GO y subcategoría ID.GO-1

Determinamos que, para la subcategoría: “ID.GO-1”, el nivel de madurez alcanzado corresponde al Nivel 1. Esto se debe a que el organismo ha ejecutado todas las actividades requeridas para este nivel, como se muestra en la Tabla 8, dichas actividades son y evidencias son:

- T058 - Desarrollar una Política de seguridad de la información (PSI).

La CSI desarrolló una PSI en julio de 2023.

- T059 - Disponer del acta de Resolución con la aprobación y adopción de la PSI.

El Directorio aprobó la PSI en julio de 2024 y ordenó su difusión, así como la adhesión de todo el personal.

- T060 - Comunicar la PSI a todo el organismo.

En agosto de 2024, el Departamento de Comunicaciones envió un correo electrónico a todo el personal para informar sobre la entrada en vigencia de la PSI y solicitar una notificación de aceptación de la PSI en la Intranet del organismo.

Madurez	Madurez Nivel	Cumplimiento	Actividades para alcanzar nivel de madurez	Evidencia	Nivel Alcanzado
Se cuenta con una política de seguridad de la información aprobada por la Dirección. La política de seguridad de la información se difunde al personal.	1	SI	T058 - Desarrollar una Política de seguridad de la información (PSI). T059 - Disponer del acta de Resolución con la aprobación y adopción de la PSI. T060 - Comunicar la PSI a todo el organismo.	E058 - Política de seguridad de la información. E059 - Acta de Resolución con la aprobación de la PSI. E010 - Plan de comunicación de la PSI.	1
Se definen formalmente políticas sobre temas específicos que dan soporte a la política de seguridad de la información.	2	NO	T061 - Identificar áreas clave que requieren políticas específicas y desarrollarlas. T062 - Desarrollar políticas adicionales alineadas con la política general y manual de políticas asociadas. T063 - Aprobación del Directorio todas las políticas pendientes.	E061 - Lista de áreas clave identificadas y sus políticas desarrolladas. E062 - Políticas adicionales alineadas con la política general y Manual de Políticas. E063 - Acta de Resolución de aprobación de políticas.	1
La política de seguridad de la información y las políticas específicas son revisadas cuando ocurren cambios significativos (ambiente de negocio, ambiente técnico, normativa, etc.) para analizar su vigencia, idoneidad y pertinencia, siendo deseable que las mismas sean revisadas formalmente a intervalos regulares. El resultado de estas revisiones se documenta y comunican al CSI y demás partes interesadas.	3	NO	T064 - Establecer una periodicidad de revisión de las políticas para determinar su vigencia y, si corresponde, actualizarlas. T065 - Difusión de políticas actualizadas a todo el organismo.	E064 - Acta de revisión de las políticas. E065 - Plan de difusión de políticas actualizadas.	1
Se ha desarrollado un conjunto razonable de políticas y procedimientos específicos alineados al Marco de Ciberseguridad y a la guía de implementación conformando un SGSI. Se definen indicadores para medir la efectividad del SGSI y se planifica y realiza la revisión formal de éste por parte del CSI.	4	NO	T066 - Diseñar y documentar un SGSI alineado al Marco de Ciberseguridad. T067 - Definir procedimientos específicos para cada componente del SGSI. T068 - Establecer indicadores clave de desempeño (KPIs) para medir la efectividad del SGSI. T069 - Planificar y ejecutar revisiones periódicas formales del SGSI. T070 - Presentar los resultados de las revisiones al CSI para toma de decisiones	E066 - Documento del SGSI alineado al marco de Ciberseguridad. E067 - Procedimientos específicos documentados. E068 - KPIs definidos y reportados periódicamente para medir la efectividad del SGSI. E069 - Plan de ejecución de revisión del SGSI. E070 - Informes de revisión del SGSI y planes de mejora.	1

Tabla 8: Tabla de actividades para subcategoría ID.GO-1 por nivel de madurez

6.3. Situación actual en ciberseguridad

Identificamos que el organismo se encuentra en un nivel inicial en materia de ciberseguridad. Existen múltiples áreas que requieren mejoras significativas para fortalecer su postura de seguridad. A continuación, se destacan algunos aspectos clave:

6.3.1. Responsable en ciberseguridad

Actualmente, el organismo no cuenta con un rol designado formalmente para liderar las actividades relacionadas con la ciberseguridad.

6.3.2. Referente de Datos Personales

El organismo cuenta con un Referente de Datos Personales, responsable de garantizar la protección de la información y el cumplimiento de la Ley N° 18.331.

6.3.3. Comisión de Seguridad de la Información (CSI)

A mediados de 2023, el Directorio conformó una comisión dedicada a la seguridad de la información. Esta comisión está integrada por el Director de TIC, el Director de Jurídica, el Director de Auditoría Interna, el Director de Planeamiento y Presupuesto Estratégico, y el Referente de Datos Personales, y tuvo como objetivo inicial la creación de una PSI.

6.3.4. Política de Seguridad de la Información (PSI)

Actualmente, solo se ha desarrollado una primera versión de la PSI, que representa un primer paso, pero entendemos que tiene oportunidades de mejora.

6.3.5. Capacitación y formación en Seguridad de la Información

No se ofrece capacitación o formación regular a sus colaboradores en el ámbito de seguridad de la información.

6.3.6. Enfoque reactivo ante incidentes de seguridad

Los incidentes de seguridad se gestionan de manera reactiva, es decir, se resuelven solo cuando ocurren, en lugar de tener un enfoque proactivo que incluya la prevención,

detección temprana y respuesta estructurada. Esto refleja la ausencia de un plan formal de respuesta a incidentes y protocolos establecidos.

7. Análisis de la situación actual del organismo

Este capítulo presenta un análisis de la situación actual del organismo. A partir de las evidencias obtenidas para las actividades de cada nivel de madurez de las Funciones, Categorías y Subcategoría del MCS, se identificaron las actividades que se realizan actualmente en el organismo y el nivel de madurez alcanzado por este. La lista completa de las actividades que identificamos como logradas por el organismo se encuentra en el ANEXO 2 - Entregable 1: Situación actual de la Seguridad de la Información en el organismo, punto 5.

7.1. Perfil Actual del Organismo

El organismo presenta importantes brechas en su estrategia de ciberseguridad, con debilidades clave en la identificación de riesgos, respuesta a incidentes y recuperación. Aunque cuenta con algunos controles de protección, estos no están respaldados por procesos sólidos ni por una gestión estratégica de la seguridad.

A continuación se detallan los descubrimientos clave:

- **Falta de gobernanza y gestión de riesgos:** No hay una estrategia clara ni procesos definidos para identificar y mitigar amenazas.
- **Protección parcial y con deficiencias:** Se han implementado algunas medidas de seguridad, pero sin una adecuada capacitación del personal ni procesos estandarizados.
- **Capacidad de detección limitada:** No hay mecanismos efectivos para identificar amenazas en tiempo real, lo que aumenta la posibilidad de ataques sin ser detectados.
- **Respuesta a incidentes deficiente:** El organismo no cuenta con protocolos claros para actuar ante un ciberataque, lo que podría generar una respuesta lenta y descoordinada.

- **Recuperación incierta:** En caso de un incidente grave, la recuperación sería lenta y sin aprendizajes que permitan mejorar la resiliencia ante futuros eventos.

A continuación, se muestra un detalle de los resultados alcanzados, estos se agruparon por función y categoría a los efectos de dar una idea del nivel de madurez de cada una de ellas.

7.1.1. Identificar

La función Identificar obtuvo un nivel de madurez promedio de 0.6 (ver Tabla 9 e Ilustración 6), lo que evidencia una implementación baja de las prácticas necesarias para conocer y gestionar adecuadamente los riesgos de ciberseguridad.

Función	Descripción Categoría	Categoría	Nivel Alcanzado
IDENTIFICAR (ID)	Gestión de riesgos en la cadena de suministros	ID.CS	0.6
	Estrategia para la gestión de riesgos	ID.GR	-
	Evaluación de riesgos	ID.ER	0.8
	Gobernanza	ID.GO	0.8
	Ambiente del negocio	ID.AN	0.3
	Gestión de activos	ID.GA	1.2
	Total		0.6

Tabla 9: Resultados de la Función Identificar

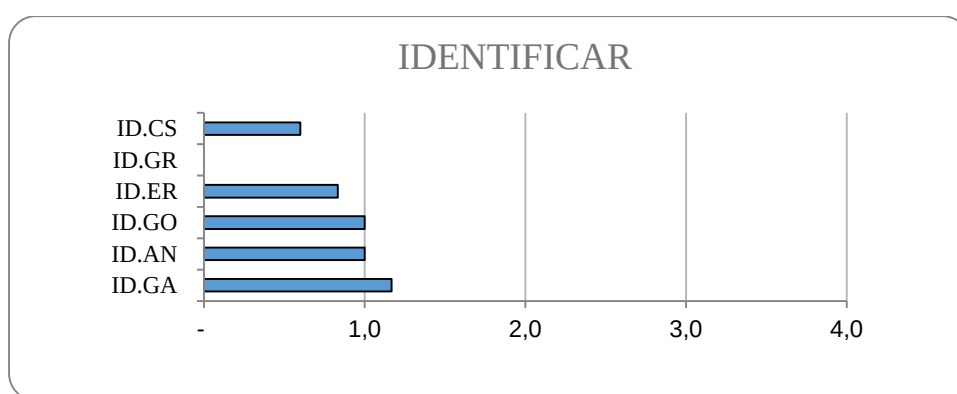


Ilustración 6: Resultados de Función Identificar

La subcategoría Estrategia para la gestión de riesgos (ID.GR) no presenta ningún nivel de madurez, lo que refleja la falta de una política formal y procedimientos para identificar, analizar y mitigar riesgos. Esto es especialmente crítico, ya que, sin una visión clara de los riesgos y su impacto potencial en los activos del organismo, es difícil establecer prioridades o tomar decisiones informadas sobre seguridad.

Por otro lado, las subcategorías Evaluación de riesgos (ID.ER) y Gobernanza (ID.GO) alcanzaron un nivel de madurez de 0.8, lo que indica que existen algunas prácticas dispersas o no formalizadas. En el caso de evaluación de riesgos, no se aplican metodologías estandarizadas ni se realiza de forma periódica, lo que limita la capacidad de anticipación, en cuanto a gobernanza, si bien se han definido ciertos roles y responsabilidades, aún no hay una estructura de supervisión ni políticas consolidadas que garanticen una gestión estratégica y continua de la ciberseguridad.

La subcategoría Gestión de activos (ID.GA) alcanzó el nivel más alto dentro de esta función (1.2), lo que demuestra esfuerzos por identificar y mantener un inventario de los recursos tecnológicos y de información. Sin embargo, esta gestión no se vincula aún con los procesos de evaluación de riesgo ni con una estrategia organizacional clara.

Finalmente, Ambiente del negocio (ID.AN) obtuvo un nivel bajo (0.3), lo que señala una débil comprensión del entorno operativo, regulatorio y de amenazas que rodean al organismo. Esta falta de contexto impide adecuar las prácticas de seguridad a las necesidades reales del organismo.

7.1.2. Proteger

La función Proteger alcanzó un nivel de madurez promedio de 1.3 (ver Tabla 10 e Ilustración 7), siendo la mejor evaluada entre todas las funciones del marco. Esto indica que se han implementado diversas medidas orientadas a reducir la probabilidad de ocurrencia de incidentes de ciberseguridad.

Función	Descripción Categoría	Categoría	Nivel Alcanzado
PROTEGER (PR)	Tecnología de protección	PR.TP	2.0
	Mantenimiento	PR.MA	1.0
	Procesos y procedimientos para la protección de la información	PR.PI	0.8
	Seguridad de los datos	PR.SD	1.4
	Concientización y formación	PR.CF	1.0
	Control de acceso	PR.CA	1.9
	Total		1.3

Tabla 10: Resultados de la Función Proteger

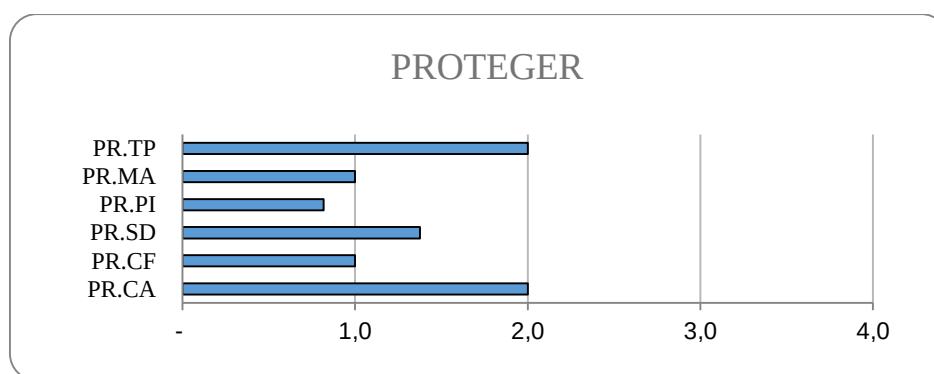


Ilustración 7: Resultados de la Función Proteger

Las subcategorías mejor posicionadas fueron Tecnología de protección (PR.TP) con 2.0 y Control de acceso (PR.CA) con 1.9, lo que muestra una adopción relevante de herramientas tecnológicas y mecanismos de restricción de acceso a la información.

No obstante, la categoría Procesos y procedimientos para la protección de la información (PR.PI) alcanzó apenas un 0.8, lo que evidencia la falta de documentación, estandarización y control formal de los procesos implementados. Esta debilidad representa un riesgo, ya que sin procedimientos definidos es difícil asegurar la coherencia en la aplicación de medidas de protección entre distintas áreas o ante cambios en la infraestructura. Asimismo, la subcategoría Concientización y formación (PR.CF) se encuentra en nivel 1.0, lo que indica que, si bien se han hecho algunos esfuerzos en capacitación, aún no se ha consolidado una cultura organizacional de seguridad.

Otra debilidad relevante se identifica en la subcategoría Mantenimiento (PR.MA) con un nivel de 1.0, que refleja una implementación parcial de rutinas para revisar, actualizar o reemplazar componentes críticos. Estas tareas son clave para asegurar la continuidad operativa y la adaptación a nuevos riesgos.

Por su parte, Seguridad de los datos (PR.SD) obtuvo un 1.4, lo que indica que se han establecido algunas prácticas para proteger la integridad y confidencialidad de la información, aunque es se ha hecho de forma parcial o sin monitoreo adecuado.

7.1.3. Detectar

La función Detectar presenta un nivel de madurez promedio de 0.9 (ver Tabla 11 e Ilustración 8), lo que indica que el organismo se encuentra en una etapa temprana de desarrollo de capacidades para identificar eventos anómalos o amenazas en tiempo real.

Función	Descripción Categoría	Categoría	Nivel Alcanzado
DETECTAR (DE)	Procesos de detección	DE.PD	0.8
	Monitoreo continuo de la seguridad	DE.MC	1.3
	Anomalías y eventos	DE.AE	0.6
	Total		0.9

Tabla 11: Resultados de la Función Detectar

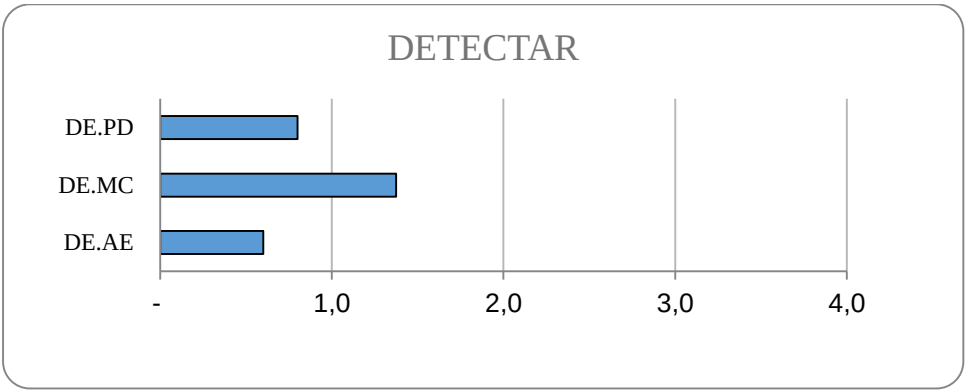


Ilustración 8: Resultados de la Función Detectar

La subcategoría Monitoreo continuo (DE.MC) alcanza el valor más alto (1.3), lo que demuestra la existencia de herramientas y acciones orientadas a la supervisión

constante de algunos activos y servicios críticos. Sin embargo, este monitoreo no está plenamente integrado ni cubre todo el entorno de TI.

En contraste, la subcategoría Anomalías y eventos (DE.AE), con un nivel de 0.6, revela que no existen mecanismos suficientes para identificar patrones inusuales, fallas o comportamientos anómalos que puedan ser indicio de un incidente. Esto limita gravemente la capacidad de anticipación frente a ciberataques o fallos de seguridad.

A su vez, la subcategoría Procesos de detección (DE.PD), con un nivel de 0.8, muestra que aún no se han definido ni formalizado procedimientos claros para la recolección, análisis y correlación de eventos de seguridad. Estas carencias reducen significativamente la capacidad de respuesta oportuna, ya que no es posible generar alertas efectivas, por lo que no existe una detección temprana para mitigar impactos.

7.1.4. Responder

La función Responder fue la peor calificada, con un nivel de madurez promedio de 0.4 (ver Tabla 12 e Ilustración 9), lo que representa un área crítica de mejora. Esta situación indica que el organismo no cuenta con capacidades efectivas para gestionar incidentes de seguridad cuando estos ocurren.

Función	Descripción Categoría	Categoría	Nivel Alcanzado
RESPONDER (RE)	Mejoras	RE.ME	-
	Mitigación	RE.MI	-
	Análisis	RE.AN	0.4
	Comunicaciones	RE.CO	0.6
	Planificación de la respuesta	RE.PR	1.0
	Total		0.4

Tabla 12: Resultados de la Función Responder

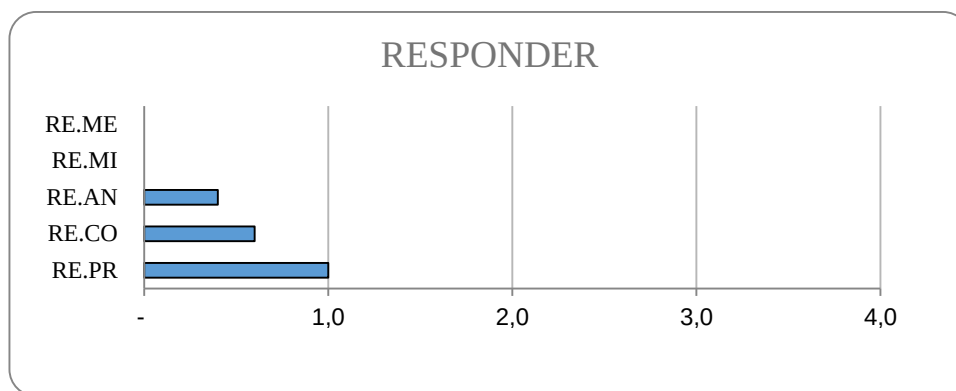


Ilustración 9: Resultados de la Función Responder

Las subcategorías Mitigación (RE.MI) y Mejoras (RE.ME) no alcanzan ningún nivel de madurez, lo que significa que no existen procedimientos establecidos para contener el impacto de incidentes ni para analizar su causa y generar aprendizajes.

La subcategoría Planificación de la respuesta (RE.PR) es la única que alcanzó un nivel básico (1.0), lo que sugiere que existen lineamientos generales sobre cómo actuar ante incidentes, aunque sin procedimientos específicos ni responsables claramente definidos.

Las subcategorías Análisis (RE.AN) y Comunicaciones (RE.CO), con niveles de 0.4 y 0.6 respectivamente, muestran que tampoco hay mecanismos sólidos para comprender la magnitud y causa de los incidentes ni para coordinar las comunicaciones internas y externas durante un evento de ciberseguridad. Esta debilidad puede tener consecuencias graves, ya que, ante un incidente real, el organismo podría responder de forma improvisada, sin coordinación entre áreas ni capacidad de limitar el daño.

7.1.5. Recuperar

La función Recuperar obtuvo un nivel de madurez promedio de 0.7 (ver Tabla 13 e Ilustración 10), lo que evidencia que el organismo ha comenzado a incorporar prácticas orientadas a restablecer sus operaciones tras un incidente, pero aún se encuentra lejos de alcanzar un nivel adecuado de resiliencia.

Función	Descripción Categoría	Categoría	Nivel Alcanzado
RECUPERAR (RC)	Comunicaciones	RC.CO	1.0
	Mejoras	RC.ME	-
	Planificación de la recuperación	RC.PR	1.0
	Total		0.7

Tabla 13: Resultados de la Función Recuperar

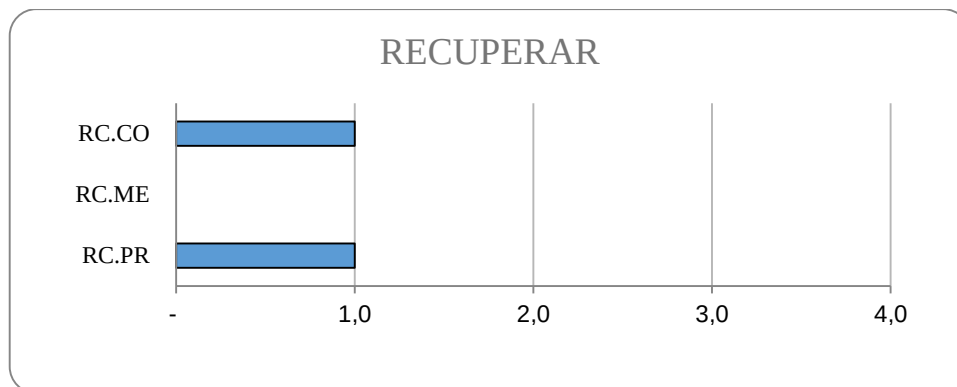


Ilustración 10: Resultados de la Función Recuperar

Las subcategorías Planificación de la recuperación (RC.PR) y Comunicaciones (RC.CO) alcanzaron un nivel de 1.0, lo que sugiere que existen medidas iniciales para planificar la continuidad de los servicios y comunicar el estado de recuperación a las partes interesadas.

Sin embargo, la subcategoría Mejoras (RC.ME) no presenta ningún nivel de madurez, lo que indica que no se realiza un análisis posterior a los incidentes para identificar debilidades, ajustar planes o prevenir recurrencias. Esta falta de retroalimentación limita la capacidad de adaptación y mejora continua, lo cual es fundamental para consolidar un enfoque resiliente frente a futuros eventos.

7.2. Recomendaciones propuestas

A partir del análisis de los datos obtenidos elaboramos una serie de recomendaciones con relación a la seguridad de la información en la División TIC, que se describen a continuación.

1. Fortalecer la gestión de riesgos en **Identificar**: la categoría Estrategia para la gestión de riesgos no ha alcanzado ningún nivel, lo que significa que no hay una planificación clara en este aspecto. Es importante desarrollar procedimientos para evaluar y mitigar riesgos, especialmente en la cadena de suministro.
2. Mantener y reforzar la función **Proteger**: si bien se alcanzó el nivel más alto de todas las funciones, la categoría Procesos y procedimientos para la protección de la información, sigue siendo un área de oportunidad. Se recomienda fortalecer la documentación y estandarización de los procedimientos de seguridad para reducir riesgos.
3. Mejorar la detección temprana de amenazas: Aunque la categoría de monitoreo continuo en la función **Detectar** ha pasado el nivel básico de madurez, las categorías de Procesos de detección, y Anomalías y eventos deben fortalecerse para mejorar la identificación de amenazas antes de que causen daño.
4. Enfocarse en mejorar la respuesta a incidentes: la función **Responder** tiene la menor madurez, lo que puede comprometer la capacidad del organismo para reaccionar eficazmente ante ataques. Se deben desarrollar estrategias para las subcategorías de Mitigación y Mejoras, que actualmente no tienen nivel.
5. Optimizar los procesos de **Recuperación**: aunque se han alcanzado ciertos niveles en planificación y comunicación, no hay un enfoque claro en mejoras post-incidente, lo que puede hacer que el organismo no aprenda de experiencias pasadas.

8. Mejoras introducidas en temas de Políticas de Seguridad y Capacitación

El este capítulo se presenta las mejoras introducidas en temas de Políticas de Seguridad y Capacitación. Luego de obtener un diagnóstico del estado actual de la ciberseguridad en el OP, se avanzó en la elaboración de la documentación necesaria para la implementación de las actividades del MCS, con el propósito de sentar bases que permitan avanzar con el cumplimiento de las actividades de madurez.

Alineados con los objetivos entregables de este trabajo, además del diagnóstico inicial del organismo, este proceso implicó la actualización de la PSI existente, la creación de un Manual de Políticas de Seguridad de la Información, así como el desarrollo de nuevas políticas complementarias. Estas últimas fueron creadas utilizando como referencia las políticas compartidas por el MCS de AGESIC para ser utilizadas como base por las organizaciones para definir o actualizar sus propias políticas [11]. Además, se elaboró material de capacitación orientado a fortalecer el conocimiento y la concienciación en seguridad de la información entre los colaboradores del organismo.

8.1. Principales modificaciones en la PSI

Tras la revisión de la PSI vigente (ver ANEXO 7 - Política de Seguridad de Información vigente), se identificaron oportunidades de mejora que permitieron optimizar su estructura y contenido. A continuación, en la Tabla 14, se detallan los principales cambios realizados, junto con las buenas prácticas que respaldan estas modificaciones.

Modificación	Detalle	Buenas prácticas
Cambio en la estructura del documento	La versión original contenía anexos con guías de uso detalladas sobre dispositivos móviles, correo electrónico, divulgación de información, seguridad ligada a recursos humanos, entre otros. La versión modificada eliminó estos anexos y se enfocó en una política más general, dejando de lado detalles operativos.	Separar políticas generales de procedimientos específicos. Las políticas deben establecer principios y responsabilidades generales, mientras que los procedimientos operativos pueden documentarse en anexos o manuales específicos.
Mayor énfasis en el enfoque estratégico	En la versión modificada, se destaca el compromiso del Directorio con el desarrollo progresivo de un SGSI basado en el Marco de Ciberseguridad de AGESIC.	Incluir un marco de referencia reconocido (como AGESIC) ayuda a dar solidez a la política y facilita su alineación con estándares nacionales e internacionales.
Definición clara de roles y responsabilidades	La versión modificada establece la figura del RSI, encargada de guiar la implementación y mantenimiento del SGSI.	Asignar responsabilidades específicas mejora la gobernanza y facilita la rendición de cuentas.
Mayor enfoque en sensibilización y formación	Se refuerza la necesidad de capacitar al personal en Seguridad de la Información mediante actividades formativas.	La capacitación continua es clave para minimizar riesgos de seguridad relacionados con el factor humano.
Revisión y actualización periódica más clara	Se mantiene la revisión cada tres años, pero en la versión modificada se detalla que esto responde a cambios tecnológicos, normativos y organizacionales.	Especificar criterios para la revisión asegura que la política no quede obsoleta.
Mayor alineación con normativa vigente	Se mantienen referencias a leyes clave como la Ley N°18.331 (Protección de Datos Personales) y la Ley N° 18.381 (Acceso a la Información Pública) [12].	Mantener referencias normativas relevantes refuerza la legitimidad de la política.

Tabla 14: Principales modificaciones de la PSI

8.2. Generación de nuevas Políticas

Con el propósito de alcanzar los niveles de madurez mínimos establecidos por el MCS, se decidió desarrollar un conjunto de políticas complementarias a la PSI, junto con su respectivo Manual de Políticas de Seguridad de la Información (ver ANEXO 3 - Entregable 2: Políticas a medida del organismo).

Este manual tiene como objetivo definir los lineamientos y el marco de referencia necesarios para la implementación efectiva del Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la preservación de la confidencialidad, integridad y disponibilidad de los activos de información del organismo. Los criterios para la construcción de estas políticas fueron elaborados conforme a las directrices establecidas por la Dirección de TIC, asegurando su alineación con los requerimientos y necesidades del organismo, identificados a partir de reuniones de seguimiento.

Este documento establece las bases para la correcta elaboración de procedimientos, instructivos y demás documentación asociada al SGSI, proporcionando un marco estructurado que permita su aplicación coherente en todo el organismo.

Asimismo, se definen una serie de lineamientos de seguridad de la información, los cuales deberán ser cumplidos por funcionarios, contratistas, terceros, usuarios y visitantes del organismo. Dichos lineamientos han sido categorizados en distintas temáticas, considerando el contexto interno y externo del organismo, con el fin de asegurar su aplicabilidad y efectividad.

El Manual de Políticas y todas las políticas de seguridad desarrolladas que se enumeran a continuación, se encuentran en el ANEXO 3 - Entregable 2: Políticas a medida del organismo.

- Pol 01 - Política de Seguridad de la Información
- Pol 02 - Política de Gestión de Incidentes de Seguridad de la Información
- Pol 03 - Política de Uso Aceptable de Activos
- Pol 04 - Política de Intercambio y Traslado Físico de la Información
- Pol 05 - Política de Control de Acceso Lógico

- Pol 06 - Política de Gestión de Usuarios y Contraseñas
- Pol 07 - Política de Gestión de Usuarios de Acceso Privilegiado
- Pol 08 - Política de Control de Acceso Físico a Áreas Seguras
- Pol 09 - Política de Seguridad del Equipamiento
- Pol 10 - Política de Respaldo de Información
- Pol 11 - Política de Protección contra Software Malicioso
- Pol 12 - Política de Separación de Entornos
- Pol 13 - Política de Registro y Auditoría de Eventos de Sistemas de Información
- Pol 14 - Política de Protección y Privacidad de los Datos
- Pol 15 - Política de Clasificación de la Información
- Pol 16 - Política de Uso Aceptable de Dispositivos Móviles
- Pol 17 - Política de Uso de Controles Criptográficos
- Pol 18 - Política de Continuidad Operativa y Recuperación ante Desastres
- Pol 19 - Política de Cumplimiento
- Pol 20 - Política de Escritorio y Pantalla Limpios
- Pol 21 - Política de Gestión de Riesgos de Seguridad de la Información
- Pol 22 - Política de Gestión de Cambios
- Pol 23 - Política de Finalización o Cambio en la Relación Laboral
- Pol 24 - Política de Acceso Remoto y Teletrabajo
- Pol 25 - Política de Eliminación y Destrucción de la Información
- Pol 26 - Política de Relacionamiento con Proveedores
- Pol 27 - Política De Uso Institucional De Redes Sociales
- Pol 28 - Política de Uso de Internet
- Pol 29 - Política de Desarrollo de Software Seguro
- Pol 30 - Política de Gestión de la Seguridad de las Redes
- Pol 31 - Política de Gestión de Riesgos de Proveedores
- Pol 32 - Política de Gestión de Activos
- Pol 33 - Política de Gestión de Riesgos

8.3. Capacitaciones

Luego de algunas reuniones con el responsable de capacitaciones del Departamento de Personal, y en línea con el compromiso de fortalecer los conocimientos clave en Seguridad de la Información, se diseñó y elaboró un plan de capacitación. La administración de dicho plan quedó bajo la responsabilidad del Departamento de Personal, quién definirá la forma de implementarlo y el correspondiente calendario. Además, dicho departamento será responsable de realizar las evaluaciones una vez finalizadas las capacitaciones, con el fin de medir su impacto en el personal del organismo.

El Plan de Capacitación elaborado, así como las diferentes inducciones y capacitaciones desarrolladas, se encuentran en el ANEXO 4 - Entregable 3: Plan y material de capacitaciones.

8.3.1. Plan de Concientización y Sensibilización

Para fomentar una cultura de responsabilidad y conciencia en el personal y reducir los riesgos e incidentes asociados a la seguridad de la información, se desarrolló un Plan de Capacitaciones alineado con las recomendaciones del NIST SP 800-50r1. Este plan establece un programa de formación y concientización en seguridad de tecnologías de la información.

Como parte de esta estrategia, también se diseñó un plan de comunicaciones para garantizar que todos los colaboradores del organismo estuvieran informados, motivados e involucrados en el cumplimiento de los controles de seguridad. La propuesta incluye los objetivos, actividades, métodos de ejecución, tiempos, recursos necesarios y resultados esperados, alineados con los objetivos institucionales.

La implementación de este plan tiene como propósito comunicar, sensibilizar y capacitar a todo el personal y proveedores sobre el manejo adecuado de la información institucional, asegurando el cumplimiento de las directivas, lineamientos, disposiciones y procedimientos de seguridad.

Para su ejecución, se definieron actividades específicas dentro del Plan de Concientización y Sensibilización en Seguridad de la Información, considerando los objetivos y la audiencia. El Departamento de Personal será responsable de una campaña de expectativa que incluirá:

- **Actividad 1:** Aplicación de una encuesta para evaluar el nivel de conocimiento y concientización de los colaboradores sobre seguridad de la información, con el objetivo de identificar áreas de mejora en la formación del personal.
- **Actividad 2:** Diseño y envío de comunicaciones periódicas sobre temas clave de seguridad de la información, mediante correo electrónico o herramientas colaborativas, para mantener informados a los colaboradores sobre buenas prácticas y actualizaciones relevantes.
- **Actividad 3:** Envío de actualizaciones regulares sobre buenas prácticas en el manejo de la información institucional, nuevas amenazas y vulnerabilidades, y el uso seguro de Internet, a través de correo electrónico o herramientas colaborativas, para reforzar la cultura de seguridad y mantener a los colaboradores al tanto de los riesgos emergentes.
- **Actividad 4:** Realización de charlas virtuales de 30 a 45 minutos, con presentaciones o videos sobre seguridad de la información, con el objetivo de sensibilizar al personal y proporcionar un espacio para resolver dudas y consultas sobre el tema.

8.3.2. Material de Capacitaciones

Por otro lado, se desarrollaron materiales didácticos que incluyen presentaciones, manuales y guías prácticas, con el objetivo de garantizar un programa de formación efectivo y aplicable a todo el organismo, como resultado de las reuniones previamente mencionadas. En dichas reuniones se identificaron las necesidades formativas del personal y se definieron los contenidos clave para asegurar un enfoque integral.

El plan de capacitación se estructuró en seis pilares fundamentales para reforzar los conceptos esenciales en Seguridad de la Información:

- 1. Seguridad de la Información:** Busca introducir a los participantes en los conceptos clave de la Seguridad de la Información y su impacto en el organismo, con énfasis en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Se busca que comprendan la importancia de las normativas, los beneficios del SGSI, los riesgos asociados a la protección de la información y el papel de los controles y políticas en la mitigación de amenazas y vulnerabilidades.
- 2. Protección y privacidad de los datos:** Tiene como objetivo concientizar a los participantes sobre la importancia de la protección de la privacidad y los datos personales, identificando la información de valor que manejan, los riesgos asociados y las mejores prácticas para su resguardo. Además, se abordará el marco legal vigente y las medidas necesarias para garantizar la seguridad de los activos de información.
- 3. Políticas de seguridad:** Su finalidad es explicar el rol y la importancia de las políticas de seguridad de la información dentro del SGSI, asegurando que los participantes comprendan sus lineamientos, su impacto en el trabajo diario y la necesidad de su cumplimiento para la protección de los activos de información.
- 4. Gestión de riesgos:** Esta capacitación tiene como objetivo brindar a los participantes los conocimientos esenciales sobre la gestión de riesgos en seguridad de la información, basados en la norma ISO/IEC 27.001:2022 . Se busca que comprendan los procesos de análisis, evaluación, tratamiento y aceptación de riesgos, así como la importancia de implementar controles para mitigar amenazas y proteger los activos de información.
- 5. Sistema de Gestión de Seguridad de la Información (SGSI):** Su fin es proporcionar una visión integral del SGSI, abordando sus definiciones, principios y aplicación práctica. Se busca que los participantes comprendan el ciclo de vida y la protección de la información, el cumplimiento legal y regulatorio, y los

controles de seguridad física y lógica, incluyendo su impacto en servicios, aplicaciones, dispositivos móviles, medios extraíbles e incidentes de seguridad.

- 6. ISO 27001:** Esta capacitación tiene como objetivo familiarizar a los participantes con la norma ISO/IEC 27001:2022 y su importancia en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Además, se creó un material complementario denominado "TIPS", diseñado para abordar de manera sencilla y accesible temas clave como la concienciación en seguridad, el uso adecuado de medios de almacenamiento y las buenas prácticas en redes sociales. Este material fue elaborado en formatos visuales y de fácil comprensión, con el fin de reforzar hábitos seguros en el uso de la información dentro del organismo.

9. Resumen de actividades realizadas a la fecha de presentación de este trabajo

En los últimos tres meses de ejecución del proyecto se implementaron diversas acciones orientadas a fortalecer la gestión de la seguridad de la información dentro del organismo. Entre ellas, se destacan el desarrollo de políticas y la elaboración de material para capacitaciones, las cuales permitirán mejorar la comprensión y aplicación de buenas prácticas de seguridad de la información.

Si bien estas iniciativas representan un avance significativo en términos de alineación con los estándares de ciberseguridad, su impacto en la evaluación del nivel de madurez no ha generado cambios significativos en la clasificación general.

A continuación, se presenta el nivel de implementación de las tareas acordadas al momento de la presentación de este informe. En los ANEXO 3 - Entregable 2: Políticas a medida del organismo y ANEXO 4 - Entregable 3: Plan y material de capacitaciones se encuentra el detalle de las tareas realizadas durante el proyecto, reflejando los avances en la definición de políticas y capacitaciones.

Por otro lado, las Tablas 15, 16 y 17 presentan un resumen de la cantidad de tareas completadas y aquellas que aún están pendientes para alcanzar el nivel máximo de madurez (nivel 4) en las actividades de prioridad P1, P2 y P3. (ver el listado de actividades pendientes en ANEXO 5 - Listado de actividades pendientes). Este análisis permite evaluar el progreso actual y cuantificar las tareas pendientes, las cuales el organismo deberá revisar y gestionar en su ejecución cuando lo considere oportuno.

	Logradas por el OP	Realizadas durante el proyecto	Pendientes	Totales
IDENTIFICAR (ID)	24	4	89	117
PROTEGER (PR)	44	4	79	127
DETECTAR (DE)	3	0	6	9
RESPONDER (RE)	3	1	9	13
RECUPERAR (RC)	0	0	0	0
Totales	74	9	183	266

Tabla 15: Detalle de cantidad de tareas por función y estado para P1

	Logradas por OP	Realizadas durante el proyecto	Pendientes	Totales
IDENTIFICAR (ID)	0	3	75	78
PROTEGER (PR)	0	6	146	152
DETECTAR (DE)	0	0	95	95
RESPONDER (RE)	0	1	83	84
RECUPERAR (RC)	0	1	14	15
Totales	0	11	413	424

Tabla 16: Detalle de cantidad de tareas por función y estado para P2

	Logradas por OP	Realizadas durante el proyecto	Pendientes	Totales
IDENTIFICAR (ID)	0	0	27	27
PROTEGER (PR)	0	0	70	70
DETECTAR (DE)	0	0	68	68
RESPONDER (RE)	0	0	10	10
RECUPERAR (RC)	0	0	11	11
Totales	0	0	186	186

Tabla 17: Detalle de cantidad de tareas por función y estado para P3

10. Conclusiones

De acuerdo con los objetivos planteados al inicio de este proyecto, vemos con satisfacción que las estimaciones de tiempo y esfuerzo estuvieron dentro de lo esperado, y que tuvimos la capacidad de gestionar los riesgos del proyecto, de forma de poder cumplir con los objetivos que nos planteamos inicialmente.

Se logró diagnosticar la situación del organismo respecto al MCS de AGESIC, visualizando las políticas, procedimientos y controles existentes al comienzo del proyecto.

Se realizó la revisión de la política de seguridad de la información en el organismo, a la que se le realizaron las modificaciones correspondientes, quedando pendiente la aprobación de la misma por parte de la Comisión de Seguridad y por el Directorio del organismo.

Asimismo, se desarrollaron la mayoría de las políticas de seguridad complementarias que dan soporte a la implementación de la seguridad de la información en el organismo. También se desarrolló un Plan de Concientización y Sensibilización en Seguridad de la Información y se elaboraron los materiales para las primeras capacitaciones y concientizaciones en temas de Seguridad de la Información, Protección de Datos, y Sistema de Gestión de Seguridad de la Información entre otros.

Cabe destacar que, debido a la ausencia por licencias y otras cuestiones de agenda, aún no se realizó la reunión de cierre y definición de los siguientes pasos (traspaso), pero ya fue acordada para realizarse próximamente.

Finalmente, teniendo en cuenta lo limitado del tiempo de ejecución del proyecto de tesis, como se señaló anteriormente, elaboramos la lista de actividades pendientes (ver ANEXO 5 - Listado de actividades pendientes) de concreción por parte del organismo, las cuales permitirán implementar las bases de un Sistema de Gestión de Seguridad de la Información.

Referencias bibliográficas

- [1] IMPO - Ley N° 18.331, Ley de protección de datos personales. Recuperado de: <https://www.impocom.uy/bases/leyes/18331-2008> (último acceso: 15 de Enero de 2.025).
- [2] AGESIC - Marco de Ciberseguridad. Recuperado de: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad> (último acceso: 18 de Enero de 2.025).
- [3] AGESIC - Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento. Recuperado de: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/> (último acceso: 25 de Enero de 2.025).
- [4] NIST SP 800-50r1. Recuperado de: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.ipd.pdf> (último acceso: 25 de Enero de 2.025).
- [5] ISO/IEC 27.001:2022. Recuperado de: <https://www.iso.org/es/norma/27001> (último acceso: 31 de Enero de 2.025).
- [6] Cobit 5. Recuperado de: <https://articulosit.wordpress.com/wp-content/uploads/2013/07/cobit5-framework-spanish.pdf> (último acceso: 5 de Febreo de 2.025).
- [7] AGESIC - Guía de Implementación. Recuperado de: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-implementacion/guia-implementacion-0> (último acceso: 12 de Febreo de 2.025).
- [8] CERTuy - Servicios del CERT/SOC. Recuperado de: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tramites-y-servicios/servicios/certuy> (último acceso: 15 de Febreo de 2.025).
- [9] ITIL. Recuperado de: <https://www.peoplecert.org/browse-certifications/it-governance-and-service-management/ITIL-1/itil-4-foundation-2565> (último acceso: 16 de Febreo de 2.025).
- [10] IMPO - Decreto N° 66/025. Recuperado de: <https://www.impocom.uy/bases/decretos/66-2025> (último acceso: 20 de Febreo de 2.025).

- [11] AGESIC - Políticas sobre el Marco de Ciberseguridad. Recuperado de:
<https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/politicas-sobre-marco-ciberseguridad>
(último acceso: 22 de Febreo de 2.025).
- [12] IMPO - Ley N° 18.381, Ley sobre el derecho de acceso a la información Pública. Recuperado de:
<https://www.impo.com.uy/bases/leyes/18381-2008> (último acceso: 25 de Febreo de 2.025).

ANEXO 1 - Carta de consentimiento

Este anexo incluye la carta de consentimiento con los acuerdos de confidencialidad establecidos con el organismo.

Montevideo, 26 de octubre de 2024.-

Nosotros, Katherine Venegas, Ma. Mercedes Schicht y Luis Jaunarena estudiantes de la Universidad ORT Uruguay, solicitamos formalmente su autorización para llevar a cabo un proyecto de mejora de seguridad de la información [REDACTED] en el marco de nuestros estudios académicos. Este proyecto forma parte de nuestra tesis para el postgrado de Máster en Gestión de Sistemas de Información.

Nos comprometemos a:

- Respetar y cumplir con todas las normativas del organismo.
- Manejar con estricta confidencialidad cualquier dato o información sensible a la que tengamos acceso durante el desarrollo del proyecto.
- No divulgar, compartir ni publicar, en ningún medio físico o digital, información del organismo sin previa autorización escrita.
- Usar la información únicamente para los fines académicos relacionados con el presente proyecto.
- Entregar una copia de toda la documentación generada al [REDACTED]

Agradecemos su apoyo y autorización para la realización de este proyecto. Quedamos atentos a cualquier requisito adicional o lineamiento que el organismo considere necesario para llevar a cabo el proyecto.

Director de TIC



Katherine Venegas



Luis Jaunarena



Mercedes Schicht

División Tecnologías de la Información y Comunicaciones

ANEXO 2 - Entregable 1: Situación actual de la Seguridad de la Información en el organismo

Tabla de Contenido

1.	Introducción.....	73
2.	Entrevistas iniciales	74
3.	Planilla de evaluación.....	77
4.	Revisión de las tareas terminadas	105

Índice de Ilustraciones

Ilustración 11: Hoja Resumen	77
Ilustración 12: Hoja Radar.....	78
Ilustración 13: Hoja Barras.....	78
Ilustración 14: Hoja Madurez	80
Ilustración 15: Hoja Madurez_Evidencia	81
Ilustración 16: Hoja Evidencia	83
Ilustración 17: Hoja Evidencias completada	83
Ilustración 18: Hoja Madurez_Evidencia completada.....	101
Ilustración 19: Hoja Madurez completada.....	101
Ilustración 20: Ejemplo para definición de nivel de madurez	102
Ilustración 21: Hoja Radar completada	102
Ilustración 22: Hoja Barras completada	103
Ilustración 23: Hoja Resumen completada.....	103

Índice de Tablas

Tabla 16: Detalle de cantidad de tareas por función y estado para P2	66
Tabla 17: Detalle de cantidad de tareas por función y estado para P3	66
Tabla 18: Capítulos de evidencias	81
Tabla 19: Listado de preguntas con respuestas del cuestionario	100
Tabla 20: Tareas logradas por el organismo.....	109

1. Introducción

El presente anexo describe el proceso de relevamiento realizado en el organismo para evaluar el nivel de seguridad mediante la aplicación del MCS de AGESIC. Este relevamiento tuvo como objetivo evaluar el nivel de madurez, identificar fortalezas y oportunidades de mejora, y establecer una base para futuras acciones de fortalecimiento en la gestión de seguridad.

En la primera sección, se detallan las entrevistas iniciales realizadas con los responsables clave del área de TIC e infraestructura. Estas entrevistas permitieron comprender el contexto institucional, los procesos existentes y los desafíos en materia de ciberseguridad.

A continuación, en la segunda sección, se presenta la planilla de evaluación utilizada en el relevamiento, explicando su estructura y los diferentes componentes que la conforman, como el resumen de resultados, gráficos de madurez y evidencias recopiladas. Posteriormente, se describe el proceso de aplicación de dicha evaluación, incluyendo las metodologías empleadas para la recolección y validación de información, la determinación del nivel de madurez alcanzado y la consolidación de este en un resumen.

Finalmente, en la última sección, se detallan las tareas identificadas como logradas por el organismo, extraídas de un listado más amplio de actividades identificadas para alcanzar los diferentes niveles de madurez (Ver Anexo 6).

Este anexo complementa el documento principal proporcionando una visión detallada del proceso de diagnóstico y evaluación, sirviendo como referencia para la planificación y ejecución de mejoras en la gestión de ciberseguridad del organismo.

2. Entrevistas iniciales

Para obtener una primera aproximación a la situación actual de ciberseguridad del organismo, se realizaron entrevistas con el Director de TIC y el Director de Infraestructura.

2.1. Entrevista al Director de TIC (29/10/2024)

1) ¿Qué áreas más relevantes dentro del organismo?

El área más relevante es la del propio servicio que brinda el organismo (la denominaremos áreas de servicio), Dirección General, Jurídica, Planeamiento y Presupuesto Estratégico, TIC, Financiero Contable, Adquisiciones, Gestión y Desarrollo Humano, Comunicación Institucional y Logística Centro de Capacitación y Formación.

2) ¿Existe una estrategia formal de ciberseguridad en el organismo?

No, actualmente el organismo no cuenta con una estrategia formal de ciberseguridad. Si bien se ha conformado una comisión de seguridad de la información con el objetivo inicial de crear una Política de Seguridad de la Información, todavía no existe una estrategia integral que abarque políticas, procedimientos y controles.

3) ¿Hay responsable en ciberseguridad o responsable de seguridad de la información?

No, el organismo no cuenta con un rol formalmente designado para liderar las actividades de ciberseguridad o seguridad de la información. Si existe un área de Datos Personales con un referente formalmente designado que trabaja en la protección de datos y el cumplimiento de la Ley N° 18.331.

4) ¿Quiénes integran la CSI?

La CSI está formada por los directores de TIC, Jurídica, Auditoría Interna, Planeamiento y Presupuesto Estratégico, y el Referente de Datos Personales.

5) ¿Cada cuánto tiempo se reúne la CSI? ¿Hay actas?

Al comienzo con la creación de la comisión las reuniones eran semanales o cada 15 días hasta desarrollar y aprobar la PSI. Actualmente, las reuniones se llevan a cabo cada tres meses. Se mantiene un registro de actas de reunión, que incluye una minuta firmada por todos los participantes.

6) ¿El personal firma acuerdos de confidencialidad de la información a la cual tienen acceso?

Sí, al ingresar al Organismo, antes de firmar la toma de puesto, el personal debe firmar un acuerdo de confidencialidad sobre la información a la que tendrá acceso. Este documento es resguardado por el Departamento de Personal.

7) ¿Los funcionarios firman el cumplimiento de políticas de seguridad?

Sí, es la idea. Para contar con la aprobación de la PSI todo el personal tuvo que aprobar su contenido completando un formulario en la Intranet. A medida que surjan más políticas la idea es llevar un control de la aprobación del personal.

8) ¿Los funcionarios reciben formación en ciberseguridad?

No, actualmente el organismo no ofrece capacitación regular a sus funcionarios sobre seguridad de la información. Estamos trabajando en campañas de phishing que lleva adelante el Departamento de Infraestructura.

2.2. Entrevista al Director de Infraestructura (29/10/2024)

1) ¿Cómo percibe la situación actual de la seguridad de la información en el organismo?

Actualmente, el nivel de ciberseguridad en el organismo es bajo, lo que representa un desafío para nosotros. Somos conscientes de esta situación y estamos implementando medidas para mejorar la seguridad. Pero tenemos limitaciones en términos de personal y recursos, lo que dificulta la implementación inmediata de mejoras.

2) ¿Cuáles son las principales tecnologías utilizadas para proteger la información y la infraestructura del organismo?

Entre las principales soluciones que utilizamos, desde el punto de vista de red, contamos con firewalls Fortigate y Mikrotik para el control del tráfico. La solución Fortigate está implementada en los cuatro edificios centrales de Montevideo, mientras que Mikrotik se utiliza en aproximadamente 150 sitios adicionales. Además, disponemos de una red MPLS que conecta nuestras sedes departamentales.

En cuanto a la infraestructura de servidores, utilizamos VMware como plataforma de virtualización en nuestro centro de datos y también contamos con un espacio contratado en la nube empresarial de Antel para alojar las aplicaciones más críticas.

3) ¿Cómo se gestionan los incidentes de ciberseguridad?

No contamos con una gestión formal de incidentes, tratamos de resolver los incidentes de la mejor manera posible cuando ocurren.

4) ¿Se realizan análisis de vulnerabilidades regularmente?

Actualmente, no realizamos análisis de vulnerabilidades de manera regular, nos esforzamos por mantener actualizados los firmwares de los routers y aplicar los últimos parches soportados para la versión de VMware que utilizamos.

5) A nivel de ciberseguridad, ¿qué es lo que más le preocupa?

Lo que más me preocupa es la filtración de información sensible y la alta frecuencia de ataques de phishing a la que nos enfrentamos a diario.

3. Planilla de evaluación

Para realizar el relevamiento del nivel de madurez se utilizó una planilla que se describe a continuación.

3.1. Composición del Documento

El documento utilizado para la evaluación del nivel de madurez en ciberseguridad se estructura en varias hojas interconectadas, cada una con un propósito específico:

3.1.1. Resumen

Esta hoja sirve para evaluar y visualizar el estado general actual de ciberseguridad en una organización, permitiendo identificar en qué nivel de madurez se encuentra cada área (función) y cuáles requieren mejoras. La hoja se divide en:

- Funciones principales basadas en el marco de ciberseguridad
- Categorías dentro de cada función con su descripción
- Sección de evaluación del "Nivel Alcanzado" en una escala del 0. al 4, donde el usuario puede indicar el nivel actual de cada subcategoría

Función	Categoría	Descripción Categoría	Nivel Alcanzado	0,5	1	1,5	2	2,5	3	3,5	4
IDENTIFICAR (ID)	ID-SA	Gestión de activos	-								
	ID-AN	Ambiente del negocio	-								
	ID-GO	Gobernanza	-								
	ID-ER	Evaluación de riesgos	-								
	ID-GR	Estrategia para la gestión de riesgos	-								
	ID-CS	Gestión de riesgos en la cadena de suministros	-								
PROTEGER (PR)	PR-CA	Control de acceso	-								
	PR-CF	Concientización y formación	-								
	PR-SD	Seguridad de los datos	-								
	PR-PI	Procesos y procedimientos para la protección de la información	-								
	PR-MA	Mantenimiento	-								
	PR-TP	Tecnología de protección	-								
DETECTAR (DE)	DE-AE	Anomalías y eventos	-								
	DE-MC	Monitoreo continuo de la seguridad	-								
	DE-PD	Procesos de detección	-								
RESPONDER (RE)	RE-PR	Planificación de la respuesta	-								
	RE-CO	Comunicaciones	-								
	RE-LAN	Análisis	-								
	RE-MI	Mitigación	-								
	RE-ME	Mejoras	-								
RECUPERAR (RC)	RC-PR	Planificación de la recuperación	-								
	RC-ME	Mejoras	-								
	RC-CO	Comunicaciones	-								

Ilustración 11: Hoja Resumen

3.1.2. Radar

Representa gráficamente, mediante un diagrama de radar, el promedio del nivel de madurez alcanzado por función, facilitando la comparación entre distintas áreas.

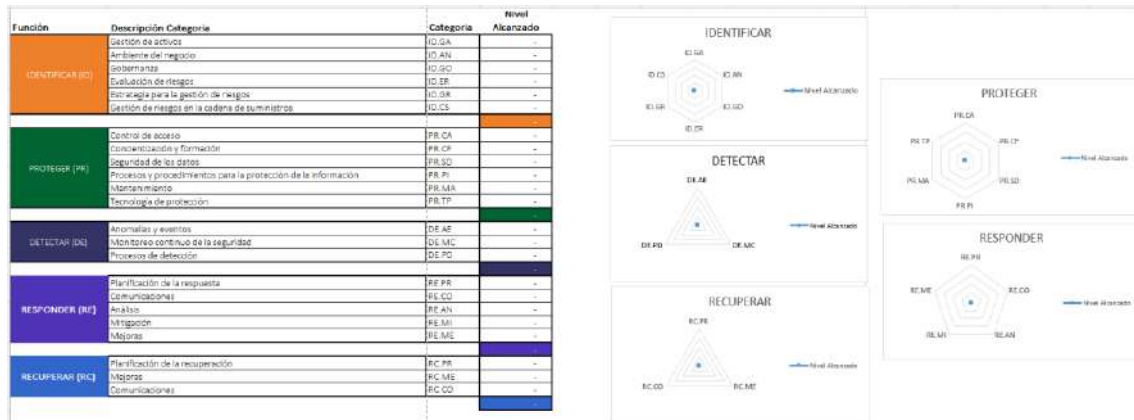


Ilustración 12: Hoja Radar

3.1.3. Barras

Muestra a través de gráficos de barras el promedio del nivel de madurez por función, permitiendo visualizar tendencias y áreas de mejora.

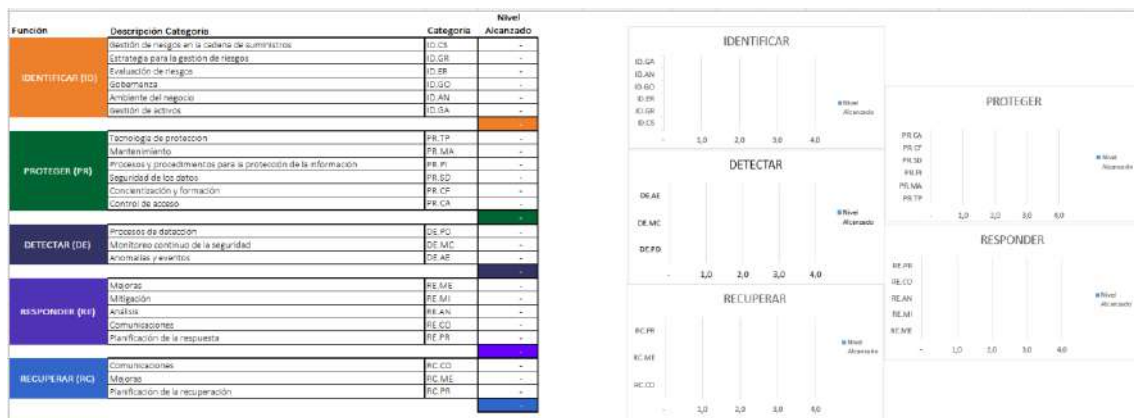


Ilustración 13: Hoja Barras

3.1.4. Madurez

Esta hoja es la base de la evaluación del nivel de madurez en ciberseguridad, permitiendo analizar el estado actual del organismo en función del MCS de AGESIC. Cada función de seguridad se divide en categorías y subcategorías, con un nivel de madurez alcanzado, una prioridad asignada y un estado de cumplimiento. Además, se documentan las acciones necesarias para mejorar el nivel de madurez, los responsables de la implementación y las evidencias que respaldan el cumplimiento. Su objetivo es proporcionar una visión estructurada del estado de seguridad de la organización.

Columnas:

- **Función:** Indica la función del MCS evaluada (IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER, RECUPERAR).
- **Cat (Categoría):** Código de la categoría evaluada dentro de la función.
- **Cat_Nombre:** Nombre de la categoría evaluada.
- **Cat_Descripción:** Explicación de la categoría dentro de la función.
- **Subcat (Subcategoría):** Código de la subcategoría dentro de la categoría.
- **Subcat_Descripción:** Explicación de la subcategoría evaluada.
- **Nivel Alcanzado:** Nivel actual de madurez registrado en una escala de 0 a 4.
- **Prioridad B (Básico):** Prioridad asignada para la subcategoría básica.
- **Madurez Nivel:** Nivel de madurez esperado o requerido para la subcategoría.
- **Madurez:** Descripción del estado de madurez alcanzado.
- **Cumplimiento:** Indica si la subcategoría cumple con los requisitos definidos (SI/NO).
- **Observaciones:** Comentarios adicionales sobre la evaluación.
- **¿Se Repite?:** Indica si la subcategoría se repite en otra función/categoría/subcategoría.
- **Tareas pendientes para alcanzar nivel de madurez:** Acciones necesarias para alcanzar el nivel de madurez de la función/categoría/subcategoría.
- **Responsable:** Persona o equipo encargado de realizar la Tarea.
- **Evidencia:** Documentos específicos para la tarea que respaldan el nivel alcanzado.

Revisión	Cat.	Ent. Nombre	Ent. Descripción	Subcat.	Subcat. Descripción	Nivel	Madurez	Prioridad	Madurez	Cumplimiento	Se	Notas pendientes que se deben incluir	Requisito	Observación
EVIDENCIA	ICGA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que pertenecen a la organización alcanzan los objetivos de seguridad, se identifican y gestionan en forma consistente, en relación con los capítulos y la estrategia de riesgo de la organización.	ICGA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	0	1	PL	Se configuran y mantienen inventarios de dispositivos físicos (servidores, redes, dispositivos de almacenamiento, etc.) del centro de datos.	1001 - Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. 1002 - Implementar un mecanismo para mantener el inventario actualizado por ejemplo, mediante periodicidad o actualización manual. 1003 - Asegurar que el inventario incluya información clave como ubicación, estado, fecha de compra, etc.	1001 - Director de Infraestructura 1002 - Director de Infraestructura 1003 - Director de Infraestructura	1001 - Director de Infraestructura 1002 - Director de Infraestructura 1003 - Director de Infraestructura	1001 - Director de Infraestructura 1002 - Director de Infraestructura 1003 - Director de Infraestructura	
									Se incluyen en el inventario los dispositivos físicos (PC, servidores, dispositivos de almacenamiento, etc.) que pertenecen al centro de datos, así como los dispositivos de almacenamiento de datos, etc.	1004 - Ampliar el inventario de dispositivos físicos a los dispositivos de almacenamiento de datos. 1005 - Establecer un sistema unificado de registro que permita integrar información de todos los dispositivos físicos y sistemas. 1006 - Implementar un mecanismo para registrar los dispositivos de almacenamiento de datos, etc.	1004 - Director de Infraestructura 1005 - Director de Infraestructura 1006 - Director de Infraestructura	1004 - Director de Infraestructura 1005 - Director de Infraestructura 1006 - Director de Infraestructura	1004 - Director de Infraestructura 1005 - Director de Infraestructura 1006 - Director de Infraestructura	
EVIDENCIA	ICGA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que pertenecen a la organización alcanzan los objetivos de seguridad, se identifican y gestionan en forma consistente, en relación con los capítulos y la estrategia de riesgo de la organización.	ICGA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	0	2	PL	Se configuran y mantienen inventarios de dispositivos físicos (servidores, redes, dispositivos de almacenamiento, etc.) del centro de datos, así como los dispositivos de almacenamiento de datos, etc.	1007 - Implementar un mecanismo para actualizar el inventario de dispositivos físicos y sistemas. 1008 - Implementar un mecanismo para actualizar el inventario de dispositivos de almacenamiento de datos, etc.	1007 - Director de Infraestructura 1008 - Director de Infraestructura	1007 - Director de Infraestructura 1008 - Director de Infraestructura	1007 - Director de Infraestructura 1008 - Director de Infraestructura	
									Los dispositivos y sistemas se encuentran inventariados y se actualizan de manera oportuna.	1009 - Realizar auditorías periódicas para verificar el cumplimiento de los requisitos de seguridad. 1010 - Asegurar el cumplimiento de los requisitos de seguridad.	1009 - Director de Infraestructura 1010 - Director de Infraestructura	1009 - Director de Infraestructura 1010 - Director de Infraestructura	1009 - Director de Infraestructura 1010 - Director de Infraestructura	
EVIDENCIA	ICGA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que pertenecen a la organización alcanzan los objetivos de seguridad, se identifican y gestionan en forma consistente, en relación con los capítulos y la estrategia de riesgo de la organización.	ICGA-2	Los dispositivos físicos y sistemas se encuentran inventariados.	0	3	PL	Se configuran y mantienen inventarios de dispositivos físicos (servidores, redes, dispositivos de almacenamiento, etc.) del centro de datos, así como los dispositivos de almacenamiento de datos, etc.	1009 - Realizar auditorías periódicas para verificar el cumplimiento de los requisitos de seguridad. 1010 - Asegurar el cumplimiento de los requisitos de seguridad.	1009 - Director de Infraestructura 1010 - Director de Infraestructura	1009 - Director de Infraestructura 1010 - Director de Infraestructura	1009 - Director de Infraestructura 1010 - Director de Infraestructura	
									Se revisan los datos y dispositivos físicos y sistemas de manera oportuna para verificar el cumplimiento de los requisitos de seguridad.	1011 - Realizar auditorías periódicas para verificar el cumplimiento de los requisitos de seguridad. 1012 - Asegurar el cumplimiento de los requisitos de seguridad.	1011 - Director de Infraestructura 1012 - Director de Infraestructura	1011 - Director de Infraestructura 1012 - Director de Infraestructura	1011 - Director de Infraestructura 1012 - Director de Infraestructura	
EVIDENCIA	ICGA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que pertenecen a la organización alcanzan los objetivos de seguridad, se identifican y gestionan en forma consistente, en relación con los capítulos y la estrategia de riesgo de la organización.	ICGA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	0	4	PL	Se revisan los datos y dispositivos físicos y sistemas de manera oportuna para verificar el cumplimiento de los requisitos de seguridad.	1013 - Realizar auditorías periódicas para verificar el cumplimiento de los requisitos de seguridad. 1014 - Asegurar el cumplimiento de los requisitos de seguridad.	1013 - Director de Infraestructura 1014 - Director de Infraestructura	1013 - Director de Infraestructura 1014 - Director de Infraestructura	1013 - Director de Infraestructura 1014 - Director de Infraestructura	
									Se revisan los datos y dispositivos físicos y sistemas de manera oportuna para verificar el cumplimiento de los requisitos de seguridad.	1015 - Realizar auditorías periódicas para verificar el cumplimiento de los requisitos de seguridad. 1016 - Asegurar el cumplimiento de los requisitos de seguridad.	1015 - Director de Infraestructura 1016 - Director de Infraestructura	1015 - Director de Infraestructura 1016 - Director de Infraestructura	1015 - Director de Infraestructura 1016 - Director de Infraestructura	

Ilustración 14: Hoja Madurez

3.1.5. Madurez_Evidencia

Esta hoja complementa la evaluación de madurez al relacionar cada subcategoría con requisitos específicos y su cumplimiento. Permite verificar si el organismo cuenta con controles y documentación que respalden su nivel de madurez. A través de la conexión con la hoja Madurez, se establecen las bases para demostrar si el nivel registrado en cada subcategoría tiene un sustento verificable. Además, se incluyen observaciones sobre el estado de cumplimiento y se identifican oportunidades de mejora.

Columnas:

- **Función:** Función del MCS a la que pertenece la evaluación.
- **Categoría:** Código y nombre de la categoría dentro de la función.
- **Descripción:** Explicación de la categoría evaluada.
- **Subcategoría:** Código y nombre de la subcategoría dentro de la categoría.
- **Requisitos:** Código del requisito que debe cumplirse en la subcategoría, y que se vincula con la columna requisito de la hoja Evidencia
- **Requisitos Descripción:** Descripción del requisito que debe cumplirse.
- **Cumplimiento:** Indica si el requisito ha sido cumplido en el organismo (SI/NO).
- **Observaciones:** Notas adicionales sobre el estado de cumplimiento o faltantes.

Función	Categoría	Descripción	Subcategoría	Requisitos	Requisitos descripción	Cumplimiento	Observaciones
IDENTIFICAR (IS)	ID-GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID-GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	GA.1	Identificar formalmente los activos de la organización junto con la definición de su responsable.		
IDENTIFICAR (IS)	ID-GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID-GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	GA.3	Restringir el uso aceptable de los activos.		
IDENTIFICAR (IS)	ID-GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID-GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	GA.5	Restringir el uso de dispositivos móviles.		
IDENTIFICAR (IS)	ID-GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID-GA-2. Las plataformas de software y aplicaciones se encuentran inventariadas.	GA.1	Identificar formalmente los activos de la organización junto con la definición de su responsable.		
IDENTIFICAR (IS)	ID-GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID-GA-2. Las plataformas de software y aplicaciones se encuentran inventariadas.	GA.3	Restringir el uso aceptable de los activos.		
IDENTIFICAR (IS)	ID-GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID-GA-2. Las plataformas de software y aplicaciones se encuentran inventariadas.	GA.4	Gestionar las licencias de software.		
IDENTIFICAR (IS)	ID-GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID-GA-3. Se utilizan medidas de seguridad y procedimientos de gestión para proteger y controlar el flujo de información	SC.14	Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.		

Ilustración 15: Hoja Madurez_Evidencia

3.1.6. Evidencias_Intro

Explica la organización del cuestionario de evidencias contenido en la hoja Evidencias y menciona los capítulos que se tratan en este:

Id Capítulo	Descripción
01 - OR	Organización y Gobernanza
02 - GR	Gestión de Riesgos
03 - PL	Planificación
04 - GH	Gestión Humana
05 - GA	Gestión de Activos
06 - CA	Control de Acceso
07 - SF	Seguridad Física y del Ambiente
08 - SO	Seguridad de las Operaciones
09 - SC	Seguridad en las Comunicaciones
10 - AD	Adquisición, Desarrollo y Mantenimiento de los Sistemas
11 - RP	Relación con Proveedores
12 - GI	Gestión de Incidentes
13 - CO	Continuidad de las Operaciones
14 - CN	Cumplimiento Normativo

Tabla 18: Capítulos de evidencias

3.1.7. Evidencias

La hoja Evidencia contiene un cuestionario estructurado en los 14 capítulos antes mencionados, actúa como un respaldo documental, permitiendo verificar si existen políticas, inventarios y controles de seguridad necesarios para cumplir con los requisitos evaluados en la hoja Madurez_Evidencia. Se recopilan preguntas clave utilizadas para validar la existencia de documentos de respaldo. También se incluyen comentarios sobre el estado actual de la evidencia, ubicación de los documentos y tareas necesarias para subsanar deficiencias. Cada capítulo se relaciona con las subcategorías del marco de AGESIC, siguiendo las directrices de la Guía de Implementación del Marco de Ciberseguridad de AGESIC

Columnas:

- **Id_Cap (Identificador de Capítulo):** Código del capítulo dentro del MCS.
- **Capítulo:** Nombre del capítulo al que pertenece el requisito.
- **Id_Req (Identificador de Requisito):** Código del requisito evaluado.
- **Requisito:** Descripción del requisito evaluado.
- **Evidencia para la auditoría de acuerdo con la Guía de Implementación v4.2:** Pregunta específica de la evidencia para la auditoría que se encuentra en la Guía de implementación, utilizada para validar el cumplimiento del requisito.
- **Se Repite en:** Indica si el requisito se repite.
- **Existe?:** Indica si la evidencia documental del requisito existe (SI/NO).
- **Ubicación:** Lugar donde se encuentra la evidencia.
- **Comentario:** Observaciones sobre el estado de la evidencia o su relevancia.

Id. Cap.	Capítulo	Id. Req.	Requisito	Evidencia para la auditoría de acuerdo con la Guía de Implementación	Se repite en	Existe?	Ubicación	Comentarios
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se da a conocimiento público dentro de la organización de la política de Seguridad de la Información y evidencia de su difusión?				
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se realizan reuniones con el personal para corroborar el conocimiento de la política de Seguridad de la Información?				
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone de evidencia de la revisión de la política de Seguridad de la Información por parte de la Dirección (minutas, actas, correos, formularios, otros)?				
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone de registros de los cambios realizados a la política de Seguridad de la Información?				
01 - OR	Organización y Gobernanza	01.02 - OR.1	Designar un Responsable de la Seguridad de la Información.	¿Se dispone de la designación de la función o rol de Responsable de la Seguridad de la Información?				
01 - OR	Organización y Gobernanza	01.02 - OR.1	Designar un Responsable de la Seguridad de la Información.	¿Se ha dado difusión de la designación del rol o función de Responsable de la Seguridad de la Información?				
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone del Acta de Resolución de la creación del CSI?				
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone de la aprobación de las responsabilidades del CSI por la Dirección?				
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone del reglamento o pautas de funcionamiento del CSI?				
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone de actas o evidencia de las reuniones mantenidas por el CSI durante el periodo auditado (actas, orden del día, correos, otros)?				
01 - OR	Organización y Gobernanza	01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de un plan de comunicación ante incidentes de seguridad de la información o crisis?				
01 - OR	Organización y Gobernanza	01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de un plan de gestión de incidentes de seguridad de la información?				
01 - OR	Organización y Gobernanza	01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de evidencia de haber realizado el contacto con autoridades de acuerdo a los planes y procedimientos definidos para los incidentes (o potenciales incidentes) de seguridad de la información que se registraron en el periodo auditado?				
01 - OR	Organización y Gobernanza	01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de evidencias de incidentes o sospechas de seguridad reportados al CSI?				

Ilustración 16: Hoja Evidencia

3.2. Aplicación de la Evaluación y Determinación del Nivel de Madurez

Para determinar el nivel de madurez en ciberseguridad del organismo, se llevó a cabo un proceso estructurado basado en el MCS de AGESIC. Este proceso incluyó las siguientes etapas:

3.2.1. Recolección de información

Se aplicó el cuestionario contenido en la hoja Evidencias, por medio de entrevistas, el cual está alineado con la Guía de Implementación del MCS de AGESIC y se evaluaron aspectos clave de la gestión de seguridad de la información.

Id. Cap.	Capítulo	Id. Req.	Requisito	Evidencia para la auditoría de acuerdo con la Guía de Implementación	Se repite en	Existe?	Ubicación	Comentarios
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone del Acta de Resolución de la Dirección con la aprobación y adopción de la política de Seguridad de la Información?	SI	SI	Acta de Resoluciones	Aprobación de Acta: Resoluciones - Resolución 006/2020
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se da a conocimiento público dentro de la organización de la política de Seguridad de la Información y evidencia de su difusión?	SI	SI	Correos electrónicos a todos	Difusión: correos electrónicos enviados 1/5/2024 a todo el personal PS en intranet
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se realizan reuniones con el personal para corroborar el conocimiento de la política de Seguridad de la Información?	NO	Pendiente		No hay revisiones de conocimiento del personal sobre la PS
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone de evidencia de la revisión de la política de Seguridad de la Información por parte de la Dirección (minutas, actas, correos, formularios, otros)?	SI	SI	Minutas de reunión	Existen minutas de la reunión y la firman todos los miembros del comité SI
01 - OR	Organización y Gobernanza	01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone de registros de los cambios realizados a la política de Seguridad de la Información?	NO	Pendiente		¿Todavía no hubo cambios en la PS?
01 - OR	Organización y Gobernanza	01.02 - OR.1	Designar un Responsable de la Seguridad de la Información.	¿Se dispone de la designación de la función o rol de Responsable de la Seguridad de la Información?	NO	Pendiente		¿Todavía no existe un RS?
01 - OR	Organización y Gobernanza	01.02 - OR.1	Designar un Responsable de la Seguridad de la Información.	¿Se ha dado difusión de la designación del rol o función de Responsable de la Seguridad de la Información?	NO	Pendiente		¿Todavía no existe un RS?
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone del Acta de Resolución de la creación del CSI?	SI	SI	Acta de Resoluciones	Creación de Comité: Resoluciones - Resolución 006/2020
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone de la aprobación de las responsabilidades del CSI por la Dirección?	SI	SI	Acta de Resoluciones	Creación de Comité: Resoluciones - Resolución 006/2020
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone del reglamento o pautas de funcionamiento del CSI?	NO	Pendiente		¿Hay que averiguar el existe o no?
01 - OR	Organización y Gobernanza	01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone de actas o evidencia de las reuniones mantenidas por el CSI durante el periodo auditado (actas, orden del día, correos, otros)?	SI	SI	Minutas de reunión	Existen minutas de la reunión y la firman todos los miembros del comité SI
01 - OR	Organización y Gobernanza	01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de un plan de comunicación ante incidentes de seguridad de la información o crisis?	NO	Pendiente		No existe plan de comunicación de incidentes
01 - OR	Organización y Gobernanza	01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de un plan de gestión de incidentes de seguridad de la información?	NO	Pendiente		No existe plan de gestión de incidentes
01 - OR	Organización y Gobernanza	01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de evidencia de haber realizado el contacto con autoridades de acuerdo a los planes y procedimientos definidos para los incidentes (o potenciales incidentes) de seguridad de la información que se registraron en el periodo auditado?	NO	Pendiente		No existe plan de gestión de incidentes

Ilustración 17: Hoja Evidencias completada

A continuación, se presenta el listado de preguntas del cuestionario junto con las respuestas proporcionadas por los entrevistados. Aunque disponemos de información sobre la ubicación y los comentarios que respaldan dónde y cómo obtener esa evidencia, no la incluimos en este listado por razones de confidencialidad del organismo.

Id_Req	Requisito	Evidencia para la auditoría de acuerdo con la Guía de implementación v4.2	Se repite en:	Existe?
01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone del Acta de Resolución de la Dirección con la aprobación y adopción de la política de Seguridad de la Información?		SI
01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se da a conocimiento público dentro del organismo la política de Seguridad de la Información y evidencia de su difusión?		SI
01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se realizan revisiones con el personal para corroborar el conocimiento de la política de Seguridad de la Información?		NO
01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone de evidencia de la revisión de la política de Seguridad de la Información por parte de la Dirección (minutas, actas, correos, formularios, otros)?		SI
01.01 - PS.1	Adoptar una política de Seguridad de la Información.	¿Se dispone de registros de los cambios realizados a la política de Seguridad de la Información?		NO
01.02 - OR.1	Designar un responsable de la Seguridad de la Información.	¿Se dispone de la designación de la función o rol de responsable de la Seguridad de la Información?		NO
01.02 - OR.1	Designar un responsable de la Seguridad de la Información.	¿Se ha dado difusión de la designación del rol o función de responsable de la Seguridad de la Información?		NO
01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone del Acta de Resolución de la creación del CSI?		SI
01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone de la aprobación de las responsabilidades del CSI por la Dirección?		SI
01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone del reglamento o pautas de funcionamiento del CSI?		NO
01.03 - OR.2	Conformar un Comité de Seguridad de la Información.	¿Se dispone de actas o evidencia de las reuniones mantenidas por el CSI, durante el período auditado (actas, orden del día, correos, otros)?		SI
01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de un plan de comunicación ante incidentes de seguridad de la información o crisis?		NO
01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de un plan de gestión de incidentes de seguridad de la información?		NO
01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de evidencia de haber realizado el contacto con autoridades de acuerdo a los planes y procedimientos definidos para los incidentes (o potenciales incidentes) de seguridad de la información que se registraron en el período auditado?		NO

01.04 - OR.3	Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.	¿Se dispone de evidencias de incidentes o sospechas de seguridad reportados al CERTuy?		SI
01.05 - OR.4	Abordar la seguridad de la información en la gestión de los proyectos.	¿Se dispone de una lista de proyectos llevados a cabo o en proceso durante el período a auditar?		SI
01.05 - OR.4	Abordar la seguridad de la información en la gestión de los proyectos.	¿Se dispone de documentación de los proyectos (por ejemplo, acta de constitución del proyecto, lista inicial de requerimientos, etc.) que incluya requisitos de seguridad de la información requeridos?		NO
01.05 - OR.4	Abordar la seguridad de la información en la gestión de los proyectos.	¿Se dispone de evidencia de realización y seguimiento de la evaluación de riesgos de los proyectos que incluyan riesgos relativos a la seguridad de la información?		NO
01.05 - OR.4	Abordar la seguridad de la información en la gestión de los proyectos.	¿Se dispone de informes de avance de los proyectos donde se incluye puntos que tratan sobre la evaluación de los riesgos de seguridad de la información?		NO
01.06 - OR.5	Pautar el uso de dispositivos móviles.	¿Se dispone de una política de dispositivos móviles?		NO
01.06 - OR.5	Pautar el uso de dispositivos móviles.	¿Se dispone de un procedimiento, manuales y/o instructivos para asegurar el adecuado uso de los dispositivos móviles?		SI
01.06 - OR.5	Pautar el uso de dispositivos móviles.	¿Se dispone de un inventario de dispositivos móviles propiedad de la organización?		SI
01.06 - OR.5	Pautar el uso de dispositivos móviles.	¿Se dispone de un inventario de dispositivos móviles personales pero que se conectan a algún servicio de la organización?		NO
01.07 - OR.6	Establecer controles para proteger la información a la que se accede de forma remota.	¿Se dispone de una política de acceso remoto?		NO
01.07 - OR.6	Establecer controles para proteger la información a la que se accede de forma remota.	¿Se dispone de mecanismos de autenticación para la conexión remota documentados en la política?		NO
01.07 - OR.6	Establecer controles para proteger la información a la que se accede de forma remota.	¿Se dispone de un procedimiento de altas, bajas y modificaciones de acceso remoto?		SI
01.07 - OR.6	Establecer controles para proteger la información a la que se accede de forma remota.	¿Se dispone de un procedimiento de revisión de usuarios con acceso remoto?		NO
01.07 - OR.6	Establecer controles para proteger la información a la que se accede de forma remota.	¿Se dispone de un listado de servidores críticos que permiten acceso remoto?		SI
01.07 - OR.6	Establecer controles para proteger la información a la que se accede de forma remota.	¿Se dispone de un listado con la identificación de los usuarios habilitados para acceder remotamente a sistemas críticos?		SI
02.01 - GR.1	Adoptar una metodología de Evaluación de Riesgos alineadas a las necesidades del SGSI.	¿Se dispone de una metodología de gestión de riesgos de seguridad de la información (identificación, evaluación, tratamiento, seguimiento y comunicación a los interesados)?		NO
02.01 - GR.1	Adoptar una metodología de Evaluación de Riesgos alineadas a las necesidades del SGSI.	¿Se dispone de una política de Gestión de Riesgos?		NO
02.01 - GR.1	Adoptar una metodología de Evaluación de Riesgos alineadas a las necesidades del SGSI.	¿Se dispone de una política de Gestión de Riesgos de Seguridad de la Información?		NO
02.01 - GR.1	Adoptar una metodología de Evaluación de Riesgos alineadas a las necesidades del SGSI.	¿Se dispone de evidencia de que La política de gestión de riesgos es conocida por el personal?		NO
02.01 - GR.1	Adoptar una metodología de Evaluación de Riesgos alineadas a las necesidades del SGSI.	¿Se dispone de un Registro de los cambios a la política de Gestión de Riesgos?		NO
02.02 - GR.2	Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.	¿Se dispone de un inventario de riesgos identificados y se le hace seguimiento?		NO

02.02 - GR.2	Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.	¿Se realizan evaluaciones y/o análisis de riesgos en la organización?		NO
02.02 - GR.2	Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.	¿Se realizan evaluaciones de riesgo de los proveedores?		NO
02.03 - GR.3	Tratamiento o un plan de acción correctivo sobre los riesgos encontrados y, de acuerdo a su resultado, implementar las acciones correctivas y preventivas correspondientes.	¿Se cuenta con un plan de tratamiento de riesgos incluyendo al menos, orden de prioridad y plazos de implementación de los controles identificados para tratar los riesgos?		NO
02.03 - GR.3	Tratamiento o un plan de acción correctivo sobre los riesgos encontrados y, de acuerdo a su resultado, implementar las acciones correctivas y preventivas correspondientes.	¿Se realizan certificaciones funcionales y técnicas de las pruebas realizadas en los ambientes de test o calidad de que las vulnerabilidades han sido mitigadas?		NO
02.03 - GR.3	Tratamiento o un plan de acción correctivo sobre los riesgos encontrados y, de acuerdo a su resultado, implementar las acciones correctivas y preventivas correspondientes.	¿Se cuenta con la aprobación de los controles de cambio para las correcciones en los ambientes de producción?		NO
02.03 - GR.3	Tratamiento o un plan de acción correctivo sobre los riesgos encontrados y, de acuerdo a su resultado, implementar las acciones correctivas y preventivas correspondientes.	¿Se genera un Informe de re evaluación de mitigación o control de las vulnerabilidades?		NO
03.01 - PL.1	Establecer objetivos anuales con relación a la seguridad de la información.	¿Se dispone de un listado con los objetivos anuales de la organización relacionados con seguridad de la información?		NO
03.01 - PL.1	Establecer objetivos anuales con relación a la seguridad de la información.	¿Se dispone de un plan de acción?		NO
03.01 - PL.1	Establecer objetivos anuales con relación a la seguridad de la información.	¿Se definen proyectos de seguridad de la información?		NO
03.01 - PL.1	Establecer objetivos anuales con relación a la seguridad de la información.	¿Se dispone de una estrategia de ciberseguridad y seguridad de la información?		NO
03.01 - PL.1	Establecer objetivos anuales con relación a la seguridad de la información.	¿Se dispone de un conjunto de indicadores de seguimiento?		NO
03.02 - PL.2	Revisión periódica y mejora continua del SGSI.	¿Se dispone de un plan de acción para la revisión de controles, procesos, estrategias y políticas?		NO
03.02 - PL.2	Revisión periódica y mejora continua del SGSI.	¿Se realiza un análisis de riesgos asociados a la mejora continua?		NO
03.02 - PL.2	Revisión periódica y mejora continua del SGSI.	¿Se dispone de un conjunto de indicadores de seguimiento y de mejora?		NO
04.01 - GH.1	Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información.	¿Se dispone de un listado de personal contratado en el período auditado?		SI
04.01 - GH.1	Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información.	¿Se dispone de contratos firmados del personal que pertenezcan al período auditado?		SI
04.01 - GH.1	Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información.	¿Se dispone de un listado de personal desvinculado en el período auditado?		SI
04.01 - GH.1	Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información.	¿Se dispone de evidencia de cumplimiento con las actividades definidas en los procedimientos de desvinculación de personal durante el período auditado, por ejemplo, planillas, formularios de solicitud de revocación de permisos, notas, cartas de desvinculación, correos donde se demuestre el cumplimiento con los procedimientos definidos, etc.?		NO
04.01 - GH.1	Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información.	¿Se dispone de acuerdos de no divulgación firmados del período auditado?		SI
04.02 - GH.2	Concientizar y formar en materia de seguridad de la información a todo el personal.	¿Se dispone de documentación que evidencie la ejecución del programa de concientización: realización de charlas,		NO

		capacitaciones, divulgación, actividades de concientización, calificaciones obtenidas por los participantes, entre otros, que se hayan realizado en el período auditado?		
04.02 - GH.2	Concientizar y formar en materia de seguridad de la información a todo el personal.	¿Se dispone de un programa anual de concientización en seguridad de la información?		NO
04.02 - GH.2	Concientizar y formar en materia de seguridad de la información a todo el personal.	¿Se dispone de material de sensibilización y capacitación?		NO
04.02 - GH.2	Concientizar y formar en materia de seguridad de la información a todo el personal.	¿Se realizan campañas de sensibilización y capacitación mediante el uso de correos electrónicos, carteles, artículos, etc.?		SI
04.02 - GH.2	Concientizar y formar en materia de seguridad de la información a todo el personal.	¿Se dispone de registros de capacitaciones ante la eventualidad de entrevistas aleatorias para evaluar el conocimiento sobre la política de seguridad de la información?		NO
05.01 - GA.1	Identificar formalmente los activos de la organización junto con la definición de su responsable.	¿Se dispone de un inventario de los activos de la organización?	05.01 - GA.1 05.02 - GA.2	SI
05.01 - GA.1	Identificar formalmente los activos de la organización junto con la definición de su responsable.	¿Se dispone de la información del responsable de cada uno de los activos definidos en el inventario de activos?		SI
05.02 - GA.2	Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.	¿Se dispone de un procedimiento de administración de activos?		SI
05.02 - GA.2	Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.	¿Se dispone de un inventario de los activos de la organización?	05.01 - GA.1 05.02 - GA.2	SI
05.02 - GA.2	Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.	¿Se dispone de la información del dueño de cada uno de los activos definidos en el inventario de activos?		SI
05.02 - GA.2	Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.	¿Se dispone de la clasificación de cada uno de los activos definidos en el inventario de activos?		SI
05.02 - GA.2	Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.	¿Se dispone de un procedimiento para el etiquetado de activos?		SI
05.03 - GA.3	Pautar el uso aceptable de los activos.	¿Se dispone de una política de uso aceptable de activos (genérica o específica para algún tipo de activo)?		SI
05.03 - GA.3	Pautar el uso aceptable de los activos.	¿Se dispone de evidencia de difusión de la política de uso aceptable de activos?		SI
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de pautas para el manejo de medios de almacenamiento?		NO
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de un listado de medios de almacenamiento externos utilizados por la organización?		NO
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de un inventario de los activos de la organización con identificación de los medios de almacenamiento?		NO
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de un procedimiento para la gestión de los medios de almacenamiento externos?		NO
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de evidencia de solicitudes, entrega o devolución de medios para el período auditado?		NO
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de evidencia de autorizaciones para transportar medios fuera de la organización?		NO
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de evidencia de medios de almacenamiento debidamente etiquetados?		NO
05.04 - GA.4	Gestionar los medios de almacenamiento externos.	¿Se dispone de evidencia del mecanismo de encriptación de los medios de almacenamiento?		NO

05.05 - GA.5	Establecer los mecanismos para destruir la información y medios de almacenamiento.	¿Se dispone de una política de destrucción de medios de almacenamiento?		NO
05.05 - GA.5	Establecer los mecanismos para destruir la información y medios de almacenamiento.	¿Se dispone de un procedimiento para la destrucción segura de medios de almacenamiento?		SI
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de una política de control de acceso lógico?	06.01 - CA.1 06.02 - CA.2	NO
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de una política de gestión de usuarios y contraseñas?		SI
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de una descripción de los mecanismos de autenticación utilizados?		SI
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de un esquema de seguridad de las aplicaciones críticas?		SI
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de un listado de ingresos y egresos de funcionarios en el período auditado con detalle de su cargo y accesos otorgados o dados de baja (RRHH)?		SI
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de formularios de solicitud de Alta/Baja de cuentas de usuario para acceso a equipos de red y comunicaciones, sistemas operativos, aplicativos, otros, para una muestra de funcionarios tomada del listado de ingresos y egresos obtenido de RRHH, para el período auditado?		NO
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de formularios de solicitud de modificaciones de privilegios de cuentas de usuario para acceso a equipos de comunicaciones, sistemas operativos, aplicativos y otros, dentro del período auditado?		NO
06.01 - CA.1	Gestionar el acceso lógico.	¿Se dispone de listados de altas y bajas de funcionarios a los equipos de comunicaciones, sistemas operativos y aplicativos (sistemas), dentro del período auditado?		NO
06.02 - CA.2	Revisar los privilegios de acceso lógico.	¿Se dispone de una política de control de acceso lógico?	06.01 - CA.1 06.02 - CA.2	NO
06.02 - CA.2	Revisar los privilegios de acceso lógico.	¿Se dispone de un procedimiento de revisión de privilegio de acceso?		NO
06.02 - CA.2	Revisar los privilegios de acceso lógico.	¿Se dispone de un listado de usuarios con acceso privilegiado?		NO
06.02 - CA.2	Revisar los privilegios de acceso lógico.	¿Se dispone de evidencia de la revisión de usuarios y usuarios privilegiados en el período auditado (en el caso de los usuarios privilegiados, se busca contar con evidencia de que la organización determina lo adecuado de su asignación)?		NO
06.03 - CA.3	Establecer controles criptográficos.	¿Se dispone de una política y procedimientos para el uso de criptografía y control criptográfico?		NO
06.03 - CA.3	Establecer controles criptográficos.	¿Se dispone de un registro de revisión y actualización de estos protocolos?		NO
06.03 - CA.3	Establecer controles criptográficos.	¿Se dispone de un listado de sistemas desarrollados por la organización y aquellos que usan firma electrónica avanzada?		SI
06.03 - CA.3	Establecer controles criptográficos.	¿Se dispone de un listado de sistemas que soportan uso de dispositivos criptográficos?		SI
06.03 - CA.3	Establecer controles criptográficos.	¿Se dispone de mecanismos de validación de firmas y de certificados electrónicos?		SI

06.03 - CA.3	Establecer controles criptográficos.	¿Se dispone de soluciones utilizadas para la firma de transacciones?		SI
06.04 - CA.4	Establecer los controles para el uso de firma electrónica.	¿Se dispone de documentación de los detalle técnico de la solución (aplicativo, módulo, etc.) que implementa firma electrónica avanzada?		SI
07.01 - SF.1	Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas.	¿Se dispone de una política de control de acceso físico?		NO
07.01 - SF.1	Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas.	¿Se dispone de un procedimientos de control de acceso físico incluyendo la gestión de autorizaciones?		NO
07.01 - SF.1	Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas.	¿Se dispone de un listado de áreas seguras y personas autorizadas a acceder?		NO
07.01 - SF.1	Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas.	¿Se dispone de un registros de accesos físicos en áreas seguras para el período auditado?		NO
07.02 - SF.2	Implementar controles ambientales en los centros de datos y áreas relacionadas.	¿Se dispone de la habilitación de bomberos?		NO
07.02 - SF.2	Implementar controles ambientales en los centros de datos y áreas relacionadas.	¿Se dispone de contratos con proveedores (alarmas, aire acondicionado, etc.)?		SI
07.02 - SF.2	Implementar controles ambientales en los centros de datos y áreas relacionadas.	¿Se dispone de sistemas de protección ambiental (alarma, extintores, sistemas de extinción, aire acondicionado, etc.)?		SI
07.02 - SF.2	Implementar controles ambientales en los centros de datos y áreas relacionadas.	¿Se dispone de planos en los que se identifica la ubicación de la sala de cómputo y la sala de energía?		SI
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de un conjunto de herramientas utilizadas para el monitoreo?		NO
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de un procedimiento de monitoreo?		NO
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de un plan de mantenimiento?		NO
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de reportes de fallas y alertas dentro del período auditado?		NO
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de evidencia de la revisión de fallas y alertas dentro del período auditado?		NO
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de documentación de registros del mantenimiento histórico de los valores monitoreados dentro del período auditado?		NO
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de una bitácora de acceso de personal interno o externo que realice las actividades o labores de mantenimiento al equipamiento en general?		NO
07.03 - SF.3	Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.	¿Se dispone de documentación de los controles de cambio para el mantenimiento de los componentes críticos?		NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de un Inventario de activos?		SI
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de pautas para la gestión de vulnerabilidades y parches?		NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de un procedimiento para la gestión de vulnerabilidades y parches?		NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de un registro de vulnerabilidades y parches, y detalle de su tratamiento internamente en la organización en el período auditado?		NO

08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de un procedimiento de gestión de cambios?	08.01 - SO.1 10.01 - AD.1	NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de un procedimiento de gestión de cambios de emergencia?		NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de un procedimiento de gestión de incidentes?		NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de una lista de las actualizaciones críticas para cada sistema operativo a ser aplicada?		NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de una lista de las actualizaciones críticas aplicadas para cada sistema operativo?		NO
08.01 - SO.1	Gestionar las vulnerabilidades técnicas.	¿Se dispone de evidencia del análisis realizado por la organización acerca de los cambios previo a instalar un parche?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de una política de gestión de cambios?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de un procedimiento para la gestión de cambios?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de un procedimiento para cambios de emergencia?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de un listado de los cambios realizados en el período auditado?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de evidencia para una muestra de cambios dentro del período auditado, para verificar que se ha cumplido con los procedimientos definidos de gestión de cambios (análisis de riesgos, aprobación, etc.)?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de un listado los de cambios de emergencia realizados en el período auditado?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de evidencia de la realización de las actividades descriptas en los procedimientos: análisis de riesgos, autorización, aprobación, registro, etc.		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de pautas de desarrollo seguro de aplicaciones?		NO
08.02 - SO.2	Gestionar formalmente los cambios.	¿Se dispone de una metodología de desarrollo incluyendo aspectos de seguridad?		NO
08.03 - SO.3	Gestionar la capacidad de los servicios y recursos que se encuentran operativos.	¿Se dispone de un plan de capacidad?		NO
08.03 - SO.3	Gestionar la capacidad de los servicios y recursos que se encuentran operativos.	¿Se dispone de registros que demuestren que se han realizado mediciones de los recursos críticos (hardware, software, etc.) en el período auditado?		NO
08.03 - SO.3	Gestionar la capacidad de los servicios y recursos que se encuentran operativos.	¿Se dispone de actividades realizadas para proporcionar o mejorar la capacidad en el período auditado, de acuerdo al plan de capacidad?		NO
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de una política de separación de entornos?		NO
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de un procedimiento para el pasaje a producción?		NO
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de un procedimiento o metodología de pruebas?		NO
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de documentación que detalle los diferentes ambientes existentes?		NO
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de un listado de sistemas en desarrollo y producción y ambientes definidos?		SI
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de una lista de cambios realizados en el período auditado?		NO
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de un registro de solicitudes de cambio, análisis de riesgos,		NO

		aprobaciones, rechazos de cambios y de los pasajes entre ambientes?		
08.04 - SO.4	Definir entornos separados para desarrollo, pruebas y producción.	¿Se dispone de un ambiente de desarrollo, producción y pruebas para los sistemas seleccionados?		SI
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una política de Seguridad de la Información?		SI
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una política de protección contra software malicioso y otros archivos provenientes de redes externas u otros medios y medidas preventivas que deberán tomarse?		NO
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de un procedimiento para el control y detección de software no autorizado o malicioso?		NO
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una lista de aplicaciones permitidas?		SI
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una lista de aplicaciones no permitidas?		NO
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de sitios web no autorizados o reglas que los filtran?		SI
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una lista de equipos que cuentan con el antivirus actualizado?		NO
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una lista de equipos que cuentan con las últimas actualizaciones de seguridad instaladas?		NO
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una lista de equipos que cuentan únicamente con el software permitido instalado?		SI
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una política y procedimiento de gestión de incidentes?		NO
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de una lista de incidentes y su gestión?		NO
08.05 - SO.5	Controlar software malicioso.	¿Se dispone de filtros aplicados en correo y Gateway?		SI
08.06 - SO.6	Respalidar la información y realizar pruebas de restauración periódicas.	¿Se dispone de una política de respaldos?		NO
08.06 - SO.6	Respalidar la información y realizar pruebas de restauración periódicas.	¿Se dispone de un plan de respaldos?		SI
08.06 - SO.6	Respalidar la información y realizar pruebas de restauración periódicas.	¿Se dispone de un registro (muestra) de los respaldos realizados para el período auditado?		SI
08.06 - SO.6	Respalidar la información y realizar pruebas de restauración periódicas.	¿Se dispone de una bitácora de la herramienta utilizada para los respaldos con detalle de respaldos realizados?		SI
08.06 - SO.6	Respalidar la información y realizar pruebas de restauración periódicas.	¿Se dispone de un listado de pruebas de restauración (muestra) realizadas en el período auditado?		NO
08.06 - SO.6	Respalidar la información y realizar pruebas de restauración periódicas.	¿Se dispone de una prueba de restauración de una muestra de archivos o carpetas seleccionadas?		NO
08.06 - SO.6	Respalidar la información y realizar pruebas de restauración periódicas.	¿Se dispone de un registro donde se documente las actividades de supervisión de los respaldos e inconvenientes o fallas encontradas?		NO
08.07 - SO.7	Registrar y monitorear los eventos de los sistemas.	¿Se dispone de una política de auditoría y registro de eventos?		NO
08.07 - SO.7	Registrar y monitorear los eventos de los sistemas.	¿Se dispone de la configuración del registro de eventos?		NO
08.07 - SO.7	Registrar y monitorear los eventos de los sistemas.	¿Se dispone de herramientas utilizadas para el monitoreo de los eventos, excepciones y fallas utilizadas y su configuración?		NO
08.07 - SO.7	Registrar y monitorear los eventos de los sistemas.	¿Se dispone de un procedimiento de revisión periódica de los registros generados?		NO
08.07 - SO.7	Registrar y monitorear los eventos de los sistemas.	¿Se dispone de un procedimiento de detección y monitoreo?		NO
08.07 - SO.7	Registrar y monitorear los eventos de los sistemas.	¿Se dispone de un listado de las revisiones periódicas realizadas durante el período auditado?		NO

08.07 - SO.7	Registrar y monitorear los eventos de los sistemas.	¿Se dispone de un listado de las revisiones realizadas sobre las actividades de los administradores de sistemas y redes en el período auditado?		NO
08.08 - SO.8	Gestionar la instalación de software.	¿Se dispone de un procedimiento de instalación de software?		SI
08.08 - SO.8	Gestionar la instalación de software.	¿Se dispone de un procedimiento para la administración de las licencias de software?		SI
08.08 - SO.8	Gestionar la instalación de software.	¿Se dispone de un listado con el resultado de las auditorías o revisiones internas sobre software instalado?		NO
08.08 - SO.8	Gestionar la instalación de software.	¿Se dispone de un listado de software instalado en los equipos dentro del período auditado?		NO
08.08 - SO.8	Gestionar la instalación de software.	¿Se dispone de un listado de software base permitido?		NO
08.08 - SO.8	Gestionar la instalación de software.	¿Se dispone de un listado de software especial y usuarios autorizados a su instalación?		NO
08.08 - SO.8	Gestionar la instalación de software.	¿Se dispone de los requerimientos a nivel legal y normativo para la instalación y uso de las licencias de software?		NO
09.01 - SC.1	Los portales Web institucionales de los organismos de la Administración Central y sus dependencias deben identificarse con la extensión “gub.uy” y “mil.uy”, según corresponda.	¿Se dispone de accesos a los dominios y subdominios con su identificación?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.01 - SC.1	Los portales Web institucionales de los organismos de la Administración Central y sus dependencias deben identificarse con la extensión “gub.uy” y “mil.uy”, según corresponda.	¿Se dispone de un listado de los portales Web que tiene el organismo con dominios y subdominios?		SI
09.01 - SC.1	Los portales Web institucionales de los organismos de la Administración Central y sus dependencias deben identificarse con la extensión “gub.uy” y “mil.uy”, según corresponda.	¿Se dispone de acceso a los servidores DNS?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.02 - SC.2	Los portales Web institucionales de Unidades Ejecutoras, aplicaciones, portales y sitios Web correspondientes a proyectos y programas, sitios promocionales y temáticos, incluyendo zonas restringidas de acceso mediante usuario y contraseña disponibles.	¿Se dispone de accesos a los dominios y subdominios con su identificación?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.02 - SC.2	Los portales Web institucionales de Unidades Ejecutoras, aplicaciones, portales y sitios Web correspondientes a proyectos y programas, sitios promocionales y temáticos, incluyendo zonas restringidas de acceso mediante usuario y contraseña disponibles.	¿Se dispone de listados de los portales Web que tiene el organismo con dominios y subdominios?		SI
09.02 - SC.2	Los portales Web institucionales de Unidades Ejecutoras, aplicaciones, portales y sitios Web correspondientes a proyectos y programas, sitios promocionales y temáticos, incluyendo zonas restringidas de acceso mediante usuario y contraseña disponibles.	¿Se dispone de acceso a los servidores DNS?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.02 - SC.2	Los portales Web institucionales de Unidades Ejecutoras, aplicaciones, portales y sitios Web correspondientes a proyectos y programas, sitios promocionales y temáticos, incluyendo zonas restringidas de acceso mediante usuario y contraseña disponibles.	¿Se dispone de portales web?	09.02 - SC.2 09.03 - SC.3	SI

	restringidas de acceso mediante usuario y contraseña disponibles.		09.04 - SC.4	
09.03 - SC.3	El portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos WEB que le reporten.	¿Se dispone de accesos a los dominios y subdominios con su identificación?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.03 - SC.3	El portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos WEB que le reporten.	¿Se dispone de listados de los portales Web que tiene el organismo con dominios y subdominios?	09.03 - SC.3 09.04 - SC.4	SI
09.03 - SC.3	El portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos WEB que le reporten.	¿Se dispone de acceso a los servidores DNS?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.03 - SC.3	El portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos WEB que le reporten.	¿Se dispone de portales web?	09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.03 - SC.3	El portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos WEB que le reporten.	¿Se dispone de listados de los subdominios en la página institucional del organismo jerarca?		SI
09.04 - SC.4	Los nombres de dominio del organismo o dependencias serán sus iniciales, su acrónimo, o el nombre con el cual se los conoce públicamente. Deberá justificarse que la denominación elegida sea la más representativa.	¿Se dispone de accesos a los dominios y subdominios con su identificación?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.04 - SC.4	Los nombres de dominio del organismo o dependencias serán sus iniciales, su acrónimo, o el nombre con el cual se los conoce públicamente. Deberá justificarse que la denominación elegida sea la más representativa.	¿Se dispone de listados de los portales Web que tiene el organismo con dominios y subdominios?	09.03 - SC.3 09.04 - SC.4	SI
09.04 - SC.4	Los nombres de dominio del organismo o dependencias serán sus iniciales, su acrónimo, o el nombre con el cual se los conoce públicamente. Deberá justificarse que la denominación elegida sea la más representativa.	¿Se dispone de acceso a los servidores DNS?	09.01 - SC.1 09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.04 - SC.4	Los nombres de dominio del organismo o dependencias serán sus iniciales, su acrónimo, o el nombre con el cual se los conoce públicamente. Deberá justificarse que la denominación elegida sea la más representativa.	¿Se dispone de portales web?	09.02 - SC.2 09.03 - SC.3 09.04 - SC.4	SI
09.05 - SC.5	La información de contacto de los responsables de los dominios y subdominios deberá ser comunicada a AGESIC y actualizada en períodos de seis meses.	¿Se dispone de un proceso de registro y mantenimiento de dominios y subdominios?		SI
09.05 - SC.5	La información de contacto de los responsables de los dominios y subdominios deberá ser comunicada a AGESIC y actualizada en períodos de seis meses.	¿Se dispone de los datos del responsable de los dominios y/o subdominios actualizada en la documentación relativa a los dominios y subdominios?		SI
09.05 - SC.5	La información de contacto de los responsables de los dominios y subdominios deberá ser comunicada a AGESIC y actualizada en períodos de seis meses.	¿Se dispone de un listado de las revisiones y actualizaciones de la información de contacto en el plazo establecido en el procedimiento de		NO

		mantenimiento de los dominios y subdominios?		
09.06 - SC.6	Establecer acuerdos de no divulgación.	¿Se dispone de una plantilla de Acuerdos de no divulgación (para personal y/o proveedores)?		SI
09.06 - SC.6	Establecer acuerdos de no divulgación.	¿Se dispone de copias de acuerdos firmados con el personal (selección de muestra aleatoria para el período auditado)?		SI
09.06 - SC.6	Establecer acuerdos de no divulgación.	¿Se dispone de copias de acuerdos firmados con proveedores (selección de muestra aleatoria para el período auditado)?		SI
09.06 - SC.6	Establecer acuerdos de no divulgación.	¿Se dispone de procedimiento para la revisión de los acuerdos de no divulgación?		NO
09.06 - SC.6	Establecer acuerdos de no divulgación.	¿Se dispone de evidencia de la revisión periódica del contenido de los acuerdos?		NO
09.07 - SC.7	Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su implementación sobre tecnologías que no garanticen dicho requerimiento.	¿Se dispone de registros MX y whois de las IP de los registros MX?		SI
09.07 - SC.7	Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su implementación sobre tecnologías que no garanticen dicho requerimiento.	¿Se dispone de Infraestructuras Cloud y/o proveedores que brindan este servicio al organismo?		SI
09.07 - SC.7	Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su implementación sobre tecnologías que no garanticen dicho requerimiento.	¿Se dispone de rangos de IP con la que cuentan las interfaces de red que están conectadas a Internet?		SI
09.07 - SC.7	Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su implementación sobre tecnologías que no garanticen dicho requerimiento.	¿Se dispone de servidores de correo que procesan correos con dominios gub.uy?		SI
09.07 - SC.7	Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su implementación sobre tecnologías que no garanticen dicho requerimiento.	¿Se dispone de la ubicación física de los correos y respaldos?		SI
09.07 - SC.7	Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su implementación sobre tecnologías que no garanticen dicho requerimiento.	¿Se dispone de acuerdos de niveles de servicio con los proveedores en caso de infraestructura que no esté administrada por el organismo (por ejemplo, Cloud privada)?		N/A
09.08 - SC.8	Garantizar que los correos electrónicos en tránsito entre dos MTAs, o entre un MUA y un MTA, no comprometa la confidencialidad de la información cuando esto sea posible.	¿Se dispone de evidencia de aplicación de los protocolos que usen algoritmos de cifrado de datos?		SI
09.08 - SC.8	Garantizar que los correos electrónicos en tránsito entre dos MTAs, o entre un MUA y un MTA, no comprometa la confidencialidad de la información cuando esto sea posible.	¿Se dispone de respaldo de la configuración del servidor?		SI
09.08 - SC.8	Garantizar que los correos electrónicos en tránsito entre dos MTAs, o entre un MUA y un MTA, no comprometa la confidencialidad de la información cuando esto sea posible.	¿Se dispone de pruebas del cliente de correo utilizado?		SI
09.09 - SC.9	La implementación de canales de comunicación cifrados entre MTA de dominios gubernamentales es obligatoria y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales deberán interrumpir el intento de entrega o recepción.	¿Se dispone de un proceso o guía para la configuración de los servidores de correo?		N/A
09.09 - SC.9	La implementación de canales de comunicación cifrados entre MTA de dominios gubernamentales es obligatoria y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales deberán interrumpir el intento de entrega o recepción.	¿Se dispone de la configuración de los servidores de correo, configuraciones de reglas de distribución de correos, etc.?		N/A

09.09 - SC.9	La implementación de canales de comunicación cifrados entre MTA de dominios gubernamentales es obligatoria y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales deberán interrumpir el intento de entrega o recepción.	¿Se dispone de protocolos que se utilizan para el intercambio de correos?		SI
09.10 - SC.10	La implementación de canales de comunicación cifrados con protocolos seguros entre MTA de dominios gubernamentales y un MTA de terceros deberá ser el método preferido de comunicación. Cuando el establecimiento de estos canales cifrados no sea posible.	¿Se dispone de la configuración que indique que MTA se encuentra establecido como método preferido?		N/A
09.11 - SC.11	La implementación de canales de comunicación cifrados entre MUA y MTA de dominios gubernamentales es mandatorio, y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales no deberán aceptar la descarga o entrega de correos por parte de MUA si este canal cifrado no se puede negociar. Los MTA no deberán aceptar la descarga o consulta de correos electrónicos sobre canales en texto claro.	¿Se dispone de la configuración que indique que MTA se encuentra establecido como método preferido?		N/A
09.12 - SC.12	Los servicios de Webmail deben implementarse sobre el protocolo HTTPS utilizando un certificado de seguridad válido. Cuando la información a transmitir vía email represente un riesgo alto para la organización, se recomienda implementar un modelo de cifrado a nivel del mensaje.	¿Se dispone de una lista de los servicios de Webmail que utiliza la organización, con información sobre dónde se encuentran implementados y sobre qué plataformas (para verificar que no se puede ingresar por http) así como los protocolos implementados (por ejemplo, HTTPS)?		SI
09.12 - SC.12	Los servicios de Webmail deben implementarse sobre el protocolo HTTPS utilizando un certificado de seguridad válido. Cuando la información a transmitir vía email represente un riesgo alto para la organización, se recomienda implementar un modelo de cifrado a nivel del mensaje.	¿Se dispone de certificados de seguridad válidos (que no sean auto firmados)?		SI
09.12 - SC.12	Los servicios de Webmail deben implementarse sobre el protocolo HTTPS utilizando un certificado de seguridad válido. Cuando la información a transmitir vía email represente un riesgo alto para la organización, se recomienda implementar un modelo de cifrado a nivel del mensaje.	¿Se dispone de evidencia de que no se puedan chequear las cuentas institucionales desde otros sistemas Webmail (por ejemplo, verificación con el administrador del correo, del log del servidor en busca de entradas desde servicios externos)?		N/A
09.12 - SC.12	Los servicios de Webmail deben implementarse sobre el protocolo HTTPS utilizando un certificado de seguridad válido. Cuando la información a transmitir vía email represente un riesgo alto para la organización, se recomienda implementar un modelo de cifrado a nivel del mensaje.	¿Se dispone de una circular o nota donde se indica que está prohibido chequear las cuentas de correo institucionales desde otros servicios de correo?		
09.12 - SC.12	Los servicios de Webmail deben implementarse sobre el protocolo HTTPS utilizando un certificado de seguridad válido. Cuando la información a transmitir vía email represente un riesgo alto para la organización, se recomienda implementar un modelo de cifrado a nivel del mensaje.	¿Se dispone de un chequeo de existencia de reenvío de correos institucionales a otras casillas de correo no pertenecientes al organismo?		
09.13 - SC.13	Debe existir segregación a nivel de servicios de información.	¿Se dispone de un procedimiento para la segregación de las redes?		SI
09.13 - SC.13	Debe existir segregación a nivel de servicios de información.	¿Se dispone de un diagrama de red detallado indicando la segregación definida en caso de que exista?		SI
09.13 - SC.13	Debe existir segregación a nivel de servicios de información.	¿Se dispone de un organigrama de la organización donde se pueda identificar la ubicación del rol o función de seguridad de la información y determinar la segregación de funciones/tareas?		NO

09.13 - SC.13	Debe existir segregación a nivel de servicios de información.	¿Se dispone de un rol o función de administrador de seguridad con descripción de tareas que realiza?		NO
09.13 - SC.13	Debe existir segregación a nivel de servicios de información.	¿Se dispone de personal asignado a la administración de la red, al monitoreo y revisión?		SI
09.14 - SC.14	Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.	¿Se dispone de una política y procedimientos para la transferencia de información tanto física como electrónica?		NO
09.14 - SC.14	Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.	¿Se dispone de un detalle del uso de criptografía?		SI
09.14 - SC.14	Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.	¿Se dispone de un listado de acuerdos o cláusulas de los acuerdos con relación a la transferencia segura de la información, entre la organización y terceras partes?		SI
09.14 - SC.14	Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.	¿Se dispone de información de la configuración del correo electrónico?		SI
09.15 - SC.15	Todo sitio Web que contenga u oficie de enlace a un trámite en línea debe tener un firewall de aplicación Web (Web Application Firewall – WAF).	¿Se dispone de respaldo de la configuración de WAF?		SI
09.15 - SC.15	Todo sitio Web que contenga u oficie de enlace a un trámite en línea debe tener un firewall de aplicación Web (Web Application Firewall – WAF).	¿Se dispone de reportes realizados al CERTuy o equipo de respuesta correspondiente?		SI
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de pautas de desarrollo seguro?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de metodología de gestión de proyectos?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de metodología de desarrollo que incluya aspectos de seguridad y evidencia de su revisión periódica?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de la lista de proyectos (desarrollado internamente o adquirido a un tercero) durante el período auditado?		SI
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de un listado de aplicaciones?		SI
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de la especificación de requerimientos para algunos proyectos seleccionados como muestra, donde se incluyan los requerimientos relativos a seguridad de la información?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de trazabilidad de requerimiento – persona de contacto?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de documentación generada en relación con los proyectos de desarrollo?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de una lista de versionado de archivos para el período auditado?		SI
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de una política de gestión de cambios?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de un procedimiento de gestión de cambios?	08.01 - SO.1 10.01 - AD.1	NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone del detalle de la herramienta (si existiera) que asiste en la gestión de los cambios?		NO
10.01 - AD.1	Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.	¿Se dispone de un listado de solicitudes de cambios en el período auditado?		NO

11.01 - RP.1	Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.	¿Se dispone de un listado de proveedores de servicios críticos?		SI
11.01 - RP.1	Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.	¿Se dispone de una política de relacionamiento con proveedores?		NO
11.01 - RP.1	Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.	¿Se dispone de un procedimiento de gestión de proveedores?		NO
11.01 - RP.1	Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.	¿Se dispone de un contrato con proveedores y acuerdos de nivel de servicio (SLA)?		SI
11.01 - RP.1	Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.	¿Se dispone de registro de las mediciones del desempeño, acciones de mejora para ajustar el servicio, llevadas a cabo durante el período auditado?		NO
11.01 - RP.1	Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.	¿Se dispone de un listado con el registro de incidentes con proveedores con tiempo de respuesta y resolución?		NO
11.02 - RP.2	Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.	¿Se dispone de una política de relación con proveedores?		NO
11.02 - RP.2	Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.	¿Se dispone de una lista de proveedores de servicios críticos?		SI
11.02 - RP.2	Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.	¿Se dispone de contrato con los proveedores?		SI
11.02 - RP.2	Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.	¿Se dispone de Acuerdos de Nivel de Servicio (SLA) con los proveedores?		SI
11.02 - RP.2	Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.	¿Se dispone de registro de revisiones regulares de los SLA y contratos con proveedores de servicios?		NO
12.01 - GL.1	Planificar la gestión de los incidentes de seguridad de la información.	¿Se dispone de una política de gestión de incidentes de seguridad de la información?		NO
12.01 - GL.1	Planificar la gestión de los incidentes de seguridad de la información.	¿Se dispone de un procedimiento para la gestión de incidentes de seguridad de la información?		NO
12.01 - GL.1	Planificar la gestión de los incidentes de seguridad de la información.	¿Se dispone de un listado de incidentes del período auditado?		NO
12.01 - GL.1	Planificar la gestión de los incidentes de seguridad de la información.	¿Se dispone de una mesa de ayuda o mesa de servicios formalmente constituida?		SI
12.01 - GL.1	Planificar la gestión de los incidentes de seguridad de la información.	¿Se dispone de una herramienta de software de apoyo a la gestión de incidentes?		NO
12.01 - GL.1	Planificar la gestión de los incidentes de seguridad de la información.	¿Se dispone de responsables definidos para la gestión de incidentes?		NO
12.02 - GL.2	Contar con mecanismos que permitan evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	¿Se dispone de una política de gestión de incidentes de seguridad de la información?	12.02 - GL.2 12.03 - GL.3 12.04 - GL.4 12.05 - GL.5	NO
12.02 - GL.2	Contar con mecanismos que permitan evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	¿Se dispone de pautas o procedimiento para la clasificación de los posibles incidentes?		NO
12.02 - GL.2	Contar con mecanismos que permitan evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	¿Se dispone de un procedimiento de reporte de incidentes de seguridad de la información?		NO
12.02 - GL.2	Contar con mecanismos que permitan evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	¿Se dispone de un listado de incidentes de seguridad de la información del período auditado?		NO

12.02 - GL2	Contar con mecanismos que permitan evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	¿Se dispone de mecanismos y procedimientos empleados para el registro de incidentes de seguridad?		NO
12.02 - GL2	Contar con mecanismos que permitan evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información.	¿Se dispone de un listado de la información o consultas enviadas al CERTuy o equipo de respuesta correspondiente?		NO
12.03 - GL3	Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy o equipo de respuesta externo correspondiente.	¿Se dispone de una política de gestión de incidentes de seguridad de la información?	12.02 - GL2 12.03 - GL3 12.04 - GL4 12.05 - GL5	NO
12.03 - GL3	Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy o equipo de respuesta externo correspondiente.	¿Se dispone de un procedimiento para el reporte de incidentes de seguridad de la información?		NO
12.03 - GL3	Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy o equipo de respuesta externo correspondiente.	¿Se dispone de una lista de incidentes de seguridad de la información reportados al CERTuy o equipo de respuesta correspondiente con detalle de seguimiento, fecha y hora de registro?		NO
12.04 - GL4	Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.	¿Se dispone de una política de gestión de incidentes de seguridad de la información?	12.02 - GL2 12.03 - GL3 12.04 - GL4 12.05 - GL5	NO
12.04 - GL4	Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.	¿Se dispone de un procedimiento de reporte de incidentes de seguridad de la información?		NO
12.04 - GL4	Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.	¿Se dispone de un procedimiento de clasificación de incidentes?		NO
12.04 - GL4	Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.	¿Se dispone de una lista de incidentes reportados en el período auditado?		NO
12.06 - GL6	Establecer los mecanismos para recuperarse luego de un incidente.	¿Se dispone de un Informe de evaluación de daños?		NO
12.06 - GL6	Establecer los mecanismos para recuperarse luego de un incidente.	¿Se dispone de un Informe de lecciones aprendidas?		NO
12.06 - GL6	Establecer los mecanismos para recuperarse luego de un incidente.	¿Se dispone de un repositorio de lecciones aprendidas?		NO
12.05 - GL5	Responder ante incidentes de seguridad de la información.	¿Se dispone de una política de gestión de incidentes de seguridad de la información?	12.02 - GL2 12.03 - GL3 12.04 - GL4 12.05 - GL5	NO
12.05 - GL5	Responder ante incidentes de seguridad de la información.	¿Se dispone de un plan de respuesta a incidentes de seguridad de la información?		NO
12.05 - GL5	Responder ante incidentes de seguridad de la información.	¿Se dispone de un procedimiento de respuesta a incidentes de seguridad de la información?		NO
12.05 - GL5	Responder ante incidentes de seguridad de la información.	¿Se dispone de un registro y seguimiento de los incidentes de seguridad de la información para el período auditado?		NO
12.05 - GL5	Responder ante incidentes de seguridad de la información.	¿Se dispone de evidencia de la comunicación al CERTuy o equipo de respuesta correspondiente?		SI

12.05 - GI.5	Responder ante incidentes de seguridad de la información.	¿Se dispone de evidencia de la respuesta del CERTuy o equipo de respuesta correspondiente?		SI
13.01 - CO.1	Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos.	¿Se dispone de un generador de energía?		NO
13.01 - CO.1	Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos.	¿Se dispone de UPS?		SI
13.01 - CO.1	Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos.	¿Se dispone de líneas eléctricas independientes?		NO
13.01 - CO.1	Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos.	¿Se dispone de control del tablero (exclusividad para cada rack de las acometidas eléctricas desde el tablero general)?		SI
13.01 - CO.1	Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de datos.	¿Se dispone de un sistema de aire acondicionado?		SI
13.02 - CO.2	Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia.	¿Se dispone de un plan de continuidad de las operaciones?	13.02 - CO.2 13.05 - CO.5	NO
13.02 - CO.2	Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia.	¿Se dispone de evidencia de las pruebas realizadas al plan en el período auditado (resultados de las pruebas, aprobaciones requeridas, actividades correctivas y de mejora continua)?		NO
13.02 - CO.2	Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia.	¿Se dispone de un sitio de contingencia y facilidades operativas de contingencia?	13.02 - CO.2 13.04 - CO.4	NO
13.03 - CO.3	Establecer los medios necesarios para garantizar la continuidad de las operaciones.	¿Se dispone de una planificación anual en tareas de contingencia aprobada por la Dirección?		NO
13.04 - CO.4	Planificar la continuidad de las operaciones y recuperación ante desastres.	¿Se dispone de un plan de contingencia y recuperación de las operaciones?	13.04 - CO.4 13.06 - CO.6	NO
13.04 - CO.4	Planificar la continuidad de las operaciones y recuperación ante desastres.	¿Se dispone de un plan de recuperación ante desastres?	13.04 - CO.4 13.05 - CO.5	NO
13.04 - CO.4	Planificar la continuidad de las operaciones y recuperación ante desastres.	¿Se dispone de un plan de pruebas del plan de contingencia y recuperación?		NO
13.04 - CO.4	Planificar la continuidad de las operaciones y recuperación ante desastres.	¿Se dispone de resultados de las pruebas realizadas al plan en el período auditado (resultados, aprobaciones requeridas, actividades correctivas y de mejora continua)?		NO
13.04 - CO.4	Planificar la continuidad de las operaciones y recuperación ante desastres.	¿Se dispone de un sitio de contingencia y facilidades operativas de contingencia?	13.02 - CO.2 13.04 - CO.4	NO
13.04 - CO.4	Planificar la continuidad de las operaciones y recuperación ante desastres.	¿Se dispone de evidencia de capacitaciones realizadas sobre continuidad operativa?		NO
13.05 - CO.5	Definir las ventanas de tiempo soportadas para la continuidad de las operaciones.	¿Se dispone de un plan de continuidad de las operaciones?	13.02 - CO.2 13.05 - CO.5	NO
13.05 - CO.5	Definir las ventanas de tiempo soportadas para la continuidad de las operaciones.	¿Se dispone de un plan de recuperación ante desastres?	13.04 - CO.4 13.05 - CO.5	NO
13.06 - CO.6	Definir los mecanismos de comunicación e interlocutores válidos.	¿Se dispone de un plan de contingencia y recuperación de las operaciones?	13.04 - CO.4 13.06 - CO.6	NO
13.06 - CO.6	Definir los mecanismos de comunicación e interlocutores válidos.	¿Se dispone de un plan de comunicaciones ante crisis?		NO

14.01 - CN.1	Cumplir con los requisitos normativos.	¿Se dispone de la resolución del directorio con la adopción de la política de Seguridad de la Información?		SI
14.01 - CN.1	Cumplir con los requisitos normativos.	¿Se dispone de una planilla de cumplimiento y plan de acción (Según Decreto 092/014)?		NO
14.01 - CN.1	Cumplir con los requisitos normativos.	¿Se dispone del registro de las bases de datos (Protección de datos, Derecho de acceso a la información pública)?		SI
14.02 - CN.2	Realizar auditorías independientes de seguridad de la información.	¿Se dispone de informes de revisiones independientes de seguridad de la información?		NO
14.02 - CN.2	Realizar auditorías independientes de seguridad de la información.	¿Se dispone de seguimiento realizado por la organización para eliminar las observaciones de las revisiones realizadas en forma independiente?		NO
14.03 - CN.3	Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades.	¿Se dispone de evidencia de la realización de pruebas de intrusión?		NO
14.03 - CN.3	Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades.	¿Se dispone de un plan de acción para las acciones correctivas?		NO
14.04 - CN.4	Gestionar las licencias de software.	¿Se dispone de documentación asociada al licenciamiento?		SI
14.04 - CN.4	Gestionar las licencias de software.	¿Se dispone de evidencia de las revisiones de licenciamiento realizadas en el período auditado?		NO
14.04 - CN.4	Gestionar las licencias de software.	¿Se dispone de un inventario de equipamiento y detalle de software instalado?		SI
14.04 - CN.4	Gestionar las licencias de software.	¿Se dispone de una lista de cada software instalado, indicando detalle del servidor, si se utiliza virtualización, detalle de la contingencia (hot, warm, etc.), entre otros?		SI

Tabla 19: Listado de preguntas con respuestas del cuestionario

3.2.2. Verificación y validación de evidencias

Se utilizó la hoja Madurez_Evidencia para contrastar las evidencias recolectadas con los criterios de cumplimiento definidos en el MCS. Para la comparación, se utilizaron las columnas “Id. Req” de la hoja *Evidencia* y “Requisito” de Madurez-Evidencia. Con esta información pudimos definir el valor del cumplimiento.

Fuente	Categoría	Descripción	Subcategoría	Recurso	Resultados Esperados	Cumplimiento	Observaciones
IDENTIFICAR 001	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	GA-1	Identificar formalmente los activos de la organización junto con la definición de su responsable.	SI	Tiene el inventario completo, en integración con la
IDENTIFICAR 002	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	GA-3	Realizar el uso actualizado de los activos.	SI	
IDENTIFICAR 003	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	GA-5	Realizar el uso de dispositivos móviles.	SI	Si, pero no se dispone de un inventario de dispositivos móviles personal para que se conecten a algún servicio de la organización. No hay una política formal, figura como anexo en la ISO.
IDENTIFICAR 004	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-2. Los plataformas de software y aplicaciones se encuentran inventariados.	GA-1	Identificar formalmente los activos de la organización junto con la definición de su responsable.	SI	
IDENTIFICAR 005	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-2. Los plataformas de software y aplicaciones se encuentran inventariados.	GA-3	Realizar el uso actualizado de los activos.	SI	
IDENTIFICAR 006	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-2. Los plataformas de software y aplicaciones se encuentran inventariados.	GA-4	Realizar las licencias de software.	SI	
IDENTIFICAR 007	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-3. Se utilizan medidas de seguridad y procedimientos de gestión para proteger y controlar el flujo de información interna e externa.	GA-4	Mantener la seguridad de la información durante su almacenamiento dentro o fuera de la organización.	SI	
IDENTIFICAR 008	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-4. El equipamiento y los sistemas de información almacenados dentro de las instalaciones se encuentran identificados y se valoran periódicamente para mantener la seguridad de la información.	GA-5	Realizar el uso actualizado de los activos.	SI	
IDENTIFICAR 009	ID.GA. Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-5. Los activos (por ejemplo hardware, dispositivos, datos y software) se encuentran identificados en función del tipo de información que contienen y procesan y en el valor que poseen para el negocio.	GA-2	Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.	SI	

Ilustración 18: Hoja Madurez_Evidencia completada

3.2.3. Determinación del nivel de madurez alcanzado

A partir de la información recopilada y utilizando el campo “Subcategoría” de las hojas Madurez_Evidencia y Madurez, se logró determinar el nivel de madurez en el que se encuentra el organismo, registrándolo en la hoja Madurez.

Función	Cat_Madurez	Cat_Descripción	Subcategoría	Subcategoría Descripción	Nivel Alcanzado	Madurez Nivel	Madurez B (Base)	Madurez	Cumplimiento	Temas para alcanzar nivel de madurez	Responsable	Evidencia
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	1	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	2	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	3	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	4	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-2	Los dispositivos físicos y sistemas se encuentran inventariados.	2	1	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-2	Los dispositivos físicos y sistemas se encuentran inventariados.	2	2	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-2	Los dispositivos físicos y sistemas se encuentran inventariados.	2	3	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.
IDENTIFICAR	ID.GA	Gestión de activos	ID.GA-2	Los dispositivos físicos y sistemas se encuentran inventariados.	2	4	PI	Se conformaron inventarios de los dispositivos físicos, dispositivos de networking, UPS, etc. del centro de datos.	SI	T001-Crear un inventario físico que registre todos los dispositivos físicos del centro de datos. T002- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T003- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). T004- Implementar la actualización de inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos).	T001-Director de Infraestructura T002-Director de Infraestructura T003-Director de Infraestructura T004-Director de Infraestructura	E001-Inventario físico de los dispositivos físicos del centro de datos. E002- Procedimiento para mantener el inventario actualizado (por ejemplo, mediante procedimientos automatizados basados en el centro de datos). E003- Registro de actualizaciones al inventario.

Ilustración 19: Hoja Madurez completada

La madurez de la subcategoría se define por el máximo nivel alcanzado según la columna “Cumplimiento”, por ejemplo, la subcategoría ID.GA – 1 tiene un nivel de madurez 2 porque su “Cumplimiento” solo fue SI hasta el nivel de madurez 2 y no cumplía el 3 y el 4 (ver ilustración 20)

Función	Cat	Cat_Nombre	Cat_Descripción	Subcat	Subcat_Descripción	Nivel Alcanzado	Madurez Nivel	Prioridad (Básico)	Madurez	Cumplimiento
IDENTIFICAR (ID)	ID.GA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	1	P1	Se confeccionan y mantienen inventarios de los dispositivos físicos (servidores, racks, dispositivos de networking, UPS, etc.) del centro de datos.	SI
IDENTIFICAR (ID)	ID.GA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	2	P1	Se incluyen en el inventario los dispositivos físicos (PC, almacenamiento extraíble, dispositivos de networking, impresoras, otro tipo de equipamiento utilizado, etc.) y sistemas de otras áreas de la organización.	SI
IDENTIFICAR (ID)	ID.GA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	3	P1	Los procesos y procedimientos de actualización de inventario se encuentran documentados y están basados en software de inventario. Se automatiza el proceso cuando esto es posible.	NO
IDENTIFICAR (ID)	ID.GA	Gestión de activos	Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.	ID.GA-1	Los dispositivos físicos y sistemas se encuentran inventariados.	2	4	P1	Se realizan actividades periódicas de control interno para verificar el cumplimiento y alineación con los procedimientos establecidos.	NO

Ilustración 20: Ejemplo para definición de nivel de madurez

Posterior a definir los niveles de Madurez por subcategoría, se calcularon los promedios de madurez por función y se visualizaron en las hojas Radar y Barras, proporcionando una representación gráfica del estado actual.

Radar:

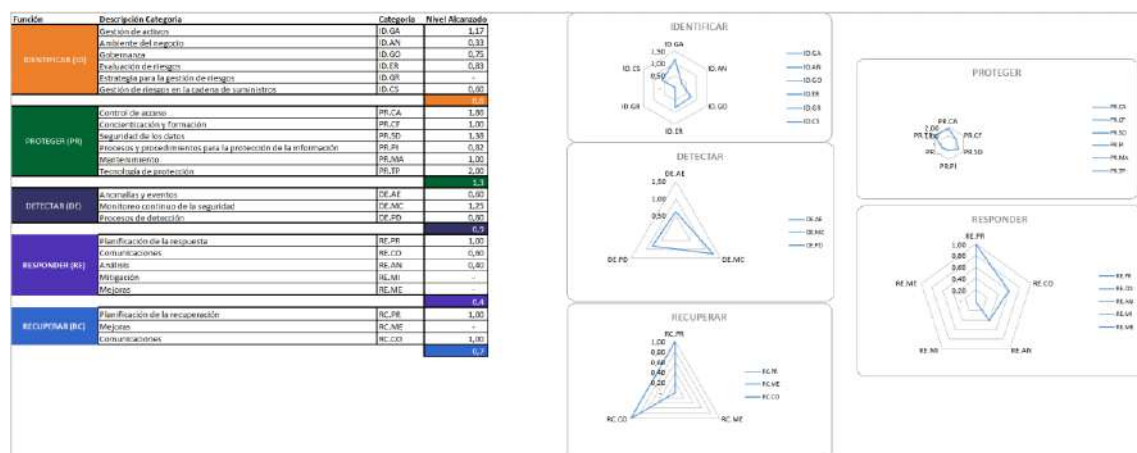


Ilustración 21: Hoja Radar completada

Barras:

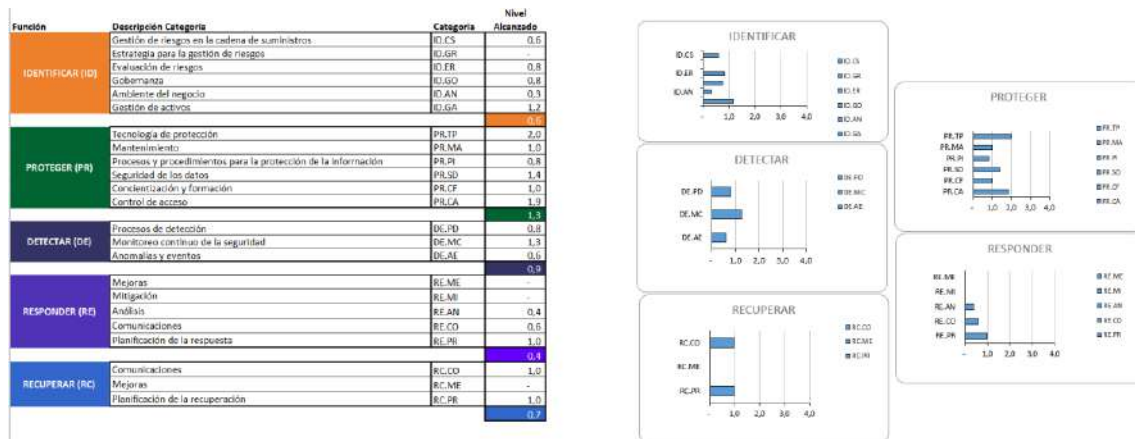


Ilustración 22: Hoja Barras completada

3.2.4. Generación del informe de resumen

La hoja Resumen consolidó los resultados finales, indicando el nivel de madurez alcanzado por categoría para identificar brechas, permitiendo la planificación de acciones para elevar el nivel de madurez en seguridad de la información.

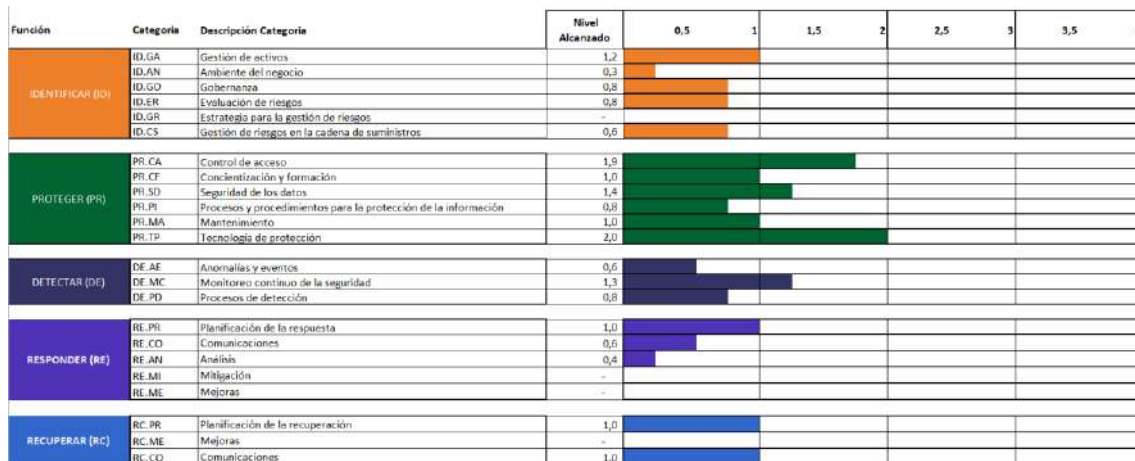


Ilustración 23: Hoja Resumen completada

3.3.Estado actual de madurez del organismo según el relevamiento

El organismo muestra un desarrollo parcial en su marco de ciberseguridad, con avances en la protección de la información y tecnologías de seguridad, sin embargo, la identificación de activos, riesgos y gobernanza aún requieren mejoras, ya que la mayoría de estas categorías se encuentran en niveles iniciales.

En cuanto a la detección de incidentes, el monitoreo continuo muestra un desarrollo moderado, mientras que la identificación de anomalías y la implementación de procesos de detección aún están lejos de los niveles más altos.

En la capacidad de respuesta, se han implementado planes básicos, pero todavía es necesario fortalecer el análisis, la mitigación y las mejoras para acercarse a un nivel óptimo.

La recuperación cuenta con una planificación inicial y mecanismos de comunicación, aunque sin estrategias avanzadas de optimización.

En general, el organismo está avanzada en la función de Proteger, pero necesita fortalecer sus capacidades en todas las funciones para acercarse al nivel máximo de madurez en ciberseguridad. El detalle de estos Niveles se encuentra en el documento general, punto 6. Análisis de la situación actual.

4. Revisión de las tareas terminadas

En función de la información obtenida a partir de las entrevistas y los cuestionarios iniciales, procedimos a revisar la hoja Madurez del documento de trabajo. En esta revisión, analizamos las tareas registradas en la columna "Tareas para alcanzar nivel de madurez", con el objetivo de identificar aquellas que ya habían sido realizadas por el organismo antes de la evaluación del nivel de madurez.

Además, este análisis nos permitió determinar las tareas que aún quedan pendientes por realizar, lo que brinda una visión clara sobre los pasos necesarios para continuar avanzando en el modelo de madurez.

Esta verificación nos permitió contrastar el estado actual del organismo con los requerimientos del modelo, asegurando así un registro preciso de las actividades ya implementadas y de las acciones que aún deben ejecutarse para alcanzar el nivel de madurez deseado. Tareas identificadas como logradas por el organismo en el relevamiento

Este apartado presenta la lista de tareas identificadas como cumplidas por el organismo al momento de realizar el relevamiento. La información recopilada permite evaluar el estado actual del organismo en relación con los niveles de madurez establecidos y reconocer las acciones ya implementadas en el proceso de mejora de la ciberseguridad.

Para facilitar su análisis, la lista de tareas se organiza en las siguientes columnas:

- **Prioridad:** Indica la importancia relativa de cada tarea dentro del proceso de evaluación.
- **Tareas para alcanzar el nivel de madurez:** Describe las actividades necesarias para alcanzar el nivel de madurez definido; en este caso, se listan aquellas que el organismo ya cumple.
- **Responsable:** Especifica la persona o área encargada de ejecutar la tarea.
- **Evidencia:** Detalla los documentos, registros u otros elementos que validan el cumplimiento de la tarea.

Este documento sirve como referencia para la evaluación del estado actual del organismo y proporciona insumos para la planificación de futuras acciones de mejora en ciberseguridad.

Prioridad	Tareas para alcanzar nivel de madurez	Responsable	Evidencia
P1	T001 - Crear un inventario inicial que registre todos los dispositivos físicos del centro de datos.	Director de Infraestructura	E001 - Inventario documentado y actualizado de dispositivos físicos del centro de datos.
P1	T002 - Implementar un mecanismo para mantener el inventario actualizado (por ejemplo, revisiones periódicas o automatización básica).	Director de Infraestructura	E002 - Procedimiento para mantener el inventario.
P1	T003 - Asegurar que el inventario incluya información clave como ubicación, estado, y fecha de última revisión.	Director de Infraestructura	E003 - Registro de actualizaciones al inventario.
P1	T004 - Ampliar el inventario existente para incluir dispositivos de todas las áreas del organismo.	Director de Desarrollo	E004 - Inventario consolidado que incluya dispositivos de todas las áreas del organismo.
P1	T005 - Establecer un sistema unificado de registro que permita integrar información de todos los dispositivos físicos y sistemas.	Director de Desarrollo	E005 - Procedimientos documentados para la gestión del inventario ampliado.
P1	T006 - Implementar revisiones regulares del inventario para asegurar su precisión y vigencia.	Director de Desarrollo	E006 - Registros de revisiones periódicas del inventario.
P1	T007 - Capacitar al personal de las áreas involucradas sobre la importancia del inventario y cómo reportar cambios.	Director de Desarrollo	E007 - Evidencia de capacitaciones realizadas al personal de áreas involucradas.
P1	T015 - Identificar y registrar el software de base (sistemas operativos, bases de datos, middleware) y software de aplicación utilizado en el centro de datos.	Director de TIC	E015 - Inventario documentado y actualizado del software de base y de aplicación del centro de datos.
P1	T016 - Establecer un procedimiento para mantener actualizado el inventario de software.	Director de Infraestructura	E016 - Procedimientos documentados para la gestión del inventario de software.
P1	T017 - Asegurar que el inventario incluya información relevante como nombre del software, versión, fecha de instalación, y estado actual.	Director de Infraestructura	E017 - Registros de actualizaciones o revisiones del inventario de software.
P1	T018 - Ampliar el inventario existente para abarcar plataformas de software y aplicaciones utilizadas en todas las áreas del organismo.	Director de TIC	E018 - Inventario consolidado de plataformas de software y aplicaciones de todas las áreas del organismo.
P1	T019 - Implementar un sistema centralizado para registrar y gestionar el inventario de software de todo el organismo.	Director de Desarrollo	E019 - Registros de licencias del software utilizado en servidores y otros equipos críticos.
P1	T020 - Registrar las licencias asociadas al software utilizado, incluyendo información como tipo de licencia, proveedor, fecha de expiración y cumplimiento de términos.	Director de Soporte y Director de Infraestructura	E020 - Resultados de auditorías periódicas de licenciamiento.
P1	T058 - Desarrollar una Política de seguridad de la información (PSI).	CSI	E058 - Política de seguridad de la información.
P1	T059 - Disponer del acta de Resolución con la aprobación y adopción de la PSI.	RSI y Comunicaciones	E059 - Acta de Resolución con la aprobación de la PSI.
P1	T060 - Comunicar la PSI a todo el organismo.	CSI	E060 - Plan de comunicación de la PSI.
P1	T080 - Designar rol de responsable de datos personales (RDP).	Directorio	R080 - Resolución con designación del RDP.
P1	T081 - Identificar y listar los requisitos normativos aplicables a el organismo relacionados con seguridad de la información y ciberseguridad.	CSI	R081 - Listado documentado de normativas aplicables.
P1	T082 - Revisar las pautas internas del organismo para asegurarse de que están alineadas con las normativas legales identificadas.	CSI	E082 - Informe de revisión y cumplimiento de las pautas internas.
P1	T083 - Modificar o actualizar las pautas organizacionales para reflejar la normativa vigente.	CSI	E083 - Documento actualizado de pautas organizacionales.
P1	T090 - Identificar las amenazas y vulnerabilidades de los activos de información del centro de datos.	Director de Infraestructura	E090 - Documento con la lista de amenazas y vulnerabilidades identificadas.
P1	T091 - Realizar una primera revisión de los riesgos de manera ad-hoc.	Director de Infraestructura	E091 - Informe de la revisión ad-hoc de riesgos.
P1	T099 - Identificar los principales riesgos de seguridad de la información para el organismo.	CSI	E099 - Documento con identificación de riesgos y su clasificación (cualitativa por impacto y probabilidad).
P1	T119 - Identificar proveedores de los activos y servicios críticos del centro de datos.	Director de TIC y CSI	E119 - Lista de proveedores de los activos y servicios críticos del centro de datos.
P1	T140 - Configurar controles de acceso lógico basados en usuarios nominados.	Director de TIC	E140 - Configuración de acceso lógico documentada que muestra la asociación entre usuarios y accesos.
P1	T141 - Establecer un registro inicial de usuarios nominados que tienen acceso a redes, recursos y sistemas.	Director de TIC	E141 - Lista de usuarios con acceso a redes, recursos y sistemas con permisos asignados.
P1	T142 - Definir pautas para gestionar altas, bajas y modificaciones de acceso lógico.	Director de TIC	E142 - Documento de pautas para la gestión de accesos lógicos.
P1	T143 - Establecer un flujo de aprobaciones para gestionar cambios en los accesos lógicos.	Director de TIC	E143 - Registro de aprobaciones para modificaciones de acceso lógico.
P1	T144 - Implementar un sistema para registrar y monitorear las altas, bajas y modificaciones realizadas.	RSI y Director de TIC	E144 - Registro histórico de cambios en accesos lógicos.
P1	T152 - Implementar controles básicos de acceso físico a los activos críticos del centro de datos.	Director de Infraestructura	E152 - Configuración inicial de sistemas de control de acceso físico y su documentación.
P1	T153 - Crear un registro de autorizaciones para acceder a los activos físicos del centro de datos.	Director de Infraestructura	E153 - Registro con el listado de personas autorizadas

P1	T164 - Implementar credenciales nominadas para todos los usuarios con acceso a la red y sistemas.	Director de Infraestructura	E164 - Listado de usuarios nominados con accesos de red otorgados.
P1	T165 - Definir controles básicos para el uso de usuarios privilegiados.	Director de Infraestructura	E165 - Listado de controles básicos para usuarios privilegiados.
P1	T166 - Eliminar el uso de cuentas genéricas o compartidas, reemplazándolas por usuarios nominados con permisos controlados.	Director de Infraestructura	E166 - Listado de bajas de usuarios genéricos.
P1	T167 - Establecer roles y permisos basados en los principios de menor privilegio y segregación de funciones.	Director de Infraestructura	E167 - Documentación de roles y permisos asignados.
P1	T168 - Implementar autenticación fuerte para usuarios críticos mediante métodos como doble factor de autenticación.	Director de Infraestructura	E168 - Configuración de doble factor de autenticación y listado de usuarios críticos.
P1	T169 - Centralizar la administración de usuarios y permisos mediante herramientas específicas.	Director de Infraestructura	E169 - Herramienta centralizada para la gestión de usuarios.
P1	T176 - Definir roles y perfiles específicos para el personal con acceso al centro de datos.	Director de Infraestructura	E176 - Listado de roles y perfiles segregados al centro de datos.
P1	T177 - Implementar un registro de actividades realizadas en el centro de datos.	Director de Infraestructura	E177 - Logs de actividades realizadas en el centro de datos.
P1	T178 - Revisar esporádicamente los registros de actividades para detectar anomalías.	Director de Infraestructura	E178 - Informes de revisiones de acceso al centro de datos.
P1	T189 - Implementar autenticación obligatoria en todos los sistemas del organismo.	Director de Desarrollo	E189 - Registros de autenticación habilitada en los sistemas.
P1	T190 - Garantizar que todos los usuarios sean nominados y cumplan con la política de control de acceso.	Director de Desarrollo	E190 - Listado de usuarios nominados con roles asignados.
P1	T191 - Autorizar y registrar dispositivos que se conecten a la red del organismo.	Director de Infraestructura	E191 - Registro de dispositivos autorizados para conexión.
P1	T203 - Iniciar actividades de difusión de información relacionada con seguridad de la información, incluyendo la difusión de políticas y mecanismos de protección.	RSI y Comunicaciones	E203 - Registro de las actividades realizadas (presentaciones, correos electrónicos, boletines informativos) y lista de distribución o participantes.
P1	T213 - Identificar a los usuarios privilegiados y comunicarles la importancia de sus roles y responsabilidades.	RSI y Comunicaciones	E213 - Lista de usuarios privilegiados identificados y correo o registro de comunicación oficial.
P1	T214 - Realizar una reunión inicial para explicar las implicancias y riesgos asociados a sus roles.	RSI	E214 - Cada Director de División explica los riesgos asociados a sus roles
P1	T222 - Identificar a los interesados externos clave y documentar sus roles y responsabilidades en relación con la seguridad de la información.	CSI	E222 - Listado de interesados externos con roles y responsabilidades en relación con la seguridad de la información.
P1	T223 - Comunicar las pautas definidas a los interesados externos mediante un canal formal (ej., contrato, acta o correo oficial).	Alta Dirección	E223 - Registro de pautas de seguridad con a los interesados externos que detalle su rol y responsabilidad.
P1	T231 - Realizar una sesión informativa inicial a la Alta Dirección sobre los riesgos de seguridad de la información relevantes para el organismo.	CSI	E231 - Acta de la sesión informativa sobre riesgos de seguridad de la información realizada con la Alta Dirección.
P1	T232 - Documentar los principales riesgos de seguridad de la información y compartirlo con el Directorio.	CSI	E232 - Documento con los principales riesgos de seguridad de la información, firmado por los asistentes.
P1	T240 - Definir pautas estándar para la instalación de software en los equipos del personal.	Director de Soporte	E240 - Documento con pautas estándar para la instalación de software.
P1	T241 - Instalar software antivirus en los equipos del personal.	Director de Soporte	E241 - Informe de implementación del software antivirus en los equipos del personal.
P1	T242 - Realizar tareas de concientización sobre prevención ante software malicioso.	Director de Soporte y Capacitación	E242 - Registro de actividades de concientización realizadas.
P1	T243 - Restringir la instalación de software en los equipos a usuarios autorizados.	Director de Soporte	E243 - Registro de usuarios autorizados para instalar software en los equipos.
P1	T244 - Desarrollar un procedimiento para la instalación de software en producción, asignando responsables.	Director de Infraestructura	E244 - Procedimiento para la instalación de software en producción.
P1	T245 - Instalar soluciones antivirus en servidores de archivos y correo electrónico.	Director de Infraestructura	E245 - Informe de implementación de soluciones antivirus en servidores.
P1	T254 - Realizar respaldos periódicos de los activos del centro de datos.	Director de Infraestructura	E254 - Cronogramas documentados de respaldos.
P1	T255 - Documentar los activos críticos de información que requieren respaldo.	Director de Infraestructura	E255 - Registro de activos respaldados.
P1	T256 - Almacenar los respaldos en una ubicación inicial definida.	Director de Infraestructura	E256 - Logs del sistema que evidencien la realización de respaldos.
P1	T257 - Implementar una solución automatizada para respaldos.	Director de Infraestructura	E257 - Logs y reportes generados por las soluciones automatizadas.
P1	T258 - Definir ubicaciones seguras para respaldos con acceso restringido.	RSI y Director de Infraestructura	E258 - Documento de políticas de acceso a los respaldos.
P1	T259 - Documentar medidas de seguridad asociadas a los respaldos.	RSI y Director de Infraestructura	E259 - Registro de ubicaciones seguras y medidas de seguridad implementadas.
P1	T279 - Implementar el cifrado de comunicación entre MTAs como método preferido.	Director de Infraestructura	E279 - Configuración de cifrado entre MTAs completada.
P1	T280 - Configurar los servicios de Web mail con HTTPS utilizando certificados válidos.	Director de Infraestructura	E280 - Certificados válidos configurados en servicios de Web mail.
P1	T281 - Proteger todas las aplicaciones Web disponibles en Internet mediante WAF configurado en modo detección.	Director de Infraestructura	E281 - Configuración de WAF en modo detección para aplicaciones Web.

P1	T282 - Evolucionar el WAF de producción de modo detección a modo bloqueo.	Director de Infraestructura	E282 - Configuración de WAF en modo bloqueo en ambiente de producción.
P1	T283 - Implementar un WAF en ambiente de prueba para realizar pruebas funcionales.	Director de Infraestructura	E283 - Instalación y pruebas funcionales documentadas en ambiente de prueba del WAF.
P1	T284 - Centralizar los registros del WAF en un repositorio único.	Director de Infraestructura	E284 - Centralización de registros del WAF en repositorio de logs.
P1	T291 - Establecer un procedimiento básico para resolver problemas de malware de forma ad-hoc.	Director de Soporte	E291 - Documento con el procedimiento básico para resolver problemas de malware.
P1	T293 - Configurar chequeos periódicos automáticos en los equipos del personal.	Director de Soporte	E293 - Logs de chequeos periódicos en las estaciones de trabajo.
P1	T294 - Diseñar y realizar actividades de concientización sobre riesgos de software malicioso para el personal.	RSI y Capacitación	E294 - Material utilizado en las actividades de concientización sobre software malicioso.
P1	T302 - Definir los mecanismos de respuestas a incidentes.	RSI	E302 - Documento con los mecanismos de respuesta de incidentes.
P1	T303 - Implementar las herramientas para detectar y reportar incidentes.	RSI	E303 - Herramienta de reporte de incidentes.
P1	T304 - Establecer los pasos para informar al CERTuy cuando se detecte un incidente.	RSI	E304 - Documento con los pasos para informar incidentes al CERTuy, incluyendo tiempos de respuesta y contenido de la información a compartir.

Tabla 20: Tareas logradas por el organismo

ANEXO 3 - Entregable 2: Políticas a medida del organismo

Tabla de Contenido

Man 01 - Manual de Políticas de Seguridad de la Información.....	114
Pol 01 - Política de Seguridad de la Información	126
Pol 02 - Política de Gestión de Incidentes de Seguridad de la Información.....	133
Pol 03 - Política de Uso Aceptable de Activos	153
Pol 04 - Política de Intercambio y Traslado Físico de la Información	157
Pol 05 - Política de Control de Acceso Lógico.....	160
Pol 06 - Política de Gestión de Usuarios y Contraseñas	164
Pol 07 - Política de Gestión de Usuarios de Acceso Privilegiado	168
Pol 08 - Política de Control de Acceso Físico a Áreas Seguras.....	172
Pol 09 - Política de Seguridad del Equipamiento	178
Pol 10 - Política de Respaldo de Información	181
Pol 11 - Política de Protección contra Software Malicioso	184
Pol 12 - Política de Separación de Entornos	189
Pol 13 - Política de Registro y Auditoría de Eventos de Sistemas de Información.....	192
Pol 14 - Política de Protección y Privacidad de los Datos	195
Pol 15 - Política de Clasificación de la Información	204
Pol 16 - Política de Uso Aceptable de Dispositivos Móviles	212
Pol 17 - Política de Uso de Controles Criptográficos	216
Pol 18 - Política de Continuidad Operativa y Recuperación ante Desastres	220
Pol 19 - Política de Cumplimiento.....	226
Pol 20 - Política de Escritorio y Pantalla Limpios	229
Pol 21 - Política de Gestión de Riesgos de Seguridad de la Información.....	232
Pol 22 - Política de Gestión de Cambios	239
Pol 23 - Política de Finalización o Cambio en la Relación Laboral	245

Pol 24 - Política de Acceso Remoto y Teletrabajo	248
Pol 25 - Política de Eliminación y Destrucción de la Información.....	252
Pol 26 - Política de Relacionamiento con Proveedores	256
Pol 27 - Política De Uso Institucional De Redes Sociales.....	259
Pol 28 - Política de Uso de Internet	262
Pol 29 - Política de Desarrollo de Software Seguro	268
Pol 30 - Política de Gestión de la Seguridad de las Redes.....	281
Pol 31 - Política de Gestión de Riesgos de Proveedores	285
Pol 32 - Política de Gestión de Activos	292
Pol 33 - Política de Gestión de Riesgos	298
ANEXO 4 - Entregable 3: Plan y material de capacitaciones	305
Plan de Concientización y Sensibilización en Seguridad de la Información.....	308
Material de Capacitación de Seguridad de la Información	324
ANEXO 5 - Listado de actividades pendientes	448
ANEXO 6 - Listado completo de actividades.....	475
ANEXO 7 - Política de Seguridad de Información vigente.....	540
Política de Seguridad de Información.....	541

Índice de Tablas

Tabla 21 - Actividades relacionadas al Manual de Políticas y Políticas complementarias	113

Dado que la seguridad de la información es un tema relevante para el organismo y para alcanzar los niveles de madurez establecidos por el MCS, se identificó la necesidad de desarrollar un conjunto de políticas complementarias a la Política de Seguridad de la Información (PSI), acompañado de un Manual de Políticas de Seguridad de la Información. Para ello, se realizaron las actividades que se detallan en la Tabla 21.

Prio	Tareas para alcanzar nivel de madurez	Evidencia
P1	T008 - Desarrollar una política de Uso Aceptable de los Activos Móviles.	E008 - Política de Uso Aceptable de Dispositivos Móviles.
P1	T062 - Desarrollar políticas adicionales alineadas con la política general y manual de políticas asociadas.	E062 - Políticas adicionales alineadas con la política general y Manual de Políticas.
P1	T094 - Definir una política de gestión de riesgos.	E094 - Política de gestión de riesgos.
P1	T122 - Desarrollar una política de gestión de riesgos de proveedores.	E122 - Política de gestión de riesgos de proveedores.
P1	T145 - Desarrollar una política de acceso lógico.	E145 - Política de acceso lógico.
P1	T157 - Desarrollar una política de control de acceso físico que abarque todos los activos críticos.	E157 - Política de control de acceso físico.
P1	T248 - Desarrollar una política de protección contra software malicioso.	E248 - Política de protección contra software malicioso.
P1	T262 - Desarrollar una política de respaldo de información.	E262 - Política de respaldo de información.
P1	T308 - Desarrollar una política de gestión de incidentes de seguridad de la información.	E308 - Política de gestión de incidentes de seguridad de la información.
P2	T322 - Desarrollar una política para el uso adecuado de activos.	E322 - Política de uso aceptable de activos.
P2	T341 - Desarrollar una política de gestión de riesgos de seguridad de la información.	E341 - Política de Gestión de Riesgos de Seguridad de la Información.
P2	T392 - Desarrollar una política de gestión de proveedores.	E392 - Política de Gestión de Proveedores.
P2	T435 - Desarrollar una política de uso de controles criptográficos.	E435 - Política de uso de controles criptográficos.
P2	T465 - Desarrollar una política de destrucción de la información.	E465 - Política de destrucción de información.
P2	T490 - Desarrollar una política de separación de entornos.	E490 - Política de separación de entornos.

P2	T514 - Desarrollar una política de gestión de cambios.	E514 - Política de Gestión de Cambio.
P2	T525 - Desarrollar una política de seguridad del equipamiento.	E525 - Política de seguridad del equipamiento.
P2	T587 - Desarrollar una política de registro y auditoría de eventos de sistemas de información.	E587 - Política de registro y auditoría de eventos de sistemas de información
P2	T857 - Desarrollar una política de continuidad de las operaciones y recuperación ante desastres.	E857 - Política de Continuidad de las Operaciones y Recuperación ante Desastres.

Tabla 21 - Actividades relacionadas al Manual de Políticas y Políticas complementarias

Man 01 - Manual de Políticas de Seguridad de la Información

1.- Objetivo

El objetivo del presente Manual de Políticas de Seguridad de la Información es establecer los lineamientos y el marco de referencia para la exitosa implementación del Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información del Organismo.

1.1.- Vigencia

El presente manual entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez Y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

El Manual de Políticas de Seguridad de la Información establece el marco para el correcto desarrollo de todos los procedimientos, instructivos y demás documentación asociada a la implementación del SGSI.

Alcanza a todos los funcionarios del Organismo sin importar la modalidad de contratación, así como también a los proveedores y demás partes involucradas que interactúan con activos de información del Organismo.

3.- Definiciones

- **Activo:** Se refiere a cualquier elemento que tiene valor para el Organismo.
- **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas, etc.) que tenga valor para el Organismo.
- **Activo crítico:** Instalaciones, sistemas y equipos, los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos del Organismo.
- **Administración de riesgos:** Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o del Organismo.
- **Análisis de Impacto al Negocio (BIA):** Es una metodología que permite identificar los procesos críticos que apoyan los servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Cifrado:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrada adecuada para descodificarlo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Confiabilidad de la Información:** Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Control:** Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Código malicioso:** Es un código informático que crea brechas de seguridad para dañar un sistema informático.
- **Custodio:** Es una parte designada del Organismo, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de activo haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinada o determinables. Debe entonces entenderse el “dato personal”, como una información relacionada con una persona natural (persona individualmente considerada).
- **Dato personal público:** Toda información personal que es de conocimiento libre y abierto para el público en general.
- **Dato personal privado:** Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.
- **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.
- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y a los datos biométricos.
- **Data Center:** Se denomina también Centro de Procesamiento de Datos (CPS) a aquella ubicación o espacio donde se concentran los recursos necesarios de tecnologías de la información (TI) para el procesamiento de la información de un Organismo.
- **Departamento de Atención a Usuarios:** Constituye el único punto de contacto con los usuarios finales para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Es a través de la gestión proactiva del Departamento de Atención a Usuarios que el Organismo recolecta las necesidades que tienen dependencias en cuanto a los recursos tecnológicos.

- Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- Dispositivos móviles: Equipo celular, equipos portátiles, tabletas, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet, y cuenta con capacidad de procesamiento.
- Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- Incidente de seguridad: Evento o serie de eventos de seguridad de la información no deseado o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- Integridad: Propiedad de la información que busca preservar su exactitud y completitud.
- Impacto: Resultado de un incidente de seguridad de la información.
- Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta del Organismo.
- No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío.
- Partes interesadas: Persona u Organismo que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.
- Plan de Continuidad del Negocio: Actividades documentadas que guían al Organismo en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.
- Privacidad de la Información: El derecho que tienen todos los titulares de la información en relación con la Información que involucre datos personales y la información clasificada

que estos hayan entregado o esté en poder del Organismo en el marco de las funciones que a este le compete realizar y que generan en las organizaciones destinatarias la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- Propietario de la información (titular): Es una parte designada del Organismo, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- Sistema de Gestión de Seguridad de la Información: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad y salvaguardar todos los activos que se manejan dentro del Organismo.
- Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión, y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso del Organismo.
- Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio al Organismo y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.
- Test de penetración: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.
- VPN: Red virtual privada por sus siglas en inglés, *Virtual Private Network*.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4.- Fundamento Legal

El Manual de Políticas de Seguridad de la Información sigue las recomendaciones establecidas en el Marco de Ciber Seguridad de AGESIC v4.2.

A su vez, está alineado a las buenas prácticas internacionales recomendadas por:

- NIST CSF v1.1 – Marco de Ciber Seguridad del NIST
- ISO/IEC 27001:2022 – Requisitos para la certificación en Seguridad de la Información
- ISO/IEC 27002:2022 – Buenas Prácticas de Seguridad de la Información
- ISO/IEC 27005:2022 – Gestión de Riesgos de Seguridad de la Información
- ISO 55000: 2014 – Gestión de Activos
- ISO 22300:2021 – Mejorando la Gestión de la Resiliencia

El Manual de Políticas de Seguridad de Información también cumple con la normativa nacional en materia de ciberseguridad, que incluye entre otros:

- Ley 18331 - Protección de Datos Personales y Acción de Habeas Data

5.- Responsabilidad

Los roles y responsabilidades en el marco del SGSI se encuentran en el Manual de Gestión del SGSI.

En relación con las políticas de Seguridad de la Información, se detallan las siguientes responsabilidades:

- **Directorio**
Aprueba la Política de Seguridad de la Información y Protección de Datos y vela por el cumplimiento de la normativa y legislación vigente al respecto, poniendo a disposición para ello los recursos necesarios para dar cumplimiento a lo establecido. Delega en la Comisión de Seguridad de la Información (CSI) la aprobación del presente Manual de Políticas de Seguridad de la Información, y de las restantes políticas complementarias de política principal.
- **Comisión de Seguridad de la Información**
Aprueba el presente Manual de Políticas de Seguridad de la Información. Establece las responsabilidades específicas para su ejecución, control, monitoreo y mejora.
- **Responsable de Seguridad de la Información (RSI)**
Colabora en la elaboración del presente Manual de Políticas de Seguridad de la Información. Elabora la documentación necesaria para la correcta implementación de las políticas y vela por el cumplimiento de estas.
- **Personal del Organismo**
Todo el personal del Organismo es responsable de cumplir con lo establecido en cada una de las políticas incluidas en el presente Manual.

6.- Políticas

El Organismo establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas teniendo en cuenta el contexto interno y externo del organismo.

6.01.- Pol-01 - Política de Seguridad de la Información

Establece los principios rectores para asegurar la protección de los activos de información y para fundamentar el desarrollo de un Sistema de Gestión de la Seguridad de la Información en el organismo.

6.02.- Pol-02 - Política de Gestión de Incidentes de Seguridad de la Información

Establece los criterios, comunicaciones y formas que definen el tratamiento, identificación y respuesta ante incidentes de Seguridad de la Información en el Organismo.

6.03.- Pol-03 - Política de Uso Aceptable de los Activos

Detalla las buenas prácticas aplicadas a describir qué es considerado uso aceptable de los activos del Organismo.

6.04.- Pol-04 - Política de Intercambio y Traslado Físico de la Información

Define los criterios a seguir para el traslado de información desde el organismo hacia clientes y proveedores.

6.05.- Pol-05 - Política de Control de Acceso Lógico

Establece quién, cómo y cuándo se puede acceder a los activos de información del organismo.

6.06.- Pol-06 - Política de Gestión de Usuarios y Contraseñas

Establece, difunde y provee criterios para el cumplimiento de las buenas prácticas en el uso de contraseñas.

6.07.- Pol-07 - Política de Gestión de Usuarios de Acceso Privilegiado

Establece la gestión adecuada de las cuentas de usuarios privilegiado para prevenir riesgos asociados al uso de permisos privilegiados.

6.08.- Pol-08 - Política de Control de Acceso Físico a Áreas Seguras

Determina lineamientos para controlar el acceso físico a las áreas seguras del Organismo y pretende reducir los riesgos de accesos no autorizados.

6.09.- Pol-09 - Política de Seguridad del Equipamiento

Establece cómo se protege la seguridad en los equipos del organismo.

6.10.- Pol-10 - Política de Respaldo de la Información

Define como se deben generar los respaldos para la información cuyo tratamiento es responsabilidad del Organismo.

6.11.- Pol-11 - Política de Protección contra Software Malicioso

Establece los mecanismos de protección antivirus, antimalware, etc.

6.12.- Pol-12 - Política de Separación de Entornos

Establece los criterios a considerar en la segregación o separación de los ambientes operativos.

6.13.- Pol-13 - Política de Registro y Auditoría de Eventos de Sistemas de Información

Define cómo, cuándo y qué debe ser incluido en los registros de eventos auditables.

6.14.- Pol-14 - Política de Protección y Privacidad de Datos

Establece los principios rectores para asegurar la protección y la privacidad de los datos.

6.15.- Pol-15 - Política de Clasificación de la Información

Define los criterios de la clasificación de los activos de información en uso dentro del organismo.

6.16.- Pol-16 - Política de Uso Aceptable para Dispositivos Móviles

Establece como utilizar los dispositivos móviles en el organismo.

6.17.- Pol-17 - Política De Uso De Controles Criptográficos

Define los criterios de uso para los controles criptográficos.

6.18.- Pol-18 - Política de Continuidad de las Operaciones y Recuperación Ante Desastres

Determina los criterios a aplicar en relación con los controles de gestión de la seguridad de la información en el contexto de los planes de continuidad operativa del organismo.

6.19.- Pol-19 - Política de Cumplimiento

Define el contexto normativo y la interacción con el mismo desde el organismo.

6.20.- Pol-20 - Política de Escritorio y Pantalla Limpios

Establece la definición y el alcance del concepto de escritorio y pantalla limpia, sean estos físicos o virtuales.

6.21.- Pol-21 - Política de Gestión de Riesgos de Seguridad de la Información

Establece los criterios para el tratamiento del riesgo de seguridad de la información dentro del organismo en todas sus áreas de acción.

6.22.- Pol-22 - Política de Gestión de Cambios

Define como procesar el cambio entre actores y partes interesadas dentro del organismo y en relación con su vínculo con productos y servicios que se ofrecen a clientes.

6.23.- Pol-23 - Política de Finalización o Cambio en la Relación Laboral

Establece los lineamientos para el proceso de finalización de vínculos laborales en relación con la seguridad de la información.

6.24.- Pol-24 - Política de Acceso Remoto y Teletrabajo

Establece los criterios a seguir para implementar conexiones de acceso remoto en el organismo.

6.25.- Pol-25 - Política de Eliminación y Destrucción de la Información

Establece los criterios para implementar la disposición final de los activos de información en el organismo.

6.26.- Pol-26 - Política de Relacionamiento con Proveedores

Define aspectos de la gestión del vínculo con empresas proveedoras de servicios y productos al organismo.

6.27.- Pol-27 - Política de Uso Institucional de Redes Sociales

Establece prácticas obligatorias para el uso institucional de las redes sociales en modo seguro.

6.28.- Pol-28 - Política de Uso de Internet

Define el uso adecuado para los accesos a Internet que provee el organismo y define buenas prácticas para los usuarios.

6.29.- Pol-29 - Política de Desarrollo de Software Seguro

Establece los criterios para el desarrollo seguro de aplicaciones.

6.30.- Pol-30 - Política de Gestión de la Seguridad de las Redes

Establece las reglas necesarias para garantizar el funcionamiento correcto y seguro de las redes de datos y de comunicaciones del organismo.

6.31.- Pol-31 - Política de Gestión de Riesgos de Proveedores

Define los criterios para la detección de los riesgos vinculados con los proveedores que pueden afectar a las diferentes áreas del organismo, a las actividades del organismo y a los objetivos que están asociados a ella.

6.32.- Pol-32 - Política de Gestión de Activos

Define los criterios para la obtención del máximo rendimiento de los bienes o recursos, es decir de todo aquello que tenga valor para el organismo.

6.33.- Pol-33 - Política de Gestión de Riesgos

Define los criterios para el desarrollo formal de las actividades relacionadas con la Gestión del Riesgo en el organismo tal como deben desplegarse en sus áreas operativas.

7.- Comunicación, Sensibilización, Y Capacitación

El organismo definirá un “Plan de Comunicación en Seguridad de la Información” a través de la Gerencia de Administración y a través del Departamento de Personal, donde se planificará anualmente la manera en que se comunicarán recomendaciones o tips de seguridad de la información por diferentes medios a todos sus funcionarios y colaboradores, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos del organismo. La creación de los contenidos se hará con apoyo del Oficial de Seguridad de la Información.

El organismo, a través de la Gerencia de Administración y a través del Departamento de Personal, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule al organismo tenga pleno conocimiento de las políticas de seguridad de la información. El Oficial de Seguridad de la Información apoyará en dichas inducciones.

8.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Dirección del Organismo, a través del Departamento de Personal podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 01 - Política de Seguridad de la Información

1.- Trámite Y Revisiones

1.1.- Trámite

El documento “Política de Seguridad de la Información” (PSI) fue diseñado por la Comisión de Seguridad de la Información (CSI).

La CSI está conformada por representantes de Dirección General, Área de Planificación Estratégica y Presupuestal, División Tecnologías de la Información y Comunicaciones, Auditoría Interna de Gestión y División Jurídica.

1.2.- Revisiones

Fecha	N° de versión	Elaborado por	Aprobado por	Párrafos modificados	Surge de:
04/11/2022	01	Comisión de Seguridad de la Información		Documento nuevo	TIC
02/03/2023	02	Comisión de Seguridad de la Información			

2.- Objetivo

El objeto de la presente política es proteger la información y preservar su integridad, confidencialidad y disponibilidad contra posibles amenazas.

2.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

2.2.- Validez Y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

3.- Alcance

Se aplica en todo el ámbito del organismo y para todos los usuarios que tengan acceso a activos de información del este.

4.- Responsabilidades

El Directorio del organismo es responsable por difundir la presente política a todo el personal, independientemente del cargo que desempeñe.

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política.

5.- Referencias Normativas

5.1.- Marcos Legales Que Aplican A Esta Política

- Ley N° 18.331 – Protección de Datos Personales y Acción de “HABEAS DATA”
- Ley N° 18.381 – Ley Sobre el derecho de acceso a la información pública

5.2.- Resoluciones

- Res. 2526/22 - Creación de la Comisión de Seguridad de la Información.

6.- Política de Seguridad de la Información

El Directorio del organismo reconoce la importancia de identificar y proteger sus activos de información. Para ello, velará por evitar la destrucción, divulgación, modificación y utilización no autorizada de toda la información, mediante el compromiso de desarrollar progresivamente, implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, basado en el Marco de Ciberseguridad propuesto por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC).

El Directorio del organismo declara su compromiso con el cumplimiento de la normativa y legislación vigente en relación con los diversos aspectos de la Seguridad de la Información.

La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger los activos de información. La Seguridad de la Información se caracteriza como

la preservación de:

- su confidencialidad, asegurando que sólo quienes estén autorizados puedan efectivamente acceder a la información;
- su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos;
 - su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura. Los controles deberán establecerse de manera progresiva, acompañados de adecuadas campañas de comunicación interna, con el fin de garantizar los objetivos de seguridad de la información del organismo.

Por este motivo el Directorio del organismo designa un Responsable de la Seguridad de la Información (RSI), quien se encarga de la guía, implementación y del mantenimiento del Sistema de Gestión de Seguridad de la Información.

Esta Política de Seguridad de la Información se integrará a la normativa básica del organismo, asegurando su difusión previa y la implementación de medidas para gestionar posibles incumplimientos, así como para regular los documentos relacionados.

La presente Política de Seguridad de la Información debe ser conocida y cumplida por todas las personas vinculadas al organismo, independientemente del cargo que desempeñe y de su situación contractual.

En este contexto, se establecen los siguientes lineamientos:

- Establecer objetivos anuales con relación a la Seguridad de la Información y, en función de tales objetivos, publicar políticas y comunicar los controles que complementan este documento.

- Desarrollar un proceso de evaluación y tratamiento de los riesgos de seguridad. De acuerdo con su resultado, implementar progresivamente acciones correctivas y preventivas, así como elaborar y actualizar el plan de acción como parte de las iniciativas de mejora continua.
- Establecer los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgo surjan del proceso de análisis de riesgos manejados.
- Clasificar y proteger la información de acuerdo con la normativa vigente y a los criterios de valoración según sea la importancia que tenga cada activo de información.
- Brindar las mayores garantías para salvaguardar la integridad, confidencialidad y disponibilidad de la información custodiada por el organismo, velando por la privacidad de todos los datos sensibles almacenados en los sistemas que administra.
- Organizar periódicamente instancias de concientización que también sirvan para la formación en materia de Seguridad de la Información para todo el personal del organismo.
- Contar con una política de gestión de incidentes de seguridad de la información y seguir los lineamientos establecidos por la normativa vigente y el CERTuy.
- Establecer que todo el personal del organismo es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes que se establezcan.
- Establecer los medios necesarios para garantizar la continuidad de las operaciones del organismo.

La seguridad de la información requiere el compromiso y respaldo de todos los niveles directivos, asegurando su integración y alineación con los objetivos estratégicos del organismo para una gestión coherente y eficaz.

La CSI tendrá como principal objetivo promover, difundir y apoyar la seguridad de la información, garantizando que la misma sea parte del proceso de planificación, definiendo estrategias, planes, políticas y todo aquello que incremente y mejore la seguridad de la información.

7.- Obligaciones del Personal y Colaboradores

Todo el personal del organismo, así como los terceros colaboradores que presten servicios con acceso a datos personales bajo su responsabilidad, están obligados a conocer y cumplir lo establecido en la presente PSI, así como en las normas y procedimientos que la desarrollen. Además, deben colaborar activamente en la mejora continua de las medidas de seguridad de la

información, contribuyendo a prevenir y mitigar los riesgos que puedan comprometer la protección de los datos personales y demás información bajo responsabilidad del organismo.

Específicamente, es responsabilidad de todo el personal del organismo, incluido el personal temporario, terceras partes debidamente autorizadas y, en general, de cualquier persona física o jurídica que acceda legítimamente a información bajo custodia del organismo, reportar y registrar cualquier violación a la seguridad de la información, ya sea confirmada o sospechada. Dichos reportes deberán realizarse siguiendo los procedimientos establecidos, los cuales deben estar previamente planificados y protocolizados.

8.- Capacitación y Concientización

El organismo implementará actividades formativas específicas orientadas a la concientización y formación del personal, con el objetivo de reforzar el conocimiento de sus deberes y obligaciones en relación con la presente PSI, así como en identificar y prevenir los riesgos asociados al tratamiento de la información.

9.- Anexo 1 – Glosario

Término	Significado
Activo de información	Cualquier información o elemento relacionado con el tratamiento de la misma que tenga valor para el organismo.
Alcance	Ámbito del organismo sometido al SGSI.
Amenaza	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o al organismo.
Análisis de riesgos	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Análisis de riesgos cualitativo	Análisis de riesgos basado en escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.
Análisis de riesgos cuantitativo	Análisis de riesgos basado en identificar las pérdidas financieras asociadas a la materialización del riesgo.
Auditoría	Proceso sistemático, independiente y documentado, para obtener evidencia que verifique el cumplimiento de los requisitos solicitados por normas, políticas o estrategias impuestas por el Directorio.
Confidencialidad	Propiedad de la información de no ponerse a disposición o no ser revelada a individuos, entidades o procesos no autorizados.
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para modificar el riesgo y mantenerlo por debajo del nivel de riesgo asumido.
Disponibilidad	Propiedad de la información de estar accesible y utilizable.

Estimación de riesgos	Valoración de los resultados del análisis de riesgos para determinar si la magnitud del riesgo es tolerable.
Gestión de claves	Controles referidos a la gestión de claves criptográficas.
Gestión de incidentes de seguridad de la información	os para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Impacto	Costo de un incidente.
Integridad	Propiedad de la información relativa a su exactitud y completitud.
No conformidad	Incumplimiento de un requisito.
RSI	Responsable de Seguridad de la Información.
Proceso	Actividades sucesivas de elaboración y transformación aplicadas vinculadas a personas y activos de información de la empresa.
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Selección de controles	Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
SGSI	Sistema de Gestión de la Seguridad de la Información: es un conjunto de políticas de administración de la información adaptándose a los cambios internos de la organización, así como los externos del entorno.
Tratamiento de riesgos	Modificar el riesgo mediante la implementación de controles.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Tabla 1: Definiciones

Pol 02 - Política de Gestión de Incidentes de Seguridad de la Información

1.- Objetivo

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información en el organismo, con el fin de prevenir y mitigar el impacto de estos.

El objetivo principal de esta política es contar con un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información.

Los objetivos de esta política son:

- Definir roles y responsabilidades dentro del organismo, como eje puntual para evaluar los riesgos y que se permita mantener la operación, la continuidad y la disponibilidad del servicio.
- Gestionar los eventos de seguridad de la información desde su detección, con el fin de identificar si se requiere clasificarlos como incidentes de seguridad de la información.
- Permitir identificar los incidentes de seguridad de la información para ser evaluados y dar respuesta de la manera más eficiente y adecuada.
- Minimizar el impacto adverso de los incidentes en el Organismo y sus operaciones, mediante la utilización de las salvaguardas adecuadas como parte de la respuesta a tal incidente.
- Consolidar las lecciones aprendidas que dejan los incidentes de seguridad de la información y su gestión para evitar la repetición de estos eventos. Con lo anterior, se reduce la ocurrencia de futuros incidentes, mejora la implementación y el uso de las salvaguardas y mejora el esquema global de la gestión de incidente de seguridad de la información
- Definir los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes de seguridad de la información, a través de

una base de conocimiento y registro de incidentes, y a través de los indicadores del Sistema de Gestión de Seguridad de la Información (SGSI).

- Definir los lineamientos para el procedimiento formal de reporte y escalamiento de los incidentes de seguridad de la información.
- Desarrollar un marco detallado para la clasificación y priorización de incidentes, vinculando directamente con los niveles de riesgo y los impactos sobre la confidencialidad, la integridad y la disponibilidad.
- Implementar un proceso formalizado de revisión y actualización de esta política que incluya evaluaciones periódicas basado en cambios tecnológicos y amenazas emergentes.
- Fortalecer las actividades de formación y concientización sobre la gestión de incidentes para todo el personal, asegurando que están actualizados sobre las últimas prácticas y procedimientos de seguridad.
- Integrar los procesos de gestión de incidentes con el SGSI, a los efectos de facilitar la gestión coordinada de la seguridad y mejorar la coherencia en la aplicación de políticas y procedimientos de seguridad.
- Establecer métricas claras y KPIs para evaluar la efectividad de la gestión de incidentes y su impacto en la seguridad general de la información.
- Reforzar la gestión de cambios post-incidentes para garantizar que las lecciones aprendidas se implementen efectivamente en el mejoramiento continuo del SGSI.

1.1.- VIGENCIA

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- VALIDEZ Y GESTIÓN DOCUMENTAL

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo que tenga legítimo acceso a los sistemas informáticos del organismo, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

3.- Responsabilidades

El Directorio del organismo es responsable por difundir la presente política a todo el personal, independientemente del cargo que desempeñe.

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política, y reportar los eventos de seguridad que detecte al RSI, siguiendo los procedimientos operativos establecidos para tal fin.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos

5.- Descripción

5.1.- Declaración Y Notificación De Incidentes

Un incidente de seguridad de la información se define como cualquier acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de la información. También incluye cualquier interrupción en la operación normal de redes, sistemas o recursos informáticos, o una violación de una de las Políticas de Seguridad del organismo.

La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades, minimizando la pérdida de información, la interrupción de los servicios, el

proceso de tratamiento de incidentes y que se manejen correctamente los aspectos disciplinarios y legales que pudieran surgir durante este proceso.

Algunos ejemplos de incidentes:

- Pérdida de información que comprometa la confidencialidad, integridad y disponibilidad
- Un acceso no autorizado
- El robo de contraseñas
- Prácticas de Ingeniería Social
- La utilización de fallas en los procesos de autenticación para obtener accesos indebidos
- El robo de información
- El borrado de información de terceros
- La alteración de la información de terceros

Para lograr los objetivos, la gestión de incidentes de seguridad de la información involucra los siguientes procesos de manera cíclica como lo muestra la siguiente imagen:



Figura 1 – Ciclo de vida para la respuesta a incidentes de seguridad de la información según el NIST (Instituto Nacional de Estándares y Tecnología de los Estados Unidos)

- Planificación y Preparación para la Gestión del Incidente
- Detección y Análisis
- Contención, Erradicación y Recuperación

- Actividades Post-Incidentes

El organismo debe generar un equipo de atención de incidentes de seguridad (CSIRT), quiénes se encargarán de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargarán de:

- Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.
- Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.
- Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.
- Anuncios de Seguridad: Debe mantener informados a los funcionarios, proveedores o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática, a través de algún medio de comunicación (web, Intranet, correo).
- Auditoría y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- Certificación de productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- Configuración y Administración de Dispositivos de Seguridad Informática: Se encargarán de la administración adecuada de los elementos de seguridad informática.
- Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- Investigación y desarrollo: Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.

Este grupo está enfocado principalmente en atender los incidentes de seguridad de la información que se presentan sobre los activos soportados por la plataforma tecnológica.

6.- Gestión de Incidentes

6.1.- Preparación

En esta etapa dentro del ciclo de vida de respuesta a incidentes se debe crear un modelo que permita a el Organismo estar en capacidad de responder a los incidentes, y así mismo, velar por que los mismos puedan ser detectados, evaluados y gestionar las vulnerabilidades, para prevenir la ocurrencia y la mitigación de estas, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros.

La etapa de preparación debe ser apoyada por la Dirección de TIC, y la misma debe incluir las mejores prácticas para el aseguramiento de redes, sistemas y aplicaciones, por ejemplo:

- **Gestión de Parches de Seguridad:** Se debe contar con un programa de gestión de vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, Otro Software Instalado), este programa ayudará a los administradores en la identificación, adquisición, prueba e instalación de los parches.
- **Aseguramiento de la infraestructura:** Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben evitar configuraciones por defecto (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el registro de eventos.
- **Seguridad en redes:** Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como Firewalls deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red

deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis y correlación.

- Prevención de código malicioso: Todos los equipos de la infraestructura (servidores y equipos de usuarios) deben tener activo su antivirus, antimalware con las firmas de actualización al día.
- Sensibilización y entrenamiento de usuarios: Los usuarios, incluidos los administradores, deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad. Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos.
- Establecer métricas claras y KPIs: A los efectos de medir la efectividad de la gestión de incidentes y evaluar su impacto en la seguridad de la información.

Estas actividades buscan prevenir la ocurrencia de incidentes de seguridad de la información. Adicionalmente será necesario realizar revisiones periódicas para confirmar la efectividad de dichas actividades.

6.1.1.- Recursos de Comunicación

Los elementos necesarios para la comunicación del equipo de atención de incidentes.

Información de Contacto: Se debe tener un alista de información de contactos de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.

Información de Escalamiento: Se debe contar con información de contacto para el escalamiento de incidentes según la estructura del Organismo:

Información de los administradores de la plataforma tecnológica (Servicios, Servidores, etc.).

- Contacto con el área de recursos humanos.

- Contacto con áreas interesadas o grupos de interés (AGESIC, URCDP, Policía, etc.)

Política de Comunicación: Se debe contar con una política de comunicación de los incidentes de seguridad para definir que incidente puede ser comunicado a los medios y cual no.

6.1.2.- Hardware y Software

Para una correcta y eficiente gestión de incidentes el Organismo debería tener en cuenta los siguientes elementos:

- Portátiles Forenses
- Analizadores de protocolos
- Software de adquisición
- Software de recolección de evidencias
- Kit de respuesta a incidentes
- Software de análisis forense
- Medios de almacenamiento

6.1.3.- Recursos para el Análisis de Incidentes

Al momento de la realización del análisis del incidente, se debe disponer de:

- Listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Diagrama de red para tener la ubicación rápida de los recursos existentes.
- Una línea base de información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios). Esta información siempre debe estar actualizada para poder conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Un análisis del comportamiento de red estándar y que es recomendable que incluya: puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

6.1.4.- Recursos para la Mitigación y Remediación

Se deben considerar los elementos básicos para la contención de un posible incidente, respaldo de información, imágenes de servidores, y cualquier información base que pueda recuperar el funcionamiento normal del sistema.

6.2.- Detección, Evaluación y Análisis

6.2.1.- Detección, Identificación y Gestión de Elementos Indicadores de un Incidente

Se debe detectar, identificar y gestionar los incidentes de acuerdo con los indicadores de los eventos, los que señalan que posiblemente un incidente ha ocurrido.

La identificación y gestión de elementos que alertan sobre un incidente nos proveen información que puede alertarnos sobre la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto.

Algunos de estos elementos pueden ser:

- Alerta en sistema de seguridad
- Caídas de enlaces
- Caídas de servidores
- Reportes de actividad de usuarios en la red
- Reportes del software antivirus
- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad

6.2.2.- Análisis

Las actividades de análisis del incidente involucran otra serie de componentes, es recomendable tener en cuenta los siguientes:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Los administradores de infraestructura deben tener conocimiento total sobre los comportamientos de la infraestructura que están administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).
- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.
- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (Sincronización de Relojes) ya que esto facilita la correlación de eventos y el análisis de información.
- Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores.
- Crear matrices de diagnóstico e información para los administradores menos experimentados.

6.2.3.- Evaluación

Para realizar la evaluación de un incidente de seguridad se debe tener en cuenta los niveles de impacto con base en los insumos entregados por el análisis de riesgos y la clasificación de activos de información.

6.2.3.1.- Niveles de Impacto

La severidad del incidente puede ser:

- Alto Impacto: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos del Organismo. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

- Medio Impacto: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.
- Bajo Impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

6.2.3.2.- Clasificación de Incidentes

Algunos ejemplos de clasificación de incidentes podrían ser (esta clasificación está sujeta a los criterios que defina el organismo dependiendo de la infraestructura, de los riesgos y criticidad de los activos. La clasificación dada es solo un ejemplo).

- Acceso no autorizado: Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.
- Modificación de recursos no autorizado: Un incidente que involucra a una persona, sistema o código malicioso que afecta a la integridad de la información o de un sistema de procesamiento.
- Uso inapropiado de recursos: Un incidente que involucra a una persona que viola alguna política de uso de recursos.
- No disponibilidad de los recursos: Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.
- Multicomponente: Un incidente que involucra más de una categoría anteriormente mencionada.
- Otros: Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías.

6.2.3.3.- Priorización de los Incidentes y Tiempos de Respuesta

Con el fin de permitir una atención adecuada a los incidentes (análisis, contención y erradicación) se debe determinar el nivel de prioridad del mismo, y de esta manera atenderlos adecuadamente según la necesidad.

A manera de ejemplo se definen una serie de variables que podrán ser utilizadas para realizar la evaluación de los incidentes.

- Prioridad
- Criterio de impacto
- Impacto actual
- Impacto futuro

Nivel de Prioridad: Depende del valor o importancia dentro de la entidad y del proceso que soporta el o los sistemas afectados.

Nivel Criticidad	Valor	Definición
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso
Medio	0,50	Sistemas que apoyan más de una dependencia o proceso
Alto	0,75	Sistemas pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas
Superior	1,00	Sistemas críticos

Tabla 1 – Niveles de Criticidad de Impacto

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que puede causar el incidente si no es contenido, ni erradicado.

Nivel Impacto	Valor	Definición
Inferior	0,10	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo
Medio	0,50	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información
Superior	1,00	Impacto alto en uno o más componentes de más de un sistema de información

Tabla 2 – Niveles de Impacto Actual y Futuro

Impacto Actual: Depende de la cantidad de daño que ha provocado el incidente en el momento de ser detectado.

Impacto Futuro: Depende de la cantidad de daño que puede causar el incidente si no es contenido, ni erradicado.

Luego de tener definidas las variables se obtiene la prioridad mediante la siguiente fórmula:

$$\text{Nivel Prioridad} = (\text{Impacto actual} * 2,5) + (\text{Impacto futuro} * 2,5) + (\text{Críticidad del sistema} * 5)$$

Y los resultados obtenidos se deben comparar con la siguiente tabla para determinar la prioridad de atención:

Nivel Prioridad	Valor
Inferior	00,00 – 02,49
Bajo	00,25 – 03,74
Medio	00,50 – 04,99
Alto	00,75 – 07,49
Superior	07,50 - 10,00

Tabla 3 – Niveles de Prioridad del Incidente

6.2.3.4.- Priorización de los Incidentes y Tiempos de Respuesta

Para el caso de la atención de incidentes de seguridad se ha establecido unos tiempos máximos de atención de los mismos, con el fin de atender adecuadamente los incidentes de acuerdo a su criticidad e impacto. Los tiempos expresados en la siguiente Tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Nivel Prioridad	Tiempo de Respuesta
Inferior	3 horas
Bajo	1 hora
Medio	30 minutos
Alto	15 minutos
Superior	5 minutos

Tabla 4- Tiempos Máximos de Atención de Incidente

Cabe resaltar que cada entidad está en la libertad de definir tiempos de atención a incidentes como crean conveniente y dependiendo de la criticidad de los activos impactados.

6.3.- Contención, Erradicación Y Recuperación

Es importante para el Organismo implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

En algunas ocasiones puede ser necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.

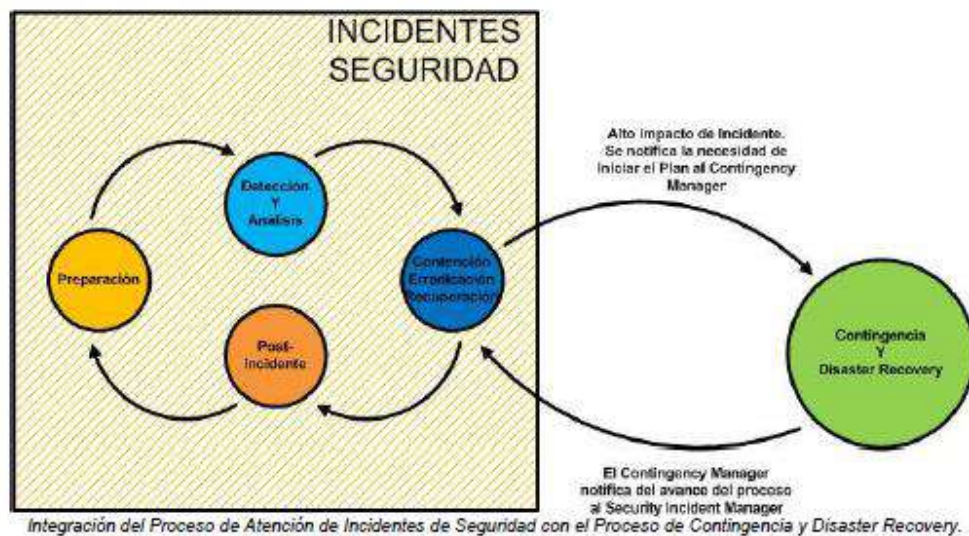


Figura 2 - Integración de; Proceso de Atención de Incidentes de Seguridad con el Proceso de Contingencia y Recuperación de Desastres.

6.3.1.- Contención

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Es importante para el organismo implementar una estrategia que permita tomar decisiones oportunamente.

Esta actividad busca la detección del incidente con el fin de que no se propague y pueda genera más daños a la información o a la arquitectura de TI, para facilitar esta tarea se debe poseer una estrategia de contención previamente definida para poder tomar decisiones, por ejemplo; apagar sistema, desconectar red, deshabilitar servicios.

Ejemplos de estrategias de contención a incidentes:

Incidente	Ejemplo	Estrategia de contención
Acceso no autorizado	Sucesivos intentos fallidos de login	Bloqueo de cuentas
Código Malicioso	Infección con virus	Desconexión de la red del equipo afectado
Acceso no autorizado	Compromiso del ROOT	Apagado del sistema
Reconocimiento	Scanning de puertos	Incorporación de reglas de filtrado en el firewall

Tabla 5 - Ejemplos de estrategias de contención a incidentes

La estrategia de contención varía según el tipo de incidente y los criterios deben estar bien documentados para facilitar la rápida y eficaz toma de decisiones.

Algunos criterios que pueden ser tomados como base son:

- Criterios forenses
- Daño potencial y hurto de activos
- Necesidades para la preservación de evidencia
- Disponibilidad de servicio
- Tiempo y recursos para implementar la estrategia
- Efectividad de la estrategia para contener el incidente (parcial o total)
- Duración de la solución

6.3.2.- Erradicación y Recuperación

Después de que el incidente ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente como código malicioso y posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados para lo cual el Director de Infraestructura o quién haga sus veces deben restablecer la funcionalidad de los sistemas afectados, y realizar un endurecimiento del sistema que permita prevenir incidentes similares en el futuro.

Ejemplos de estrategias de erradicación de incidentes:

Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Tabla 6 - Ejemplos de estrategias de erradicación a incidentes

Ejemplos de estrategias de recuperación de incidentes:

Incidente	Ejemplo	Estrategia de erradicación
DoS (denegación de servicio)	SYN Flood	Restitución del servicio caído
Virus	Gusano en la red	Corrección de efectos producidos. Restauración de backups
Vandalismo	Defacement a un sitio web	Reparar el sitio web
Intrusión	Instalación de un rootkit	Reinstalación del equipo y recuperación de datos

Tabla 7- Ejemplos de estrategias de recuperación a incidentes

6.4.- Actividades Post-Incidente

Las actividades Post-Incidente básicamente se componen del reporte apropiado del incidente, de la generación de lecciones aprendidas, del establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias, así como el registro en la base de conocimiento para alimentar los indicadores.

Reforzar la gestión de cambios post-incidente para asegurar que las lecciones aprendidas se implementen efectivamente en el mejoramiento continuo del SGSI.

6.4.1.- Informe del Incidente

Una vez atendido y solucionado el incidente, se debe estructurar el informe de la siguiente manera:

- Resumen ejecutivo: Relata lo sucedido de forma clara y concisa, sin terminología técnica.
- Línea de tiempo del incidente: Describe lo sucedido, paso a paso, según la bitácora de incidentes.
- Datos del entorno.
- Gestión del incidente: Describe las acciones realizadas para responder al incidente.
- Análisis forense: Describe los procedimientos forenses realizados para poder explicar el incidente (pueden ir como un anexo al informe).
- Impacto del incidente: Describe el impacto del incidente (datos perdidos, equipos afectados, daños causados, etc.).
- Atribución: Debe indicar (en la medida de lo posible) qué o quién ha podido ser el causante del incidente.
- Recomendaciones de seguridad: Descripción de las medidas a ser tomadas para evitar que este incidente no se repita.
- Lecciones aprendidas: Descripción de qué se hizo bien, qué se hizo mal, y qué acciones se deben tomar para hacerlo mejor en el próximo incidente.
- Anexo: Lista de evidencias (todo aquello que por su extensión no tiene cabida en la gestión del incidente).

Teniendo en cuenta lo anterior, existen tipos de informes que deben estar contemplados dentro del diligenciamiento de la bitácora y la gestión del incidente:

- Informe de detección: Informe dirigido a los responsables técnicos, en el que se describe brevemente sobre lo que se sabe del incidente hasta el momento, estimando los sistemas afectados y el impacto. El objetivo es iniciar la respuesta ante el incidente, dando prioridad a la rapidez sobre la exactitud.
- Informes “de campo”: Son actualizaciones del informe de detección, resumiendo las acciones tomadas por el equipo de respuesta ante incidentes. A medida que se va avanzando en la respuesta estos informes tendrían que incrementar su exactitud (vamos sabiendo con más detalle lo sucedido).
- Informes de crisis: El objetivo es el mismo que los informes de batalla, pero la audiencia pasa a ser personal no técnico (dirección y/o legal). Prima la claridad del mensaje, y se debe de tener cuidado con lo que se dice (debe ser exacta la información).
- Informes de IoC (Indicadores de Compromiso): Son informes destinados a compartir inteligencias con otros departamentos o entidades. En muchos casos están anonimizados (sin información de origen), y constan de una breve introducción y de un listado de IoC para que sean comprobados por los destinatarios.

6.4.2.- Lecciones Aprendidas

Una de las partes más importantes de un plan de respuesta a incidentes es la de aprender y mejorar. Cada equipo de respuesta a incidentes debe evolucionar para reflejar las nuevas amenazas, la mejora de la tecnología, y las lecciones aprendidas. Mantener un proceso de “lecciones aprendidas” después de un incidente grave, y periódicamente después de los incidentes menores, es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes.

Mantener un adecuado registro de lecciones aprendidas permite conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.

- Los procedimientos documentados.
- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.
- Cuáles herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

El proceso de lecciones aprendidas puede poner de manifiesto la falta de un paso o una inexactitud en un procedimiento y son un punto de partida para el cambio, y es precisamente debido a la naturaleza cambiante de la tecnología de la información y los cambios en el personal, que el equipo de respuesta a incidentes debe revisar toda la documentación y los procedimientos para el manejo de incidentes en determinados intervalos.

7.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 03 - Política de Uso Aceptable de Activos

1.- Objetivo

El organismo dispone de un conjunto de activos de información tales como equipos (por ejemplo, PCs, laptops, medios de almacenamiento, dispositivos móviles, etc.), el acceso a Internet, las aplicaciones, documentación y los servicios de mensajería electrónica para el normal desempeño de sus actividades profesionales.

El organismo entiende necesario establecer una política que regule la forma en que dichos activos deben ser utilizados, y garantizar que nuestros colaboradores, empleados, personal contratado y proveedores del mismo, comprendan que los activos de información antes mencionados son exclusivamente para fines laborales.

Se pretende que cada lector de este documento conozca las pautas y tome los recaudos necesarios para proteger los activos de información del organismo.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo que hace uso de activos de información para desempeñar sus responsabilidades laborales.

Todos los proveedores que hacen uso de activos de información del organismo para desarrollar la atención y los requisitos relacionados con sus propios servicios.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Uso de Redes Sociales
- Política de Uso de Internet
- Política de clasificación de la información
- Política de Uso Aceptable de Dispositivos Móviles
- Política de escritorio y pantalla limpios
- Política de destrucción de la información

5.- Uso Aceptable De Los Activos De Información

El organismo debe pautar los lineamientos de uso de los activos de información tales como correo electrónico, aplicaciones, equipos, recursos de comunicación, uso de Internet, uso de redes sociales, entre otros y establecer los controles que realizará y las responsabilidades de los usuarios.

Se deberán implementar los controles necesarios en función de la evaluación de riesgo realizado al tipo de activo que se compartirá por parte del organismo, basándose en la Política de Gestión de Riesgos, y de acuerdo con lo estipulado en el Sistema de Gestión de Seguridad de la Información, basándose en la norma ISO-IEC 27001:2022.

Se documentarán y reforzarán los mecanismos de control y monitoreo para prevenir y detectar usos no autorizados o contrarios a la política aquí establecida.

Se implementarán indicadores de rendimiento clave para monitorear la efectividad de la política de uso aceptable y evaluar el cumplimiento de los usuarios.

Desarrollar y documentar un programa formal de capacitación y concientización que incluya aspectos específicos relacionados con el uso de los activos, y los riesgos involucrados.

El personal del organismo y/o los proveedores, deben:

- Usar los equipos y recursos de comunicación del Organismo para los fines exclusivos de éste y dentro de los lineamientos de seguridad y demás requisitos establecidos.
- Respetar la normativa vigente.
- Proteger las cuentas y/o contraseñas, no permitiendo a otras personas usar las mismas bajo ningún concepto.
- Cumplir con los procedimientos de seguridad de la información para proteger la información sensible y el tratamiento de datos en el organismo.

Dentro de sus oficinas y áreas de trabajo, el organismo provee a todos sus usuarios y colaboradores los recursos (PCs, acceso a Internet, correo electrónico, conexiones seguras, claves de acceso, etc.) de acuerdo con lo necesario para desempeñar sus responsabilidades y las tareas que se les asigna.

En ese contexto, todas las herramientas y servicios ofrecidos podrán ser controlados y monitoreados.

6.- Uso Prohibido

El uso de cualquier PC, laptop, medio de almacenamiento de datos, etc., de uso personal dentro de las áreas de trabajo y operación del Organismo debe estar autorizado.

Los usuarios no deberán utilizar los servicios de Internet o de correo electrónico del organismo para ver, descargar, guardar, recibir o enviar material relativo a, o incluyendo:

- Aplicaciones no licenciadas
- Material pornográfico
- Fomentar cualquier tipo de discriminación

- Comportamiento amenazante o violento
- Actividades ilegales
- Juegos de apuestas
- Reenvío de “cadenas” por correo electrónico
- Envíos masivos de correos electrónicos no solicitados desde una cuenta del organismo o desde equipos de la empresa

7.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Dirección del organismo, a través de Capital Humano podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 04 - Política de Intercambio y Traslado Físico de la Información

1.- Objetivo

Establecer los criterios sobre la protección de la información cuando la misma es objeto de traslado o intercambio por medios físicos como papel, medios magnéticos de almacenamiento o cualquier otro medio tangible conocido o por conocer, que oficie de contenedor de dicha información; así como la información contenida en medio lógicos; debiendo velar en todo momento por la cadena de custodia.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Toda la información más allá de su clasificación, de su propietario, que se encuentre bajo la custodia y responsabilidad del organismo, y que en el accionar del mismo, sea objeto de manipulación, traslado o intercambio por medios físicos.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Personal del organismo y/o proveedores deben cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Uso de Controles Criptográficos
- Política de Control de Acceso Lógico

5.- Descripción

El organismo debe:

- Definir controles y procedimientos para asegurar la protección de la información durante su intercambio. En particular, se deberá establecer un procedimiento formal que describa las actividades necesarias para el traslado físico de información
- Establecer acuerdos de no divulgación con el personal, clientes y proveedores externos que por diversas razones requieran conocer o intercambiar información restringida o confidencial del organismo
- Establecer acuerdos de intercambio de información (incluyendo la trazabilidad, el no repudio, etiquetado, cadena de custodia, control de acceso) para intercambiar información entre las diferentes áreas del organismo, y proveedores
- La información transmitida por correo electrónico desde y hacia direcciones pertenecientes a el organismo o sus clientes debe estar protegida
- Implementar evaluaciones de riesgo específicas para cada tipo de información y medio de traslado, identificando y analizando las vulnerabilidades y amenazas potenciales.
- Establecer procedimientos formales para la documentación y el seguimiento de la cadena de custodia, incluyendo registros digitales seguros y verificables.
- Establecer planes de formación y concientización sobre la política de traslado de información para todo el personal, enfatizando la identificación de riesgos y respuestas adecuadas ante incidentes.
- Implementar tecnologías de cifrado avanzado para todos los traslados de información, especialmente cuando se manejan datos confidenciales, o críticos, basado en la evaluación de riesgos.
- Refinar los procedimientos de control de acceso para incluir autenticación y verificación robusta, aplicables especialmente a información sensible o

confidencial, asegurando que solo las personas autorizadas puedan acceder a la información durante su traslado, protegiendo contra accesos no autorizados.

El medio en el cual se traslade la información, física o lógica, debe garantizar su integridad durante todo el tiempo que insuma el traslado de la información, siempre en la medida razonable en relación al carácter de la información contenida y su clasificación.

Si así lo requiere la información contenida, el medio debe garantizar la reserva o confidencialidad de ésta, incluso ante la o las personas que efectúen el traslado o manipulación.

Atento al carácter de la información, de acuerdo a su clasificación, el medio debe resguardar el acceso a la misma durante el traslado o manipulación. El medio debe proporcionar información básica suficiente que haga inequívoca la identificación de lo que contiene y el asunto o tema que involucra el contenido.

En lo que se refiere a información en soporte físico, se deberá detallar de forma clara y comprensible, el remitente y destinatario, sean estas personas físicas o jurídicas, así como fecha completa de envío y hora si corresponde, por ejemplo, a efectos de requerimientos jurídicos.

6.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento la Dirección del organismo, a través del Departamento de Personal, podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 05 - Política de Control de Acceso Lógico

1.- Objetivo

Para acceder a los sistemas informáticos del organismo se requerirá del uso de una identificación de usuario y de una contraseña.

El objetivo de esto documentos es establecer las reglas para el acceso a los diversos sistemas, equipos, instalaciones e información, de acuerdo con los requisitos de acceso funcional y de seguridad.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez Y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo que accede a los sistemas informáticos, equipos, instalaciones e información gestionados por el organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Clasificación de la Información

5.- Control de Acceso

5.1.- Introducción

El acceso a todos los sistemas informáticos, redes, equipos, e información gestionados por el organismo está prohibido, a menos que se permita expresamente a usuarios individuales o grupos de usuarios.

El acceso a todas las áreas físicas del organismo está permitido, excepto a las áreas para las cuales se requiere un acceso privilegiado otorgado por una persona autorizada.

Esta política especifica las reglas para el acceso a los sistemas, servicios e instalaciones, mientras que la Política de Clasificación de la Información define las reglas para el acceso a los documentos y registros individuales.

5.2.- Matriz de Control de Acceso

Se deberá establecer una matriz de control de acceso que especifique que usuarios o grupos de usuarios tienen asignados accesos a cada recurso, y con qué permisos se pueden realizar dichos accesos.

La responsabilidad de la asignación de los permisos de acceso será de los propietarios de cada sistema o instalación, y podrán estar sujetos a las recomendaciones de seguridad según corresponda.

Se adoptará e implementarán sistemas de autenticación de múltiples factores para el acceso a todos los sistemas y recursos críticos, complementando la actual política de gestión de usuario y contraseña.

5.3.- Revisión Periódica De Los Derechos De Acceso

Los derechos de acceso otorgados a los usuarios deberán ser revisados en forma periódica, a los efectos de verificar que los mismos se ajusten a los requisitos del organismo y de la seguridad.

Los propietarios de cada sistema o instalación son los responsables de realizar dicha revisión, con la frecuencia que se establezca para cada caso.

Los resultados de las revisiones deben ser presentadas y quedar registradas en la CSI.

5.4.- Cambio de Estado o Rescisión de Contrato

Cuando se produzca un cambio de función o la finalización de la vinculación con el organismo, el Departamento de Personal deberá notificar de manera inmediata a los responsables de gestionar los privilegios asignados al colaborador en cuestión.

Del mismo modo, cuando se modifiquen las relaciones contractuales con partes externas que tengan acceso a sistemas, servicios o instalaciones, o al vencimiento del contrato, el propietario del contrato deberá informar de manera inmediata a los responsables de gestionar los privilegios asignados a dichas partes externas.

Los derechos de acceso de todas las personas que hayan cambiado de función, vinculación con el organismo o relación contractual deberán ser eliminados o modificados de manera inmediata por los responsables de gestionar los privilegios asignados, conforme a lo establecido en el siguiente apartado.

5.5.- Gestión de Acceso de Usuarios

Los usuarios únicamente podrán acceder a los recursos para los que hayan sido debidamente autorizados.

El acceso deberá cumplir con el principio de “Privilegio Mínimo”, el cual establece que cada usuario solo debe tener acceso a la información y recursos estrictamente necesarios para cumplir con su propósito legítimo.

Las solicitudes de acceso lógico deberán ser realizadas por el interesado o por el responsable del sector correspondiente, mediante la creación de un ticket en el Sistema de Gestión.

Si la solicitud es realizada directamente por el interesado, se requerirá la justificación de la necesidad del acceso por parte del responsable del sector.

Todas las solicitudes deberán especificar el nombre del usuario, el rol y los permisos solicitados.

Cualquier modificación posterior a los accesos a los sistemas de información deberá gestionarse a través de la creación de un nuevo ticket en el Sistema de Gestión.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 06 - Política de Gestión de Usuarios y Contraseñas

1.- Objetivo

Para acceder a los sistemas informáticos del organismo se requerirá del uso de una identificación de usuario y de una contraseña.

El objetivo de este documento es establecer las reglas necesarias para garantizar la administración segura de las contraseñas y del uso seguro de las mismas.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez Y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo que accede a los sistemas informáticos o sectores restringidos, que requieren el uso de identificación de usuario y de su contraseña correspondiente.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Control de Acceso Lógico

5.- Obligaciones del Usuario

Los usuarios deben aplicar buenas prácticas de seguridad al seleccionar y utilizar contraseñas:

- Las contraseñas no deben ser reveladas a otras personas, incluyendo supervisores y administradores de sistemas.
- Las contraseñas no deben anotarse, a menos que un método seguro haya sido aprobado por la Comisión de Seguridad de la Información (CSI).
- Las contraseñas generadas por los usuarios no deben distribuirse a través de ningún canal (utilizando la distribución oral, escrita o electrónica, etc.).
- Las contraseñas deben cambiarse si hay indicios de que las mismas o el sistema pueden haber sido comprometido - en ese caso debe ser reportado un incidente de seguridad.
- Se deben seleccionar contraseñas seguras, de la siguiente manera:
 - utilizar al menos 10 caracteres
 - utilizar al menos un carácter numérico
 - utilizar al menos una letra en mayúscula
 - utilizar al menos una letra en minúscula
 - utilizar al menos un carácter especial
 - una contraseña no debe ser una palabra del diccionario o jerga de cualquier idioma, o cualquiera de estas palabras escritas hacia atrás
 - las contraseñas no deben basarse en datos personales (por ejemplo, fecha de nacimiento, dirección, nombre del miembro de la familia, etc.)
 - las tres últimas contraseñas no deben ser reutilizadas
- Las contraseñas deben cambiarse al menos una vez cada 3 meses.
- La contraseña debe cambiarse al primer inicio de sesión en un sistema.

- Las contraseñas no deben almacenarse en un sistema de registro automatizado (por ejemplo, macro o navegador).
- Las contraseñas utilizadas con fines personales no deben utilizarse para fines laborales.

6.- Gestión de Contraseñas de Usuario

Al asignar y usar contraseñas de usuario, deben seguirse las siguientes reglas:

- Al firmar el Acuerdo de Confidencialidad, los usuarios también aceptan la obligación de mantener confidenciales las contraseñas, según lo prescrito en este documento.
- Cada usuario puede utilizar solo su propio nombre de usuario asignado de forma exclusiva.
- Cada usuario debe tener la opción de elegir su propia contraseña, cuando corresponda
- La contraseña temporal utilizada para el primer inicio de sesión del sistema debe ser única y fuerte, como se prescribió anteriormente.
- Las contraseñas temporales deben ser comunicadas al usuario de manera segura y la identidad del usuario debe ser previamente verificada.
- El sistema de gestión de contraseñas debe requerir al usuario que cambie la contraseña temporal al iniciar la sesión en el sistema.
- El sistema de gestión de contraseñas debe obligar al usuario a seleccionar contraseñas seguras.
- El sistema de gestión de contraseñas debe requerir que los usuarios cambien sus contraseñas al menos una vez cada 3 meses.
- Si el usuario solicita una nueva contraseña, el sistema de gestión de contraseñas debe determinar la identidad del usuario.
- La contraseña no debe ser visible en la pantalla durante el inicio de sesión.
- Sí un usuario introduce una contraseña incorrecta cinco veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión por un lapso tiempo
- Las contraseñas creadas por el fabricante del software o hardware deben cambiarse durante la instalación inicial.

- Los archivos que contengan contraseñas deben almacenarse por separado de los datos del sistema de la aplicación.
- Las contraseñas tienen carácter de información CONFIDENCIAL de acuerdo con la política de clasificación de información vigente.
- Las excepciones a la presente política deben ser aprobados por la CSI y mantenerse registro de dichas excepciones.

7.- Gestión Avanzada

Se deberá integrar la autenticación multifactor (MFA) como un requisito estándar para el acceso a todos los sistemas críticos, complementado el uso de nombre de usuario y contraseña.

Se deberá implementar, en la medida de lo posible, herramientas de gestión de contraseñas que faciliten la creación, almacenamiento y recuperación segura de contraseñas.

Establecer un proceso de revisión y actualización regular de las características de las contraseñas, que considere las últimas vulnerabilidades y amenazas, ajustando los requerimientos de complejidad y rotación de contraseñas según sea necesario.

Desarrollar un plan de formación y concientización continua para todos los usuarios sobre la importancia de las prácticas seguras de gestión de contraseñas.

8.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 07 - Política de Gestión de Usuarios de Acceso

Privilegiado

1.- Objetivo

Definir una adecuada gestión de las cuentas de usuario privilegiado del organismo, como forma de prevenir los riesgos ocasionados por el uso de permisos privilegiados.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez Y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo involucrado en la gestión y uso de cuentas de usuario privilegiado.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de TIC deberá habilitar los recursos para instrumentar esta política.

El personal del organismo con usuario privilegiado deberá responder directamente por las operaciones y transacciones que se ejecuten con las cuentas de usuario asignadas bajo su responsabilidad.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Gestión de Usuario y Contraseña
- Política de Control de Acceso Lógico

5.- Descripción

El organismo debe contar con procedimientos formalmente definidos y documentados que cubran los siguientes puntos:

- Altas, bajas y modificaciones de usuarios y derechos de acceso lógico.
- Altas, bajas y modificaciones de usuario con acceso privilegiado (gestión y autorización).
- Asignación, uso y revocación de cuentas de usuario privilegiado (gestión técnica).
- Autorizaciones de acceso lógico.
- Revisión de los derechos de acceso lógico.
- Procedimiento de gestión de las cuentas administradoras de los diferentes sistemas, las que deberán permanecer guardadas, bajo la custodia correspondiente, y se deberá llevar registro de la solicitud, uso y devolución de la misma.

La solicitud de una cuenta de usuario privilegiado debe estar acompañada por una justificación de necesidad de uso, y ser autorizada formalmente por el Director de TIC.

La solicitud debe cumplir con lo establecido en el procedimiento para alta, baja y modificación de usuarios con acceso privilegiado.

Las cuentas de usuario privilegiado sólo deben ser otorgadas al personal de nivel técnico apropiado y únicamente para el cumplimiento de sus funciones.

Los accesos realizados con cuentas de usuario privilegiados deben ser registradas y controladas periódicamente.

Una cuenta de usuario privilegiado sólo podrá ser utilizada en la actividad de administración o configuración del sistema para el cual se requieren dichos privilegios.

No podrá ser utilizada en actividades rutinarias para la que existe un perfil de menores privilegios que lo permita.

Las cuentas de usuario privilegiado tipo ADMIN; ROOT, o similares, definidas por defecto, en sistemas y componentes, no pueden ser usadas, salvo necesidad expresa.

Siempre que sea posible las mismas deben ser eliminadas o deshabilitadas, además de modificadas sus contraseñas por defecto.

Se debe contar con un mecanismo de recuperación de acceso privilegiado, siempre que sea posible, y dicho mecanismo debe mantener las garantías de reserva.

El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.

Se deberá implementar tecnologías de monitoreo en tiempo real y análisis de comportamiento para identificar y alertar sobre actividades sospechosas o no autorizadas realizadas por cuentas de acceso privilegiado.

Establecer un protocolo de autorización de dos pasos para la activación de cuentas privilegiadas, asegurando que cada uso de una cuenta privilegiada sea justificado, registrado y aprobado por más de una persona autorizada.

Desarrollar un programa de capacitación específico para los usuarios con acceso privilegiado, enfocado en las mejores prácticas de seguridad, riesgos asociados al mal uso de estos accesos y las responsabilidades legales que conlleva.

Revisar y actualizar periódicamente esta política para adaptarse a los cambios tecnológicos y a las nuevas amenazas de seguridad, asegurando que las medidas de control sean efectivas y actuales.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 08 - Política de Control de Acceso Físico a Áreas Seguras

1.- Objetivo

Establecer los lineamientos generales para controlar el acceso físico a las áreas seguras del organismo, con el objetivo de minimizar el riesgo de accesos no autorizados.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo, proveedores, visitantes, etc. que necesiten acceder a áreas seguras y tengan la autorización correspondiente.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de TIC es responsable por otorgar los recursos necesarios para el cumplimiento de la presente política.

El Director de Infraestructura es el responsable de asignar los accesos permanentes y temporales al centro de datos.

El personal del Departamento de Infraestructura es responsable de gestionar el control de acceso al área segura y comunicar las asignaciones de los roles entre todas las

partes interesadas. Es responsable del registro y acompañamiento de los visitantes y de la revisión de las actividades que se realizan en el centro de datos.

El personal con acceso a otras áreas seguras es responsable de controlar los accesos a dichas áreas, así como realizar el acompañamiento de los visitantes y controlar las actividades que se llevan a cabo en dichas áreas.

Todo el personal del organismo y los proveedores son responsables de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Control de Acceso Lógico

5.- Descripción

Se debe contar con un procedimiento formal para gestionar y revisar periódicamente los accesos a las áreas seguras.

El acceso a las áreas seguras deberá ser concedido únicamente por motivos específicos y autorizados.

5.1.- Áreas Seguras

El organismo mantendrá controles de seguridad básicos, como cerraduras en puertas exteriores y un sistema de alarma, para asegurar los activos de diferentes zonas de seguridad dentro de las instalaciones.

Las zonas de seguridad incluyen:

- Público: Esto incluye áreas del edificio u oficina que estén destinadas para el acceso público.
 - Restricciones de acceso: ninguna
 - Controles de seguridad adicionales: ninguno
 - Ejemplo: recepción principal

- Privado: Esto incluye las áreas del edificio u oficina que solo utilizan los empleados y otras personas autorizadas por el organismo.
 - Restricciones de acceso: solo el personal del organismo e invitados autorizados y acompañados
 - Controles de seguridad adicionales: se usarán controles de acceso adicionales, como pin, tarjetas de acceso, o dispositivos similares
 - Ejemplo: pasillos, oficinas privadas, áreas de trabajo, salas de reuniones, etc.
- Restringido: esto incluye áreas que están restringidas al uso de ciertas personas dentro del organismo por razones de seguridad o protección.
 - Restricciones de acceso: solo personal específicamente autorizado
 - Controles de seguridad adicionales: se deben usar controles de acceso adicionales, como pin, tarjeta de acceso o dispositivos similares. Deben mantenerse y revisarse los registros de acceso a estas áreas.
 - Ejemplo: centro de datos

5.2.- Controles De Acceso

Los controles de acceso son necesarios para restringir el ingreso a las instalaciones y zonas de seguridad del organismo solo a personas autorizadas. Se han identificado diversos controles, que se describen en esta sección, junto con las pautas para su uso.

- Llaves

El uso de llaves está prohibido como el único mecanismo de seguridad para el acceso a las zonas de seguridad designadas como restringidas. Este mecanismo de seguridad es el más económico y es el más familiar para los usuarios. La desventaja es que el organismo no tiene control, además de cambiar las cerraduras, sobre cómo y cuándo se usa el acceso. Las llaves se pueden copiar.

- Tarjetas de acceso

El organismo requiere que las tarjetas deben ser utilizadas para acceder a las zonas de seguridad designadas como privadas. Se debe considerar el uso de estos métodos para todas las zonas, aunque no es obligatorio.

Este método permite controlar adecuadamente los niveles de acceso.

En caso de pérdida o robo de una tarjeta, se desactivará de inmediato en el sistema de control de acceso. Lo mismo se aplica si un empleado termina su vínculo laboral, se deberá desactivar los accesos del usuario en forma inmediata.

- Teclado (PIN)

El organismo requiere que los ingresos a las zonas de seguridad designadas como restringidas sea mediante control de acceso por teclado con PIN único e individual. Este control se combina con las tarjetas de acceso ya que siempre se pasa por zonas privadas para acceder a las zonas restringidas. En caso de que un empleado termine el vínculo laboral, se deberá desactivar los accesos del usuario en forma inmediata.

5.3.- Gestión de Accesos

Los accesos de tipo permanente deben ser asignados por el Director de Infraestructura, a aquel personal que así lo requiera en base a requisitos basados en su función en el organismo.

Los accesos de tipo temporal, por ejemplo, para el caso de proveedores externos y contratistas, deben ser solicitados al responsable de accesos y autorizados por el responsable de seguridad de la información y se debe proveer al menos la siguiente información: nombre, apellido, cédula de identidad, empresa, fecha de inicio de acceso temporal, fecha fin de acceso temporal, motivo. Los visitantes temporales que requieran acceso a áreas seguras o a los centros de datos deberán permanecer acompañados de personal con permisos de acceso y portar una identificación visible.

En el caso del centro de datos, se debe registrar la visita en una bitácora de ingresos que deberá contener al menos la siguiente información: fecha, nombre, apellido, cédula de identidad, empresa, hora de entrada, hora de salida, nombre y apellido del funcionario que lo acompaña.

5.4.- Sistema de Control de Acceso

En relación con el acceso al centro de datos, se deberá cumplir con lo establecido a continuación.

- El acceso al centro de datos deberá realizarse mediante un sistema de autónomo de control de acceso, por ejemplo, con lectores de tarjetas magnéticas, identificación por radiofrecuencia (RFID) o sistemas biométricos.
- El sistema de control de acceso puede ser administrado remotamente y debe mantener información histórica de accesos al centro de datos.
- Se debe contar con un sistema cerrado de TV.

5.5.- Revisión de Accesos al Centro de Datos

Se debe establecer un procedimiento formal de revisión periódica y de auditorías independientes de los accesos al centro de datos que contemple la información del sistema de control de acceso, el registro de ingresos al centro de datos, el personal con acceso permanente y con acceso temporal, para asegurar la efectividad y la conformidad con las políticas de seguridad vigentes. Todas las solicitudes deberán especificar el nombre del usuario, el rol y los permisos solicitados.

Cualquier modificación posterior a los accesos a los sistemas de información deberá gestionarse a través de la creación de un nuevo ticket en el Sistema de Gestión.

5.6.- Medidas de Seguridad Interna

Se prohíbe el ingreso al centro de datos con material combustible, líquidos, productos volátiles, y todo producto o sustancia que pudiera ocasionar una reacción química perjudicial para la infraestructura del centro de datos.

Los pasillos de circulación interna deben mantenerse despejados de todo objeto.

5.7.- Capacitación y Concientización

Se debe desarrollar un plan de capacitación y concientización específico para todo el personal sobre las políticas de control de acceso físico, enfocando en la importancia de la seguridad física y las consecuencias de los accesos no autorizados.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 09 - Política de Seguridad del Equipamiento

1.- Objetivo

El equipamiento debe protegerse contra amenazas, tanto físicas como ambientales. Para esto se debe reducir el riesgo de accesos no autorizados, así como también prevenir pérdidas, daños, hurtos o comprometer los activos y/o la interrupción de las actividades del organismo.

Se pretende garantizar la continuidad de las operaciones y reducir los efectos causados por errores humanos (accidentales o intencionales) o desastres naturales a través de la implementación de controles físicos y ambientales en los centros de datos y áreas relacionadas (por ejemplo, recinto donde se almacenan los respaldos).

En este sentido, se deberá realizar evaluaciones de riesgo específicas para el equipamiento crítico de manera semestral, para ajustar los controles de seguridad física y ambiental basados en las tendencias emergentes y los avances tecnológicos.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez Y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Afecta a toda la infraestructura tecnológica del organismo, en especial a los centros de datos y áreas relacionadas.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Protección y Privacidad de los Datos
- Política de Control de Acceso Físico a Áreas Seguras
- Política de Destrucción de Información
- Política de Intercambio y Traslado Físico de la Información

5.- Descripción

Los equipos que conforman la infraestructura tecnológica del organismo tales como, servidores, equipos de comunicaciones, centrales telefónicas, estaciones de trabajo, dispositivos de almacenamiento, etc., que procesen información, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado, adoptando los controles necesarios para mantener estos equipos alejados de sitios que puedan tener riesgo de amenazas físicas y/o ambientales. Las medidas tomadas deberán ser proporcionales a los riesgos identificados.

El Director de Infraestructura monitoreará, mediante mecanismos adecuados, las condiciones ambientales de las zonas donde se encuentre el equipamiento.

En caso de pérdida o robo de un equipo, se deberá comunicar a la gerencia de Infraestructura para que esta pueda informar inmediatamente a la autoridad correspondiente y denunciar ante la autoridad competente, y al Oficial de Seguridad de la Información para que lo registre como incidente de seguridad de la información y realice el tratamiento que corresponda.

6.- Retiro del Equipamiento Fuera de las Instalaciones

Todos quienes trabajan en el organismo son responsables de velar por la seguridad de los equipos propiedad del organismo, que se encuentren fuera de las instalaciones de esta, siguiendo las siguientes directrices:

- No dejar los equipos de cómputo desatendidos en lugares públicos o a la vista.
- Los equipos de infraestructura deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano.
- El retiro de equipamiento, propiedad del organismo, fuera de las instalaciones del organismo, debe seguir los procedimientos establecidos, contemplando cláusulas de confidencialidad, e integridad de la información sensible que está contenida en dicho equipamiento.

7.- Eliminación o Reutilización Segura de Equipos y Medios

El organismo debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura, alineado a la política de destrucción de información.

Cuando un equipo sea reasignado o dado de baja, se deberá asegurar la información existente en el equipo para luego eliminarla, con el fin de evitar pérdida y/o recuperación no autorizada de la misma.

8.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 10 - Política de Respaldo de Información

1.- Objetivo

El objetivo de este documento es garantizar que la información del organismo, o en poder de ésta, pueda ser restaurada en tiempo y forma en caso de enfrentar una situación de pérdida de información.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Toda la información que esté soportada en medios de almacenamiento lógico del organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Los propietarios de los activos de información son responsables por establecer la frecuencia de respaldo y el tiempo de retención de éstos.

El Director de Infraestructura es responsable por proveer los medios técnicos para la realización de los respaldos y el cumplimiento de la presente política.

4.- Políticas Relacionadas

- Política de Política de continuidad de las operaciones y recuperación ante desastres
- Política de Control de Controles Criptográficos

5.- Descripción

El organismo debe contar con un plan y un procedimiento formales para la realización de los respaldos, para garantizar que la información pueda ser construida en caso de pérdida u otra necesidad.

Los propietarios del activo determinarán la frecuencia y tiempo de retención del respaldo, teniendo en cuenta el marco normativo aplicable, así como la valoración del activo a fin de minimizar la pérdida o destrucción total o parcial del mismo, su disponibilidad y confidencialidad. Esta información debe reflejarse en el plan y procedimiento de respaldos.

Los respaldos deben ser probados en intervalos regulares a los efectos de garantizar su confiabilidad ante la necesidad de uso en caso de emergencia. Se debe definir un procedimiento de prueba de respaldos, así como la periodicidad de su ejecución. Por ejemplo, trimestralmente.

Se debe tener en consideración la confidencialidad de la información y en caso de que sea requerido, los respaldos deberán estar cifrados de conformidad con la política establecida. En este sentido, se debería implementar encriptación de última generación para todos los respaldos, garantizando que la información sensible esté protegida contra accesos no autorizados durante su almacenamiento y transferencia.

El organismo debe disponer de un lugar adecuado para el almacenamiento seguro de los respaldos que sea consistente con las medidas de protección ambiental del sitio principal.

Se debe contar con respaldos fuera del sitio principal (off-site), conservando las condiciones ambientales consistentemente con las del sitio operativo y con controles de seguridad física adecuados. Debe definirse un procedimiento donde se defina la

frecuencia y las actividades necesarias para la transferencia de los respaldos fuera del organismo.

Se debe establecer un protocolo de rotación de medios de respaldo y una política de destrucción segura para medios desactualizados o que ya no se utilicen, incluyendo procedimientos de destrucción certificados.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 11 - Política de Protección contra Software Malicioso

1.- Objetivo

Garantizar la protección de la información y los sistemas informáticos del organismo contra software malicioso (por ejemplo: virus, gusanos, troyanos, spyware, adware intrusivo, crimeware, entre otros).

1.1.- Vigencia

El presente manual entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todos los sistemas informáticos que soportan el proceso de operación del organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de Infraestructura es responsable por la gestión técnica relacionada a la presente política.

Todo el personal del organismo, así como los proveedores, deben cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos

5.- Descripción

Se debe utilizar una solución antivirus corporativo que cumpla con:

- Estar posicionado entre las de mejor desempeño por parte de al menos un análisis periódico, independiente e internacionalmente reconocido en las últimas dos revisiones.
- De preferencia incluir dispositivos móviles como parte de la solución.
- De preferencia implementar seguridad de navegación y correo.

El organismo debe garantizar los siguientes controles contra el código malicioso:

- Definir procedimientos y responsabilidades de gestión para la protección de los sistemas ante software malicioso.
- Definir procedimientos para la correcta instalación de parches de seguridad proporcionados por los proveedores. Debe llevarse un registro de los parches de seguridad instalados.
- Brindar capacitación al personal afectado en la operación y uso de la solución antivirus, así como cualquier otro mecanismo utilizado para la detección de software malicioso.
- Concientizar a los usuarios finales sobre las formas en las que se puede adquirir el software malicioso, los riesgos y problemas que acarrea, así como sobre el procedimiento que se debe seguir en caso de sospechar o constatar estar afectado (tanto en los equipos informáticos a los cuales accede regularmente como otros en los que haya detectado su presencia). Este procedimiento debe estar formalizado y difundido a nivel de todo el organismo.
- La conexión a la red informática de cualquier dispositivo móvil está sujeta a previa aprobación y verificación de la disponibilidad de una solución activa contra

código malicioso por parte del personal técnico. En el caso de terceros contratados se requiere también la aprobación del responsable por la gestión del contrato.

- Toda conexión a una red externa a el organismo debe considera obligatoriamente una solución contra código malicioso.
- La instalación de software requiere el previo aseguramiento de la inexistencia de código malicioso.
- Debe usarse, mantener vigente la licencia de uso, y configurar una solución antivirus con las siguientes características mínimas:
 - Actualizar regularmente y de forma automática el padrón de archivos de firmas, y del propio software
 - Actualización automática de las estaciones clientes sin participación del usuario.
 - Explorar en tiempo real todos los adjuntos de correo electrónico transmitidos por Internet o Intranet.
 - Verificar la información desde sitios WEB, incluyendo la bajada de archivos.
 - Verificar los medios removibles antes de que los mismos sean usados, sin participación del usuario.
 - Verificar la instalación y ejecución de cualquier archivo con código ejecutable, archivo de secuencia de comandos, o macros.
- Los usuarios finales no deben tener suficientes permisos como para deshabilitar o reconfigurar software antivirus. Esas actividades son propias del personal del Departamento de Soporte Técnico.
- Cualquier detección, o síntoma de existencia de código malicioso debe ser reportada como un incidente de seguridad.
- Cualquier computador infectado por código malicioso debe ser desconectado inmediatamente de la red hasta que el mismo se encuentre libre de código malicioso.
- Queda prohibida la instalación de cualquier software sin la debida autorización de la Comisión de Seguridad de la Información (CSI).

- Los usuarios de la red no deben tratar de erradicar un código malicioso. Esta actividad debe ser desarrollada por el personal técnico del Departamento de Soporte Técnico.
- Los computadores o dispositivos usados en comunicaciones remotas deben tener un software antivirus instalado y activado de acuerdo a las recomendaciones de Departamento de Infraestructura.
- La CSI debe promover cursos, material educativo, o buenas prácticas en el uso de los recursos informáticos como forma de minimizar el impacto del código malicioso en el organismo.
- Debe comunicar formalmente a todos los usuarios de la red, directrices sobre uso, que como mínimo establezcan:
 - Nunca abrir un archivo adjunto que es parte de un correo electrónico de origen desconocido.
 - Eliminar sin abrir cualquier spam, cadena o correo electrónico de origen desconocido o sospechoso.
 - Nunca bajar archivos de sitios web, o instalar software bajado desde sitios webs, o portados en dispositivos móviles sin la previa autorización del personal técnico del Departamento de Soporte.
- Contar con controles que prevengan y detecten el uso de software no autorizado (por ejemplo, lista blanca de aplicaciones), ya que estos pueden abrir la puerta a software malicioso.
- Contar con controles que eviten el acceso a sitios web maliciosos y/o no autorizados (por ejemplo, listas negras).
- Analizar periódicamente los sistemas informáticos en búsqueda de software malicioso.
- Analizar periódicamente los logs de los sistemas en búsqueda de actividades inusuales.

Todo equipo informático, tanto de escritorio, portátil, servidores y demás, debe estar protegido por una solución técnica residente en el equipo contra software malicioso, gestionado de forma centralizada. Esta solución técnica, así como la base de datos y registro de las amenazas a detectar, deben estar actualizadas y acompañadas de un

procedimiento que explice un comportamiento preventivo de los usuarios y personal especializado de TI.

Sería importante que el organismo pudiera contar con:

- Un sistema automatizado de respuesta y recuperación que activen protocolos de aislamiento y restauración inmediatos para dispositivos infectados.
- Adoptar tecnologías avanzadas de análisis de comportamiento para detectar actividades anómalas que pueden indicar la presencia de malware antes de que se propague o cause daños.
- Incrementar la frecuencia y el alcance de las pruebas de penetración y los simulacros de ataque con software malicioso para evaluar regularmente la eficacia de las defensas, considerando una frecuencia anual mínima.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 12 - Política de Separación de Entornos

1.- Objetivo

Reducir el riesgo de cambios o accesos no autorizados en el ambiente de producción.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todas las aplicaciones, sean o no desarrolladas por el organismo, que requieran o sufran cambios a lo largo de su ciclo de vida.

Este alcance, tal como queda definido, también incluye, sin ser taxativo, herramientas para la administración de la red, configuraciones de sistemas, seguridad, incidentes, antivirus, gestión de parches, etc.

3.- Responsabilidades

El Director de TIC es responsable por otorgar los recursos necesarios para el cumplimiento de la presente política.

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de Infraestructura es el responsable de coordinar la gestión técnica que requiere el cumplimiento de la presente política.

El Director de Desarrollo y Gestión de Aplicaciones es responsable por coordinar la ejecución de la validación final de los cambios funcionales en las aplicaciones informáticas del organismo en base al alcance de cada una de ellas a los efectos de su futura liberación.

El personal del organismo y los proveedores deben cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Gestión de Cambios

5.- Descripción

El organismo debe:

- Definir entornos operativos separados, disponiendo por lo menos de los entornos correspondientes a las actividades de desarrollo de aplicaciones (Desarrollo), prueba de aplicaciones (Testing), y operación de las aplicaciones (Producción).
- Definir, en el marco de la política de gestión de cambios, un procedimiento que se formalice para la gestión de los mismos.
- Definir un procedimiento formal de pasaje entre los diferentes entornos, así como los responsables de dichos pasajes (Pasaje de Desarrollo a Testing, y Pasaje de Testing a Producción).
- Comunicar que los pasajes al entorno de producción deben ser formalmente documentados según se establezca en el procedimiento.
- Asegurar que los pasajes a producción están siempre alineados con la política y procedimiento de gestión de cambios.

Todos los cambios deben ser probados, validados y aceptados previamente por personal técnico del organismo privilegiando el principio de segregación de funciones.

Los sistemas o herramientas provistas por terceras partes deben existir en los ambientes definidos, al menos en ambiente de pruebas y producción, para que el organismo pueda realizar los controles pertinentes antes de cualquier instalación, actualización y aplicación de cambios.

El ambiente de pruebas debe estar adecuadamente identificado de forma tal de diferenciarlo del ambiente de producción.

El personal que realiza las pruebas debe utilizar cuentas de usuario específicas del ambiente de pruebas para la realización de éstas.

Se deberían implementar herramientas de Integración Continua y Entrega Continua (CI/CD) que automatizan el proceso de despliegue desde el desarrollo hasta la producción, para asegurar que todos los cambios sean sometidos a pruebas exhaustivas y validación automática, minimizando el riesgo de errores y accesos no autorizado al ambiente de producción.

Establecer procedimientos más detallados para la revisión y aprobación de cambios, incluyendo revisiones de seguridad obligatorias y pruebas de penetración para nuevas aplicaciones antes de su puesta en producción.

Fortalecer los sistemas de monitoreo para todos los entornos operativos, implementando soluciones que detecten y alerten en tiempo real sobre actividades anómalas o no autorizadas.

Desarrollar y ejecutar un programa de formación continua sobre gestión de cambios y seguridad de aplicaciones para el personal técnico y de desarrollo.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 13 - Política de Registro y Auditoría de Eventos de Sistemas de Información

1.- Objetivo

Monitorear y registrar los eventos de dispositivos de red y sistemas informáticos para detectar posibles fallas o situaciones inesperadas, generar evidencia y actuar con la mayor premura posible.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez Y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todos los sistemas informáticos y dispositivos de red del organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de Infraestructura es responsable por la gestión del monitoreo de los elementos que componen la red, recursos de red y/o cualquier sistema informático del organismo, así como de la revisión periódica de los registros.

4.- Políticas Relacionadas

- Política de Gestión de Cambios
- Política de Gestión de Incidentes de Seguridad de la Información

5.- Descripción

El organismo debe:

- Contar con procedimientos formales que soporten la gestión del monitoreo de los elementos de red y sistemas informáticos
- Registrar los eventos y definir el tiempo de retención de éstos
- Definir la periodicidad de las revisiones de los registros
- Revisar periódicamente los registros de eventos

Se debe registrar, al menos:

- Fechas y horarios
- Origen
- Destino
- Conexiones
- Acciones
- Inicio de sesión fallidos
- Cambios en las configuraciones de los sistemas

La hora de los sistemas informáticos debe estar sincronizada con una sola fuente de referencia de tiempo.

Los registros deben estar protegidos contra posibles alteraciones o accesos no autorizados.

Se deberían desarrollar procedimientos más detallados para la revisión y análisis de registros, incluyendo directrices específicas para la identificación y manejo de incidentes basados en los datos de los registros.

En este sentido, se debería tener la capacidad de poder integrar sistemas avanzados de gestión de información y eventos de seguridad (SIEM) para automatizar la correlación de eventos y el análisis de comportamiento anómalos a través de todos los sistemas y redes. Incorporar herramientas de inteligencia artificial y aprendizaje automático para mejorar la detección proactiva de amenazas y anomalías en los registros de eventos, permitiendo respuestas más rápidas y precisas.

Se debe implementar un protocolo de entrenamiento regular para el personal técnico y de seguridad sobre las últimas técnicas de monitorización, análisis de registros y respuesta a incidentes para asegurar una gestión eficaz de los registros de eventos.

6.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Dirección del organismo, a través del Departamento de Personal podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 14 - Política de Protección y Privacidad de los Datos

1.- Aspectos Generales

El Directorio del organismo reconoce la importancia de identificar y proteger los activos de información del organismo. Para ello, se evitará la destrucción, divulgación, modificación o uso no autorizado de la información, mediante el compromiso de desarrollar progresivamente, implantar mantener y mejorar continuamente políticas y procedimientos requeridos. Estos serán revisados de forma periódica, con una frecuencia anual, y los resultados de dichas evaluaciones serán documentados y, cuando corresponda, comunicados a todo el organismo.

El Directorio del organismo declara su compromiso con el cumplimiento de la normativa y legislación vigente en relación con los diversos aspectos de la Seguridad de la Información.

La Seguridad de la Información se caracteriza como la preservación de:

- su confidencialidad, asegurando que sólo quienes estén autorizados puedan efectivamente acceder a la información;
- su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos;
- su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

En el organismo se desarrollará la adopción de la Seguridad de la Información implantando progresivamente un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura.

Estos controles deberán ser establecidos paulatinamente con adecuadas campañas de comunicación interna para asegurar los objetivos de seguridad y protección de datos del organismo.

Por este motivo el Directorio designa un Referente de Protección de Datos Personales.

Esta Política de Protección y Privacidad de los Datos (PPPD) debe ser conocida, y por lo tanto es divulgada y revisada periódicamente, para que pueda ser cumplida por todos los colaboradores y por el personal del organismo, independientemente del cargo que desempeñe cada uno de ellos y de su situación contractual.

La PPPD se integrará a la normativa básica del organismo. Tal integración incluye la difusión previa de la Política, la edición de todos los documentos relacionados a la misma y la instrumentación de controles y mecanismos correspondientes a las situaciones de incumplimiento.

En este contexto, podemos definir que es política del organismo:

- Establecer objetivos anuales con relación a la Protección y Privacidad de los Datos y, en función de tales objetivos, publicar políticas y comunicar los controles que complementen este documento.
- Desarrollar un proceso de evaluación y tratamiento de los riesgos de seguridad. De acuerdo a su resultado, implementar progresivamente acciones correctivas y preventivas, así como elaborar y actualizar el plan de acción como parte de las iniciativas de mejora continua.
- Establecer los objetivos de control y los controles correspondientes, en virtud de las necesidades que en materia de riesgo surjan del proceso de análisis de riesgos manejados.
- Clasificar y proteger la información de acuerdo a la normativa vigente y a los criterios de valoración según sea la importancia que cada activo de información posee para la empresa.
- Brindar las mayores garantías para salvaguardar la integridad, confidencialidad y disponibilidad de la información de nuestros clientes, velando por la privacidad de toda la información sensible que se almacena en sistemas que administra el organismo.
- Cumplir con los requisitos del servicio que brindamos a la ciudadanía, asegurando el cumplimiento de las normativas legales y reglamentarias aplicables, así como de las obligaciones de seguridad que correspondan en cada caso. Estar atentos a

la evolución del marco normativo para realizar las adaptaciones necesarias ante cada cambio.

- Organizar periódicamente instancias de concientización que también sirvan para la formación en materia de Protección y Privacidad de los Datos para todo el personal del organismo.
- Contar con una política de gestión de incidentes de seguridad de la información y seguir los lineamientos establecidos por la normativa vigente y el CERTuy.
- Establecer que todos en el organismo somos responsables de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes que se establezca.
- Establecer los medios necesarios para garantizar la continuidad de las operaciones del organismo.

A su vez, la nueva normativa en materia de protección de los datos de carácter personal impone a las organizaciones el ejercicio de una responsabilidad proactiva adoptando las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de esos datos es conforme a la ley. Entre las medidas que el responsable de tratamiento debe adoptar a fin de poder demostrar tal conformidad, se encuentra la de establecer políticas internas de protección de datos personales.

La Protección de Datos Personales implementa controles que permiten asegurar la aplicación de los principios de:

- Legalidad,
- Veracidad,
- Finalidad,
- Previo consentimiento informado,
- Seguridad de los datos,
- Reserva,
- Responsabilidad.

Asimismo, también busca garantizar los derechos de los titulares de:

- Información frente al tratamiento y recolección de Datos,

- Acceso,
- Rectificación,
- Actualización,
- Inclusión,
- Supresión,
- Impugnación de valoraciones personales.

El organismo ha optado por adoptar una PPPD que permita recoger y determinar con claridad las responsabilidades y funciones en materia de protección de datos.

La protección de datos requiere contar con el compromiso y apoyo de todos los niveles directivos del organismo de forma que pueda estar coordinada e integrada con el resto de los objetivos estratégicos del organismo para conformar un todo coherente y eficaz.

El organismo conforma una Comisión de Seguridad de Información (CSI), que tendrá como principal objetivo promover, difundir y apoyar la protección de datos personales, garantizando que la misma sea parte del proceso de planificación, definiendo estrategias, planes, políticas y todo aquello que incremente y mejore la seguridad y protección de datos e información.

2.- Ámbito de Aplicación, Alcance y Marco Normativo

La presente PPPD define el marco de referencia que permite la gestión de la protección de los datos personales y se aplicará a todos los sistemas de información y a todas las actividades de tratamiento de datos de carácter personal de los que sea responsable el organismo.

La PPPD debe ser conocida y cumplida por todo el personal independientemente del cargo que desempeñe y de su situación contractual, incluyendo partes interesadas o terceros colaboradores.

La PPPD afectará a toda información y todo dato personal tratado en el ámbito de las actividades del organismo, tanto por medios electrónicos como en soporte papel.

La información de carácter personal está regulada con carácter general por la Ley N° 18.331 de 11 de agosto de 2008 y el Decreto N° 414/009 de 21 de agosto de 2009 sobre Protección de Datos Personales y Habeas Data y demás normas complementarias, modificativas y concordantes.

3.- Principios de Protección de Datos y Criterios de Aplicación

El organismo tratará la información y los datos personales bajo su responsabilidad conforme a los siguientes principios generales de protección de datos y criterios de aplicación:

- Principio de Legalidad: las bases de datos serán debidamente inscriptas en el registro de la URCDP y se observará en su operación los principios que establece la legislación de Protección de Datos Personales antes identificada.
- Principio de Veracidad: los datos personales que trate el organismo serán veraces, adecuados, ecuanímenes y no excesivos en relación con la finalidad para la cual se hubieren obtenido y, si fuera necesario, actualizados; adoptándose todas las medidas razonables para que se supriman o rectifiquen sin dilación.
- Principio de Finalidad: los datos personales serán tratados para el cumplimiento de fines determinados, explícitos y legítimos y no serán utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
- Principio de Previo consentimiento Informado: los datos personales solamente serán tratados cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado o cuando dicho tratamiento se encuentre amparado en alguna otra base legal de legitimación, que habilite el tratamiento sin requerir el consentimiento del titular.
- Principio de Seguridad de los datos: los datos personales serán tratados de tal manera que se garantice su seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas y organizativas apropiadas.
- Principio de Reserva: quienes en cualquier carácter y legítimamente, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales bajo responsabilidad del organismo, están obligados a utilizarlos en forma reservada y

exclusivamente para las operaciones autorizadas, estando prohibida toda difusión de estos a terceros, debiendo guardar estricto secreto profesional, incluso luego de extinguirse la relación con el organismo, cualquiera sea la naturaleza de ésta.

- Principio de Responsabilidad: El organismo en ejercicio de una responsabilidad proactiva adoptará las medidas técnicas y organizativas para dar cumplimiento a los principios anteriormente señalados y que le permitan estar en condiciones de demostrar dicho cumplimiento.
- Gestión de derechos de los titulares de los datos: El organismo establecerá como medida de privacidad desde el diseño, los mecanismos necesarios para asegurar el ejercicio de los derechos de los titulares de los datos personales, en los plazos previstos en la normativa.
- Análisis de riesgos y Evaluación de Impacto en la Protección de Datos (EIPD): previo al inicio de todo tratamiento de datos de carácter personal, el organismo llevará a cabo un análisis de riesgo que permita identificar y gestionar los riesgos para los derechos de las personas, minimizándolos hasta niveles que puedan considerarse aceptables y revisándolos en forma periódica y al menos cada dos (2) años y en cualquier otra oportunidad en que exista un cambio significativo en los sistemas de información y/o en los tratamientos de datos personales. Asimismo, el organismo llevará a cabo una Evaluación de Impacto en la Protección de Datos (EIPD) en los casos expresamente previstos en la normativa o cuando del análisis realizado resulte probable que el tratamiento suponga un riesgo significativo para los derechos de las personas.
- Gestión de vulneraciones de seguridad para la protección de datos: El organismo implementará los mecanismos apropiados para la correcta identificación, registro, resolución y notificación de los incidentes de seguridad que afecten datos de carácter personal, dando cumplimiento a las formalidades y plazos previstos en la normativa legal y reglamentaria aplicable.
- Privacidad desde el Diseño: en forma previa al inicio del tratamiento y durante todo su desarrollo, el organismo implantará el estándar de “Privacidad desde el Diseño” con el objetivo de cumplir con los requisitos definidos en la reglamentación de la normativa legal y siguiendo sus orientaciones, a efectos de que la protección de datos se encuentre presente desde las primeras fases de

concepción de las bases de datos, las operaciones de tratamiento, las aplicaciones, los sistemas informáticos y en general cualquier proyecto que involucre datos de carácter personal.

- Privacidad por Defecto: El organismo aplicará las medidas técnicas y organizativas apropiadas a los efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Este compromiso de mínimos refiere a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su comunicación.

4.- Roles en la Estructura Organizativa y Responsabilidades en la Implementación y Aplicación de la PPPD

El Directorio del organismo tendrá la condición de responsable de la información y de los tratamientos llevados a cabo por la misma.

En su calidad de máximo responsable corresponde al Directorio del organismo aprobar la presente política de protección y privacidad de los datos (PPPD).

Es responsabilidad del Referente de Seguridad de la Información (RSI), la guía, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.

Es responsabilidad de los equipos técnicos del área de Tecnología del organismo el diseñar, evaluar, implementar e implantar las herramientas tecnológicas que permitan asegurar la preservación de la confidencialidad, integridad y disponibilidad de información en las formas explicitadas precedentemente.

Es responsabilidad del Referente de Protección de Datos, asesorar al Directorio del organismo en la formulación, diseño y aplicación de la política de protección de datos personales y supervisar su cumplimiento en el organismo, así como proponer todas las medidas que entienda pertinentes para adecuar sus prácticas a la normativa y a los estándares internacionales en materia de protección de datos personales y verificar su realización.

5.- Obligaciones del Personal y Terceros Colaboradores

Todas las unidades del organismo prestarán su colaboración en las acciones de implementación de la presente PPPD.

Todo el personal del organismo, así como todos los terceros colaboradores que le presten servicios con acceso a datos personales bajo su responsabilidad, tienen la obligación de conocer y cumplir lo previsto en la presente PPPD, así como en las normas y procedimientos que la desarrollen. Asimismo, tienen el deber de colaborar en la mejora y requisitos en materia de protección de datos evitando y aminorando los riesgos a los que se encuentra expuesta la información y los datos personales bajo responsabilidad del organismo.

En especial, es responsabilidad de todo el personal del organismo, del personal temporario, terceras partes debidamente autorizadas y en general, de toda persona física o jurídica que legítimamente acceda a información bajo responsabilidad del organismo, el reportar y registrar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes que deberán estar planificados y protocolizados.

6.- Concientización y Capacitación

El organismo desarrollará actividades formativas específicas orientadas a la concientización y formación del personal que le presta servicios, acerca de sus deberes y obligaciones relacionadas con la presente PPPD, así como de los riesgos existentes en tratamiento de la información.

7.- Desarrollo y Revisión de la PPPD

Corresponderá al Directorio del organismo, a propuesta de la Comisión de Seguridad de Información, la adopción de los procedimientos, guías e instrucciones necesarias para el desarrollo de la PPPD.

La presente PPPD se someterá a un proceso de revisión al menos anual, a fin de adaptarse a las circunstancias técnicas u organizativas requeridas para mantener su eficacia.

8.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Dirección del organismo, a través del Departamento de Personal podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 15 - Política de Clasificación de la Información

1.- Objetivo

Este documento tiene como objetivo principal asegurar que la información esté protegida a un nivel apropiado. Para lograr dicho objetivo se establecen los criterios de clasificación de la información que se encuentre bajo la custodia del organismo sin importar el medio que la soporte.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Toda información producida, obtenida, en poder o bajo control del organismo, independientemente del medio que la soporte.

3.- Responsabilidades

El Comité de Seguridad es responsable de validar que los activos de información se encuentren clasificados e incluidos en el Inventario de Activos.

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política y confirmar la definición del procedimiento para la clasificación de la información.

Los Propietarios de los activos son responsables por las actividades de clasificación de la información en función de la evaluación de riesgo correspondiente. Asimismo, son responsables de definir los niveles y perfiles de autorización para el acceso, la modificación, y la eliminación de la misma.

Los Custodios de la Información son los responsables de implementar controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, y disponibilidad, en el marco de lo establecido en esta política.

4.- Políticas Relacionadas

- Política de Uso aceptable de los activos
- Política de Gestión de Activos

5.- Clasificación de la Información

El organismo entiende que la información debe ser clasificada.

Toda la información es por defecto, pública, pudiéndose clasificar en reservada o confidencial según lo establece la Ley 18.381 o secreta si existe alguna ley o criterio específico del organismo que así lo determine.

5.1. Criterios de Clasificación

El nivel de confidencialidad de cada documento se determina en base a los siguientes criterios:

- Valor de la información – basado en los impactos identificados en la evaluación de riesgo
- Sensibilidad y criticidad – basado en el riesgo más alto calculado para cada elemento de información durante la evaluación de riesgo
- Legales y contractuales – basado en la identificación de requisitos legales, reglamentarios y contractuales u otras obligaciones

5.2. Niveles De Confidencialidad

Se recomienda utilizar el nivel de confidencialidad más bajo que garantice un adecuado nivel de protección, a fin de evitar costos de protección innecesarios.

Toda la información bajo custodia en el organismo, la cual fuera provista por los clientes, incluyendo una determinada clasificación, podrá ser reclasificada de forma más restrictiva, si así lo considerara el organismo en función de los riesgos involucrados.

Toda la información debe clasificarse de acuerdo con los siguientes niveles de confidencialidad:

- Información pública
 - Toda información será considerada pública hasta que sea clasificada en alguna otra categoría.
 - La información estará a disposición del público.
- Información reservada
 - Se clasifica como reservada toda información que:
 - Comprometa la seguridad del organismo o de los sus clientes
 - Afecte la conducción de las actividades del organismo, incluida aquella información que terceros entreguen con carácter de reservado a el mismo
 - Dañe la estabilidad financiera o económica del organismo o de sus clientes
 - Suponga una pérdida de ventajas competitivas para el organismo o sus clientes, o pueda dañar su proceso de producción
 - Desproteja innovaciones o desarrollos tecnológicos producidos o que permanezcan en custodia del organismo.
 - Sea recibida por terceros y entregada a el organismo con esa clasificación.
 - La información estará disponible para un grupo definido de empleados y terceros autorizados.
 - Dicha información, permanecerá con tal carácter durante el máximo período de tiempo que establezca la normativa vigente. Además, su

carácter pasará a ser público cuando se extingan las causas que dieron lugar a su clasificación.

- Sólo se ampliará el periodo de Reserva sobre cierta documentación cuando permanezcan y se justifiquen las causas que le dieron origen.
- Información confidencial
 - Se clasifica como confidencial la información que:
 - Refiera al patrimonio de una persona,
 - Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica, que pudiera ser útil para un competidor,
 - Esté amparada por una cláusula contractual de confidencialidad;
 - Se componga de datos personales que requieran previo consentimiento informado
 - Sea recibida por terceros y entregada a el organismo con esa clasificación
 - La información está disponible sólo para determinados cargos identificados e individualizados dentro del organismo.
- Información secreta
 - Se clasificará como información secreta exclusivamente a la información que sea secreta por definición de la Dirección de la empresa.

5.3. Accesos Autorizados

La información clasificada como “Reservada”, “Confidencial” o “Secreta”, deberá ir acompañada de un Listado de Accesos Autorizados en la cual el propietario del activo de información especifique los cargos o personas que tienen derecho a acceder a esa información. Esta lista debe estar incluida en el Inventario de Activos de Información.

Las Listas de Accesos Autorizados deben ser revisadas, actualizadas y comunicadas a la Comisión de Seguridad con una periodicidad anual, por parte del propietario de los activos.

5.4. Reclasificación

Los propietarios de los activos deben revisar el nivel de confidencialidad de sus activos de información con una periodicidad anual, y evaluar si es necesario cambiar el nivel de confidencialidad.

De ser posible, el nivel de confidencialidad debe reducirse.

5.5. Etiquetado De La Información

Los niveles de confidencialidad deben ser etiquetados de la siguiente manera:

- Información en soporte papel – se debe indicar en una etiqueta o sello, según el caso.
- Sistemas de información – el nivel de confidencialidad de las aplicaciones y bases de datos debe indicarse en la pantalla de acceso al sistema.
- Correo electrónico – el nivel de confidencialidad se debe indicar en la base de los correos según una leyenda provista por los asesores legales donde se advierta del mal uso de la misma.
- Medio de almacenamiento electrónico – (discos, tarjetas de memoria, etc.) – el nivel de confidencialidad debe indicarse en la superficie superior de dicho medio.
- Información transmitida oralmente – los cargos que deban transmitir o recibir información no pública, que deba ser transmitida oralmente (de forma presencial, vía telefónica, o por cualquier otro medio de comunicación), están en conocimiento del uso restringido de dicha información, en función del acuerdo de confidencialidad y no divulgación, firmado.

5.6. Manejo De La Información Clasificada

Todo el personal del organismo que accedan a información clasificada debe seguir las pautas que se detallan a continuación:

- Información en soporte papel
 - Los documentos deben ser transferidos fuera y dentro del organismo en sobre cerrado, por personas con la autorización adecuada para el manejo de dicha información
 - Los documentos sólo podrán conservarse en sitios con acceso de personal autorizado.
 - Los documentos impresos deben ser retirados de las impresoras por las personas autorizadas
 - Los documentos no podrán ser enviados por vías de comunicación no autorizadas
- Información en soportes electrónicos (planillas, correos electrónicos, etc.)
 - La información solo puede ser accedida por las personas autorizadas
 - La información puede intercambiarse a través de las herramientas tecnológicas referentes a transmisión y recepción debidamente autorizadas y controladas mediante Usuario y Contraseña
 - El acceso al sistema de información donde se almacena el documento debe estar protegido y controlado mediante Usuario y Contraseña
 - Al enviarse mediante correo electrónico, se debe verificar cuidadosamente el destinatario
 - Dependiendo del nivel de clasificación, la información debe almacenarse o enviarse en forma cifrada
 - La información debe almacenarse en los servidores controlados por el organismo
 - Las pantallas en la que se visualiza el documento deben bloquearse automáticamente después de un tiempo de inactividad
- Sistemas de Información
 - La información solo puede ser accedida por las personas autorizadas
 - El acceso al sistema de información debe estar protegido y controlado mediante Usuario y Contraseña
 - El sistema de información sólo puede estar instalado en servidores controlados por el organismo

- El sistema de información sólo puede estar ubicado en sitios con acceso físico controlado
- Las pantallas en la que se visualiza el documento deben bloquearse automáticamente después de un tiempo de inactividad
- El borrado de la información debe ser realizado mediante algoritmos que garanticen su eliminación segura
- Información transmitida oralmente
 - Sólo las personas autorizadas pueden tener acceso a este tipo de información
 - Se debe evitar el manejo oral de la información en la medida de lo posible

6.- Controles

El organismo implementará los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, y disponibilidad requeridos, en el marco de lo establecido en esta política.

Se deberá establecer un protocolo para la revisión semestral de la clasificación de la información, especialmente para los datos sensibles o críticos, adaptando la clasificación a cambios en el entorno legal o tecnológico.

Se deberá implementar un sistema de auditorías internas regulares para evaluar el cumplimiento de la política de clasificación y la efectividad de los controles implementados.

7.- Capacitación y Concientización

Se deberá desarrollar e implementar un programa de formación sobre la clasificación de la información para todo el personal, enfatizando la importancia de seguir los procedimientos establecidos y las consecuencias de una clasificación incorrecta.

8.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de

Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 16 - Política de Uso Aceptable de Dispositivos Móviles

1.- Objetivo

Proteger la información del organismo, o en poder de ésta, almacenada o accesible desde dispositivos móviles.

Evitar que los dispositivos móviles sean causa de infección y distribución de código malicioso dentro del organismo y prevenir que éstos sean el origen de accesos no autorizados a las redes o recursos privados.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Toda la información más allá de su clasificación, de su propietario, que se encuentre bajo la custodia y responsabilidad del organismo, y que en el accionar del mismo, sea objeto de manipulación, traslado o intercambio por medios físicos.

3.- Responsabilidades

La Dirección es responsable por planificar acciones de sensibilización al personal del organismo y proveedores autorizados respecto a la importancia de esta política.

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Las Gerencias son responsables de proveer y mantener las condiciones necesarias para el cumplimiento de esta política, así como establecer lugares seguros para la guarda de los dispositivos móviles.

La Gerencia de Infraestructura es responsable de proveer los medios técnicos para el cumplimiento de esta política.

El personal del organismo y los proveedores autorizados para utilizar dispositivos móviles, son responsables por cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Uso Aceptable de los Activos
- Política de Uso de Controles Criptográficos
- Política de Destrucción de la Información

5.- Definiciones

- Dispositivo móvil: tipo de computadora que presenta las siguientes características:
- Movilidad: puede ser transportada con frecuencia y facilidad
- Tamaño pequeño: esta característica está ligada a la anterior, para que sea fácil de transportar, su tamaño es pequeño
- Comunicación inalámbrica: tiene la capacidad de enviar y recibir datos sin ningún tipo de cableado
- Capacidad de interacción con las personas mediante pantalla y/o teclado

6.- Descripción

Se debe garantizar que la información del organismo no se vea comprometida.

Para ello, es necesario el cumplimiento de las directivas que se describen a continuación:

- Los dispositivos móviles deben estar inventariados.

- Los dispositivos móviles que contengan información sensible del organismo o de sus clientes deben estar cifrados.
- Los dispositivos móviles deben contar con mecanismos de protección contra código malicioso.
- Los sistemas o servicios que puedan ser accedidos mediante dispositivos móviles deben estar identificados.
- Los dispositivos móviles deben contar con bloqueo mediante contraseña, pin u otro medio robusto de autenticación.
- Se debe reportar la pérdida o extravío de dispositivos móviles de forma inmediata a la toma de conocimiento, de acuerdo con los procedimientos y/o protocolos establecidos.
- Los dispositivos móviles deben tener un sistema operativo obtenido por canales oficiales, o instalado de fábrica, y contar con la última actualización validada instalada.
- Las aplicaciones instaladas en el dispositivo deben ser obtenidas por canales oficiales y con el licenciamiento debido.
- Se debe implementar, para los dispositivos que lo soporten, instrumentos y herramientas técnicas (hardware, software) que permitan bloquear y/o borrar la información de forma remota. Se deberá evaluar puntualmente los riesgos asociados al uso de dispositivos que no permitan el cumplimiento de este control.
- Se debe contar con procedimientos para la reutilización y/o eliminación de dispositivos (cambio de usuario, equipos en desuso, etc.) que garanticen la eliminación completa y segura de la información previa y sensible allí almacenada.
- Se debe implementar una solución de gestión de dispositivos móviles (MDM) que permita la segregación efectiva de datos y aplicaciones empresariales de los personales, asegurando la confidencialidad e integridad de la información corporativa.
- Fortalecer los protocolos de autenticación en dispositivos móviles incorporando métodos biométricos, como reconocimiento facial o huellas dactilares, en combinación con contraseñas o PIN, para una seguridad de múltiples factores.

- Se debe establecer un sistema de alertas y procedimientos para la respuesta rápida en caso de pérdida o robo de dispositivos móviles, incluyendo la capacidad de borrado remoto de la información sensible almacenada.
- Revisar o desarrollar una política más detallada para la instalación y actualización de aplicaciones en dispositivos móviles, asegurando que solo las aplicaciones aprobadas por el organismo puedan ser instaladas y que todas las actualizaciones sean gestionadas de forma centralizada.

7.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 17 - Política de Uso de Controles Criptográficos

1.- Objetivo

Definir reglas para el uso de controles criptográficos, así como las reglas para el uso de claves criptográficas, con el fin de proteger la confidencialidad, integridad, autenticidad y no repudio de la información.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Toda la información digital más allá de su clasificación, que requiera ser protegida para mantener la confidencialidad, integridad y la autenticidad.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de Infraestructura es el responsable de la gestión técnica de los controles criptográficos.

Todo el personal del organismo y sus proveedores deben cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información y Protección de Datos
- Política de Clasificación de Información
- Política de Intercambio y Traslado Físico de la Información

5.- Control de Acceso

El organismo deberá determinar las herramientas criptográficas basadas en algoritmos probados y aceptados por la industria que serán utilizados para proteger la información. Proporcionará también los recursos necesarios para el soporte del equipamiento adecuado, así como para su protección física y lógica.

Se deben utilizar controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito de la organización.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos.

Se debe:

- Definir procedimientos para la gestión de claves, la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de claves de cifrado.
- Asignar los roles del responsable de la gestión de claves.
- Establecer los algoritmos de cifrado a utilizar para los distintos escenarios, así como la longitud de la clave.

6.- Controles Criptográficos

El organismo debe proteger los sistemas de información o la información por medio de los siguientes controles criptográficos:

Nombre del sistema / tipo de información	Herramienta criptográfica	Algoritmo de cifrado	Tamaño de clave
Túneles VPN del Firewall	FortiNet SSL VPN	AES	256 bits
CA Interna	Microsoft Windows® Active Directory Certificate Services	SHA	256 bits
Notebooks, Discos y memorias USB	Microsoft BitLocker®	AES	256 bits
Documentos electrónicos con información confidencial	7zip	AES	256 bits

Tabla 1 – Controles Criptográficos

La Comisión de Seguridad (CSI) es responsable de preparar instrucciones detalladas sobre el uso de las herramientas criptográficas mencionadas.

Los propietarios de los activos individuales a los que se aplican controles criptográficos son responsables de la aplicación apropiada de los controles criptográficos individuales.

7.- Claves Criptográficas

La CSI es responsable de prescribir las siguientes reglas con respecto a la administración de las claves:

- generar claves criptográficas privadas y públicas
- activación y distribución de claves criptográficas
- definir el límite de tiempo para el uso de claves y su actualización periódica (de acuerdo con la evaluación de riesgos)
- archivar claves inactivas que son necesarias para archivos electrónicos cifrados
- destrucción de claves

Las claves son administradas por sus propietarios de acuerdo con las reglas mencionadas anteriormente.

Las claves criptográficas estarán protegidas contra pérdida, cambio o destrucción.

Se deberá desarrollar y adoptar un protocolo para la gestión de claves criptográficas que incluya procedimientos automatizados y revocación de claves, mejorando la seguridad y eficiencia del proceso.

Se implementará una evaluación continua de las necesidades criptográficas que ajuste dinámicamente los controles basados en el panorama cambiante de amenazas y las nuevas regulaciones de protección de datos.

8.- Capacitación y Concientización

Se deberá ampliar la capacitación y concientización sobre el uso seguro y efectivo de la criptografía a todos los empleados, especialmente aquellos que gestionan y utilizan información sensible o crítica, para garantizar una comprensión profunda y el cumplimiento de las políticas criptográficas.

9.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 18 - Política de Continuidad Operativa y Recuperación ante Desastres

1.- Objetivo

Establecer y lograr la planificación y gestión de la continuidad operativa de los procesos críticos del organismo ante la eventualidad de ocurrencia de eventos que provoquen la interrupción de las operaciones críticas que viabilizan la operativa del organismo.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todos los procesos críticos del organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Directorio debe establecer los criterios de Alcance y Priorización para la planificación de la Continuidad Operativa y los correspondientes Planes de Contingencia y Recuperación a elaborar, probar, mantener y mejorar de forma periódica.

La Comisión de Seguridad de la Información (CSI) llevará a cabo la coordinación formal de las pruebas de los planes, involucrando a todas las partes necesarias y apoyando la gestión del RSI. Además, será responsable, junto con los referentes de las Divisiones que se requiera convocar, de ejecutar las pruebas del plan de contingencia y recuperación.

El RSI deberá informar al CSI sobre los resultados de las pruebas, documentar las lecciones aprendidas y elaborar un plan de acción para su mejora. Estas pruebas del plan de continuidad operativa y de recuperación se llevarán al menos una vez al año.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Respaldo de Información
- Política de Gestión de Riesgos
- Política de Gestión de Activos

5.- Estrategias de Recuperación

Ante la ocurrencia de eventos de la magnitud que menciona el objetivo de esta política, se desea lograr operar en contingencia, afectando lo menos posible los servicios internos y externos. El organismo se propone lograr una recuperación ante desastres que permita el restablecimiento de las operaciones del mismo a su situación normal en plazos razonables.

Esta política declara la necesidad de establecer las mejores prácticas para la elaboración del Plan de Continuidad del Negocio y los diferentes Planes de Contingencia.

El organismo asume de esta manera, la necesidad de garantizar los recursos necesarios para su desarrollo, ejecución, prueba y mejora continua, ajustándose a las necesidades cambiantes del servicio público.

Para la implementación de esta política, se considerarán todos los documentos que establezcan los requisitos de las partes interesadas, así como los aspectos técnicos, administrativos, operativos, legales y de recursos necesarios para asegurar la continuidad y eficiencia de los servicios del organismo, de acuerdo con su alcance.

6.- Planificación de Continuidad y Recuperación

6.1.- Relevamiento y Evaluación de Procesos Críticos

La metodología se basa inicialmente en el trabajo de la CSI para definir los requisitos asegurando dar continuidad a cada área operativa y sus procesos.

La CSI debe evaluar la criticidad de cada proceso y sus necesidades, estableciendo así los requisitos para la planificación.

6.2.- Evaluación de Riesgos Asociados a los Procesos y sus Componentes

Se establece una metodología para la evaluación de los Riesgos, acorde a la evaluación de Riesgos del organismo en su contexto general.

También se establece la necesidad de contemplar para este análisis los riesgos asociados a cada proceso que se considere endémicos por su naturaleza o por su contexto.

6.3.- Declaración de Cumplimiento de Marcos Legales

El Directorio de organismo debe garantizar los recursos necesarios para las consultas legales pertinentes, con el fin de determinar los requisitos de los marcos normativos y regulatorios aplicables a la continuidad operativa en relación con sus contrapartes, incluyendo otros organismos, proveedores, entes reguladores y demás partes involucradas.

6.4.- Requerimientos de Seguridad en los Plan de Continuidad del Negocio y de Contingencia

El Plan de Continuidad del Negocio y los Planes de Contingencias respectivos, estarán alineados a los requisitos de la Norma ISO 27.001.

Cuando se produzcan cambios o nuevos Planes de Contingencia, al CSI deberá asegurar en su revisión que se mantiene ese cumplimiento ya mencionado.

6.5.- Plan de Continuidad Operativa y Planes de Contingencia

El Plan de Continuidad Operativa puede estar comprendido por varios Planes de Contingencia para cada línea de proceso o servicio. Esto implica la necesidad de crear equipos de trabajo responsables para cada plan, a efectos de poder mantener y mejorar la planificación, teniendo como principal insumo el conocimiento que tienen de sus procesos o servicios.

Debe notarse que los Planes de Contingencia de cada proceso, pueden tener dependencias de ejecución. En dichos planes, deberán estar especificadas esas relaciones de dependencias.

6.6.- Comprobación y Pruebas del Plan de Continuidad

A intervalos regulares establecidos para cada Plan de Contingencia, se realizarán las Pruebas de los mismos. Será obligatorio por parte de cada equipo que realiza una prueba, elaborar un informe de evaluación al final para el RSI que lo elevará a la CSI.

Estos simulacros de desastres deberán tener una frecuencia, de por lo menos una vez al año, y deberá incluir escenarios variados, tanto digitales como físicos, para probar la efectividad del Plan de Continuidad y Recuperación en diferentes condiciones.

6.7.- Aprobación del Plan de Continuidad Operativa

El Directorio del organismo es responsable de aprobar el Plan de Continuidad Operativa, dado que allí se definen prioridades para su desarrollo, implementación, ejecución, recursos y pruebas.

6.8.- Cambios en la Estrategia Institucional

El Directorio del organismo se compromete a mantener alineado su Plan de Continuidad Operativa ante cambios en la estrategia institucional, asegurando los ajustes necesarios.

Los planes de continuidad y recuperación serán revisados y actualizados periódicamente para garantizar que reflejen los cambios en el entorno tecnológico, normativo y operativo, así como la aparición de nuevas amenazas.

6.9.- Aprobación de los Planes de Contingencias

La CSI es responsable de velar por el cumplimiento, aprobación y mejora de los Planes de Contingencia de cada proceso.

6.10.- Ejecución del Plan de Continuidad Operativa

El Directorio del organismo será el responsable de decidir en qué momento se activa el Plan de Continuidad Operativa.

6.11.- Ejecución de Planes de Contingencia

Los Planes de Contingencia serán ejecutados por el responsable del activo que se ve afectados, a los efectos de minimizar los tiempos de no disponibilidad de los sistemas afectados por dicha contingencia.

Integrar sistemas avanzados de monitorización y alerta que automaticen la detección de posibles amenazas o desviaciones en los procesos críticos, facilitando una respuesta más rápida y eficiente ante incidentes que provocan la contingencia.

7.- Control de Cambios

Dada la relación de dependencia de los Sistemas y las Tecnologías como soporte de los Servicios, se determina necesario que cada cambio en los Sistemas (Arquitectura, Software, Hardware, Infraestructura, Conectividad, etc.) deberá contemplar, de parte del rol de Control de Cambios, la necesidad de informar a los responsables de los Planes de Contingencia para analizar e incorporar esos cambios en los procesos ya documentados y probados.

8.- Recursos y Capacitaciones

La necesidad de mantener actualizados los planes, las pruebas y la efectividad de los mismos está dada por la preparación del personal que es afectado a cada Plan de Contingencia.

Para contemplar ese aspecto, el Directorio del organismo establece fomentar la capacitación y comunicación interna del personal involucrado en los Planes.

Mejorar la formación de todo el personal en prácticas de continuidad operativa, enfocándose no solo en sus roles específicos durante un incidente, sino también en la importancia de la resiliencia operativa general.

9.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 19 - Política de Cumplimiento

1.- Objetivo

Lograr que todas las obligaciones legales, reglamentarias y contractuales que afecten al organismo estén debidamente identificadas, documentadas y actualizadas.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todas las operaciones del organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

La Dirección es responsable de identificar toda la normativa aplicable con el fin de cumplir con los requisitos de acuerdo al contexto en el que cumple sus funciones, teniendo en cuenta aspectos legales y regulatorios, contratos, etc.

4.- Políticas Relacionadas

El organismo debe tener identificada toda la normativa vigente relacionada a sus operaciones.

A continuación, se lista de forma no taxativa, la normativa en materia de seguridad de la información que podría aplicar:

- Ley N° 18.331: Protección de datos personales y acción de habeas data
- Ley N° 18.381: Acceso a la información pública
- Decreto 451/009: Centro Nacional de Respuesta a Incidentes de Seguridad Informática
- Decreto 452/009: Política de Seguridad de la Información
- Decreto 92/014: Ciberseguridad
- Leyes que declaren secreta información (secreto tributario, secreto estadístico, secreto bancario, etc.)

Si como parte de los procesos operativos del organismo, se debe relacionar con otros países, la Dirección deberá considerar el cumplimiento de toda la normativa extranjera que sea pertinente.

Se debe hacer uso legal de los productos de software e información y mantener control de las licencias de software.

Se deben realizar revisiones de seguridad de la información para asegurar la adecuación del sistema de gestión de seguridad de la información, y su cumplimiento con la normativa vigente y el Marco de Ciberseguridad.

Estas revisiones podrán constar de hackeos éticos, pruebas de penetración, evaluación de vulnerabilidades y auditorías de seguridad de la información, y deben ser realizadas por personal (interno o externo) independientemente del área donde se encuentran los servicios bajo revisión.

Los resultados de las revisiones serán informados a las Gerencias, al Oficial de Seguridad de la Información, a la Comisión de Seguridad de la Información, y a la Dirección.

Se debe establecer un protocolo para la revisión y actualización periódica de la política de cumplimiento, asegurando que se realicen ajustes proactivos en respuesta a cambios legislativos.

Desarrollar e implementar un sistema integral de gestión de cumplimiento que incluya herramientas automatizadas para el seguimiento continuo y la evaluación de la conformidad con todas las normativas aplicables, tanto nacionales como internacionales.

5.- Capacitación y Concientización

Se debe desarrollar e implementar un plan de capacitaciones sobre cumplimiento normativo a todos los empleados, con sesiones específicas adaptadas a diferentes roles y responsabilidades dentro del organismo, reforzando la importancia del cumplimiento como un componente crítico de la cultura corporativa.

6.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Dirección del organismo, a través de Capital Humano podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 20 - Política de Escritorio y Pantalla Limpios

1.- Objetivo

Promover conductas que colaboren con la reducción de los riesgos de acceso no autorizado, pérdida o alteración de la información.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo y los proveedores que hacen uso de escritorios, información en papel y/o medios de almacenamiento del organismo.

Afecta a toda la información del organismo, independientemente del medio de soporte de la misma.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todos los Directores de las diferentes áreas de TIC son responsables de promover el cumplimiento de esta política en sus subordinados, proporcionar y mantener las condiciones necesarias con este objetivo.

Deberán establecer lugares para la guarda de dispositivos, medios y de la información de uso temporal en los puestos de trabajo, mover llaves, así como la infraestructura necesaria para salvaguardar los activos de información.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Clasificación y Manejo de la Información
- Política de Destrucción de la Información

5.- Descripción

La información sensible o crítica, en formato papel o en medios de almacenamiento, debe ser guardada en un lugar seguro con acceso restringido, una vez utilizada.

Al final de la jornada laboral, o al retirarse de su puesto de trabajo, el personal del organismo y los proveedores que trabajan en el mismo deberán:

- Guardar todos los papeles, documentos, medios removibles o similares que se encuentren en los escritorios en los lugares previstos para tal fin y bajo llave cuando la información así lo requiera.
- Bloquear los equipos (PCs, laptops, etc.) cada vez que queden desatendidos.
- Retirar los medios instalados en dispositivos, unidades lectoras/grabadoras o puertos y guardarlos en los lugares previstos.
- Los dispositivos móviles (notebooks, tablets, celulares, etc.) deben quedar bajo llave, o con cables de seguridad, de forma de evitar su hurto o uso indebido, cuando estén desatendidos.
- La destrucción de hojas, papeles, borradores o medios con información debe asegurar la confidencialidad de la información, siguiendo los lineamientos de la política de referencia.
- Los documentos deben ser retirados de las bandejas de las impresoras, fax, fotocopadoras o similares inmediatamente después de impresos.

Definir los protocolos de seguridad para dispositivos móviles, incluyendo el uso obligatorio de cables de seguridad y la implementación de una política de dispositivos bajo llave o almacenados en áreas seguras cuando no estén en uso, especialmente en áreas de alto tráfico o accesible al público.

6.- Capacitación y Concientización

Se debe desarrollar un programa de formación y concientización exhaustivo, específicamente diseñado para promover prácticas de escritorio y pantalla limpios entre todos los empleados, subrayando la importancia de mantener la confidencialidad y seguridad de la información en todo momento.

7.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 21 - Política de Gestión de Riesgos de Seguridad de la Información

1.- Objetivo

Definir la metodología para la evaluación y el tratamiento de los riesgos de seguridad de la información del organismo y definir el nivel de riesgo aceptable de acuerdo con lo establecido por el Marco de Ciberseguridad de AGESIC en su versión vigente.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

La evaluación de riesgos y el tratamiento de los mismos se aplican a todo el alcance de un Sistema de Gestión de la Seguridad de la Información (SGSI) actualmente en desarrollo, es decir, a todos los activos que se utilizan dentro del organismo o que por sus características se entiende que podrían tener un impacto identificable en la seguridad de la información dentro del SGSI.

Esta política debe ser aplicada en todos los niveles y actividades significativas del organismo, donde se evidencie riesgos u oportunidades que impacten el cumplimiento de los objetivos propuestos.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

La Dirección es responsable de identificar toda la normativa aplicable con el fin de cumplir con los requisitos de acuerdo con el contexto en el que cumple sus funciones, teniendo en cuenta aspectos legales y regulatorios, contratos, etc.

4.- Metodología de Evaluación y Tratamiento de Riesgos

Los riesgos de seguridad de la información pueden provenir de diversas fuentes, y en un panorama de amenazas en constante evolución, el proceso de identificación podría ser muy complejo y difícil si no definimos un abordaje metodológico que contemple esas características.

5.- Identificación y Clasificación Sistemática de Riesgos

El organismo utiliza una clasificación basada en los eventos de riesgos para lograr mayor claridad y consistencia en la identificación de riesgos. Los controles se establecen proactivamente obteniendo el entendimiento y la comprensión de la siguiente secuencia de eventos:

- Causa del riesgo
- Evento de riesgo resultante
- Impactos
- Oportunidades de remediación

6.- Clasificación de Riesgos

Clasificar los riesgos permite describir una visión consolidada de los eventos de riesgo a los que el organismo tiene exposición. Esto resulta especialmente importante en el contexto de la información que gestiona y administra el organismo como encargado del tratamiento de datos personales en los que nuestros clientes son responsables del tratamiento.

Para los eventos de riesgo, cuando se procede a evaluar el riesgo y priorizarlo, se debe considerar como guía los siguientes escenarios representativos:

Evento de Riesgo	Acceso no autorizado, alteración, robo, pérdida o fuga de información o sistema por colaborador interno
Escenario	El riesgo de robo, pérdida, fuga, divulgación, ya sea intencional o no, o el acceso no autorizado o alteración de la información del organismo como resultado de un acto de un colaborador de la empresa. Esto incluye al personal y a cualquier otro colaborador no perteneciente al personal del organismo pero que trabaje en las instalaciones de la empresa o que utilice la infraestructura del organismo para desarrollar su labor. El alcance de este escenario incluye toda información que resida en el organismo en forma electrónica o física. Hay un impacto claro sobre confidencialidad, integridad y disponibilidad, que resulta de, pero no se limita a: • Robo deliberado: llevar los datos a un nuevo empleador. • Pérdida accidental: pérdida de recursos de procesamiento de la información y archivos en papel. • Fugas accidentales: enviar correo electrónico a un destinatario incorrecto. • Divulgación deliberada: filtración de información de usuarios a terceros. • Acceso no autorizado: explorar información de los clientes. • Alteración no autorizada: cambio de la configuración en los sistemas de seguridad.
Evento de Riesgo	Acceso no autorizado, alteración, robo, pérdida o fuga de información o sistema por una tercera parte

Escenario	El riesgo de robo, pérdida, fuga, divulgación, intencional o no intencional o el acceso no autorizado o alteración de la información del organismo, o de sus clientes, confiada a terceros como resultado de un acto por parte de su personal, cualquiera de sus agentes u otras partes. En este escenario, el alcance incluye cualquier información del organismo o sus clientes que sea manejada por el tercero en forma electrónica o física. Hay impacto sobre las dimensiones de confidencialidad y disponibilidad, que resulta de, pero no se limita a: • Robo deliberado: utilizar la información del organismo para el negocio de terceros. • Pérdida accidental: pérdida de registros en archivos de terceros. • Fuga accidental: información manejada incorrecta por terceros. • Divulgación deliberada: transmisión a terceros de información confidencial del organismo o de sus clientes. • Acceso no autorizado: empleados de limpieza/personal de servicio/proveedores que acceden a información que está almacenada en las oficinas del organismo. • Alteración no autorizada: cambiar la configuración de control de acceso en determinados sistemas para otorgar acceso de privilegio a ellos mismos.
Evento de Riesgo	Ataque de parte(s) externa(s) en la infraestructura del organismo, incluidos sistemas e información residente en los mismos
Escenario	En este escenario se considera el riesgo de un acto negligente o deliberado destinado a interrumpir los servicios, dañar la reputación o comprometer de algún modo la información o los sistemas del organismo y sus clientes mediante el uso de equipamiento y redes de datos que forman parte de la infraestructura institucional. En este tipo de evento de riesgo se genera un impacto sobre las dimensiones de confidencialidad y disponibilidad, que resulta de, pero no se limita a: • Ataque: ataque de denegación de servicio sobre equipamiento de la infraestructura del organismo. • Ataque: para deshabilitar los sistemas y evitar que éstos se ejecuten

Evento de Riesgo	Acceso no autorizado, alteración, robo o fuga de información o robo de un sistema o aplicación por un externo
Escenario	El alcance incluye cualquier información del organismo o de sus clientes que se almacene en formato electrónico o físico. El impacto se extiende a las dimensiones de confidencialidad, integridad y disponibilidad, y resulta de, pero no se limita a: • Acceso no autorizado: recopilación de credenciales de acceso para su uso en futuros ataques. • Alteración no autorizada: alteración de cuentas de usuario estándar que permiten otorgar acceso de privilegio. • Acceso no autorizado: información confidencial de clientes robada de los sistemas en los que el organismo es encargado del tratamiento de datos.
Evento de Riesgo	La infraestructura o servicios de apoyo no están disponibles
Escenario	Este escenario considera el riesgo de que la infraestructura para la prestación de los servicios a clientes o los servicios operativos esenciales no esté disponible. Esto puede deberse a diversos eventos o condiciones de error que impactan la infraestructura y los servicios críticos que opera el organismo para sus propios procesos internos y para los de sus clientes. Este escenario considera un impacto evidente sobre la dimensión de disponibilidad, que resulta de, pero no se limita a: • No se certifica que los edificios estén disponibles debido a eventos naturales (vientos fuertes, ubicación en un área susceptible a inundaciones), incendios, situaciones peligrosas para la salud o cuestiones ambientales. • Falla en asegurar que los edificios estén disponibles cuando se producen inestabilidades, alteraciones o interrupciones, en el suministro de los servicios de energía eléctrica. • No se prueba que los edificios estén disponibles debido a fallas en el mantenimiento de servicios, actividades de mantenimiento o falta de planes de continuidad.

Evento de Riesgo	Incumplimiento del marco legal de la Protección de Datos Personales
Escenario	Este escenario considera la participación del organismo como encargado en los tratamientos de datos de sus clientes involucrando un gran volumen de datos sensibles y el marco regulatorio específico que los regula. Este tipo de evento de riesgo complementa todos los anteriores y tiene impacto sobre las dimensiones de confidencialidad, integridad y disponibilidad. De acuerdo con el marco legal vigente, considerando el ciclo de vida del dato, se pone el foco en la gestión, transmisión, almacenamiento, procesamiento y disposición final de los datos personales.
Evento de Riesgo	Ausencia de la Alta Dirección o personal clave
Escenario	Aquí se considerará el riesgo de ausencia prolongada o permanente de personal clave. Signados por los acontecimientos de los últimos tiempos, se considera que este escenario puede ser causado por amenazas diversas como pandemias y epidemias. Este tipo de evento de riesgo tiene impacto sobre las dimensiones de integridad y disponibilidad.

Tabla 1: Guía para evaluar el riesgo y priorizarlo con escenarios representativos

7.- Capacitación y Concientización

Desarrollar un programa de capacitación y concientización para todos los empleados sobre la importancia de la gestión de riesgos, incluyendo la identificación y reporte de riesgos potenciales.

8.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Dirección del organismo, a través del Departamento de Personal podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 22 - Política de Gestión de Cambios

1.- Objetivo

Este documento tiene como objetivo definir una serie de pautas que nos permitan controlar los cambios en el organismo, los procesos, las instalaciones de procesamiento de información y los sistemas que afectan a la Seguridad de la Información.

Siendo el objetivo del presente documento definir cómo controlamos los cambios en los sistemas de información, se aplica a todo el alcance del SGSI; esto es, se aplica a todas las tecnologías de la información y de la comunicación utilizadas dentro del alcance del SGSI.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

. La política debe ser aplicada por aquellos miembros del organismo dado que forman parte de las áreas dedicadas a la tecnología de la información, de la comunicación, así como al desarrollo, mantenimiento y soporte de todos los productos y servicios.

Es responsabilidad de cada uno de los miembros del organismo implementar y cumplir con los controles establecidos para la gestión de los cambios.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de Desarrollo y Gestión de Aplicaciones es responsable por coordinar la ejecución de la validación final de los cambios funcionales en las aplicaciones informáticas del organismo en base al alcance de cada una de ellas a los efectos de su futura liberación.

El personal del organismo y los proveedores deben cumplir con lo establecido en la presente política.

4.- Criterios Básicos de Referencia

4.1- Acerca De La Solicitud De Cambio

Cada cambio puede iniciarse como una “Solicitud de Cambio”. Esta solicitud también nos servirá como registro y como prueba de que se nos ha solicitado un cambio concreto. El cambio puede ser iniciado internamente (por un miembro del organismo) o externamente (por un representante de un determinado cliente), y se registrará en un formulario específico en el Sistema de Gestión de Solicitudes.

Los cambios pueden afectar a los activos del organismo (hardware, software, redes, etc.), pero también pueden afectar a procesos, servicios, acuerdos, etc. Por ello, es importante que se registre en la “Solicitud de Cambio” toda la información detallada sobre el tipo de cambio.

También es importante incluir y registrar toda la información que sea posible relevar, como la persona que solicita el cambio, función, rol, la fecha, el área (o parte interesada) afectada, etc.

4.2.- Sobre el Proceso de Aprobación

La “Solicitud de Cambio” en general es recibida por una persona en el organismo que se encarga de analizarla, por lo que esta persona puede considerarse un primer filtro. Sólo es responsable de estudiar los detalles de la solicitud e identificar el impacto

potencial para las operaciones, incluyendo los impactos económicos y los relacionados con la seguridad de la información (por ejemplo, si el cambio es para actualizar el sistema operativo de un servidor que está en el entorno de producción y que puede ser parte de un sistema de misión crítica para el organismo).

Más adelante, deberá ser otra persona en el organismo (normalmente el responsable de los cambios, por ejemplo, un gerente o el gestor del cambio específico) o un equipo de personas, que, basándose en la información generada anteriormente, decidirá si el cambio se aprueba o se rechaza.

Para tomar esa decisión, es importante considerar todas las implicaciones que puede tener el cambio, tanto las internas (áreas, cumplimiento de requisitos de Seguridad de la Información, objetivos, etc.) como las externas (clientes, proveedores, procesos, etc.).

Si se aprueba el cambio, se designa un recurso técnico para la aplicación del cambio, quien se encarga de planificar su aplicación. También planificará las pruebas que permitan comprobar que los cambios se realizan de forma correcta.

Eventualmente estas tres personas pueden ser la misma y puede observarse que, en algunos casos específicos, puede no ser posible separar los roles/funciones. Sin embargo, el registro del rol en cada función se deberá mantener siempre, en todos los casos, para asegurar la trazabilidad en la toma de decisiones y en las autorizaciones necesarias.

Es oportuno señalar que la experiencia indica que no todos los cambios son igual de importantes, y por ello es fundamental clasificarlos en base a su impacto para el organismo, para el usuario o para el SGSI, por ejemplo: Impacto Bajo, Medio, Alto y Cambio de Emergencia.

En base al análisis de impacto puede luego clasificarse la Solicitud de Cambio. Esa calificación es la que permitirá establecer la ventana de tiempo que se solicitará para la implantación del cambio solicitado.

Dependiendo de la duración y del contenido del cambio se fijará el horario para su ejecución. En los ambientes productivos los días y horarios disponibles para la aplicación de cambios están predeterminados por cada cliente y el establecimiento de ventanas de tiempo debe alinearse con dichos horarios. Solamente ante cambios de emergencia podría coordinarse la ejecución en horarios excepcionales. Para ello se requiere presentar evidencias de la criticidad que justifique tal nivel de consideración.

Para los cambios internos del organismo es aplicable el mismo criterio respecto a los ambientes productivos, las situaciones de emergencia y las ventanas de tiempo.

El proceso de aprobación, la definición de tipo de impacto y la coordinación en base a los horarios disponibles para fijar ventanas de tiempo en ambientes productivos, es aplicable también a sistemas en los que sean proveedores externos quienes realizan las tareas de mantenimiento y quienes solicitan aplicar cambios.

Para las solicitudes de cambio en los que participan proveedores externos (ya sea porque son iniciativas de los proveedores o porque son solicitudes formuladas a proveedores) se deberá aplicar el mismo procedimiento con el agregado de controles más estrictos en relación con el control de acceso y el seguimiento de la ejecución de cada plan de implantación y de vuelta atrás.

4.3.- Los Cambios de Emergencia

Un aspecto importante a tener en cuenta es que cuando se produce un error durante la aplicación de un cambio que fue debidamente analizado, aprobado y verificado, es sumamente importante contar con un procedimiento que nos permita volver al estado anterior.

En los cambios de emergencia es necesario que la aprobación esté supeditada a la planificación detallada de un procedimiento de retorno o retroceso. El proceso de retorno debe ser considerado e incluido al momento de fijar la extensión de la ventana de tiempo que se solicita y reserva para la ejecución de un cambio.

Es recomendable que este procedimiento de retroceso quede definido en todos los cambios durante la etapa de planificación de la implantación, estableciendo con detalle y con claridad todo lo que hay que hacer para volver al estado anterior.

Por último, la persona responsable de ejecutar el procedimiento de retorno puede ser la misma persona que fue designada responsable de la implementación del cambio.

5.- Sobre la Gestión de Cambios

Cualquier cambio sobre sistemas operativos o de producción (se considera un cambio regulado por este documento, por ejemplo, la instalación de nuevo software, o la de una versión nueva de un software existente, la actualización de controladores, la instalación de parches, los cambios de configuración estén o no basados en la gestión de la capacidad, etc.) debe ser realizado de la siguiente forma:

1. Los cambios pueden ser propuestos formalmente por Gerentes y Coordinadores de Área. En el caso de cambios propuestos por usuarios, las solicitudes serán recibidas y gestionadas por la Dirección de Desarrollo que las redireccionará a las áreas respectivas del organismo según corresponda.
2. Los cambios deben ser autorizados por el Gerente del Área, que debe evaluar su justificación para las operaciones del organismo y las potenciales consecuencias negativas sobre la seguridad.
3. En el análisis de la autorización, debe documentarse, según el área de impacto y el alcance del cambio, quién será responsable de la implementación del cambio solicitado.
4. Al momento de aprobar la Solicitud de Cambio se debe establecer quién será el responsable de verificar que los cambios que se implementen queden implementados de acuerdo con los requerimientos.
5. En el proceso de aprobación del cambio debe individualizar quién será el responsable de probar y verificar la estabilidad del sistema o del proceso afectado por el cambio; en todos los casos el sistema no podrá ser puesto en producción antes de haber realizado todas las pruebas exhaustivas que determine el responsable que haya sido designado.

6. En el proceso de aprobación del cambio solicitado se debe establecer un plan de comunicación específico que permita saber de antemano a quien debe ser reportada la implementación de los cambios, detallando los respectivos datos de contacto.

Los registros sobre las Solicitudes de Cambio son llevados en el Sistema de Gestión de Solicitudes de Servicio y son identificados con una categoría específica.

6.- Gestión de Almacenamiento de Registros de Cambio

Los registros sobre las solicitudes de cambio se conservan en el Sistema de Gestión de Solicitudes de Servicio del organismo. Dichos registros deben proporcionar la siguiente información:

Nombre del registro	Ubicación de documentos asociados al cambio	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
[Nombre del registro de cambio] - en formato electrónico	[Nombre de carpeta de Intranet o número de la solicitud de cambio procesada]	[Nombre – Cargo]	Una vez procesada la solicitud de cambio el registro ya no puede ser modificado.	Según se establezca aquél que aprueba el cambio.

Tabla 1: Información de Registro de Solicitudes de Cambios.

7.- Capacitación y Concientización

Desarrollar un programa de capacitación y concientización para todos los empleados sobre la importancia de la gestión de cambios, comprendiendo su papel en la mitigación de riesgos, y estén informados de los procedimientos a seguir para la gestión de incidentes.

8.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 23 - Política de Finalización o Cambio en la Relación Laboral

1.- Objetivo

Establecer reglas para proteger los activos de información del organismo ante la finalización, temporal o definitiva, de la relación laboral de un funcionario o proveedor con el organismo, así como en casos de cambios en su relación funcional.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo que accede a los sistemas informáticos, equipos, instalaciones e información gestionados por el organismo.

3.- Responsabilidades

El Directorio es responsable por difundir la presente política a todo el personal, independientemente del cargo que desempeñe.

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Departamento de Personal será responsable de comunicar en tiempo y forma las finalizaciones o cambios en los vínculos al Departamento de Infraestructura, para que se deshabiliten los accesos lógicos y físicos que correspondan.

4.- Descripción

Todo el proceso de selección y desvinculación de personal es llevado adelante por el Departamento de Personal. En particular, el proceso de desvinculación de personal requiere de una serie de pasos previos a la terminación de la relación laboral.

El Departamento de Personal informará al Departamento de Infraestructura de la inminente desvinculación, para que tomen los recaudos a los efectos de realizar la gestión de permisos correspondiente.

Deberán retirarse los permisos de accesos lógicos y físicos, y niveles de autorización a toda persona que finalice o cambie su relación funcional o contractual.

Todo usuario de servicios que posean claves de acceso o niveles de autorización y que finalizan su relación laboral ya sea en forma definitiva o transitoria (ej. destitución, renuncia, licencia sin goce de sueldo por periodos prolongados, finalización de contrato); así como aquellos que cambien su relación funcional se le deberán retirar los permisos y niveles de autorización que ostenten hasta ese momento.

Este retiro deberá incluir:

- Correo Institucional:
 - Se dará de baja o deshabilitar la cuenta de correo que a los fines institucionales se le otorgó oportunamente.
 - Se eliminará el usuario de las listas de distribución de correo electrónico y grupo de trabajo.
- Otras aplicaciones: el usuario será dado de baja de todos los accesos a las diferentes aplicaciones en las que se encuentre activo.
- Acceso a la red institucional: se bloqueará a la red institucional, y a toda otra forma de acceso a archivos, carpetas y otra información compartida.

- Ingreso Físico: se le quitará a la persona el acceso a las diferentes áreas físicas a las que estaba autorizado a acceder.

La inhabilitación (ya sea temporal o definitiva) debe realizarse en el momento del cese, por lo cual las comunicaciones deberán efectuarse oportunamente, siendo responsables las áreas intervinientes.

Se debe definir un procedimiento específico que garantice el cumplimiento de la presente política.

5.- Capacitación y Concientización

Se deben desarrollar programas de capacitación y concientización para todo el personal involucrado en el proceso de finalización de relaciones laborales, asegurando que comprendan completamente sus roles y responsabilidades en el cumplimiento de esta política.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 24 - Política de Acceso Remoto y Teletrabajo

1.- Objetivo

Garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información del organismo, tanto por personal interno como proveedores autorizados a trabajar en esta modalidad, y definir las condiciones y restricciones del teletrabajo.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo y sus proveedores que estén autorizados a acceder remotamente a sistemas de información del organismo, así como a los dispositivos destinados a este propósito.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

La Alta Dirección del organismo es responsable por planificar acciones de sensibilización a su personal y proveedores autorizados respecto a la importancia de esta política.

Los Directores son responsables de proveer y mantener las condiciones necesarias para el cumplimiento de esta política, así como establecer las reglas de uso de acceso remoto para el personal que lo requiera.

El Director de Infraestructura es responsable por proveer los medios técnicos para el cumplimiento de la presente política.

Todo el personal del organismo y sus proveedores autorizados a trabajar remotamente son responsables por cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Gestión de Usuarios y Contraseñas
- Política de Seguridad del Equipamiento
- Política de Protección contra software malicioso

5.- Definiciones

Se debe garantizar que la información del organismo no se vea comprometida.

Para ello, es necesarios el cumplimiento de las siguientes directivas:

- Definir una lista de servicios, redes, sistemas de información que pueden ser accedidos remotamente por el personal autorizado.
- Contar con un inventario de accesos remotos otorgados identificando a la persona que cuenta con el acceso, el motivo por el cual se le otorgó y el plazo por el cual está autorizado.
- Se debe contar con una lista de equipos desde los cuales se puede acceder remotamente.
- Se debe utilizar comunicaciones seguras para el acceso remoto.
- Los equipos utilizados para el acceso remoto deben contar con protección ante software malicioso y estar encriptados con algún mecanismo robusto.

- Se deben definir los procedimientos y protocolos para la realización de teletrabajo, así como los contactos con soporte técnico para resolución de problemas.
- Se debe definir un procedimiento de revisión periódica de las condiciones de uso del acceso remoto y de los usuarios que hacen uso de éste, que contemple la revisión de los puntos anteriores.
- Adoptar métodos de autenticación de múltiple factor, incluyendo tokens físicos, autenticación biométrica, o códigos generados por aplicaciones, para todos los accesos remotos.

6.- Recomendaciones para Teletrabajo

La modalidad de teletrabajo está permitida en el organismo, y el personal debe poder identificar los riesgos vinculados con el trabajo remoto.

Los equipos móviles entregados por el organismo al personal ya cuentan con las medidas de protección requeridas para el teletrabajo.

Cuando un colaborador se conecta utilizando un equipo de su propiedad, en el cual le instaló las aplicaciones de conexión segura a el organismo, es de responsabilidad del colaborador asegurar el estado de protección de su equipo.

Todas las conexiones remotas deben estar monitoreadas a los efectos de validar que dicha conexión no permita el ingreso de malware.

Los principales riesgos vinculados con el teletrabajo incluyen, pero no son los únicos, los siguientes riesgos:

- Gestión de la seguridad del equipamiento (protección de antivirus, antimalware, etc.)
- Divulgación o filtrado de información

7.- Capacitación y Concientización

Desarrollar el programa de capacitación y concientización en seguridad para todos los usuarios con acceso remoto, incluyendo sesiones específicas sobre las mejores prácticas de seguridad y los riesgos asociados con el acceso remoto.

8.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 25 - Política de Eliminación y Destrucción de la Información

1.- Objetivo

Garantizar que la información almacenada en equipos y otros medios de soporte, así como los mismos medios físicos y lógicos sea borrada o eliminada de forma segura.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Toda información o medio de almacenamiento del organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

La Dirección debe proporcionar los recursos necesarios a fin de contribuir con una adecuada gestión de la información.

Es responsabilidad del organismo definir métodos formales de borrado seguro de la información según el tipo de soporte a destruir o de la información a eliminar.

Los Directores y mandos medios son responsables de velar por el cumplimiento de la Política.

El Propietario del activo o responsable de destruir la información deberá asegurar el adecuado registro del proceso realizado, dejando evidencia del método utilizado e indicando si la operación resultó satisfactoria.

4.- Políticas Relacionadas

- Política de Uso aceptable de los activos
- Política de Clasificación de la información

5.- Descripción

Para completar el ciclo de vida de la información es necesario incluir la ejecución del proceso de destrucción de la misma.

Todos los datos y aplicaciones almacenados en medios de almacenamiento móviles o equipos informáticos deben ser borrados o el medio destruido antes de ser eliminados o reutilizado.

La persona responsable del borrado de datos o de la destrucción de los medios deberá informar al propietario del activo correspondiente a los efectos de que actualice el Inventario de Activos.

Se deberá utilizar métodos de borrado seguro de forma de garantizar que la información y/o los medios que la contienen no se puedan recuperar.

Para el organismo los posibles métodos de borrado seguro son:

- Sobre-escritura compleja con cadenas de caracteres aleatorios
- Des-magnetización
- Trituración
- Desintegración
- Pulverización
- Fusión e incineración

Otros métodos, como la utilización de comandos de borrado y formateo lógico proporcionados por los sistemas operativos o aplicaciones de gestión de activos podrían

ser considerados métodos no seguros de destrucción de información puesto que, eventualmente y bajo ciertas condiciones específicas, permitirían la recuperación de la información.

En todos los casos de destrucción electrónica se debe borrar la información original, todas sus copias y sus respectivos respaldos de seguridad.

En el caso de la destrucción impresa se debe eliminar todas las copias y respaldos existentes.

Durante la destrucción de la información, se debe velar por el cumplimiento del conjunto de políticas que afecten a la información, especialmente las vinculadas a divulgación y acceso.

Regularmente se deberá revisar y actualizar los métodos de destrucción para asegurarse de que siguen siendo efectivos frente a las nuevas tecnologías y soportes de almacenamiento.

Se deberá implementar un sistema para la gestión y documentación del proceso de destrucción de la información, que permita la registración de cada paso, y la validación de la efectividad de la destrucción.

6.- Registro de las Operaciones de Borrado

- Deberá existir una solicitud formal indicando los medios o información a destruir dirigida al propietario del activo. La solicitud debe identificar en forma unívoca al medio o la información que requiere destrucción.
- El propietario del activo o la persona responsable del análisis de su destrucción deberá evaluar si corresponde la destrucción de dicha información tomando en cuenta en los decretos, leyes y otra normativa vigente.
- En cada proceso de destrucción se debe generar un reporte de actuación que identifique al personal que ejecuta el proceso y la metodología empleada para la destrucción de la información, así como las observaciones que éste considere pertinente. Siempre se deberá identificar claramente que el proceso se ha efectuado.

- Si la destrucción no se puede realizar correctamente, por ejemplo, por falla en la destrucción de la información contenida en un medio lógico o por no disponerse de un mecanismo adecuado, entonces esta situación debe quedar documentada y deberá utilizar otros medios de destrucción físicos para asegurar la adecuada destrucción del medio.

7.- Gestión Adecuada del Soporte

- Debe realizarse un adecuado control y mantenimiento de los dispositivos de acuerdo con los decretos, leyes, normativas, procesos y procedimientos vigentes (Ley 18.381: Acceso a la información pública, Ley N° 18.331: Protección de datos personales, acción de habeas data, Política de Uso Aceptable de los Activos y otras relacionadas).
- En caso de traslados de soportes físicos, lógicos y/o información almacenada externa al organismo, se debe asegurar que se cumpla la cadena de custodia de los mismos, para evitar fugas de información.

8.- Capacitación y Concientización

Se deberá desarrollar e implementar un programa de capacitación y concientización de todos los empleados sobre la importancia y los procedimientos de destrucción segura de la información, asegurando que todos comprendan su rol en la protección de la información.

9.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 26 - Política de Relacionamiento con Proveedores

1.- Objetivo

Mantener la seguridad de los activos de información que deban ser accedidos por proveedores.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todos los activos de información que deban ser accedidos por proveedores.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política. Deberá identificar y dar orden a los controles de seguridad de la información para habilitar el acceso de un proveedor a los activos de información.

El Propietario del activo es responsable por evaluar y, autorizar o negar las solicitudes de acceso a los activos de información que se encuentren bajo su responsabilidad.

El Director de Infraestructura es responsable por la asignación técnica de los permisos de acceso sobre los activos de información que hayan sido previamente autorizados a los proveedores

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Control de Acceso Lógico
- Política de Control de Acceso Físico a Áreas Seguras
- Política de Gestión de Incidentes de Seguridad de la Información

5.- Descripción

El organismo debe:

- Identificar todos los proveedores de servicios que requieran el acceso tanto físico como lógico a activos de información. Un manejo inadecuado de la seguridad de la información en el relacionamiento con proveedores puede poner en riesgo la imagen del organismo ante la pérdida, robo, acceso no autorizado o divulgación no autorizada de información.
- Contar con un procedimiento formal para la identificación de los proveedores, que incluya el tipo de información que deberán acceder y los requisitos de seguridad mínimos para cada tipo de activo de información. La información recabada mediante este procedimiento servirá de base para el establecimiento de la relación formal con los proveedores, contratos y acuerdos de niveles de servicios que deben existir para cada proveedor. Se debe establecer formalmente en los contratos y acuerdos las obligaciones de ambas partes (organismo y proveedor) en relación a la seguridad de la información. Asimismo, se debe establecer la posibilidad de derecho a auditar los procesos y controles de los proveedores de servicios del organismo relacionados con el acuerdo.
- Considerar la gestión de incidentes de seguridad de la información asociada al acceso a activos de información por parte de proveedores. Los incidentes de

seguridad de la información deberán ser gestionados según lo acordado en la Política de gestión de incidentes de seguridad de la información.

- Implementar los procesos de auditoría regular a proveedores para verificar el cumplimiento continuo con los requisitos de seguridad establecidos en los contratos y los acuerdos de servicio.
- Desarrollar/Actualizar los protocolos para la evaluación inicial y continua de los proveedores, incluyendo criterios específicos para la clasificación de riesgos asociados a cada tipo de proveedor y servicio.
- Implementar un sistema de gestión que asegure la trazabilidad y control sobre todos los accesos y operaciones realizadas por los proveedores en los sistemas del organismo a los que tienen accesos otorgados.

6.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 27 - Política De Uso Institucional De Redes Sociales

1.- Objetivo

Gestionar de manera segura los perfiles de redes sociales utilizados por el organismo.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todos los perfiles de carácter institucional utilizados por el organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El RSI deberá identificar y dar un orden a los controles de seguridad de la información para eventualmente habilitar el acceso a un proveedor a los activos de información.

4.- Políticas Relacionadas

- Política de Uso de aceptable de los activos

5.- Descripción

El organismo puede crear y utilizar su perfil oficial en las redes sociales (por ejemplo: Facebook, Twitter, YouTube, Instagram, LinkedIn, etc.) para dar a conocer programas, actividades y otros temas de interés, y para tener un contacto directo con el público y de esta manera poder conocer necesidades y requerimientos que están presentes en la sociedad.

Para asegurar una adecuada comunicación segura en relación con el uso de las redes sociales se debe cumplir con los lineamientos expresados a continuación.

- El organismo no se hace responsable de los sitios web no propios a los que se puede acceder mediante vínculos (links) desde perfiles del organismo o de cualquier contenido puesto a su disposición por terceros, que incluyan fotos, documentos, vídeos y otros contenidos.
- Si se detecta un contenido potencialmente inseguro, se debe reportar al RSI, y eliminar si corresponde.
- Se debe tener claramente identificado los usuarios de acceso a los perfiles del organismo en redes sociales, debiendo estos corresponder con cuentas institucionales del organismo y no cuentas personales de usuarios individuales.
- Las cuentas utilizadas para recuperación de los datos de acceso deben ser institucionales.
- Se deberán establecer las pautas y los procedimientos necesarios para el traspaso de usuarios en casos de cambio o desvinculación de los administradores de los perfiles.
- Siempre que la red social lo permita, se debe verificar la cuenta mediante la contratación del servicio de verificación de identidad, de manera de garantizar a los usuarios que es la cuenta oficial del organismo.
- La contraseña utilizada en cada cuenta de red social debe ser diferente. La misma deberá ser una contraseña segura conforme a las pautas establecidas en la política de contraseñas del organismo.
- Se deberá establecer los procedimientos para la verificación de cuentas y la gestión de cambios o desvinculaciones de administradores, asegurando que todas

las transiciones se manejen de forma segura, y que el acceso a la información se limite estrictamente a los administradores actuales.

- Se deberán implementar herramientas de monitorización continua que rastreen y analicen la actividad en los perfiles de redes sociales del organismo, para detectar comportamientos anómalos o contenido inseguro de manera automática.

6.- Capacitación y Concientización

Se deberá desarrollar e implementar un programa de capacitación y concientización específico para los administradores de redes sociales sobre las mejores prácticas de seguridad, gestión de crisis en redes sociales, y respuestas a incidentes de seguridad en línea.

7.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 28 - Política de Uso de Internet

1.- Objetivo

Regular el uso de Internet brindado por el organismo en las diferentes áreas del organismo.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Esta política aplica a todos los colaboradores empleados y personal contratado, visitante o en representación de un tercero (por ejemplo; proveedores, unidades reguladoras, clientes, etc.) con acceso al servicio de Internet del organismo.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Deberá identificar y dar un orden a los controles de seguridad de la información para habilitar el acceso a un proveedor a los activos de información.

El conjunto de los miembros del organismo y todos los usuarios autorizados a utilizar dispositivos con acceso al servicio de Internet del organismo son responsables de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Uso de aceptable de los activos

5.- Descripción

El uso del servicio de Internet por parte de toda persona alcanzada por esta política está permitido y se promueve en tanto es compatible y contribuye al cumplimiento de las metas y objetivos estratégicos del organismo.

El uso de Internet es una herramienta única para el desarrollo de nuestras actividades. Sin embargo, el uso inadecuado de este servicio puede eventualmente tener un impacto negativo, lo cual representa un riesgo y por esta razón el organismo observa (monitorea) el uso de este.

No está permitido el acceso directo a Internet a través de módems, Internet móvil, acceso celular, red inalámbrica u otros dispositivos para el acceso directo a Internet, sin la protección de un firewall autorizado por el organismo desde los dispositivos provistos por el mismo.

El organismo puede bloquear el acceso a algunas páginas de Internet para usuarios individuales, grupos de usuarios, o todos los empleados del organismo.

En el caso de tener necesidad de acceder a una página bloqueada, para el normal desempeño del trabajo, se deberá solicitar la autorización correspondiente al RSI o al Comité de Seguridad de la Información.

Se deberán desarrollar los procedimientos para la respuesta y manejo de incidentes relacionados con el uso de Internet, incluyendo pasos claros para el escalamiento y resolución de incidentes.

Se deberán implementar herramientas de monitoreo en tiempo real para supervisar el uso de Internet y detectar actividades potencialmente riesgosas o no autorizadas de manera más eficiente.

6.- Trazabilidad de Registros

El organismo monitorea las redes en general y la actividad de Internet en particular de acuerdo con el alcance de esta política. Los registros podrán ser consultados a efectos de dar solución a un incidente específico o con fines estadísticos.

En el caso de solicitudes de información referidas a incidentes específicos, los gerentes de cada área pueden solicitar al RSI reportes sobre los registros mediante correo electrónico y fundamentar la solicitud según corresponda de forma que se les pueda entregar toda la información relevante disponible.

En todos los casos su contenido sólo será de conocimiento de los roles referidos y del personal técnico responsable de extraer los registros de nuestros sistemas de información.

Dichos informes sobre los registros de uso de Internet no podrán ser divulgados, se considerará confidencial su contenido y se tomarán las previsiones pertinentes respecto a su archivo y custodia para preservar la confidencialidad correspondiente en todo momento.

7.- Disponibilidad de Servicios

El organismo proporcionará acceso a Internet con una serie de servicios básicos que incluyen:

- Libre navegación por los sitios cuyo contenido no esté comprometido dentro de las prohibiciones o limitantes dadas por las normas legales aplicables a nuestras actividades o por esta política específicamente
- Acceso a servicio de Correo Electrónico
- Acceso a servicios de Mensajería Instantánea básica

La ampliación de los servicios asignados a las personas alcanzadas por esta política debe gestionarse mediante una solicitud a través del sistema de gestión de incidentes dirigida al área del Departamento de Infraestructura.

8.- Uso Aceptable

El uso de Internet:

- Debe estar acorde con el marco legal vigente, en especial en lo que se refiere a la Protección de Datos Personales, respetando las resoluciones y pautas establecidas por cada área y el Directorio.
- Debe tener como principal utilidad servir como herramienta para cumplir las tareas asignadas. El uso fuera de esta premisa no debe interferir con el desarrollo de la actividad laboral.
- Debe regirse por los principios de buenas prácticas morales y éticas, en procura de contribuir a un mejor desempeño y a una mayor productividad de quienes lo utilizan.

9.- Uso Inaceptable

El uso de Internet considerado inaceptable puede comprender la pérdida del acceso, dar lugar a la revocación de permisos sobre Internet, la investigación de los registros de uso de Internet y/o la aplicación de las sanciones administrativas y legales correspondientes.

Sin pretender ofrecer una lista taxativa, es posible referirse a las siguientes pautas para configurar el uso inaceptable del servicio de Internet:

- Descargar material con expresa y manifiesta propiedad intelectual u otros derechos necesarios para dicha descarga o uso, sin los permisos necesarios, sin las licencias que correspondan, omitiendo intencionalmente cualquier otro formalismo que deba cumplirse.
- Utilizar Internet para almacenamiento, divulgación o transmisión de cualquier información, archivos, documentos, imágenes, sonidos u obras que puedan infringir el marco normativo vigente referido a su propiedad intelectual, a la protección de sus marcas o patentes.
- Involucrarse o participar en actividades ilícitas desde cualquier dispositivo conectado a la red mediante el servicio de acceso a Internet.

- Divulgar información deliberadamente falsa, sensible o difamatoria sobre personas o instituciones en cualquier sitio o herramienta disponible en línea (correo electrónico, webs, wiki, redes sociales, chat, foros, etc.).
- Hacer uso del servicio de Internet sin contar con las herramientas básicas de resguardo y seguridad ya instaladas en el computador o en el dispositivo a emplear, a saber: antivirus y las actualizaciones del sistema operativo que posea el computador o dispositivo. La validación de estas condiciones, pueden ser consultadas en Soporte de Infraestructura.
- Hacer uso de herramientas de software instaladas que habiliten servicios potencialmente riesgosos para el organismo. La validación de estas condiciones debe consultarse con Soporte de Infraestructura.
- El uso del servicio de Internet, en situaciones que afecten la dignidad humana, tenga carácter discriminatorio u ofensivo, sean usados para amenazar y generar persecuciones a personas o empresas, generen situaciones de acoso laboral, sexual, contrarias a la moral, pornografía o similares.

10.- Recursos de Conectividad

El organismo se reserva el derecho de establecer la prioridad para la prestación del servicio de acceso a Internet y sus servicios en función del análisis de las necesidades propias en un momento dado.

Todos los usuarios aceptan tácitamente esta pauta de la prestación del mismo.

11.- Capacitación y Concientización

Se deberá desarrollar e implementar un programa de capacitación y concientización sobre seguridad en Internet, para todos los usuarios, enfocándose en las consecuencias del uso indebido y las mejores prácticas para mantener la seguridad personal y corporativa en línea.

12.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 29 - Política de Desarrollo de Software Seguro

1.- Objetivo

El objetivo de este documento es garantizar la seguridad de la información como parte integral del ciclo de vida de los sistemas de información a ser utilizados por el organismo, el cual incluye las fases de relevamiento de requerimientos, diseño, desarrollo, prueba, integración, aceptación, y puesta en producción de los sistemas de información.

Las actividades de mantenimiento de los sistemas de información son consideradas como parte del ciclo de vida del sistema de información, y deberán cumplir con cada una de las etapas del ciclo antes mencionado.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

El alcance de esta Política incluye a todos los funcionarios del organismo, así como a las empresas o profesionales externos contratados, involucrados en el proceso de desarrollo de aplicaciones y sistemas de información.

La misma es aplicable a todos los sistemas de información desarrollados y/o mantenidos por el organismo, ya sean en forma interna, así como también por empresas o profesionales externos contratados para tales efectos.

También aplica a cualquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

La Comisión de Seguridad de la Información (CSI) debe asegurar que los temas abordados en esta política se ejecuten y se cumplan, identificando cómo se manejan los no cumplimientos, promoviendo la difusión y sensibilización sobre los temas abordados en este documento, revisando periódicamente la política detectando y proponiendo mejoras.

El Director de Desarrollo deben cumplir cabalmente con las disposiciones y requerimientos establecidos en la presente política. Asimismo, deberán velar por la correcta implementación de las normas de desarrollo seguro de sistemas promovidas por el organismo dentro de sus áreas de responsabilidad, así como del cumplimiento por parte de sus equipos de trabajo.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Gestión de Cambios

5.- Desarrollo Y Mantenimiento Seguro

5.1.- Cumplimiento De La Legislación

Serán tenidas en cuenta y serán de cumplimiento todas las normas legislativas de aplicación al momento de la realización de un desarrollo nuevo, así como se deberá adaptar cualquier desarrollo previamente realizado para dar cumplimiento a las mismas.

5.2.- Lineamientos Generales

Esta política comprende las reglas para el desarrollo de aplicaciones y sistemas de información dentro del organismo. Para esto, se establecen los siguientes lineamientos:

- Todo sistema desarrollado el organismo debe cumplir con las disposiciones de esta política.
- En el contexto de esta política, se define sistemas críticos como aquellos componentes de software desarrollados interna o externamente, que son parte sensible del organismo.
- Se deberán utilizar técnicas de programación segura tanto para los desarrollos nuevos como en las situaciones de reutilización de códigos donde es posible que no se conozcan las normas que se aplicaron al desarrollo o donde no sean coherentes con las buenas prácticas actuales.
- Se deben estandarizar los criterios de seguridad y de calidad a ser considerados durante cada fase del ciclo de desarrollo de los sistemas de información.
- Se debe estandarizar el ciclo de vida del desarrollo de software, logrando con ello los siguientes objetivos:
 - Definir actividades a llevarse a cabo en un proyecto de desarrollo de software.
 - Unificar criterios para el desarrollo de software.
 - Proporcionar puntos de control y revisión.
 - El desarrollo de trabajo externo debe seguir las mismas etapas definidas en este documento.
- Adicionalmente, en el desarrollo de sistemas por terceros, se deben celebrar contratos que contengan cláusulas que resguarden la propiedad intelectual, y aseguren los niveles de confidencialidad de la información, entre otros temas.

Los objetivos específicos de esta política son:

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- Identificar toda la información relacionada con las aplicaciones (usuarios y restricciones de acceso, interoperabilidad, reglas de respaldos, disponibilidad y ventanas de trabajo entre otros.
- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información.
- Establecer los niveles de acceso apropiados a la información institucional, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

5.3.- Consideraciones Generales

Desde las primeras etapas del proceso de desarrollo de aplicaciones deben considerarse aspectos relativos a la seguridad de las aplicaciones, además de los aspectos funcionales.

Durante la etapa de Análisis deben identificarse tanto los requisitos de seguridad como su respectiva validación.

Es la etapa de Diseño deberán diseñarse los controles necesarios para satisfacer los requisitos identificados anteriormente.

En la etapa de Implementación deben implementarse los controles de seguridad además de aplicarse los controles relativos al proceso de desarrollo de software, aquellos controles que deban estar en la aplicación, como por ejemplo validaciones a realizarse en el software, encriptación, etc.

En la fase de Verificación se debe verificar adecuadamente que los requisitos de seguridad de la aplicación se cumplen.

5.4.- Descripción del Proceso

Toda solicitud deberá estar debidamente justificada y será evaluada, en cuanto a funcionalidad y seguridad, antes de ser aceptada. Quién presenta un requerimiento, deberá hacerlo con suficiente antelación y ejecución, así como el impacto o efectos que su aplicación tendrá en los procesos de negocios y objetivos estratégicos.

5.4.1.- Análisis Previo del Sistema de Información

Como parte de la fase de evaluación se debe clarificar la problemática actual referida a la seguridad de la información, que debe ser cubierta por el nuevo sistema.

En el estudio de factibilidad, se debe considerar el aspecto de seguridad, en cuanto al nivel de criticidad del sistema, y de los controles que se deberían predefinir.

Se debe recolectar y autorizar debidamente los requerimientos de los usuarios para realizar el documento inicial para el desarrollo de este.

5.4.2.- Diseño del Sistema de Información

En el diseño de un proyecto, se deben considerar:

- Diseño de presentación – permitirá determinar cómo el usuario solicitando verá el sistema cuando esté finalizado
- Diseño de arquitectura – permitirá indicar el tipo de proyecto (web, escritorio, webservices, móvil, etc.), su interacción con otros desarrollos, definido el lenguaje en que se desarrollará.
- Diseño de base de datos – permitirá generar el diseño lógico de los datos involucrados.
- Lógica del sistema – permitirá generar el desarrollo conceptual del modelo de negocio que permita el mejor desarrollo del proyecto.

En la medida de lo posible, en todos los sistemas de información se deberá implementar la generación de registros de auditoría de las transacciones realizadas por el sistema, los cuales deberán ser protegidos contra el acceso y la manipulación no autorizada.

Dichos registros de auditoría deberían incluir la identificación de usuario que crea o modifica el registro, la fecha y hora del evento creado o modificado, así como la información que tenía originalmente y la nueva información que actualiza a la anterior.

5.4.3.- Entorno de Desarrollo Seguro

El entorno de desarrollo seguro debe considerar los aspectos de seguridad de la información en:

- La fase de diseño de los proyectos de desarrollo de aplicaciones y sistemas de información.
- El entorno de desarrollo, identificando el conjunto de procesos y herramientas que se utilizan para desarrollar un código fuente o programa.
- El ciclo de desarrollo de software, en particular:
 - Seguridad en la metodología de desarrollo de software.
 - Pautas de codificación segura para cada lenguaje de programación o sistema, que se utiliza.
 - Es establecimiento de puntos de verificación de seguridad dentro de los hitos del proyecto de desarrollo.
 - Los repositorios de información asociados a los proyectos de desarrollo.
 - El manejo del control de versiones de los proyectos de desarrollo.
 - La capacidad del equipo de desarrollo para:
 - Conocer las condiciones de seguridad de las aplicaciones desarrolladas.
 - Evitar, encontrar y resolver las vulnerabilidades de los desarrollos.
- Las condiciones contractuales de los desarrolladores externos o de las empresas contratadas.
- Los desarrollos ejecutados por los desarrolladores externos o por las empresas contratadas.

5.4.4.- Desarrollo y Testing

Existe prohibición de:

- Escribir o modificar cualquier tipo de código malicioso para ser incluido en el desarrollo de aplicaciones o sistemas de información.
- Incluir funciones u operaciones no documentadas o no autorizadas en las aplicaciones o sistemas de información.
- Modificar aplicaciones sin la correspondiente autorización.
- Modificar aplicaciones sin que quede registrado o documentado el cambio.

La generación de código fuente debe quedar en el repositorio correspondiente para tener la trazabilidad de las modificaciones.

El acceso lógico al código fuente de los distintos sistemas de información debe estar protegido con acceso restringido, exclusivamente a los funcionarios autorizados.

En caso de que el funcionario sea un profesional contratado, el acceso al código será sólo por el período que dure el proyecto.

Toda empresa externa que trabaje con código de sistemas críticos deberá haber firmado un acuerdo confidencialidad y de no divulgación.

El desarrollo de los sistemas de información se realiza en un ámbito local, utilizando datos de bases de datos propias de desarrollo, diferentes a las bases de datos de producción.

El desarrollo se basa en el documento de relevamiento de requerimientos.

Deben considerarse al menos dos tipos de pruebas, las que realizará el equipo de Testing, y las que realizará el usuario solicitando para la aceptación del sistema de información.

Las pruebas del sistema deben quedar documentadas en el plan de pruebas e incluir:

- Pruebas funcionales
- Pruebas de regresión
- Pruebas de integración
- Pruebas de rendimiento

El control de acceso usado en el ambiente de pruebas debe ser tan estricto como el usado en el ambiente de producción.

Los usuarios solicitantes que acceden al ambiente de pruebas en Pre-Producción, solo tienen acceso a lectura de la información.

Los sistemas críticos deben incluir la validación de los datos de entrada, para asegurar un correcto procesamiento.

Los sistemas críticos deben incluir controles de validación de los datos de salida, para asegurar que el procesamiento ejecutado haya sido correcto.

Los sistemas críticos que interactúan con otros sistemas deben incluir controles para asegurar la integridad de los mensajes intercambiados.

5.4.5.- Pruebas de Seguridad del Sistema de Información

Todos los sistemas de información, durante su fase de desarrollo, se someterán a pruebas y verificaciones de seguridad, incluyendo un programa de actividades detallado, entrada de pruebas, y los resultados esperados bajo una variedad de condiciones.

Se recomienda, que las pruebas del sistema incluyan entre otros aspectos, volumen, rendimiento, almacenamiento, configuración, funcionalidad, seguridad, recuperación ante errores, como mínimo.

Dentro de lo posible, las pruebas deben ser realizadas, almacenando los criterios y los datos de pruebas en archivos, de modo de permitir la verificación rápida y repetitiva.

En el contexto de la validación de los sistemas, se deberían incorporar herramientas de revisión de código y análisis de vulnerabilidades en todas las etapas del ciclo de vida del desarrollo de software, para detectar y corregir problemas de seguridad de forma continua y sistemática.

Establecer procesos formales de auditoría de seguridad luego de que la aplicación se encuentra en el entorno de producción, garantizando que se mantengan evaluaciones periódicas de seguridad que acompañen las actualizaciones y mantenimientos del software.

5.4.6.- Pre-Producción y Producción

Las pruebas de aceptación del sistema de información se deberán realizar en el entorno de Pre-Producción, (QA- Quality Assurance), de tal forma que permita, garantizar que el sistema no introducirá vulnerabilidades al entorno de Producción.

Asimismo, se deberá asegurar que las pruebas son confiables.

Para realizar las pruebas de aceptación de los sistemas de información, se podrán utilizar las herramientas automatizadas disponibles en el mercado, como las herramientas de análisis de código, o los escáneres de vulnerabilidades, y se deberá verificar la remediación de los defectos relacionados con la seguridad.

5.4.7.- Protección de los Datos en Producción

Se prohíbe el uso de bases de datos operativas (de producción), para la realización de pruebas y/o exportación de modelos y datos con externos.

5.4.8.- Separación de Ambientes

Los ambientes de desarrollo, pruebas, pre-producción y producción estarán separados preferentemente de forma física.

En el caso de los desarrollos internos se debe considerar:

- Ambiente de Desarrollo
- Ambiente de Pruebas

- Ambiente de Pre-Producción
- Ambiente de Producción

Los usuarios deben utilizar distintos perfiles de usuarios para los sistemas operacionales y los de prueba.

Los Desarrolladores tendrán acceso exclusivo al entorno de Desarrollo, no pudiendo tener acceso a ningún otro entorno operativo. Las excepciones a esta regla deberán ser aprobadas por el Oficial de Seguridad de la Información.

Los Testers tendrán acceso exclusivo al entorno de Pruebas, no pudiendo tener acceso a ningún otro entorno operativo. Las excepciones a esta regla deberán ser aprobadas por el Oficial de Seguridad de la Información.

Los funcionarios de Calidad que realizarán las pruebas de Control de Calidad (QA), y los usuarios que realizarán las pruebas de aceptación, tendrán acceso exclusivo al entorno de Pre-Preproducción y de Producción.

Ningún usuario con acceso a Producción podrá tener acceso a los entornos de Desarrollo y/o Pruebas.

Para el caso de los desarrollos externalizados, se definirán y documentarán en los Términos de Referencia, detalladamente, las reglas y pasos para la transferencia de software, desde el estado de desarrollo hacia el estado productivo.

Estas reglas deben considerar al menos los siguientes lineamientos:

- Ambiente de Desarrollo (Proveedor)
- Ambiente de Pruebas (Proveedor)
- Ambiente de Pre-Producción (OPT)
- Ambiente de Producción (OP)

Al final del proyecto, se deberá hacer el traspaso del repositorio del proyecto a el organismo.

A no ser que sea bajo circunstancias excepcionales, no se deberían realizar pruebas en los sistemas productivos. En caso de ser necesarias, estas deberán ser aprobadas por el RSI.

Toda modificación de software crítico por parches o módulos adicionales debe ser analizada previamente en el ambiente de desarrollo y/o de pruebas, antes de aplicar la misma en el entorno de Producción.

5.4.9.- Control de Cambios a Datos de Producción

Se debe planificar detalladamente las etapas de paso a producción de los cambios de datos, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, criterio de aceptación del cambio, y un plan de vuelta atrás.

Lo anterior, de acuerdo con lo establecido en el procedimiento de gestión de cambios en ambiente productivo.

5.4.10.- Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para el acceso y almacenamiento de las claves de usuarios, las bases de datos del sistema, y para la transmisión de datos del organismo.

Todo sitio o sistema web deberá encriptar todas las comunicaciones entre el cliente y el servidor. Es obligatorio utilizar el protocolo HTTPS en vez del protocolo HTTP, utilizando certificados válidamente emitidos por empresas u organizaciones debidamente acreditadas en el país.

Cumplir con lo establecido en la política de uso de controles criptográficos, sobre algoritmos de encriptación aceptados.

5.4.11.- Adquisición de Sistemas a Terceros

Se debe establecer un acuerdo previo y formal con instituciones o empresas externas, que resguarde la propiedad intelectual, uso de datos, tratamiento de datos sensibles y asegure los niveles de confidencialidad de la información manejada en el proyecto.

Además, se deberán incluir las responsabilidades de terceros en la gestión de incidentes de seguridad.

Se debe diferenciar entre el encargado de establecer y autorizar los acuerdos con terceros, de los que deban auditar su cumplimiento.

El proceso de adquisición del sistema debe ser formal y cumplir con las disposiciones de seguridad descritas en esta política.

En los casos en que se acuerde el desarrollo de aplicaciones por parte de un proveedor externo, éste deberá aceptar y aplicar las políticas de Seguridad definidas para el proceso de desarrollo, incluido los compromisos de confidencialidad, los derechos de propiedad intelectual, las condiciones de soporte y mantenimiento, y las condiciones relativas al cese de sus actividades o traspaso de sus servicios a terceros, en caso de que se permita.

Para la realización de las pruebas de software, los proveedores de desarrollo de aplicaciones deberán proveer sus propios datos de prueba. Para las pruebas de aceptación en el entorno de Pre-Producción, se podrá utilizar datos anonimizados, evitando la utilización de datos reales.

5.4.12.- Control de Acceso al Código Fuente de las Aplicaciones

Se debe restringir el acceso al código fuente de las aplicaciones y sistemas de información.

El acceso al código fuente de los programas y los elementos asociados (como diseños, especificaciones, planes de verificación y validación), se debe controlar estrictamente, para poder evitar la introducción de funcionalidades no autorizadas, y para evitar los cambios no intencionales.

Para el código fuente de aplicaciones, deberá implementar un almacenamiento central controlado para dicho código, de preferencia en bibliotecas de fuentes de aplicaciones, incluyendo un sistema de versionado.

Por lo tanto, se deben considerar las siguientes pautas para controlar el acceso a dichas bibliotecas de fuentes de aplicaciones y poder reducir el potencial de corrupción de las aplicaciones.

- Donde sea posible, las bibliotecas de fuentes de programas no se deberían mantener en los sistemas operacionales.
- El código fuente de los programas y las bibliotecas de fuentes de los programas se deben administrar de acuerdo con los procedimientos establecidos.
- El personal de apoyo no debe contar con acceso sin restricciones a las bibliotecas de fuentes de las aplicaciones.
- La actualización de las bibliotecas de los códigos fuentes de las aplicaciones y los elementos asociados, junto con la emisión de los códigos fuentes de las aplicaciones a los desarrolladores solo se debe realizar cuando se haya recibido la autorización y se realizará en un entorno seguro.
- Las listas de aplicaciones se deben mantener en un entorno seguro.
- Se debe mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes de aplicaciones.

Si el código fuente de programas está pronto para ser publicado, se debería considerar controles adicionales para ayudar a obtener una garantía de su integridad, por ejemplo, firma digital.

6.- Capacitación y Concientización

Se debe desarrollar un programa de capacitación y concientización en seguridad para desarrolladores, incluyendo formación específica en técnicas de programación segura, normativas de seguridad aplicables y metodologías de desarrollo ágil seguro.

7.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Alta Dirección del organismo, a través del Departamento de Personal podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 30 - Política de Gestión de la Seguridad de las Redes

1.- Objetivo

Establecer las reglas necesarias para garantizar el funcionamiento correcto y seguro de las redes de datos y de comunicaciones del organismo.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo que accede a la red de datos y de comunicaciones, así como los proveedores que tienen permisos de acceso a dichas redes.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Director de Infraestructura debe asegurar la correcta administración de las mencionadas redes de acuerdo a los criterios establecidos en esta política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Control de Acceso Lógico

- Política de Clasificación de la Información
- Política de Separación de Entornos
- Política de Uso de Controles Criptográficos

5.- Gestión De La Seguridad De Las Redes

5.1.- Administración Y Control De Las Redes

El organismo es responsable de administrar y controlar las redes de datos y de comunicaciones, para garantizar la seguridad de la información en las redes y para proteger los servicios conectados a las redes del acceso no autorizado.

Se requiere el cumplimiento de:

- Separar la responsabilidad operativa de las redes, de la responsabilidad de las aplicaciones sensibles y otros sistemas.
- Proteger los datos sensibles que pasan a través de la red pública de acuerdo a lo establecido en la Política de Clasificación de la Información.
- Segregar las redes cableadas e inalámbricas de acuerdo con la Política de Separación de Entornos.
- Proteger los equipos que se conectan a la red desde ubicaciones remotas empleando conexiones VPN que utilicen los algoritmos de cifrados descritos en la Política de Uso de Controles Criptográficos.
- Segregar el tráfico procedente de dispositivos móviles, configurar las políticas de firewall y de WAF, las rutas estáticas, las redes de área local virtuales (/VLAN), etc.
- Deshabilitar los puertos de red que no estén en uso en los servidores.
- Monitorear y alertar toda nueva conexión a la red del organismo.
- La Comisión de Seguridad de la Información (CSI) debe supervisar y probar regularmente los controles implementados.
- Se deben establecer revisiones y actualizaciones regulares de las configuraciones de seguridad en la red y las políticas de firewall para asegurar que se mantengan al día con las últimas amenazas y mejores prácticas.

- Se deben incorporar tecnologías de detección de anomalías y gestión de incidentes de seguridad en tiempo real, para mejorar la capacidad de respuesta a amenazas y vulnerabilidades en la red.

5.2.- Servicios de Red

La CSI debe definir las características de seguridad y el nivel de servicios esperados para todos los servicios de red, independientemente de si estos servicios se prestan de manera interna o externa. Dichos requisitos deben documentarse con los proveedores de servicios.

Si los servicios de red se subcontratan, entonces los requisitos deben especificarse en el acuerdo tal como se define en la Política de Seguridad de Relacionamiento con Proveedores.

Se adoptará e implementarán sistemas de autenticación de múltiples factores para el acceso a todos los sistemas y recursos críticos, complementando la actual política de gestión de usuario y contraseña.

5.3.- Transferencia De Información

La CSI en alineación con la Política de Clasificación de la Información, establece los canales de comunicación permitidos para cada tipo de información, así como las restricciones y permisos asociados a su uso. Asimismo, define las actividades prohibidas en dichos canales.

Los canales de comunicación para el intercambio de información incluirán, dependiendo del nivel de sensibilidad de la información, el correo electrónico, la descarga de archivos de Internet, la transferencia de datos a través de protocolos seguros (por ejemplo y no exclusivamente, implementando Redes Privadas Virtuales (VPN), SSH File Transfer Protocol (SFTP) o Secure Copy Protocol (SCP), etc.), teléfonos, máquinas de fax, mensajes de texto SMS y cualquier tecnología que pueda surgir en el futuro y sea considerada segura por la CSI.

Además de los controles prescriptos en la Política de Clasificación de la Información, la CSI prescribe controles adicionales para cada tipo de datos y canal de comunicación, en función de los resultados de la evaluación de riesgos.

6.- Capacitación y Concientización

Desarrollar programas de capacitación y concientización en seguridad de redes para todo el personal del organismo, enfocando en la importancia de las prácticas de seguridad y la detección temprana de actividades sospechosas.

7.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 31 - Política de Gestión de Riesgos de Proveedores

1.- Objetivo

Consiste en detectar a tiempo los riesgos vinculados con los proveedores que pueden afectar a las diferentes áreas del organismo. Esta detección deberá servir para generar estrategias que se anticipen a los riesgos y los conviertan en oportunidades útiles reforzando la continuidad operativa del negocio y asegurando la adaptabilidad a los cambios del entorno.

Los principales objetivos de esta política son:

- Aportar un marco de referencia para los procedimientos de Gestión del Riesgo de los Proveedores y para sus diferentes herramientas y documentos.
- Identificar los riesgos de los proveedores a los que están expuestas las diversas áreas del organismo siguiendo lineamientos definidos en la estrategia de la empresa.
- Desarrollar la evaluación de los riesgos y la medición del grado de exposición a los mismos.
- Gestionar efectivamente los riesgos.
- Facilitar la toma de decisiones que estén encaminadas a la administración y al control de los riesgos.
- Monitorear los riesgos mediante el seguimiento de los planes de acción sobre los riesgos analizados para garantizar que éstos se mantengan dentro de los niveles aceptados por el organismo.
- Desarrollar un reporte periódico sobre la Gestión del Riesgo de los Proveedores.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

La política se aplicará a todos los proveedores en todos los niveles y actividades relevantes del organismo, donde se identifiquen riesgos u oportunidades que puedan afectar el cumplimiento de los objetivos establecidos.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo que interactúen con un proveedor es responsable de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Seguridad de la Información
- Política de Protección y Privacidad de los Datos
- Política de Relacionamiento con Proveedores
- Política de Gestión de Incidentes de Seguridad de la Información

5.- Estructura

Esta política está estructurada mediante el desarrollo de los lineamientos incluidos en las secciones: Evaluación, Gestión, Exención, y Aplicación.

5.1.- Evaluación

Se mantienen todos los criterios generales de riesgo inherente del organismo para todos los proveedores.

Todo proveedor al que el organismo le haya otorgado acceso a los recursos de información del organismo debe firmar el Acuerdo de Confidencialidad de Proveedores y el Contrato de Servicios con el organismo, el cual incluirá el Acuerdo de Niveles de Servicio (si corresponde).

Todas las relaciones con proveedores deben ser evaluadas en busca de riesgos inherentes a la seguridad de la información antes de cualquier interacción con los recursos de información del organismo.

Todas las relaciones con los proveedores deben reevaluarse periódicamente para detectar riesgos inherentes a la seguridad de la información.

Cada vez que haya un cambio sustancial en la forma en que el organismo utiliza el producto o servicio del proveedor, se deberán reevaluar los riesgos inherentes del proveedor.

Las relaciones con proveedores con un riesgo inherente significativo (clasificados como “Muy Alto”, “Alto” o “Medio”) deben evaluarse para determinar el riesgo residual mediante cuestionarios, información disponible públicamente y/o herramientas técnicas.

Las evaluaciones de riesgo residuales de seguridad de la información deben tener en cuenta los controles administrativos, físicos y técnicos.

Se deben establecer umbrales de riesgo residual de seguridad de la información para las relaciones con proveedores con un riesgo inherente significativo (clasificados como “Muy Alto”, “Alto” o “Medio”).

Las relaciones con proveedores que no cumplan con los umbrales de riesgo residual de seguridad de la información establecidos:

- Deben ser terminadas.
- Debe ser aprobadas formalmente por el Directorio siguiendo un proceso de exención establecida.
- Modificada de manera que reduzca el riesgo inherente o residual de seguridad de la información, garantizando el cumplimiento de los umbrales establecidos.

Las relaciones con proveedores relacionadas con la industria y/o los requisitos regulatorios (es decir, PCI-DSS, HIPAA, etc.) deben ser revisadas con una frecuencia anual por lo menos.

5.2.- Gestión

Los acuerdos y contratos de proveedores deben especificar:

- La información del organismo a la que el proveedor debe tener acceso.
- Cómo la información del organismo debe ser protegida por el proveedor.
- Cómo se transferirá la información del organismo entre el organismo y el proveedor.
- Métodos aceptables para la devolución, destrucción o eliminación de la información del organismo en posesión del proveedor al final de la relación contractual.
- Requisitos mínimos de seguridad de la información y protección de datos.
- Derecho del organismo a auditar las protecciones y controles de seguridad de la información del proveedor.

Si el proveedor subcontrata parte del servicio de tecnología de la información y la comunicación proporcionada a el organismo, el proveedor debe garantizar que se sigan las prácticas adecuadas de seguridad de la información en toda la cadena de suministro.

El proveedor sólo debe acceder a los recursos de información del organismo para cumplir con el propósito del contrato y/o acuerdo comercial.

El trabajo fuera de los parámetros definidos en el contrato debe ser aprobado por escrito por el punto de contacto apropiado del organismo.

El rendimiento de los proveedores debe revisarse anualmente para garantizar el cumplimiento de los contratos acordados y/o los acuerdos de nivel de servicio (SLA). En caso de incumplimiento de los contratos o SLA, se realizarán revisiones regulares hasta que se cumplan los requisitos de desempeño.

Las principales actividades de trabajo de tecnología de la información del proveedor deben ingresarse o capturarse en un registro:

- Debe estar a disposición de la División TIC a pedido.
- Debe incluir eventos como cambios de personal, cambios de contraseña, hitos del proyecto, entregables y horas de llegada y salida, si correspondiera.

Cualquier otra información del organismo adquirida por el proveedor durante el contrato no puede ser utilizada para los propios fines del proveedor ni divulgada a otras partes.

El proveedor debe notificar de inmediato cualquier incidente de seguridad al personal correspondiente del organismo.

El organismo proporcionará un punto de contacto técnico para el proveedor. El punto de contacto trabajará con el proveedor para garantizar el cumplimiento de esta política.

Los proveedores deben proporcionar a el organismo una lista del personal clave que trabaja en el contrato cuando se le solicite.

Los proveedores deben proporcionar a el organismo una notificación de los cambios de personal clave dentro de las 24 horas posteriores al cambio.

Ante la salida de un empleado de un proveedor de un contrato, por cualquier motivo, el proveedor se asegurará de que toda la información confidencial se recopile y se devuelva a el organismo o se destruya dentro de las 24 horas posteriores.

Al finalizar el contrato se debe recordar a los proveedores los requisitos de confidencialidad y no divulgación vinculados.

A la terminación del contrato a solicitud del organismo, el proveedor debe entregar todas las credenciales, tarjetas de acceso, equipos y suministro del organismo de inmediato.

Cualquier equipo y/o suministro que retenga el proveedor debe ser documentado por la División TIC del organismo.

5.3.- Exenciones

Se pueden solicitar exenciones de determinadas disposiciones específicas de la política. No hay excepciones a las disposiciones señaladas en esta política hasta que se haya otorgado una exención.

5.4.- Aplicación

Esta Política de Gestión de Riesgos de Proveedores complementa todas las demás políticas de seguridad de la información relacionadas, no sustituyendo a ninguna de esas políticas y viceversa.

Cuando existan conflictos percibidos o no intencionados entre las políticas del organismo, los mismos se deben señalar a la dirección del organismo para su reconciliación inmediata.

El personal que haya violado cualquier disposición de esta política puede estar sujeto a sanciones que pueden incluir la eliminación de los derechos de acceso, la rescisión del empleo, la rescisión de los contratos y/o sanciones civiles o penales relacionadas.

6.- Marco Rector

El marco rector aplicable es el que se estableció en la Política de Gestión de Riesgos del organismo.

7.- Clasificación de Amenazas y Riesgos

La clasificación de amenazas y riesgos aplicable es la que se estableció en la Política de Gestión de Riesgos del organismo.

8.- Capacitación y Concientización

Desarrollar el programa de capacitación y concientización sobre la gestión de riesgo de proveedores a todos los niveles de la organización, enfocándose en cómo las acciones de los proveedores pueden impactar la seguridad de la información del organismo.

9.- Cumplimiento

En caso de detectarse el incumplimiento de lo establecido en la política regulada por este documento, la Alta Dirección del organismo, a través del Departamento de Personal, podrá adoptar las medidas que considere necesarias para garantizar su cumplimiento.

Pol 32 - Política de Gestión de Activos

1.- Objetivo

Un activo es cualquier elemento que tenga valor para el organismo.

El organismo comprende la importancia de una adecuada gestión de activos, por lo cual es esencial para el sistema de gestión de la seguridad de la información, contar con un inventario y clasificación de los activos, dado que a través de éste se conoce cuántos activos tiene la organización, quiénes son sus propietarios y los responsables de los mismos, así como el nivel de clasificación que tienen, para conocer qué tratamiento debe dárseles, con el fin de evitar la materialización de riesgos en la organización.

El objetivo de esta política es garantizar la adecuada gestión de los activos del organismo que incluye el inventario y la clasificación en términos de confidencialidad, integridad y disponibilidad.

Los objetivos específicos son:

- Identificar los activos y definir las responsabilidades de protección apropiadas.
- Asegurar que los activos reciban un nivel apropiado de protección de acuerdo con la importancia y criticidad para la organización.
- Evitar la divulgación, modificación, el retiro o la eliminación no autorizada de cualquier activo de información.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

Todo el personal del organismo que hace uso de activos de información para desempeñar sus responsabilidades laborales.

Todos los proveedores que hacen uso de activos de información del organismo para desarrollar la atención y los requisitos relacionados con sus propios servicios.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

Todo el personal del organismo es responsable de cumplir con lo establecido en la presente política.

4.- Políticas Relacionadas

- Política de Clasificación de la Información
- Política de Uso Aceptable de los Activos
- Política de Gestión de Riesgos
- Política de Gestión de Riesgos de Seguridad de la Información

5.- Activos

Existen diferentes tipos o formas de activos.

Los activos físicos, como ser:

- Infraestructura física y de Tecnología de la Información (TI): Edificios, oficinas, centro de datos, cuartos de servidores y equipos, armarios de red (Racks), cableado, escritorios, cajones, archivadores, salas de almacenamiento de medios físicos, dispositivos de identificación y autenticación, controles de accesos del

personal y otros dispositivos de seguridad como por ejemplo cámara de circuito cerrado de TV, lectores biométricos, etc.

- Controles del entorno de TI: Alarmas, sistema de refrigeración, sistema de supresión contra incendio, sistemas de alimentación ininterrumpida UPS), planta eléctrica, alimentación de potencia y de red.
- Hardware de TI: Computadoras de escritorio y portátiles, dispositivos de almacenamiento, servidores, dispositivos de comunicaciones, impresoras, escaners, fotocopadoras, etc.
- Documentación: Procedimientos, programas, guías, formatos, manuales, y demás documentación física de propiedad de la organización.
- Los activos de servicios de TI, como ser:
 - Servicios de autenticación y administración de usuarios, aplicaciones, servidores proxy, servicios de red, servicios web, servicios inalámbricos, antivirus, antispymware, antispam, detección y prevención de intrusos, seguridad, protocolos de transferencia de archivos (FTP), bases de datos, correo electrónico y mensajería instantánea, herramientas de desarrollo, contratos de soporte y mantenimiento de software, etc.

Los activos intangibles, como la información.

La información puede existir en muchas formas: impresa, manuscrita, almacenada en discos o en medios magnéticos, en medios electrónicos, en archivos, en presentaciones, en videos o en conversaciones, etc.

Cualquiera que sea la forma de existencia de la información, ésta siempre debe estar protegida adecuadamente, para preservar la confidencialidad, integridad y la disponibilidad de la misma.

Para esto el dueño debe clasificarla para identificar la necesidad, prioridad y el grado de protección que requiere para comunicar el requerimiento de medios de tratamiento.

6.- Gestión de los Activos de Información

La Gestión de Activos es importante para conocer todos los activos que se encuentran en la organización para que se puedan proteger de una forma adecuada, justificándolos y asegurándose que tengan un propietario asignado.

La Gestión y Clasificación de Activos de Información debe llevarse como un componente fundamental del Sistema de Gestión de Seguridad de la Información y específicamente de la Metodología de Gestión de Riesgos de la organización, a fin de identificar, analizar, valorar y administrar los riesgos de los activos de información. Así mismo, los activos de información deben ser clasificados según su sensibilidad y criticidad de la información que contienen.

La clasificación de los activos de información se debe realizar acorde con el alcance definido para la implementación del SGSI, y de la Política de Seguridad de la Información y Privacidad de Datos, y debe estar alineada con la norma ISO/IEC 27001:2022 con el objeto de garantizar el cumplimiento de los puntos descritos a continuación:

- **Inventario de archivos:** Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de activos.
- **Propiedad de los activos:** Los activos mantenidos en el inventario deben tener un propietario.
- **Clasificación de la información:** La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
- **Etiquetado de la información:** Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
- **Manejo de activos:** Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

El organismo debe mantener un inventario de activos de información, que incluya su categoría, nombre y propietario.

El propietario designado para un activo es responsable de la correcta gestión del mismo, durante todo su ciclo de vida.

El propietario del activo debe:

- Asegurar que los activos son inventariados;
- Asegurar que los activos son clasificados y protegidos adecuadamente;
- Definir y revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables de control de acceso;
- Garantizar el manejo adecuado cuando el activo es eliminado o destruido.

El propietario identificado puede ser un individuo o grupo aprobado por la dirección para el control de todo el ciclo de vida de un activo.

El propietario identificado no necesariamente tiene ningún derecho de propiedad sobre el activo.

Las tareas rutinarias pueden ser delegadas, por ejemplo, a un guardia que vigile el activo diariamente, pero la responsabilidad continúa siendo del propietario.

El inventario se debe identificar, documentar y actualizar ante cualquier modificación de la información y los activos asociados con los medios de procesamiento. Este debe ser revisado con una periodicidad no mayor a un año.

Cada uno de los activos incluidos en el inventario debe ser clasificado de acuerdo con lo establecido en la política POL-03 Política de Clasificación de la Información.

7.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la política que regula este documento, la Alta Dirección del organismo, a través del Departamento de Personal podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Pol 33 - Política de Gestión de Riesgos

1.- Objetivo

Esta política tiene como propósito, definir criterios para el desarrollo formal de las actividades relacionadas con la Gestión del Riesgo en el organismo tal como deben desplegarse en sus áreas operativas.

Como referencia documental esta política considera el marco teórico de la estructura de control de COSO II y los principios fundamentales de las normas UNIT-ISO 31000.

Los principios, el marco seleccionado, el proceso, y las normas para la gestión del riesgo, que aquí se exponen, proponen el diseño e implementación de un marco de trabajo que facilite el llevar adelante evaluaciones de riesgo de manera eficaz y eficiente en el organismo.

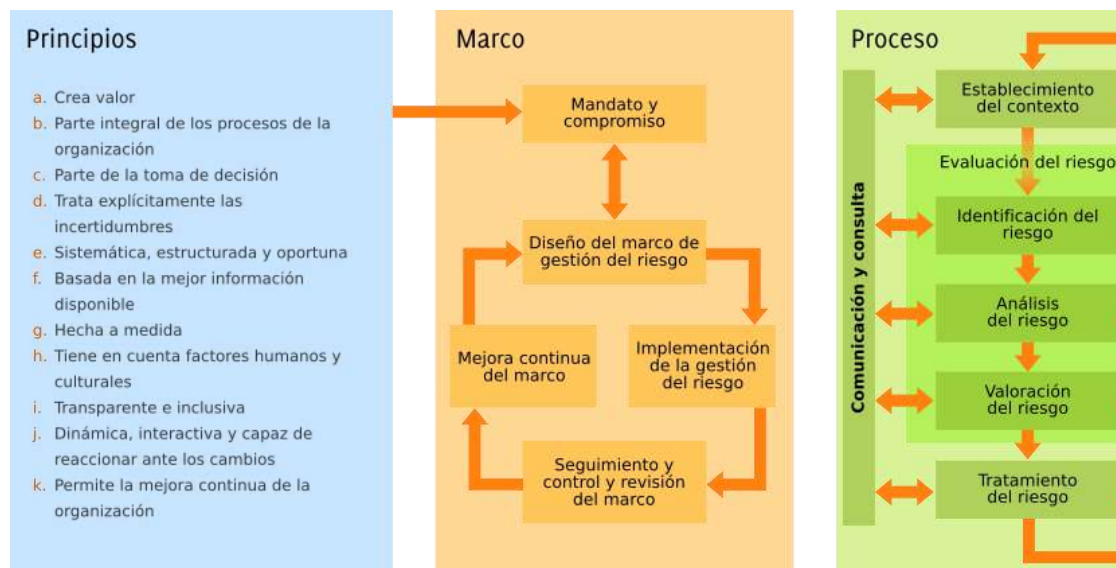


Imagen 1: Principios, marco seleccionado, proceso y normas

La Gestión del Riesgo consiste en detectar a tiempo los riesgos que pueden afectar a las diferentes áreas del organismo, a nuestras actividades en la empresa y a los objetivos que están asociados a ellas. Esta detección deberá servir para generar estrategias que se

anticipen a los riesgos y los conviertan en oportunidades útiles reforzando la continuidad operativa del negocio y asegurando la adaptabilidad a los cambios del entorno.

Los objetivos principales que persigue esta política son:

- Aportar un marco de referencia para los procedimientos de Gestión del Riesgo y para sus diferentes herramientas y documentos.
- Identificar los riesgos a los que están expuestas las diversas áreas del organismo siguiendo lineamientos definidos en la estrategia del organismo.
- Desarrollar la evaluación de los riesgos y la medición del grado de exposición a los mismos.
- Gestionar efectivamente los riesgos.
- Facilitar la toma de decisiones que estén encaminadas a la administración y al control de los riesgos.
- Monitorear los riesgos mediante el seguimiento de los planes de acción sobre los riesgos analizados para garantizar que éstos se mantengan dentro de los niveles aceptados por el organismo.
- Desarrollar un reporte periódico sobre la Gestión del Riesgo en el organismo.

1.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

1.2.- Validez y Gestión Documental

Este documento es válido a partir de la fecha de aprobación por parte de la Comisión de Seguridad de la Información (CSI).

El propietario del documento es la CSI, quien debe revisar y actualizar el documento si es necesario al menos una vez al año.

2.- Alcance

La política debe ser aplicada en todos los niveles y actividades significativas del organismo, donde se evidencien riesgos u oportunidades que impacten el cumplimiento de los objetivos propuestos.

Es responsabilidad de cada uno de los miembros del organismo implementar y cumplir con los controles establecidos para la gestión de los riesgos de forma que:

- Profundicemos en nuestra cultura de Gestión del Riesgo del organismo y en la interacción con nuestros usuarios.
- Definamos roles y responsabilidades en la Gestión del Riesgo y mecanismos de reporte y escalamiento.
- Consideremos cada uno de los riesgos derivados de las definiciones estratégicas y de los procesos del negocio para identificarlos adecuadamente, planificar su seguimiento, su evaluación y el tipo de gestión que se defina como necesaria.

3.- Responsabilidades

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento de la presente política.

El Directorio es responsable de establecer los niveles de riesgo aceptados, custodia la existencia de un adecuado sistema de control.

La Alta Dirección ejecuta el seguimiento de la realización de análisis de riesgos en las actividades de sus áreas y consolida la preparación de los planes de acción alrededor de los hechos evidenciados por cada análisis. Define el marco para las actividades de control. Monitorea los indicadores de desempeño establecidos para la gestión de riesgos. Facilita la comunicación, el entrenamiento y el proceso de gestión de riesgos dentro de la organización; centraliza el proceso de gestión de riesgos.

La Comisión de Seguridad de la Información (CSI) evalúa la eficacia del proceso de control, designa recursos para los análisis de riesgos y recomienda la implementación de medidas cuando se supera los niveles de exposición al riesgo deseables.

4.- Definiciones Generales y Conceptos Aplicables a la Gestión Del Riesgo

Los riesgos de seguridad de la información pueden provenir de diversas fuentes, y en un panorama de amenazas en constante evolución, el proceso de identificación podría ser muy complejo y difícil si no definimos un abordaje metodológico que contemple esas características.

A efectos de establecer una misma interpretación para los conceptos que se vinculan con esta política, esta sección contiene las definiciones generales que resultan relevantes para una primera aproximación al tema.

- Probabilidad: Medida para la estimación de ocurrencia ante un evento determinado, donde 0 es la no ocurrencia y 1 la ocurrencia del evento.
- Frecuencia: Número de veces que un evento ocurre en determinado tiempo.
- Severidad: Impacto que el evento tiene al materializarse. Puede ser impacto económico, reputacional, humano, operativo, técnico, ambiental, etc.
- Nivel de Riesgo: Ponderación que se otorga al riesgo.
- Tolerancia al riesgo: Nivel de riesgo aceptado para determinado evento o situación.
- Factores de influencia: Aspectos que contribuyen para que un evento se materialice.
- Perfil de riesgo: Grado de aceptación que se tiene por la ocurrencia o no de eventos negativos distinguiendo las siguientes categorías: Aversión al riesgo (Conservador), Tolerante al riesgo (Moderado) y Preferencia del riesgo (Agresivo).
- Riesgo: Posibilidad de que se materialice un evento que pueda impactar los objetivos estratégicos en una determinada organización.
- Riesgo Inherente: Riesgo que se genera por el desarrollo de la actividad de la organización sin la aplicación de controles.
- Riesgo Residual: Exposición al riesgo que tiene la organización una vez ha aplicado controles para mitigar los mismos.
- Control: Son acciones o actividades implementadas por el organismo para reducir probabilidad e impacto de la materialización de un riesgo.

5.- Marco Rector

Todos los miembros del organismo son responsables de la identificación y comunicación de los riesgos asociados a sus tareas y responsabilidades. La prevención es un mecanismo clave para el tratamiento oportuno en los aspectos que representan vulnerabilidades.

La gestión de riesgos es un proceso orientado a la generación de valor. Por ese motivo debemos tomar las decisiones respecto al riesgo de acuerdo con los niveles que fueron establecidos y previamente aceptados en la estrategia de la empresa.

La gestión de riesgos prioriza los niveles de exposición y las consecuencias por su materialización. El tratamiento del riesgo se define en función de esas variables.

La gestión de riesgos en el organismo se integra con las políticas y procesos de la empresa. Ante nuevos procesos que proyecte incorporarse, se debe verificar que sean coherentes con esta política.

La administración de los riesgos debe ser oportuna, sistemática y alineada con los objetivos estratégicos del organismo y de cada una de sus áreas.

No existiendo, en el momento actual, un área a cargo de la Gestión de Riesgos, la CSI es responsable de aprobar las propuestas para los documentos modelo con los cuales se debe reportar la gestión de riesgos, así como es responsable de designar un responsable para el diseño de la matriz y el mapa de riesgos del organismo.

El criterio de clasificación de los riesgos se basa en su severidad sobre los siguientes aspectos: humanos, económicos, técnicos (privacidad, seguridad, cumplimiento, etc.) y reputacionales. En todos los casos se expresan en niveles que se ponderan como Bajo, Medio, Alto y Muy alto.

El proceso de gestión de riesgos a seguir en el organismo deberá cumplir sistemáticamente con las siguientes etapas:

1. Contexto de los riesgos: Corresponde a una primera etapa donde las situaciones identificadas se contextualizan con la realidad de la organización.
2. Identificación de Riesgos: Es una etapa fundamental, que permite visualizar, listar, entender y definir los riesgos.
3. Análisis de los riesgos: Una vez identificados los riesgos se debe asociar a cada uno de ellos información sobre frecuencia, es decir cada cuanto ocurre el hecho identificado; severidad, es decir las consecuencias que ese hecho tiene sobre la organización en términos económicos, de imagen, seguridad, humanos y de la información; probabilidad de ocurrencia.
4. Plan de respuesta a los riesgos: Con la evaluación de riesgos, se definirá Responsables, Acciones (y estrategias) para Evitar, Mitigar, Transferir o Aceptar los riesgos identificados.
5. Monitoreo y evaluación: Se debe registrar y actualizar los riesgos y su calificación. Luego se informará periódicamente, según la frecuencia que resulte adecuada para cada situación, los resultados sobre la gestión de riesgo que realiza cada área. El informe se distribuirá al punto de contacto que se defina en cada caso.
6. Comunicación: Se definirá mecanismos para que la información de este proceso fluya dentro del organismo dado que esta política debe ser accesible para todos los miembros del organismo.

Al menos con una frecuencia anual se deberá realizar una evaluación de los riesgos en las actividades internas y externas del organismo, partiendo de los objetivos estratégicos, así como también se deberá establecer cuáles serán las acciones para mitigar el impacto de dichos riesgos.

Todos los nuevos miembros del organismo deberán recibir, durante el proceso de inducción, una capacitación sobre las actividades de gestión de riesgos de la organización. Periódicamente el organismo coordinará actividades de sensibilización y capacitación relacionadas con la gestión de riesgos.

6.- Clasificación de Amenazas y Riesgos

Para facilitar el proceso de identificación y monitoreo de los riesgos está disponible un catálogo de amenazas. Una de las primeras instancias durante el análisis de riesgo debe ser revisar e identificar las amenazas que pueden materializarse y cómo éstas pueden afectar procesos de operaciones de acuerdo con sus características.

La clasificación de amenazas y riesgos siempre se relaciona con el objeto del análisis. Por este motivo, deberá ofrecerse matrices que permitan aproximarse a cuantificar el nivel de incertidumbre y el grado de pérdidas asociadas con cada riesgo, considerando las diferentes categorías específicas presentes en el organismo: grupos de soporte, proyectos, productos, servicios, etc.

7.- Capacitación y Concientización

Desarrollar un programa de capacitación y concientización para todos los empleados sobre la importancia de la gestión de riesgos, incluyendo la identificación y reporte de riesgos potenciales.

8.- Cumplimiento

Ante la verificación del incumplimiento de lo estipulado en la Política que regula este documento, la Dirección del organismo, a través de Capital Humano podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

ANEXO 4 - Entregable 3: Plan y material de capacitaciones

Tabla de Contenido

Plan de Concientización y Sensibilización en Seguridad de la Información 308

Material de Capacitación de Seguridad de la Información..... 324

Índice de Tablas

Tabla 22: Actividad respecto a la Concientización y Sensibilización realizada posterior al relevamiento 306

Este anexo contiene un detalle del Plan de concientización y sensibilización en seguridad de la información, y el material necesario para llevar adelante capacitación de seguridad de la información.

Dado que la seguridad de la información es un componente clave para el organismo, se identificó la necesidad de desarrollar un programa de capacitación y concienciación que permitiera a todo el personal comprender y aplicar buenas prácticas en su trabajo diario reflejado en la tarea generada y trabajada por nosotros que pertenece al a categoría Responder, Nivel de Madurez 2 y Prioridad 2:

Prioridad	Tareas para alcanzar nivel de madurez	Evidencia
P2	T698 - Definir un plan de concientización y sensibilización en seguridad de la información todo el organismo.	E698 - Plan de concientización y sensibilización en seguridad de la información.

Tabla 22: Actividad respecto a la Concientización y Sensibilización realizada posterior al relevamiento

A partir de reuniones de diagnóstico con el Departamento de Personal, se definieron los contenidos clave y se elaboraron materiales didácticos, incluyendo presentaciones, manuales y guías prácticas, con el objetivo de garantizar una formación efectiva y accesible.

El plan de capacitación se estructuró en seis ejes fundamentales: una introducción a la Seguridad de la Información y su impacto en el organismo, la protección y privacidad de los datos, la importancia de las políticas de seguridad, la gestión de riesgos basada en la norma ISO/IEC 27001:2022, la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y el marco normativo de la ISO 27001. A través de estos módulos, se buscó proporcionar una visión integral de la seguridad de la información, abordando tanto la prevención de riesgos como el cumplimiento normativo y la aplicación de controles efectivos.

Como complemento, se diseñó un material denominado **“TIPS”**, enfocado en reforzar hábitos seguros mediante información clara y accesible sobre concienciación en seguridad, uso adecuado de medios de almacenamiento y buenas prácticas en redes

sociales. Este material, elaborado en formatos visuales y de fácil comprensión, facilita la asimilación de conceptos clave y promueve una cultura organizacional orientada a la protección de la información.

Este enfoque integral no solo permitió estandarizar conocimientos dentro del organismo, sino también fortalecer la gestión de la seguridad de la información, asegurando que cada miembro del equipo comprenda su rol en la protección de los activos digitales y el cumplimiento de las normativas vigentes.

Plan de Concientización y Sensibilización en Seguridad de la Información

Con el objetivo de fortalecer la cultura de seguridad de la información dentro del organismo, se diseñó un plan de comunicaciones que permitiera mantener informados, motivados e involucrados a todos los colaboradores en el cumplimiento de los controles de seguridad. Este plan busca fomentar la responsabilidad y conciencia del personal para minimizar riesgos e incidentes, siguiendo las recomendaciones del NIST SP 800-50r1 sobre programas de capacitación y concientización en seguridad de tecnologías de la información.

La propuesta establece un enfoque estructurado que define los objetivos, actividades, métodos de ejecución, tiempos y recursos necesarios, alineándose con las metas institucionales. Su implementación tiene como finalidad sensibilizar y capacitar tanto al personal como a los proveedores en el manejo adecuado de la información, asegurando el cumplimiento de directivas, lineamientos y procedimientos de seguridad.

Para la ejecución del plan, se establecieron diversas actividades orientadas a evaluar y reforzar el conocimiento del personal. Entre ellas, se aplicará una encuesta para medir el nivel de concienciación en seguridad, se enviarán comunicaciones periódicas con buenas prácticas y actualizaciones sobre amenazas, y se compartirán recomendaciones sobre el uso seguro de la información institucional. Además, se realizarán charlas virtuales con presentaciones y videos para sensibilizar al personal y resolver inquietudes sobre el tema.

El Departamento de Personal será el encargado de llevar adelante una campaña de expectativa, asegurando que la información llegue de manera clara y efectiva a todos los colaboradores. De esta forma, el plan de comunicaciones no solo refuerza la formación en seguridad de la información, sino que también promueve un entorno más seguro y resiliente frente a los riesgos digitales.

1.- INTRODUCCIÓN

El presente documento describe de manera detallada el plan de sensibilización y concientización en seguridad de la información a ser implementado en el Organismo.

A través del presente plan, se diseñan las actividades a realizar durante un determinado período de tiempo, con las cuales se busca comunicar, sensibilizar y capacitar a los colaboradores y proveedores del Organismo sobre la Seguridad de la Información (SI), para lo cual se presenta una propuesta que incluye aspectos relevantes como los objetivos, actividades a realizar, la manera como se realizarán las actividades, los tiempos y recursos necesarios, así como los resultados esperados, los cuales deben mantener relación directa con los objetivos planteados.

Es importante resaltar que, para el desarrollo e implementación del presente plan, se requiere del compromiso de todos los responsables relacionados en el presente documento, así como personas que resulten involucradas durante su ejecución en cumplimiento del cronograma de actividades propuesto.

La administración de dicho plan quedará bajo la responsabilidad del Departamento de Personal, quién definirá la forma de implementarlo y el correspondiente calendario.

2.- OBJETIVO

2.1.- OBJETIVO GENERAL

Establecer los métodos de comunicación para informar, motivar e involucrar a los colaboradores del Organismo, sobre la importancia de trabajar activamente en el cumplimiento de los controles de seguridad de la información, propiciando su compromiso, la toma de conciencia y su responsabilidad logrando con ello reducir los riesgos e incidentes de seguridad de la información.

2.2.- OBJETIVOS ESPECÍFICOS

- Generar expectativa sobre la seguridad de la información a partir de una campaña de difusión y divulgación.

- Aumentar la exposición y difusión de las disposiciones de seguridad de la información.
- Socializar los principales procedimientos de seguridad de la información.
- Dar visibilidad a los riesgos de seguridad de la información identificados en el organismo.
- Fortalecer el uso y la implementación de las disposiciones, procedimientos y controles establecidos o relacionados con la seguridad de la información en las actividades diarias del personal del organismo.

Los mencionados objetivos permitirán la difusión de los conceptos de la seguridad de la información, facilitarán su adopción y aumentarán su posicionamiento vital para el aseguramiento de la información.

3.- ALCANCE

El plan define la estrategia de difusión de la seguridad de la información; propone los recursos a utilizar para la circulación y comunicación de los servicios y beneficios del sistema, facilita la creación de contenidos y campañas enfocadas a los diferentes grupos de interés que posee el organismo.

4.- RESPONSABILIDADES

Los roles detallados a continuación serán responsables y tendrán participación en la adecuada implementación del presente Plan de Concientización y Sensibilización de la seguridad de la información del Organismo.

La Comisión de Seguridad de la Información (CSI) a través de los responsables de las diferentes áreas, darán su apoyo a la ejecución del presente plan, con acciones como:

- Participar de acuerdo con su disponibilidad en el desarrollo de las actividades programadas en el presente plan.
- Autorizar y fomentar en el personal a cargo la participación en las jornadas de sensibilización y capacitación que se desarrollen.

- Fomentar en el personal a cargo el cumplimiento de las directivas, disposiciones, procedimientos y recomendaciones, así como la aplicación de las buenas prácticas relacionadas con la seguridad de la información dadas a conocer como implementación del presente plan.
- Identificar las necesidades de capacitación y/o sensibilización en actividades relacionadas con la seguridad de la información para el personal a su cargo.

El Responsable de Seguridad de la Información (RSI) debe velar por el cumplimiento del presente plan mediante:

- Participar en la elaboración del Plan de Concientización y Sensibilización de la seguridad de la información.
- Identificar las necesidades del personal del organismo en materia de sensibilización y capacitación en seguridad de la información.
- Consolidar los resultados de las evaluaciones y seguimientos realizados a las actividades de sensibilización y capacitación de la seguridad de la información.
- Participar en el diseño de las estrategias y el material necesario para el desarrollo del presente plan.
- Participar en el desarrollo y ejecución del presente plan.
- Proponer iniciativas e identificar oportunidades de mejora para el diseño e implementación del presente plan.

El resto de los colaboradores y proveedores del Organismo deberán:

- Participar activamente en las actividades desarrolladas para el cumplimiento del presente plan.
- Aplicar en sus actividades diarias las disposiciones, directivas, procedimientos, recomendaciones y en general las buenas prácticas relacionadas con la seguridad de la información.
- Identificar oportunidades de mejora del presente plan y proponer iniciativas que puedan ser evaluadas e implementadas en versiones posteriores del presente plan.

5.- REFERENCIAS NORMATIVAS

- Ley N° 18.331 Ley de Protección de Datos Personales y Acción de Habeas Data
- Decretos adicionales que reglamentan la mencionada ley.
- Ley Nro. 18.381 Ley de Acceso a la Información Pública
- Marco de Ciberseguridad de AGESIC v4.2
- Norma ISO/IEC 27001 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos.
- Norma ISO/IEC 27002 Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información.
- NIST SP 800-50r1 Elaboración de un Programa de Capacitación y Concientización en Seguridad de Tecnologías de la Información.

6.- GLOSARIO DE TÉRMINOS

- Activo de información: Cualquier información que tiene valor para el Organismo y para la seguridad de la información. Se consideran también los recursos humanos y tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.
- Amenazas: Causa potencial de un incidente no deseado, que puede causar daños a un sistema o al organismo.
- Confidencialidad: Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.
- Control: Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- Disponibilidad: Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.

- **Gestión de riesgo:** Aplicación sistemática de políticas de gestión procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos.
- **Incidente de Seguridad de la Información:** Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operatividad de la Entidad.
- **Información:** Cualquier forma de registro de contenidos susceptibles a ser procesados, distribuidos y almacenados, pudiendo estar en formato electrónico, óptico, magnéticos u otro medio de almacenamiento.
- **Ingeniería Social:** Tipo de ataque de seguridad en la cual un individuo manipula al otro con el fin de obtener información que puede ser utilizada para acceder a un sistema no autorizado, sustraer dinero o incluso suplantar la identidad de la víctima.
- **Integridad:** Propiedad de precisión y completitud de la información.
- **Personal del Organismo:** Comprende a los colaboradores, independiente de la forma de contratación.
- **Propietario del activo:** Es el funcionario asignado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos vinculados a la seguridad de la información y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, etc.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).

- **Responsable de Seguridad de la Información:** El Responsable de Seguridad de la Información (RSI) es el responsable de la seguridad de la información y reporta a la Comisión de Seguridad de la Información (CSI).
- **Seguridad de la Información:** Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre
- **Sensibilización:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **Sistema de Gestión de la Seguridad de la Información (SGSI):** Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por el organismo, en la búsqueda de la protección de sus activos de información.
- **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.

7.- DESCRIPCIÓN GENERAL DEL PLAN

7.1. METAS

El Organismo define las siguientes metas a cumplir durante la ejecución del plan de concientización y sensibilización para la seguridad de la información.

- Formalizar la comunicación y difusión de la existencia y ejecución de las actividades vinculadas con la seguridad de la información dentro de su alcance.

- Difundir y fomentar una cultura de seguridad de la información y procedimientos que forman parte de la seguridad de la información.
- Socializar con el personal de la institución los principales riesgos de seguridad de la información.
- Prevenir la materialización de los riesgos de seguridad de la información identificados, dando a conocer y explicando al personal de la institución los mecanismos de control vinculados con la seguridad de la información.

7.2. AUDIENCIA OBJETIVA

La implementación y ejecución del presente plan está orientada a comunicar, sensibilizar y capacitar a todo el personal y proveedores, acerca del adecuado manejo de la información institucional y el cumplimiento de las directivas, lineamientos, disposiciones, procedimientos e instrucciones de trabajo establecidos para la seguridad de la información.

El organismo a través del área pertinente, podrá realizar y aplicar encuestas o actividades para recopilar información que permita identificar nuestros públicos objetivos, conocer sus características y perfiles con la finalidad de diseñar y ejecutar estrategias y/o campañas específicas que contribuyan al cumplimiento del presente plan.

Con el fin de orientar de manera efectiva las actividades y estrategias de cumplimiento se han considerado los siguientes roles:

- Gerentes y Líderes: Temas relacionados con la normalidad aplicable, generación de conciencia, compromiso y liderazgo con la seguridad de la información.
- Seguridad de la Información: Formación en temas relacionados con la norma de seguridad de la información, ciberseguridad, buenas prácticas de TI y lineamientos de seguridad. Prepararse para gestionar la seguridad de la información.
- Infraestructura: Conocer y comprender los lineamientos, procedimientos y controles de la seguridad de la información, fortalecer competencias técnicas en

seguridad informática y buenas prácticas de TI, todo ello con la finalidad de contar con la preparación para la implementación de controles de seguridad, prevención y atención de incidentes.

- Usuarios finales: Fortalecer los niveles de concienciación en seguridad de la información, cumplimiento de los lineamientos, controles, recomendaciones y buenas prácticas de la seguridad de la información, así como la responsabilidad en el uso de los sistemas y aplicaciones, así como con el manejo de información institucional.

7.3. TEMÁTICA DEL PLAN

7.3.1. CONOCIMIENTO GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

Dar a conocer los aspectos básicos relacionados con la seguridad de la información:

- Concepto de seguridad de la información
- ¿Qué es un riesgo de seguridad de la información?
- ¿Qué es el marco de ciberseguridad de AGESIC v4.2?
- ¿Qué es la norma ISO/IEC 27001:2022?
- Estructura del Sistema de Gestión de Seguridad de la Información (SGSI)
- Roles principales de la seguridad de la información
- Ley de protección de datos

7.3.2. POLÍTICAS Y DISPOSICIONES DE LA SEGURIDAD DE LA INFORMACIÓN

- Explicación de las políticas de seguridad
- Explicación del Manual de las políticas de seguridad
- Consecuencias y sanciones disciplinarias por incumplimientos de las disposiciones de la seguridad de la información

7.3.3. PROCEDIMIENTOS DE LA SEGURIDAD DE LA INFORMACIÓN

- Explicación, socialización y difusión de los principales procedimientos relacionados con la seguridad de la información.

7.3.4. AMENAZAS INFORMÁTICAS

- Virus informáticos: gusanos, troyanos, malware, keylogger, entre otros.
- Sniffer
- Denegación de servicios
- Phishing
- Ingeniería Social

7.3.5. USO DE HERRAMIENTAS INFORMÁTICAS Y BUENAS PRÁCTICAS DE TI

- Uso adecuado del correo institucional
- Identificación de correos electrónicos sospechosos
- Uso adecuado de Internet
- Lineamiento de escritorio limpio
- Lineamientos de instalación de software
- Uso de equipos y dispositivos de la institución fuera de las instalaciones
- Seguridad en el teletrabajo
- Controles de acceso (uso de contraseñas, privilegios, roles, etc.)
- Gestión de incidentes (qué, cómo, y a quién debo reportar)

7.4. INSTRUMENTOS DE CAPACITACIÓN

Los instrumentos de capacitación incluirán, entre otros:

- Campañas de sensibilización
- Mensajes de correo electrónico (boletines, infografías, etc.).
- Publicación de mensajes en la Intranet
- Publicación de mensajes en fondos y/o protectores de pantallas
- Concursos / Trivias

7.5. PLAN DE ACCIÓN Y ACTIVIDADES

Se definen las actividades a realizar para la ejecución del Plan de Concientización y Sensibilización de la seguridad de la información, considerando los objetivos y la audiencia objetiva.

En conjunto con el Departamento de Personal, crear una campaña de expectativa con las siguientes actividades:

7.5.1. ACTIVIDAD 1

- Objetivo – Generar expectativa del uso de la seguridad de la información con una breve campaña de difusión, así como incrementar la exposición y difusión de los lineamientos de seguridad de la información.
- Actividad – Aplicación de encuesta de conocimiento y concientización.
- ¿Cómo? – Diseñar y aplicar encuesta de conocimientos para establecer una línea base de percepción y concientización de seguridad de la información del Organismo.
- Fecha – A determinar por el Departamento de Personal.
- Periodicidad – Semestral
- Recursos – Personal del Departamento de Personal y del Responsable de Seguridad de la Información.
- Resultados – Obtener información que permita medir el grado de conocimiento y concientización del personal respecto de la seguridad de la información, y con ello determinar los temas en que se debe profundizar la sensibilización y capacitación.

7.5.2. ACTIVIDAD 2

- Objetivo – Dar a conocer el uso de la seguridad de la información a partir de una breve campaña de difusión, así como incrementar la exposición y difusión de los lineamientos de seguridad de la información.
- Actividad – Envío de mensajes a través del correo electrónico
- ¿Cómo? – Diseñar y enviar a través del correo electrónico o herramientas colaborativas información relacionada con la seguridad de la información.
- Fecha – A determinar por el Departamento de Personal
- Periodicidad – Semanal, Quincenal o Mensual, según las necesidades.
- Recursos – Personal del Departamento de Personal y del Responsable de Seguridad de la Información

- Resultados – El personal será informado de la existencia y conceptos del SGSI en la institución, lineamientos, procedimiento, objetivos, alcance y sus principales servicios.
- Ejemplos de Mensajes – Entre otros:
 - Los 3 Pilares de la Seguridad de la información,
 - ¿Qué es seguridad de la información?
 - ¿Qué es el Sistema de Gestión de Seguridad de la Información (SGSI)?
 - Riesgos de seguridad de la información,
 - Normativa relacionada al SGSI (Disposiciones de Seguridad),
 - Alcance del SGSI
 - Etapas del SGSI.

7.5.3. ACTIVIDAD 3

- Objetivos – Entre otros:
 - Generar expectativa del uso del SGSI con una breve campaña de difusión, así como incrementar la exposición y difusión de los lineamientos de seguridad de la información.
 - Vincular al personal con los procesos del alcance del SGSI.
 - Fomentar la interacción de las dependencias con el SGSI.
 - Fortalecer el uso e implementación de las políticas, procedimientos y controles establecidos por el SGSI para las actividades diarias de la institución.
- Actividad – Envío permanente de recomendaciones y Tips de Seguridad de la Información.
- Cómo? – Diseñar y enviar a través del correo electrónico o mensajes en herramientas colaborativas, información relacionada con la Seguridad de la Información, que mantenga actualizados a los usuarios sobre las buenas prácticas en el manejo de la información institucional, nuevas amenazas y vulnerabilidades, uso seguro de Internet y en general noticias relacionadas con el SGSI.
- Fecha – A determinar por el Departamento de Personal.
- Periodicidad – Semanal, Quincenal o Mensual, según las necesidades.

- Recursos – Personal del Departamento de Personal y del Responsable de Seguridad de la Información
- Resultados – Se actualiza permanentemente al personal de la institución en temas relacionados con el SGSI, generando conciencia y apropiación acerca del sistema.
- Ejemplos – Entre otros:
 - Uso adecuado del correo institucional
 - Identificación de correos electrónicos sospechosos
 - Uso adecuado de Internet
 - Lineamiento de escritorio limpio
 - Lineamientos de instalación de software
 - Uso de equipos y dispositivos de la institución fuera de las instalaciones
 - Seguridad en el teletrabajo
 - Controles de acceso (uso de contraseñas, privilegios, roles, etc.)
 - Gestión de incidentes (qué. Cómo y a quién debo reportar)
 - Ingeniería Social
 - Otros temas según necesidad

7.5.4. ACTIVIDAD 4

- Objetivos – Entre otros:
 - Generar expectativa del uso del SGSI con una breve campaña de difusión, así como incrementar la exposición y difusión de los lineamientos de seguridad de la información.
 - Vincular al personal con los procesos del alcance del SGSI.
 - Fomentar la interacción de las dependencias con el SGSI.
 - Fortalecer el uso e implementación de las políticas, procedimientos y controles establecidos por el SGSI para las actividades diarias de la institución.
- Actividad – Charlas de Seguridad de la Información al personal de la institución a través de sesiones virtuales.
- ¿Cómo? – Elaborar de material en presentaciones o videos para ser presentados al personal de la institución a través de charlas de 30 o 45 minutos de duración, evacuando consultas o dudas al respecto.
- Fecha – A determinar por Capital Humano.
- Periodicidad – Semanal, Quincenal o Mensual, según las necesidades.
- Recursos – Personal del Departamento de Personal y del Responsable de Seguridad de la Información
- Resultados – Se actualiza permanentemente al personal de la institución en temas relacionados con el SGSI, generando conciencia y apropiación acerca del sistema.
- Ejemplos – Entre otros:
 - Gestión de Contraseñas
 - Ingeniería Social
 - Uso adecuado de herramientas digitales
 - Gestión de Incidentes
 - Lineamientos de Seguridad
 - Otros temas según necesidad

Las actividades aquí planteadas, así como otras que puedan surgir en el futuro, serán administradas por Personal del Departamento de Personal, siendo el Responsable de Seguridad de la Información el responsable de su actualización.

7.6. RECURSOS Y PRESUPUESTO

Para el desarrollo del presente plan, el OP podrá disponer del personal requerido para cada una de las actividades a realizar de acuerdo con las funciones de los respectivos cargos y procesos, proveedores y consultorías externas.

El presupuesto requerido para la implementación del Plan de Concientización y Sensibilidad de la seguridad de la información deberá ser incluido en el rubro asignado a las actividades de capacitación y concientización, administradas por Capital Humano. Con ello se debe garantizar el desarrollo de las actividades aprobadas en el presente plan y las posteriores actualizaciones que requieran de recursos económicos para su ejecución.

7.7. MONITOREO Y EVALUACIÓN DEL PLAN

El Responsable de Seguridad de la Información (RSI), realizará el monitoreo al desarrollo del presente plan a través del seguimiento del cronograma establecido, y se generarán métricas que contribuyan al proceso de mejoramiento de este. Para ello se deberá diseñar un indicador que permita medir el cumplimiento de la ejecución del presente plan.

En la evaluación de las actividades realizadas como parte de la ejecución del presente plan, se podrán utilizar diferentes herramientas que permitan medir el grado de apropiación y cumplimiento del personal que participa en las actividades y su impacto. Su utilidad para el desarrollo de las funciones dentro de sus labores.

Para dicha evaluación se pueden realizar encuestas a los participantes, evaluaciones, trivias o cuestionarios, así como el diseño de indicadores que midan el grado de avance en el conocimiento y participación del personal en temas de seguridad de la información y el SGSI, tomando como línea base una primera encuesta que deberá realizarse anticipadamente.

7.8. REVISIÓN Y MEJORA CONTINUA DEL PLAN

Para mantener actualizado el presente plan, se debe realizar una revisión y actualización del contenido, para lo cual se deberá tener en cuenta los resultados de las

evaluaciones de las actividades desarrolladas durante la ejecución del presente plan, lo cual servirá como insumo para proyectar ajustes y mejoras pertinentes.

Así mismo, se debe tener en cuenta otros aspectos como avances tecnológicos, adquisición y desarrollo de nuevas aplicaciones e infraestructura, aparición de nuevas amenazas y/o vulnerabilidades, actualización en la normativa existente que implique cambios o adaptaciones en nuevas medidas de seguridad, sugerencias recibidas por parte del personal del Organismo, indicadores y métricas del SGSI.

8.- CUMPLIMIENTO

Ante la verificación del incumplimiento de lo estipulado en el Plan que regula este documento, la CSI del Organismo, a través del Departamento de Personal podrá tomar las medidas que sean consideradas pertinentes con el fin de darle el debido cumplimiento.

Material de Capacitación de Seguridad de la Información

Como parte del programa de formación en Seguridad de la Información, se desarrollaron materiales didácticos, incluyendo presentaciones, manuales y guías prácticas, con el fin de garantizar una capacitación efectiva y accesible para todo el organismo. Estos contenidos fueron definidos a partir de reuniones con el Departamento de Personal del Organismo en las que se identificaron las necesidades formativas del personal, asegurando así un enfoque integral que abarque los aspectos clave de la seguridad de la información.

El plan de capacitación se estructuró en seis pilares fundamentales: la introducción a la Seguridad de la Información y su impacto en el organismo; la protección y privacidad de los datos, abordando riesgos y normativas legales; las políticas de seguridad y su rol dentro del SGSI; la gestión de riesgos basada en la norma ISO/IEC 27001:2022; el funcionamiento y aplicación del Sistema de Gestión de Seguridad de la Información; y, finalmente, la capacitación en la norma ISO 27001 y su importancia en la implementación del SGSI.

Además, se elaboró un material complementario denominado "TIPS", diseñado para reforzar conceptos clave mediante información sencilla y accesible. Este material aborda temas como la concienciación en seguridad, el uso adecuado de medios de almacenamiento y las buenas prácticas en redes sociales. Presentado en formatos visuales y de fácil comprensión, busca fortalecer hábitos seguros en el manejo de la información dentro del organismo.

Con estas acciones, el programa de formación no solo busca proporcionar conocimientos teóricos, sino también fomentar una cultura de seguridad en la que cada colaborador comprenda su rol en la protección de la información institucional y en la reducción de riesgos.

Capacitación de Seguridad de la Información

Esta capacitación tiene como objetivo proporcionar a los participantes un conocimiento sólido sobre los principios fundamentales de la Seguridad de la Información y su impacto en el organismo. A través de esta formación, se busca fortalecer la comprensión sobre la importancia de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), abordando los principales riesgos, amenazas y controles necesarios para proteger los activos de información.

Durante la capacitación, se explorarán aspectos clave como el ciclo de vida de la información, la protección de los datos y el cumplimiento legal y regulatorio, además de conceptos esenciales sobre seguridad física y lógica. Asimismo, se analizarán casos prácticos y situaciones comunes relacionadas con el uso de servicios, aplicaciones, dispositivos móviles y medios extraíbles, así como la adecuada gestión de incidentes de seguridad.

El enfoque de esta formación es brindar a los participantes las herramientas necesarias para identificar vulnerabilidades, aplicar buenas prácticas y contribuir activamente a la seguridad de la información dentro del Organismo.



INDUCCIÓN

SEGURIDAD DE LA INFORMACIÓN

Agenda

- 
- ▶ Definiciones
 - ▶ Ciclo de vida de la información
 - ▶ Protección de la información
 - ▶ Cumplimiento legal y regulatorio
 - ▶ Seguridad física y lógica
 - ▶ Servicios
 - ▶ Aplicaciones
 - ▶ Actividades
 - ▶ Dispositivos móviles
 - ▶ Medios extraíbles
 - ▶ Incidentes de seguridad



Definiciones

Según la R.A.E.

Definiciones (según R.A.E.)

- ▶ **Riesgo**
 - ▶ Contingencia o proximidad de un daño
 - ▶ Similar - Peligro, Amenaza
 - ▶ Cada una de las contingencias que pueden ser objeto de un contrato de seguro
 - ▶ Similar - Contingencia
- 

Definiciones (según R.A.E.)

- ▶ Seguridad
 - ▶ Calidad de Seguro
 - ▶ Similar - Invulnerabilidad, Inmunidad, Protección, Defensa, etc.
 - ▶ Servicio encargado de la seguridad de una persona, empresa, edificio, etc.
 - ▶ Similar - Vigilante, Guardián
- ▶ Seguro
 - ▶ Libre y exento de riesgo
 - ▶ Similar - Invulnerable, Inatacable, Inexpugnable, Inmune
 - ▶ Cierto, indubitable
 - ▶ Similar - Indudable, Inequívoco, Evidente



Ciclo de vida de la Información



Ciclo de vida de la Información

- ▶ Período completo en que los datos existen en el sistema
- ▶ Etapas
 - ▶ Creación / Adquisición / Entrada / Captura de datos
 - ▶ Almacenamiento
 - ▶ Uso
 - ▶ Archivo
 - ▶ Destrucción



Protección de la Información



Protección de la Información

- ▶ Proceso de salvaguardar la información contra la corrupción, filtraciones, pérdidas o compromiso de los datos
- ▶ Pilares de la Seguridad
 - ▶ Confidencialidad
 - ▶ Integridad
 - ▶ Disponibilidad
- ▶ Acciones
 - ▶ Cifrado
 - ▶ *Hashing*
 - ▶ Respaldo
 - ▶ Recuperación de Desastres y Continuidad del Negocio



Cumplimiento Legal y Regulatorio



Cumplimiento Legal y Regulatorio

- ▶ Estamos obligados a cumplir con todo el **marco normativo y legal aplicable**
- ▶ Esto incluye cumplir con:
 - ▶ **Leyes** (nacionales e internacionales)
 - ▶ **Normativas**
 - ▶ **Gobierno** (MSP, MT, DGI, BCU, AGESIC, etc.)
 - ▶ **Industria** (Salud, Financiera, Tecnología, etc.)
 - ▶ **Políticas** (internas o externas)
 - ▶ **Reglamentos**
 - ▶ **Contratos**



Seguridad Física



Seguridad Física

- ▶ Acceso e Identificación
 - ▶ Controles en áreas de ingreso
 - ▶ Control de acceso con registro histórico y monitoreo de ingreso
 - ▶ Registrar y acompañar a los visitantes
 - ▶ Uso de tarjetas de acceso individualizables
- ▶ Análisis de Amenazas y Riesgos de las Instalaciones
 - ▶ Revisión de vías de acceso
 - ▶ Controles físicos de acceso



Seguridad Lógica



Seguridad Lógica

- ▶ Protección de los Datos, Procesos y Programas
 - ▶ Evitar compartir información
- ▶ Control del Acceso a los Sistemas
 - ▶ Evitar compartir cuentas de usuario
 - ▶ Evitar usuarios con nombres genéricos
 - ▶ Usar criterios de la Política de contraseñas
 - ▶ No compartir / No escribir las contraseñas
 - ▶ Usar administradores de contraseñas
 - ▶ Promover el uso de la autenticación de dos factores



Servicios



Servicios

▶ Correo Electrónico

- ▶ La cuenta de correo es **institucional**: debe dedicarse **exclusivamente a actividades del negocio**
- ▶ Aplicar **Políticas de uso aceptable**
- ▶ La **información confidencial** debe viajar en correos encriptados
- ▶ **Verificar** que estás enviando correo electrónico a la **persona correcta**
- ▶ **Protege tu contraseña de correo electrónico**



Servicios

▶ Correo Electrónico

- ▶ **Recordar:**
 - ▶ El correo electrónico generalmente se usa para completar el **restablecimiento de contraseñas** de aplicaciones
 - ▶ La empresa **puede monitorear y auditar** el contenido y el uso del correo electrónico institucional
 - ▶ Los servicios de Infraestructura **gestionan y supervisan** la continuidad y calidad del servicio

Servicios

- ▶ Correo Electrónico y *Phishing*
 - ▶ Ataques
 - ▶ En masa - aleatorio
 - ▶ Dirigido a empresa / persona
 - ▶ Tipos
 - ▶ Mediante un *click*
 - ▶ Archivos adjuntos
 - ▶ Formularios web



Servicios

- ▶ ¿Por qué (y cuándo) sospechar?
 - ▶ Originado en una dirección no conocida
 - ▶ Es un mensaje inesperado
 - ▶ Tiene errores ortográficos notorios
 - ▶ Falta la información personal habitual
 - ▶ Nos pide una acción
 - ▶ Solicita abrir el archivo adjunto
 - ▶ Nos obliga a ir a una página web
 - ▶ Solicita proporcionar información



Servicios



▶ Internet

- ▶ Acceso a Internet **protegido** mediante **firewall y proxy**
- ▶ Un **servicio centralizado** actualiza el **sistema operativo** de los equipos basados en **MS Windows**
- ▶ **Buenas prácticas** recomendadas:
 - ▶ **Comprobar** que las URL se corresponden con el destino indicado
 - ▶ **Preferir** el protocolo HTTPS en transacciones confidenciales
 - ▶ **Descargar** contenidos de **fuentes conocidas**
 - ▶ Visitar sitios aprobados por la **Política de Uso Aceptable de Internet**

Servicios



▶ Servicios en la Nube (*Cloud Computing Services*)

- ▶ **Uso permitido** sólo mediante **autorización formal explícita**
- ▶ En caso de uso autorizado:
 - ▶ Es recomendable **cifrar los datos** siempre que sea posible
 - ▶ Implementar **control de acceso** y construir **roles y responsabilidades** con claridad
- ▶ **Aplica** el marco jurídico nacional e internacional
- ▶ **Consecuencias graves** ante vulneración o pérdida de datos personales



Aplicaciones



Aplicaciones

- ▶ **Antivirus**
 - ▶ Mantener **siempre activa** la protección antivirus en los equipos utilizados
 - ▶ Comprobar que está **actualizada** la base de datos del antivirus
 - ▶ Agendar **periódicamente** una exploración de los contenidos
 - ▶ **Reportar a DAU** los casos de infección encontrados
- ▶ **Firewall y Proxy**
 - ▶ Controlan las conexiones autorizadas y la navegación de los usuarios



Actividades



Actividades

- ▶ Trabajo en la Oficina
 - ▶ Escritorio limpio
 - ▶ No dejar ningún tipo de información desatendida en el área de trabajo
 - ▶ Terminal desatendida
 - ▶ Bloquear la sesión cuando debo alejarme de la terminal



Actividades

- ▶ Trabajo Remoto
 - ▶ Riesgos vinculados
 - ▶ Contexto no seguro - En casa ingresa gente que la empresa no conoce
 - ▶ Comunicación no supervisada - Conectarse sin utilizar la VPN
 - ▶ Acceso al equipamiento - Otros pueden llegar a utilizar nuestro equipo
 - ▶ Protección de la Información - Controlar quién accede a nuestra información



Dispositivos Móviles



Dispositivos Móviles

▶ Celulares y Tabletas

- ▶ Se pueden **conectar en la oficina** a una red inalámbrica con **acceso monitoreado** a Internet
- ▶ **No descuidar** los dispositivos móviles en los lugares públicos o en vehículos
- ▶ **Activar** bloqueo de pantalla, usar sensores biométricos y herramientas de cifrado
- ▶ El almacenamiento de información confidencial requiere **aprobación previa**
- ▶ **Verificar** la fuente de origen al momento de instalar software
- ▶ **Programar** copias de seguridad y rutina de protección antivirus



Actividades



Actividades

- ▶ Trabajo en la Oficina
 - ▶ Escritorio limpio
 - ▶ No dejar ningún tipo de información desatendida en el área de trabajo
 - ▶ Terminal desatendida
 - ▶ Bloquear la sesión cuando debo alejarme de la terminal



Actividades

- ▶ Trabajo Remoto
 - ▶ Riesgos vinculados
 - ▶ Contexto no seguro - En casa ingresa gente que la empresa no conoce
 - ▶ Comunicación no supervisada - Conectarse sin utilizar la VPN
 - ▶ Acceso al equipamiento - Otros pueden llegar a utilizar nuestro equipo
 - ▶ Protección de la Información - Controlar quién accede a nuestra información



Dispositivos Móviles



Dispositivos Móviles

▶ Celulares y Tabletas

- ▶ Se pueden **conectar en la oficina** a una red inalámbrica con **acceso monitoreado** a Internet
- ▶ **No descuidar** los dispositivos móviles en los lugares públicos o en vehículos
- ▶ **Activar** bloqueo de pantalla, usar sensores biométricos y herramientas de cifrado
- ▶ El almacenamiento de información confidencial requiere **aprobación previa**
- ▶ **Verificar** la fuente de origen al momento de instalar software
- ▶ **Programar** copias de seguridad y rutina de protección antivirus



Medios Extraíbles



Medios Extraíbles

- ▶ Disco externo, Tarjetas de Memoria, Celulares
 - ▶ **Cualquier** dispositivo conectable con algún tipo de capacidad de almacenamiento
 - ▶ **No debe** utilizarse a menos que haya sido aprobado previamente
 - ▶ **Debe** estar encriptado si fue autorizado el almacenamiento de información confidencial
 - ▶ **No debe** utilizarse si es un dispositivo de origen desconocido



Eliminación de Información



Eliminación de Información

- ▶ La forma de eliminar información **siempre** depende del tipo de contenido
- ▶ La información confidencial **debe** ser eliminada de forma segura
 - ▶ El papel **debe** ser destruido
 - ▶ Los dispositivos o medios electrónicos **deben** ser eliminados
 - ▶ Los discos duros **deben** ser destruidos antes de ser eliminados



Incidentes de Seguridad



Incidentes de Seguridad

- ▶ Son incumplimientos **reales o potenciales** de una política o se relacionan con una pérdida de datos
- ▶ Deben **comunicarse de inmediato** a quién ejerce la función de Oficial de Seguridad de la Información
- ▶ Es **importante** establecer/delimitar (rápidamente) el área de impacto
- ▶ Cuando los incidentes afectan datos personales el Organismo **se encuentra obligado a reportarlos a la URCDP** en plazos muy breves
- ▶ **Se recomienda** generar y preservar pruebas y evidencias para su análisis posterior

▶ (URCDP - Unidad Reguladora y de Control de Datos Personales)

**Muchas
Gracias**



Capacitación de Protección y Privacidad de los Datos

Esta capacitación tiene como finalidad concientizar a los participantes sobre la importancia de la protección de la privacidad y los datos personales, resaltando la necesidad de identificar y resguardar la información de valor que manejan en su labor diaria. Se abordarán los principales riesgos asociados al manejo de datos, así como las mejores prácticas para su protección y cumplimiento normativo.

Durante la formación, se analizarán cuestiones clave como qué información es valiosa y quién más podría considerarla de interés, con el fin de comprender los riesgos de exposición y las medidas de protección adecuadas. También se explorará el marco legal vigente, enfatizando las responsabilidades individuales y organizacionales en el tratamiento de datos personales.

Asimismo, se proporcionarán herramientas para fortalecer la seguridad de los activos de información, garantizando que los participantes conozcan los procedimientos y controles esenciales para minimizar vulnerabilidades y evitar incidentes de seguridad.

El objetivo es que los participantes desarrollen una mayor conciencia sobre la importancia de la privacidad, adopten buenas prácticas y contribuyan activamente a la protección de la información del organismo.



INDUCCIÓN

PROTECCIÓN Y PRIVACIDAD DE LOS DATOS

Agenda

- 
- ¿Qué **información de valor** manejamos?
 - ¿Quién más puede considerarla valiosa?
 - ¿Cómo debemos proteger la **privacidad** y los **datos personales**?
 - ¿Qué nos dice la **ley**?
 - ¿Cómo debemos resguardar nuestros **activos de información**?



Activos de Información

Según la R.A.E.

Activos de Información

- Datos personales e información de empleados, clientes y proveedores
 - Presupuestos
 - Planes de negocio
 - Procedimientos operativos y técnicos
 - Registros de actividad de personas y sistemas
 - Acuerdos y Términos comerciales
 - Especificaciones de producto
 - Propiedad intelectual
 - Contractual y Legal
 - Financiera y Contable
- 



Interesados en nuestra Información



Interesados en nuestra Información

• ¿A quién puede interesarle nuestra información?

- Ciber delincuentes
- Activistas
- Estafadores
- Competidores
- Y en general ... a cualquier persona indiscreta



Ejemplos – ¿Qué pasaría si...?



Ejemplos – ¿Qué pasaría si...?

- Alguien más tuvo acceso a nuestros activos...
 - Pérdida de confidencialidad
- Nuestros activos fueron corrompidos de alguna manera...
 - Pérdida de integridad
- No podemos acceder a nuestros activos
 - Pérdida de disponibilidad



Contexto Normativo



Contexto Normativo

- **Constitución de la República** (Arts. 7, 28, 44, 66, 72 y 332)
- **Ley 18.331 (2008)** “Protección de Datos Personales y Acción de Habeas Data”
- **Ley 19.670 (2018)** (Arts. 37, 38, 39 y 40) – Rendición de Cuentas
- **Decretos en 2008, 2009, 2014 y 2020**

¿Qué información está alcanzada por la normativa de protección de datos personales?



Datos Personales



Datos Personales

- ▶ “Información de cualquier tipo, referida a personas física (o jurídicas) determinadas o determinables?”



Datos Personales - Elementos

1er. Elemento: Información

- “... cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a las personas...” (Decreto 414/2009: Art.1)

2do Elemento: Persona Física Determinable

- “... toda persona cuya IDENTIDAD pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona...” (RGDP: Art. 4, N°1)



Datos Personales – Otros Ejemplos

Otros Ejemplos de Datos Personales

- “... datos de geolocalización, direcciones de IP, los identificadores únicos de los dispositivos y de los clientes, registro de llamadas, SMS y mensajería instantánea, historial de navegación, dirección de correo electrónico, datos biométricos, los números de tarjeta de crédito, etc.

Datos Personales especialmente protegidos

- La ley distingue un tipo de datos personales que son especialmente protegidos (datos sensibles – inc. datos de salud-, datos de telecomunicaciones, etc.), pero todos los datos personales sin distinción están legalmente protegidos.



Responsabilidades



Principales Roles-Responsabilidades

RESPONSABLE DEL TRATAMIENTO
Es quién decide sobre la finalidad, contenido y uso del tratamiento



ENCARGADO DEL TRATAMIENTO
Es quién trata los datos personales por cuenta del responsable



**TITULARES
DE
DATOS PERSONALES**

Nota: aún cuando el **ENCARGADO** capture datos directamente del **TITULAR**, siempre lo hace por cuenta del **RESPONSABLE**, por lo que será responsabilidad de este último contar con una base de legitimación para tratar los datos

Principales Roles-Responsabilidades

RESPONSABLE DEL TRATAMIENTO

- Registro de la base de datos
- Base de legitimación del tratamiento
- Deber de información
- Seguridad de los datos
- Aplicar responsabilidad proactiva
- Aplicar **Privacidad desde el Diseño y por Defecto (PbDD)**
- Realizar **Evaluación de Impacto (EIPD)**
- Gestionar y comunicar las brechas a la URCDP y titulares
- Designar **Delegado de Datos Personales (DPD)** (si corresponde)

← OBLIGACIONES →

ENCARGADO DEL TRATAMIENTO

- Seguridad de los datos
- Aplicar responsabilidad proactiva
- Aplicar **Privacidad desde el Diseño y por Defecto (PbDD)**
- Realizar **Evaluación de Impacto (EIPD)**
- Gestionar y comunicar las brechas a las URCDP y titulares
- Designar **Delegado de Datos Personales (DPD)** (si corresponde)

Debe existir un **CONTRATO ESCRITO** u otro instrumento jurídicamente vinculante que establezca todos los aspectos relevantes del encargo

Principales Roles-Responsabilidades

¿QUÉ RESPONSABILIDADES LEGALES TIENE EL ORGANISMO Y SUS COLABORADORES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES?



Responsabilidad del Organismo

La ley determina que el Organismo es **RESPONSABLE** de los datos personales de los empleados, clientes y proveedores que gestiona para el desarrollo de su actividad

Pero también, la ley hace responsable con el mismo rigor al Organismo, por los datos personales que los clientes le confían en carácter de **ENCARGADO** del tratamiento



Responsabilidad del Colaboradores

En cuanto a la responsabilidad de los colaboradores del Organismo, resulta aplicable la norma legal que establece que “...las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieran acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligados a guardar estricto secreto profesional sobre los mismos (Artículo 302 del Código Penal)...” y que “... esta obligación subsistirá ***aún después de finalizada la relación con el responsable de la base de datos...***” (Art. 11, Ley 18.331)



Pautas



Pautas

Pautas para la **Protección de la Información** y cumplimiento de la **Protección de Datos**

- **Compromiso de la Dirección**
- **Políticas de Seguridad de la Información** y de **Protección de Datos Personales**
- Participación del **Oficial de Seguridad de la Información (OSI)** y del **Delegado de Datos Personales (DPD)** desde el diseño de todo proyecto
- **Evaluar riesgos, formalizar planes**
- **Establecer objetivos de control y controles adecuados**
- **Proporcionar recursos, formación y sensibilización**
- **Monitorear, revisar, evaluar y mejorar**
- **Cláusulas contractuales y avisos legales**
- **¡Compromiso de todos!**

Cumplimiento Legal y Regulatorio

Cumplimiento Legal y Regulatorio

Respetar los principios de la Protección de Datos Personales en todo el Ciclo



Cumplimiento Legal y Regulatorio

Garantizar los derechos de los titulares de los datos en todo el Ciclo



Cumplimiento Legal y Regulatorio

Reforma del 2018

El cambio de la Responsabilidad Proactiva





Cumplimiento Legal y Regulatorio

Nuevas Obligaciones

Las nuevas obligaciones derivadas de la Responsabilidad Proactiva

EIPD – Evaluación de Impacto en la Protección de Datos

PbDD – Privacidad desde el Diseño

DPD – Delegado de Datos Personales

GESTIONAR EL
RIESGO

REALIZAR
EIOD

APLICAR
PbDD

DESIGNAR
DPD



Resumen Final



Resumen Final

- La protección de los activos de información es clave para el Organismo
- Las consecuencias de los incidentes son potencialmente graves
- Todos tenemos una responsabilidad en la protección de datos
- Es necesario cuidado y atención, especialmente en Internet
- Ante dudas en estos temas, preguntar/consultar al:
 - Oficial de Seguridad de la Información (OSI),
 - Delegado de Datos Personales (DPD),
 - Su Gerente o Líder



**Muchas
Gracias**

Capacitación en la norma ISO/IEC 27001:2022

Esta capacitación tiene como objetivo familiarizar a los participantes con la norma ISO/IEC 27001:2022, proporcionando una comprensión clara de su estructura, requisitos y su papel fundamental en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

A lo largo de la sesión, se abordarán los principales elementos de la norma, comenzando con su objetivo y contexto dentro de la familia de estándares ISO/IEC 27000. Se explicará el Modelo PHVA (Planificar-Hacer-Verificar-Actuar) como base para la gestión continua de la seguridad de la información, así como la importancia de la gestión de riesgos, el análisis de amenazas y la aplicación de controles adecuados.

También se detallarán las cláusulas y requisitos esenciales que las organizaciones deben cumplir para lograr la certificación, junto con los controles de seguridad recomendados en el Anexo A de la norma. Finalmente, se explicará el proceso de auditoría, incluyendo su planificación, ejecución y la relevancia de la mejora continua para garantizar el cumplimiento y la efectividad del SGSI.

Esta capacitación permitirá que los participantes comprendan cómo la norma ISO/IEC 27001:2022 contribuye a fortalecer la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los activos organizacionales.



Expectativa

**ISO/IEC
27001:2022**

ISO/IEC 27001:2022



Para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), hemos adoptado el cumplimiento de la norma ISO/IEC 27001:2022 de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Sistemas de Gestión de la Seguridad de la Información - Requisitos

ISO/IEC 27001:2022

Podrías respondernos las siguientes preguntas:

- ¿Cuál es la función de una normativa de seguridad?
- ¿Por qué es importante adherir a una norma internacional?
- ¿Qué implica el cumplimiento de esta norma?
- ¿Qué son los activos de información?
- ¿Cuáles son las amenazas más comunes desde la perspectiva de infraestructura/desarrollo?
- ¿Cuáles son las vulnerabilidades vinculadas a tu entorno de trabajo?
- ¿Qué implica hacer una gestión de riesgos?
- ¿Para que se implementan los controles?

Envíanos tus respuestas, y todas las consultas de desees.

Inducción

ISO/IEC 27001:2022

Agenda

- Objetivo
- Familia ISO/IEC 27000
- Modelo PHCA
- Gestión de Riesgos
- Controles
- Cláusulas
- Auditoría



Objetivos



Objetivos

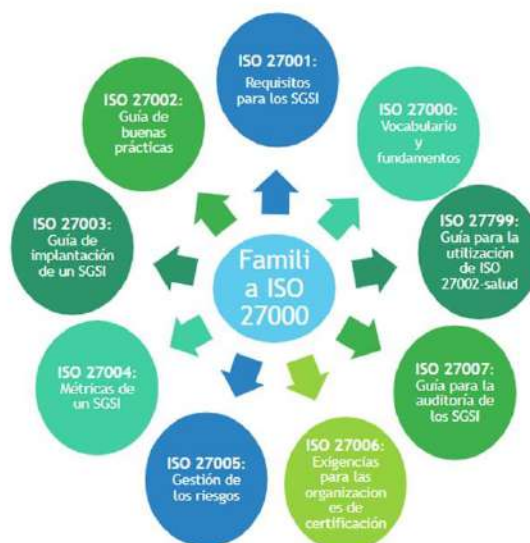
- Establecer los lineamientos y el marco de referencia para una exitosa implementación del Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de preservar la Confidencialidad, Integridad y Disponibilidad de los activos de información.
- La norma ISO/IEC 27001:2022 es la única norma internacional, auditable, que define los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información.

Familia ISO/ IEC 27000

Familia ISO/IEC 27000

La norma ISO/IEC 27001:2022 pertenece la familia de normas ISO/IEC 27000.

Esta familia está compuesta por varias normas, todas vinculadas con diferentes aspectos de la seguridad de la información.



Enfoque de SGSI

Enfoque de SGSI



Las principales normas de la familia que vamos a implementar como parte del Sistema de Gestión de Seguridad de la Información son las siguientes:

Enfoque de SGSI



El objetivo principal de un SGSI es proteger los pilares de la Seguridad de la Información, que son la **CONFIDENCIALIDAD**, la **INTEGRIDAD**, y la **DISPONIBILIDAD**.

- **CONFIDENCIALIDAD** – La información sólo es accedida por quién tiene permisos para acceder a ella.
- **INTEGRIDAD** – La información se mantienen incambiada, a menos que sea cambiada por un usuario autorizado, mediante una transacción autorizada.
- **DISPONIBILIDAD** – La información está disponible para quién tenga permisos de acceso a la misma.



Requerimientos Básicos



Requerimientos Básicos

El SGSI basado en la norma ISO/IEC 27001:2022. Los requerimientos para instalar un SGSI son:

- Compromiso de la Dirección
- Disponibilidad de recursos
 - Personas
 - Tiempo de gestión
 - Contratación de expertos
- Buen trabajo de equipo
- Paciencia
- Política de Seguridad de la Información
- Actividades de estandarización
- Requerimientos de cumplimiento
- Utilización del intelecto de los colaboradores
- Reducir la supervisión y promover la auto evaluación
- Capacitación del personal y desarrollo de competencias
- Enfocado en temas de seguridad de la información internos y externos
- Mejora continua planificada
- Ambiente de confianza y de trabajo en equipo
- Promover el uso del pensamiento basado en el riesgo, para determinar los riesgos y las oportunidades y planes de acción
- Establecer un sistema para implementar los controles de seguridad de la información
- Auditorías regulares



¿Qué nos ofrece la ISO/IEC 27001?



¿Qué nos ofrece la ISO/IEC 27001?

- Visión de Procesos alineados al ciclo PHVA (PDCA en inglés)
- Enfoque de Riesgos
- Controles de Seguridad de la Información
- Metodología estandarizada

CICLO PHVA (PDCA)

CICLO PHVA (PDCA)



► La norma ISO/IEC 27001:2022 se basa en el ciclo de mejora continua PHVA, (PLANIFICAR, HACER, VERIFICAR, ACTUAR). En inglés de este modelo se conoce como PDCA (PLAN, DO, CHECK, ACT).

- ✓ PLANIFICAR -> Desarrollo de las Políticas y del Plan
- ✓ HACER -> Poner en práctica
- ✓ VERIFICAR -> Supervisar
- ✓ ACTUAR -> Mejorar

► En base a los Requerimientos y Expectativas respecto a la Seguridad de la Información de los clientes, se implementa el modelo PHVA, a los efectos de entregar a los clientes, un Sistema de Gestión de la Seguridad de la Información controlado.

Estructura ISO/IEC 27001:2022

Estructura ISO/IEC 27001:2022



Estructura ISO/IEC 27001:2022



Proceso de Gestión de Riesgos

Proceso de Gestión de Riesgos

Gestión de Riesgo - El proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que existirán si esta acción ocurre”

Implica:

- Determinar **QUÉ** se necesita proteger.
- De **QUÉ** hay que protegerlo.
- **CÓMO** hacerlo.

Estándares y Metodologías de Gestión de Riesgo
Existen diferentes metodologías aplicables de gestión de riesgo.

Nosotros utilizaremos:

ISO/IEC 27005

MAGERIT

NIST

Proceso de Gestión de Riesgos

AMENAZA - Evento, suceso o una acción que anticipa la intención de dañar

VULNERABILIDAD - Ausencia o deficiencia de un control. Debilidad o grado de exposición de un sujeto, objeto o sistema

PROBABILIDAD - Potencial de ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas.

IMPACTO - Resultado de un suceso que afecta a los objetivos.

Proceso de Gestión de Riesgos

RIESGO para la Seguridad de la Información

La probabilidad de que una AMENAZA determinada, explote una o varias VULNERABILIDADES de un Activo o grupo de Activos de Información, causando un DAÑO a la Organización.

Se mide en términos de una combinación de la probabilidad de un evento y sus consecuencias.

$$\text{PROBABILIDAD} * \text{IMPACTO} = \text{RIESGO}$$

Proceso de Gestión de Riesgos

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	PASO
Establecimiento del contexto	1. Consideraciones Generales - Levantamiento de información inicial
	2. Establecer criterios básicos para la Gestión del Riesgo
	3. Definir alcance y límites de la Gestión del Riesgo
	4. Establecer una organización para la operación del SGRSI
Valoración del Riesgo	5. Identificar Activos de Información
	6. Identificar las amenazas y las vulnerabilidades
	7. Identificar los controles existentes
	8. Identificar consecuencias
	9. Valorar las consecuencias
	10. Valorar los incidentes
	11. Determinar el nivel de estimación del riesgo
	12. Evaluar el riesgo
Tratamiento del Riesgo	13. Seleccionar controles
Aceptación del Riesgo	14. Aceptar el riesgo
Comunicación del Riesgo	15. Comunicar el riesgo
Monitoreo y Revisión del Riesgo	16. Monitorear y revisar los riesgos



Beneficios esperados



Beneficios esperados

- ▶ Reducción del riesgo de pérdida, robo o integridad de la información sensible de la institución.
- ▶ Revisión continua de los riesgos y los controles de seguridad de la información implementados.
- ▶ Proyectos de adquisición alineados a la matriz de riesgos, que permitirán la reducción de los costos en compra sistemática de productos y tecnologías.
- ▶ Garantizar la continuidad del servicio tras un incidente de seguridad de la información de impacto alto.



Controles de Seguridad



Controles de Seguridad

- ▶ Implementar los controles necesarios para la Mitigación de los Riesgos identificados.

- ▶ ¿Qué es un Control?

Es un proceso de validación, para asegurar que las condiciones de riesgo que se habían identificado, si son detectadas, se toman acciones que evitan que dichas condiciones puedan terminar en un incidente de seguridad de la información, afectando la normal operación de los servicios y sistemas de la organización.



Controles de Seguridad - Ejemplos

- ▶ Seguridad Física - Se implementó un control de acceso mediante tarjetas inteligentes, a los efectos de controlar el ingreso a las instalaciones de UST.
- ▶ Seguridad Lógica - Se implementó un control de acceso mediante usuario y contraseña, a los efectos de controlar el ingreso a los sistemas de UST.
- ▶ Seguridad de Contraseña - Se implementó un control de vigencia de las contraseñas, que obliga al cambio de la misma de forma periódica a los efectos de ofrecer un nivel de dificultad adicional para el atacante que está intentando adivinar nuestra contraseña.
- ▶ Control de Activos - Se implementó un registro de todos los activos que tiene UST, y a quién fueron asignados. De esa forma, se sabe quién es el responsable de cada activo.
- ▶ Riesgo de Divulgación de Información - Se implementó un Acuerdo de Confidencialidad que establece los periodos de reserva y las posibles sanciones a quién incumple el mismo.



Cláusulas (Norma ISO/IEC 27001:2022)

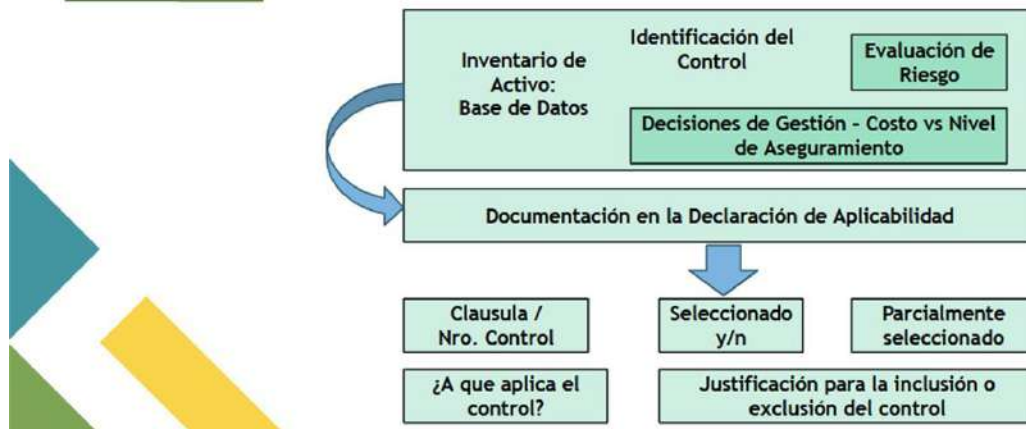
Cláusulas (Norma ISO/IEC 27001:2022)

- ▶ CLAUSULAS GENERALES
 - ▶ 1 - Alcance
 - ▶ 2 - Referencias normativas
 - ▶ 3 - Términos y definiciones
- ▶ CLAUSULAS DE REQUERIMIENTOS
 - ▶ 4 - Contexto de la organización
 - ▶ 5 - Liderazgo
 - ▶ 6 - Planificación
 - ▶ 7 - Soporte
 - ▶ 8 - Operaciones
 - ▶ 9 - Evaluación de performance
 - ▶ 10 - Mejoras
- ▶ ANEXO
 - ▶ Lista de los controles requeridos según el SOA (Declaración de Aplicabilidad)



SOA – Declaración de Aplicabilidad

SOA – Declaración de Aplicabilidad



Análisis de Brecha (Gap Analysis)

- ▶ Permite revisar la lista de controles existentes contra la lista de controles requeridos.
- ▶ Permite identificar que controles se deben desarrollar, cuales se deben actualizar, y confirmar los controles que están bien desarrollados.



Análisis de Brecha (Gap Analysis)

Auditoría



Auditoría

- ▶ De forma periódica, se realizan auditorías para verificar el cumplimiento con los requisitos de la norma, de forma de asegurar que se mantiene o mejora el nivel de seguridad de la información.
- ▶ De los hallazgos y observaciones de la auditoría, se implementan las mejoras en los controles, a efectos de mantener los niveles de riesgo en valores aceptables para la organización.



Muchas Gracias

Capacitación en Políticas de Seguridad de la Información

La seguridad de la información es un pilar fundamental en cualquier organización, y su correcta gestión depende, en gran medida, de la existencia y aplicación de políticas claras y bien definidas. Esta capacitación tiene como propósito principal familiarizar a los participantes con las Políticas de Seguridad de la Información, destacando su rol dentro del Sistema de Gestión de Seguridad de la Información (SGSI) y enfatizando la importancia de su cumplimiento para la protección de los activos organizacionales.

A lo largo de la sesión, se abordará en detalle la finalidad y el alcance de estas políticas, explicando cómo establecen las bases para un entorno seguro y confiable. Se brindará una introducción a los términos clave utilizados en la gestión de seguridad, con el objetivo de proporcionar un marco conceptual claro que permita comprender mejor la normativa vigente y su aplicación en el contexto organizacional. También se detallarán las responsabilidades de los distintos actores involucrados en la implementación y supervisión de estas políticas, asegurando que cada participante comprenda su papel dentro de este ecosistema de seguridad.

Uno de los temas centrales de la capacitación será el Manual de Políticas de Seguridad de la Información, el cual compila las directrices generales que rigen la protección de la información dentro del organismo. A partir de su análisis, se describirán los lineamientos específicos de cada una de las políticas de seguridad, abordando su impacto en las operaciones diarias y la manera en que estas contribuyen a la reducción de riesgos y vulnerabilidades.

Finalmente, para reforzar el aprendizaje y garantizar una apropiación efectiva de los conceptos, se expondrá un Plan de Concientización y Sensibilización, diseñado para fortalecer la cultura de seguridad dentro del organismo. Este plan incluirá estrategias para incrementar la comprensión y el compromiso de los colaboradores con las políticas de seguridad, promoviendo un enfoque proactivo en la gestión de riesgos.

Expectativa



Políticas de Seguridad

Políticas de Seguridad



Hemos desarrollado un conjunto de políticas de seguridad de la información como parte de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

Políticas de Seguridad



Podrías respondernos las siguientes preguntas:

- ¿Tienes claro cual es la función de una política de seguridad?
- ¿Has leído la Política de Seguridad de la Información y Protección de Datos?
- ¿Puedes comentarnos cuales son los lineamientos de la Política de Seguridad?
- ¿Cumples con las directivas indicadas por la Política de Seguridad?
- ¿Cuál debería ser la siguiente política a ser comunicada?

Envíanos tus respuestas, y todas las consultas de desees.

Políticas de Seguridad



Podrías respondernos las siguientes preguntas:

- ¿Puede una política limitar nuestra forma de trabajar?
- ¿Piensas que es posible no cumplir con los lineamientos de una política?
- ¿Cumplirías los lineamientos de las políticas, aunque esta te limitara tu trabajo?
- ¿Cuál piensas que serían las políticas que puedan afectar tu trabajo?

Envíanos tus respuestas, y todas las consultas de desees.

Políticas de Seguridad



Podrías respondernos las siguientes preguntas:

- ¿Qué crees que debería incluir una política en general?
- ¿Qué debería incluir, por ejemplo, una política de Control de Acceso?
- ¿Es posible escribir una política que no sea aplicable en la organización?
- ¿Qué se debería hacer cuando alguien no cumple con los lineamientos de una política?

Envíanos tus respuestas, y todas las consultas de desees.

Inducción



Políticas de Seguridad

Agenda

- Objetivo
- Alcance
- Definiciones
- Responsabilidades
- Manual de Políticas de Seguridad de la Información
- Descripción de las Políticas de Seguridad de la Información
- Plan de Concientización y Sensibilidad



Objetivos



Objetivos

- Establecer los lineamientos y el marco de referencia para la exitosa implementación de la Seguridad de la Información (SI) con el fin de preservar la Confidencialidad, Integridad y Disponibilidad de los activos de información.
- Una política es el conjunto de actividades que se asocian con la toma de decisiones en grupo, u otra forma de relaciones de poder entre individuos.

Alcance

Alcance



Las políticas establecen el marco para el correcto desarrollo de todos los procedimientos, instructivos y demás documentaciones asociadas a la implementación de la seguridad de la información.

Alcanza a todos los funcionarios del Organismo sin importar la modalidad de contratación, así como también a los proveedores y demás partes involucradas que interactúan con activos de información del Organismo.

Fundamento legal



Fundamento legal



Las políticas fueron desarrolladas según las recomendaciones establecidas en el Marco de Ciber Seguridad v4.2 de AGESIC.

A su vez, están alineadas a las buenas prácticas internacionales recomendadas por las siguientes normas:

NIST CSF v2.0 – Marco de Ciber Seguridad del NIST

ISO/IEC 27001:2022 – Requisitos para la certificación en Seguridad de la Información

ISO/IEC 27002:2022 – Buenas Prácticas de Seguridad de la Información.

ISO/IEC 27005:2022 – Gestión de Riesgos de Seguridad de la Información

ISO 55000:2014 – Gestión de Activos

También cumple con la normativa nacional de materia de Ciber Seguridad que incluye entre otros:

Ley 18331 – Protección de Datos Personales y Acción de Habeas Data



Responsabilidades



Responsabilidades

Directorio – Aprueba la Política de Seguridad de la Información y Protección de Datos, y vela por el cumplimiento de la normativa y legislación vigente al respecto, poniendo a disposición para ellos de los recursos necesarios para dar cumplimiento a lo establecido.

Comité de Seguridad de la Información (CSI) – Aprueba las políticas complementarias, así como el Manual de Políticas de Seguridad. También establece las responsabilidades específicas para su ejecución, control, monitoreo y mejora.

Oficial de Seguridad de la Información (OSI) – Colabora en la elaboración del Manual de Políticas de Seguridad de la Información. Elabora la documentación necesaria para la correcta implementación de las políticas y vela por el cumplimiento de las mismas.

Colaboradores – Todo el personal del Organismo es responsable de cumplir con lo establecido en cada una de las políticas aprobadas por el Comité de Seguridad o por el Directorio.



Políticas



Políticas

- El Organismo establece los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes.
- Los lineamientos de seguridad están clasificados en diferentes temáticas teniendo en cuenta el contexto interno y externo de la organización.



Manual de Políticas de Seguridad



Manual de Políticas de Seguridad

► **MAN-01 Manual de Políticas de Seguridad de la Información**

Establece el marco en el que se desarrollaron las diferentes políticas de seguridad de la información, así como también incluye una breve descripción de cada una de ellas.



Lista de Políticas de Seguridad



Lista de Políticas de Seguridad

POL-01 Política de Seguridad de la Información

Establece los principios rectores para asegurar la protección de los activos de información y para fundamentar el desarrollo de el Sistema de Gestión de la Seguridad de la Información del Organismo.

POL-02 Política de Gestión de Incidentes de Seguridad de la Información

Establece los criterios, comunicaciones y formas que definen el tratamiento, identificación y respuesta ante incidentes de seguridad de la información.

POL-03 Política de Uso Aceptable de los Activos

Detalla las buenas prácticas aplicadas para describir qué es considerado el uso aceptable de los activos.



Lista de Políticas de Seguridad

POL-04 Política de Intercambio y Traslado Físico de la Información

Define los criterios a seguir para el traslado de información desde el Organismo hacia clientes y proveedores.

POL-05 Política de Control de Acceso Lógico

Establece quién, cómo y cuándo se puede acceder a los activos de información.

POL-06 Política de Gestión de Usuarios y Contraseñas

Establece, difunde y provee criterios para el cumplimiento de las buenas prácticas en el uso de contraseñas.



Lista de Políticas de Seguridad

POL-07 Política de Gestión de Usuarios de Acceso Privilegiado

Establece la gestión adecuada de las cuentas de usuarios privilegiados para prevenir riesgos asociados al uso de premisos privilegiados.

POL-08 Política de Control de Acceso Físico a Áreas Seguras

Determina lineamientos para controlar el acceso físico a las áreas seguras y pretende reducir los riesgos de accesos no autorizados.

POL-09 Política de Seguridad del Equipamiento

Establece como se protege la seguridad de los equipos del Organismo.



Lista de Políticas de Seguridad

POL-13 Política de Registro y Auditoría de Eventos

Define cómo, cuándo y qué debe ser incluido en los registros de eventos auditables.

POL-14 Política de Protección y Privacidad de los Datos

Establece los principios rectores para asegurar la protección y la privacidad de los datos.

POL-15 Política de Clasificación de la Información

Define los criterios de la clasificación de los activos de información en uso dentro del Organismo.



Lista de Políticas de Seguridad

POL-16 Política de Uso Aceptable para Dispositivos Móviles

Establece como utilizar los dispositivos móviles (celulares, tabletas, etc.) en el Organismo.

POL-17 Política de Uso de Controles Criptográficos

Define los criterios de uso para los controles criptográficos.

POL-18 Política de Continuidad de la Operación y Recuperación ante Desastres

Determina los criterios a aplicar en relación a los controles de gestión de la seguridad de la información en el contexto de los planes de continuidad operativa del negocio.



Lista de Políticas de Seguridad

POL-19 Política de Cumplimiento

Define el contexto normativo y la interacción con el mismo desde el Organismo.

POL-20 Política de Escritorio y Pantalla Limpios

Establece la definición y el alcance del concepto de escritorio y pantalla limpia, sean estos físicos o virtuales.

POL-21 Política de Gestión de Riesgos de Seguridad de la Información

Establece los criterios para el tratamiento del riesgo de seguridad de la información dentro del Organismo en todas sus áreas de acción.



Lista de Políticas de Seguridad

POL-22 Política de Gestión de Cambios

Define como procesar el cambio entre actores y partes interesadas dentro del Organismo y en relación a su vínculo con productos y servicios que se ofrecen a clientes.

POL-23 Política de Finalización o Cambio en la Relación Laboral

Establece los lineamientos para el proceso de finalización de vínculos laborales en relación a la seguridad de la información.

POL-24 Política de Acceso Remoto y Teletrabajo

Establece los criterios a seguir para implementar conexiones de acceso remoto en el Organismo.



Lista de Políticas de Seguridad

POL-25 Política de Destrucción de la Información

Establece los criterios para implementar la disposición final de los activos de información en el Organismo.

POL-26 Política de Relacionamiento con Proveedores

Define aspectos de la gestión del vínculo con empresas proveedoras de servicios y productos al Organismo.

POL-27 Política de Uso Institucional de Redes Sociales

Establece prácticas obligatorias para el uso institucional de las redes sociales en modo seguro.



Lista de Políticas de Seguridad

POL-28 Política de Uso de Internet

Define el uso adecuado para los accesos a Internet que provee el Organismo y define buenas prácticas para los usuarios.

POL-29 Política de Desarrollo de Software Seguro

Establece los criterios para el desarrollo seguro de aplicaciones.

POL-30 Política de Gestión de la Seguridad de las Redes

Establece las reglas necesarias para garantizar el funcionamiento correcto y seguro de las redes de datos y de comunicaciones del Organismo.



Lista de Políticas de Seguridad

POL-31 Política de Gestión de Riesgos de Proveedores

Define los criterios para la detección de los riesgos vinculados con los proveedores que pueden afectar a las diferentes áreas del Organismo, a sus actividades y a los objetivos que están asociados a ella.

POL-32 Política de Gestión de Activos

Define los criterios para la obtención del máximo rendimiento de los bienes o recursos, es decir de todo aquello que tenga valor para el Organismo y sus clientes.

POL-33 Política del Sistema de Gestión de Seguridad de la Información

Define los criterios vinculados con la gestión del Sistema de Gestión de Seguridad de la Información (SGSI).



Plan de Concientización y Sensibilidad

Plan de Concientización y Sensibilidad

Se ha definido un plan de Concientización y Sensibilidad en temas de Seguridad de la Información, mediante el cual, se proveerá el Departamento de Personal, de los materiales necesarios para la realización de Campañas de Concientización y Sensibilización en temas de Seguridad de la Información, así como de Capacitaciones en temas específicos.

**Muchas
Gracias**



Capacitación en Gestión de Riesgos

La capacitación en Gestión de Riesgos tiene como propósito proporcionar a los participantes los conocimientos fundamentales sobre la gestión de riesgos en seguridad de la información, siguiendo los lineamientos de la norma ISO/IEC 27001:2022.

A lo largo de la sesión, se abordarán aspectos clave como el análisis, la evaluación, el tratamiento y la aceptación de riesgos, así como la importancia de implementar controles eficaces para mitigar amenazas y garantizar la protección de los activos de información. Se explicará el proceso de gestión de riesgos, enfatizando la necesidad de un enfoque estructurado para identificar y tratar los riesgos de seguridad. Se detallará el establecimiento del contexto, donde se definirán los factores internos y externos que pueden influir en la gestión de riesgos dentro del organismo.

Además, se abordará la evaluación del riesgo, un proceso que permite medir la probabilidad e impacto de los riesgos identificados. Dentro de esta evaluación, se explicará en profundidad el análisis de riesgos, que consiste en la identificación y caracterización de amenazas, vulnerabilidades y consecuencias potenciales. Posteriormente, se explorará el tratamiento de riesgos, que involucra la implementación de estrategias para mitigar, transferir, aceptar o evitar los riesgos detectados.

Un punto clave será la aceptación de riesgos, que se refiere a los criterios y condiciones bajo las cuales una organización decide asumir ciertos riesgos en lugar de mitigarlos completamente. Se discutirá cómo esta decisión debe estar respaldada por una evaluación adecuada y alineada con los objetivos estratégicos. Se analizará el papel fundamental de los controles de seguridad, cuyo propósito es reducir la probabilidad y el impacto de los riesgos. Se explicará cómo estos controles se implementan como parte de una estrategia de gestión integral y se ajustan a la realidad de cada organización.

Finalmente, se destacará la importancia de la comunicación del riesgo, garantizando que la información relevante se comparta con las partes interesadas, y la supervisión y revisión del riesgo, un proceso continuo que permite mejorar la gestión a lo largo del tiempo.

Expectativa



Gestión de Riesgos

Gestión de Riesgos



Para la implementación de una buena gestión de Riesgos, hemos adoptado las recomendaciones de la norma ISO/IEC 27001:2022 de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Sistemas de Gestión de la Seguridad de la Información - Requisitos

Gestión de Riesgos

Podrías respondernos las siguientes preguntas:

- ¿Qué es el análisis de riesgos?
- ¿Qué es la evaluación de riesgos?
- ¿Qué es el tratamiento de riesgos?
- ¿Qué es la aceptación de riesgos?
- ¿Para que se implementan los controles?



Envíanos tus respuestas, y
todas las consultas de deseos.

Inducción



Gestión de Riesgos

Agenda

- Objetivo
- Proceso de Gestión de Riesgos
- Establecimiento del Contexto
- Evaluación del Riesgo
- Análisis de Riesgo
- Identificación del Riesgo
- Estimación del Riesgo
- Evaluación del Riesgo
- Tratamiento del Riesgo
- Aceptación del Riesgo
- Comunicación del Riesgo
- Supervisión y Revisión del Riesgo

Objetivos

Objetivos

- Establecer los lineamientos y el marco de referencia para una exitosa evaluación de los riesgos de seguridad de la información, de acuerdo con los lineamientos definidos en el Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO/IEC 27001:2022, con el fin de preservar la Confidencialidad, Integridad y Disponibilidad de los activos de información.

Proceso de Gestión de Riesgos

Proceso de Gestión de Riesgos

Gestión de Riesgo – El proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que existirán si esta acción ocurre”

Implica:

- Determinar QUÉ se necesita proteger.
- De QUÉ hay que protegerlo.
- CÓMO hacerlo.

Estándares y Metodologías de Gestión de Riesgo
Existen diferentes metodologías aplicables de gestión de riesgo.

Nosotros utilizaremos:

- ISO/IEC 27005
- MAGERIT
- NIST

Proceso de Gestión de Riesgos

- AMENAZA – Evento, suceso o una acción que anticipa la intención de dañar
- VULNERABILIDAD – Ausencia o deficiencia de un control.
Debilidad o grado de exposición de un sujeto objeto o sistema
- PROBABILIDAD – Potencial de ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas.
- IMPACTO – Resultado de un suceso que afecta a los objetivos.

Proceso de Gestión de Riesgos

RIESGO para la Seguridad de la Información

La probabilidad de que una AMENAZA determinada explote una o varias VULNERABILIDADES de un Activo o grupo de Activos de Información, causando un DAÑO a la Organización.

Se mide en términos de una combinación de la probabilidad de un evento y sus consecuencias.

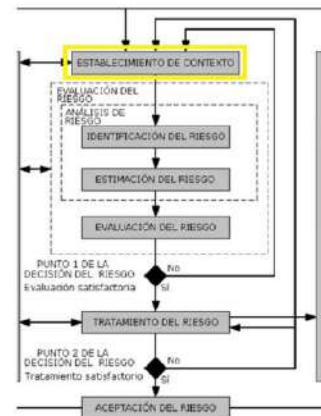
$$\text{PROBABILIDAD} * \text{IMPACTO} = \text{RIESGO}$$

Proceso de Gestión de Riesgos

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	PASO
Establecimiento del contexto	1. Consideraciones Generales - Levantamiento de información inicial 2. Establecer criterios básicos para la Gestión del Riesgo 3. Definir alcance y límites de la Gestión del Riesgo 4. Establecer una organización para la operación del SGRSI
Valoración del Riesgo	5. Identificar Activos de Información 6. Identificar las amenazas y las vulnerabilidades 7. Identificar los controles existentes 8. Identificar consecuencias 9. Valorar las consecuencias 10. Valorar los incidentes 11. Determinar el nivel de estimación del riesgo 12. Evaluar el riesgo
Tratamiento del Riesgo	13. Seleccionar controles
Aceptación del Riesgo	14. Aceptar el riesgo
Comunicación del Riesgo	15. Comunicar el riesgo
Monitoreo y Revisión del Riesgo	16. Monitorear y revisar los riesgos

Establecer el contexto

Implica **establecer los criterios básicos** necesarios para la gestión de riesgo de seguridad de la información, **definir el alcance** y los límites, y establecer una organización adecuada que opere la gestión de riesgos de seguridad de la información.



Proceso de Gestión de Riesgos

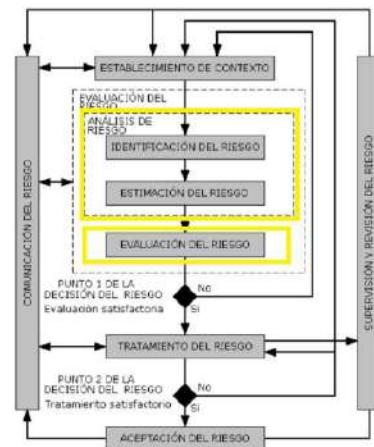
Análisis del Riesgo

La Valoración del Riesgo consta:

Identificar el riesgo
Identificar los activos
Identificar las amenazas
Identificar las vulnerabilidades
Identificar la existencia de controles

Analizar los riesgos
Estimación del riesgo

Evaluar los riesgos
Evaluar la aplicación del control



Análisis del Riesgo

Identificación de Activos

Identificación de Activos

Identificación de activos de información

Tipos de activos

Primarios

Información (Digital/Electrónica, Impresa)

Actividades y Procesos del Negocio

Soporte

Software (Aplicaciones, Herramientas, etc.)

Hardware (Servidores, Networking, otros equipos)

Servicios (Informática, Comunicaciones)

Personas (Habilidades, experiencia, calificación)

Intangibles (Reputación, marca, imagen)

Ubicación

Estructura de la Organización

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN						
No. Activo	Proceso Matriz	Subproceso	Tipo de Activo	Nombre de Activo	Descripción del activo	Ubicación
A1	Área de Tecnología de la Información y Comunicaciones	Infraestructura	Hardware	Controladora Wireless, puntos de acceso	puntos de acceso inalámbricos en toda la institución	Data Center
A2			Hardware	Firewall Fortigate	Control de acceso y permisos de seguridad perimetral para la red (institucional)	Data Center
A3		Redes y comunicaciones	Redes	Switch Core Cisco 2700	Procesamiento de tráfico de red para distribución en la red interna e Internet	Data Center
A4			Redes	Switch de Acceso Cisco 2960	Procesamiento de tráfico de red de acceso en cada piso del edificio	Data Center
A5			Software	Antivirus Institucional	Software de seguridad anti-pont	Data Center
A6		Aplicaciones informáticas	Software	Servicio de correo Exchange	Información de boletines de correo electrónico institucional	Data Center
A7			Instalaciones	Localidad	Centro de Datos Institucional	Edificio Matriz
A8		Talento Humano	Personal	Personal de soporte	Funcionarios de Soporte Técnico Nivel 1 - Institucional	Edificio Matriz
A9			Personal	Personal de desarrollo de sistemas	Personal técnico que desarrolla aplicaciones o automatiza procesos	Edificio Matriz

Identificación de Activos

Valoración de activos

CONFIDENCIALIDAD	Criterio
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

DISPONIBILIDAD	Criterio	INTEGRIDAD	Criterio
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución	Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución	Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución	Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Identificación de amenazas

Tienen el potencial de causar daños, las amenazas pueden afectar a más de un activo.

En tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

ANÁLISIS DE RIESGOS			
Subprocesos	Nro. Activo	Nombre Activo	Amenaza
Infraestructura	A1	Controladora Wireless, puntos de acceso	Intrusos en la red
			Indisponibilidad de servicios
	A2	Red de datos	Indisponibilidad de servicios
	A3	Firewall Fortigate	Acceso no deseado a activos críticos
			Indisponibilidad de servicios
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.
			Acceso de personas no deseables y/o pérdidas de activos.

Análisis del Riesgo

Identificación de vulnerabilidades

Se debe identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la organización.

ANÁLISIS DE RIESGOS				
Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad
Infraestructura	A1	Controladora Wireless, puntos de acceso	Intrusos en la red	Actualización de firmware equipo antiguo
			Indisponibilidad de servicios	No existe equipo de redundancia
	A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cable, 5e, 6u)
	A3	Firewall Fortigate	Acceso no deseado a activos críticos	Imposibilidad de actualizar firmware por falta de recursos del equipo
			Indisponibilidad de servicios	Inexistencia de equipo de redundancia
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia
			Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados

Análisis del Riesgo

Identificación de existencia de controles

Análisis de Riesgo				Evaluación de Riesgo			
Subproceso	Riesgo Activo	Activos Afectados	Amenaza	Vulnerabilidad	Probabilidad		
					Impacto	Nivel de amenaza	Nivel de vulnerabilidad
Infraestructura	A4	Controladores Windows, puertos de acceso	Indisponibilidad de servicios	Perdida de datos críticos (DB, logs)	1,57		Mantenimiento total
Infraestructura	A5	Red de datos	Acceso no deseado a activos críticos	Imposibilidad de actualizar firmware por falta de recursos del equipo	3,08		Soporte especializado
			Indisponibilidad de servicios	Exposición de datos de confidencialidad	1,25		Soporte contratado
Infraestructura	A6	Firmware Parques	Descarga de nuevos firmwares para la gestión de TPA	Indisponibilidad del software de gestión de dispositivos	1,08		Mantenimiento total
Infraestructura	A7	Bioservicios	No cumplimiento de estándares de seguridad en el equipo	Ausencia de equipos de respaldo	1,33		Mantenimiento total
			Disponibilidad de la gestión de personal	Equipos con recursos limitados	1,33		Mantenimiento total
Infraestructura	A8	Cámaras de seguridad	Acceso de personas no autorizadas a la gestión de activos	Exposición de datos de acceso sin registro	1,25		Mantenimiento total
			Acceso de personas no autorizadas a la gestión de activos	Exposición de datos de acceso sin registro	1,08		Mantenimiento total

Análisis del Riesgo

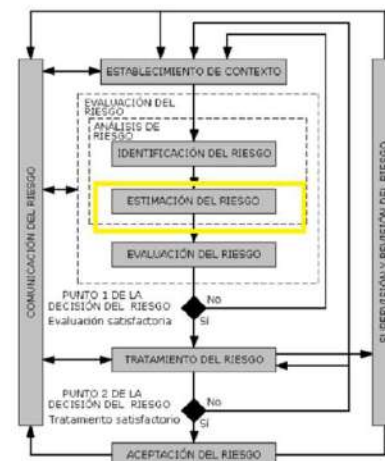
Estimación del riesgo

“Proceso para asignar valores a la probabilidad de ocurrencia y las consecuencias del impacto”

El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la probabilidad de ocurrencia de la amenaza (por ejemplo, baja, media y alta), y la magnitud de las consecuencias potenciales o impacto (por ejemplo, baja, media y alta).

En este caso el Nivel de Riesgo tendría un rango de valores de 1 a 9

Nivel de Riesgo	
1 - 2	El riesgo es BAJO
3 - 5	El riesgo es MEDIO
6 - 9	El riesgo es ALTO



Análisis del Riesgo

Evaluación del Riesgo

Otro Criterio de la Estimación de Riesgo

Considerando el Valor del Activo, el Nivel de Amenaza y el Nivel de Vulnerabilidad.

Criterios de probabilidad de ocurrencia de amenazas:

Nivel de amenaza	Criterio por probabilidad	Criterio por condiciones de amenaza	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecución y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable (probabilidad ~50%)	Por errores descuidados	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecución y la vulnerabilidad es fácilmente explotable	Falta de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad < 50%)	en rara ocasión	El atacante no se beneficia del ataque	datos no autorizados

Criterio de probabilidad de ocurrencia de vulnerabilidades

Nivel de vulnerabilidad	Criterio	Ejemplo
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Evaluación del Riesgo

Nivel de Riesgo	
1 - 2	El riesgo es BAJO
3 - 5	El riesgo es MEDIO
6 - 9	El riesgo es ALTO

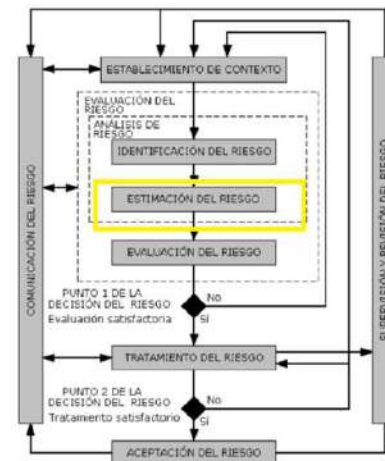
Estimación del riesgo

“Proceso para asignar valores a la probabilidad de ocurrencia y las consecuencias del impacto”

El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la probabilidad de ocurrencia de la amenaza (por ejemplo, baja, media y alta), y la magnitud de las consecuencias potenciales o impacto (por ejemplo, baja, media y alta).

En este caso el Nivel de Riesgo tendría un rango de valores de 1 a 9

Nivel de Riesgo	
1 - 2	El riesgo es BAJO
3 - 5	El riesgo es MEDIO
6 - 9	El riesgo es ALTO



Evaluación del Riesgo

Nivel del Riesgo

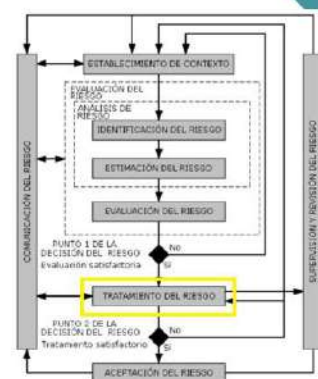
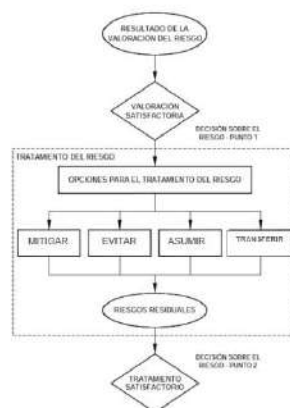
ID	Categoría	Amenaza	Impacto	Probabilidad	Frecuencia	Mitigación	Evaluación	Nivel de Riesgo
A1	Controladores Wired, puntos de acceso	Intrusión en la red	Actualización de firmware equipo antiguo	1,33	1	1	Soporte contratado	1,33
		Indisponibilidad de servicios	No existe equipo de redundancia	1,33	1	1	Soporte contratado	1,33
A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)	1,67	1	1	Mantenimiento local	1,67
A3	Firewall Fortigate	Acceso no deseado a activos críticos	Imposibilidad de actualizar firmware por falta de recursos del equipo	2,00	2	2	Soporte contratado	8,00
		Indisponibilidad de servicios	Existencia de equipo de redundancia	2,00	2	2	Soporte contratado	8,00
A4	Biometricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataformas de desarrollo actual (php)	1,00	1	1	Mantenimiento local	1,00

Evaluación del Riesgo

Tratamiento del Riesgo

Tratamiento del Riesgo

- Existen cuatro opciones disponibles para el Tratamiento del Riesgo
- Evitar
- Mitigar
- Asumir / Aceptar
- Transferir

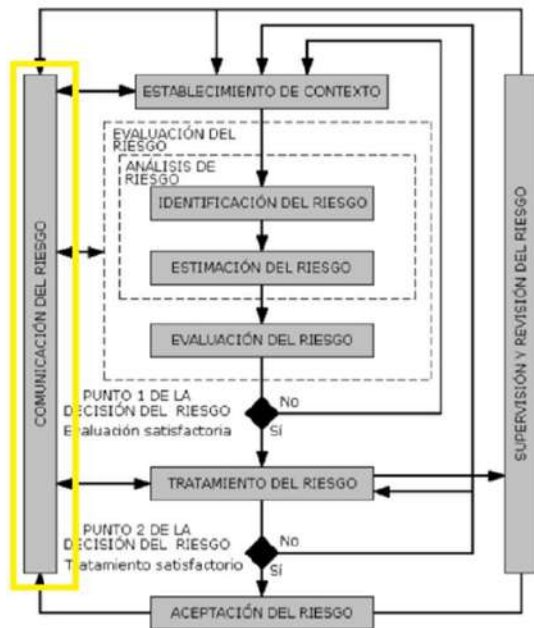


Tratamiento del Riesgo

• EJEMPLO DE TRATAMIENTO DEL RIESGO

Evaluación de Riesgos													
Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tratamiento de Riesgos							
CID	Nivel de amenaza	Nivel de vulnerabilidad				Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	Riesgo residual
157	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	157	BAJO	ACEPTABLE
157	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	157	BAJO	ACEPTABLE
157	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	157	BAJO	ACEPTABLE
157	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	Migración a Cloud	1	1	157	BAJO	ACEPTABLE
157	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	157	BAJO	ACEPTABLE
157	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	Migración a Cloud	1	1	157	BAJO	ACEPTABLE

Comunicación del Riesgo



Comunicación del Riesgo

- Garantiza que los responsables de la implementación de la gestión del riesgo y aquellos con intereses establecidos, comprendan las bases sobre las cuales toman las decisiones y por qué se requieren acciones particulares

Monitoreo y Revisión del Riesgo

Monitoreo y Revisión del Riesgo

Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación.

Por ende, es necesario el monitoreo constante para detectar estos cambios.



Revisión



Revisión

De forma periódica, se realizan revisiones de la evaluación de riesgos, a los efectos de analizar si se han producido cambios en los supuestos iniciales de amenazas y vulnerabilidades.

De los hallazgos y observaciones de las revisiones, se implementan las mejoras en los controles a efectos de mantener los niveles de riesgo en valores aceptable para la organización.



Beneficios esperados

Beneficios esperados



- ▶ Reducción del riesgo de pérdida, robo o integridad de la información sensible institucional.
- ▶ Revisión continua de los riesgos y los controles de seguridad de la información implementados en UST.
- ▶ Proyectos de adquisición alineados a la matriz de riesgos, que permitirán la reducción de los costos en compra sistemática de productos y tecnologías.
- ▶ Garantizar la continuidad del servicio tras un incidente de seguridad de seguridad de la información de impacto alto.

Muchas Gracias



Capacitación en Sistema de Gestión de Seguridad de la Información (SGSI)

Esta capacitación ofrece una visión integral sobre el SGSI, abordando sus definiciones, principios y aplicación práctica. Se explicará la importancia de la seguridad de la información y su relación con la gestión de riesgos, destacando los conceptos de activos, amenazas y vulnerabilidades. También se analizarán los beneficios y el alcance del SGSI, así como su impacto en los procesos organizacionales y el cumplimiento normativo.

Se profundizará en los controles de seguridad, tanto físicos como lógicos, y en su papel dentro de la gestión de incidentes y auditorías. Además, se discutirá la relevancia de las políticas de seguridad, su aplicación en el entorno laboral y la importancia de la norma ISO/IEC 27001:2022 en la certificación y mejora continua de la seguridad de la información.

A lo largo de la sesión, los participantes responderán preguntas clave para reforzar su comprensión, tales como la definición y función de los activos, amenazas, vulnerabilidades, riesgos e incidentes de seguridad, además de la utilidad de los controles y políticas. Finalmente, se reflexionará sobre cómo la implementación del SGSI afecta el trabajo diario y el papel de cada integrante en su aplicación efectiva dentro del organismo.

Expectativa



Sistema de Gestión de Seguridad de la Información (SGSI)



SGSI



El Organismo está en proceso de implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

SGSI

Podrías respondernos las siguientes preguntas:

- ¿Sabes qué es un SGSI?
- ¿Por qué es importante que lo implementemos en UST?
- ¿Cuáles son los beneficios de su implementación?
- ¿Tienes idea de cómo va a afectar nuestro trabajo?
- ¿Crees que tu podrías estar involucrado en esta actividad?

Envíanos tus respuestas, y todas las consultas de deseos.



SGSI

Podrías respondernos las siguientes preguntas:

- ¿Sabes qué es una norma y para qué sirve?
- ¿Conoces la norma ISO/IEC 27001:2022?
- ¿Tienes claro cómo se utiliza y qué beneficios se obtienen del uso de una norma?
- ¿Utilizas alguna norma en tu trabajo diario?

Envíanos tus respuestas, y todas las consultas de deseos.



SGSI

Podrías respondernos las siguientes preguntas:

- ¿Qué es un activo?
- ¿Qué es una amenaza?
- ¿Qué es una vulnerabilidad?
- ¿Qué es el riesgo?
- ¿Qué es un incidente de seguridad?
- ¿Para qué sirven los controles?
- ¿Para qué sirven las políticas?



Envíanos tus respuestas, y
todas las consultas de desees.

Inducción



Sistema de Gestión de Seguridad de la Información (SGSI)

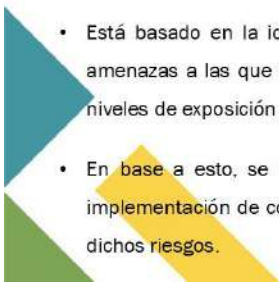
Agenda

- Objetivo
- ¿Qué es Seguridad de la Información?
- ¿Qué es un SGSI?
- Fundamentos
- Utilización
- Beneficios
- Alcance
- ¿A quién afecta?
- Objetivos de la inducción
- Políticas
- Activos, Amenazas, Vulnerabilidades y Riesgos
- Riesgos y Controles
- Revisión
- Auditoría

Objetivos



Objetivos

- Dar a conocer el proyecto de implementación del Sistema de Gestión de Seguridad de la Información, basado en la norma internacional ISO/IEC 27001:2022.
 - El proyecto es liderado por el Comité de Seguridad de la Información (CSI).
 - Está basado en la identificación y clasificación de los activos de información, en entender y analizar las amenazas a las que estos están expuestos, así como las vulnerabilidades de los activos, lo que define los niveles de exposición a dichas amenazas.
 - En base a esto, se realiza la evaluación y gestión de los riesgos correspondientes, con la consecuente implementación de controles, cuyo objetivo es el de minimizar la probabilidad de ocurrencia o el impacto de dichos riesgos.
- 



¿Qué es Seguridad de la Información?

¿Qué es Seguridad de la Información?



Conjunto de medidas **preventivas, detectivas y correctivas** que permiten resguardar y proteger la información.

Se ocupa de la información en todas sus formas, (oral, impresa, electrónica, ...), a diferencia de la seguridad informática, que se ocupa únicamente de la seguridad de los sistemas de información y la información vinculada a los mismos.

Estas medidas se definen e implementan en función del riesgo a las amenazas a las que se encuentran expuestos los activos de información, con respecto a las propiedades de Confidencialidad, Integridad y Disponibilidad.



¿Qué es el SGSI?

El SGSI, es un Sistema para Gestionar la Seguridad de la Información, con el objetivo de salvaguardar la información de posibles amenazas a las que pueden estar expuestas.

Está basado en la norma ISO/IEC 27001:2022, y consiste en preservar la Confidencialidad, Integridad y Disponibilidad de la información, además de todos los sistemas implicados en el tratamiento de la misma.

Está conformado por un conjunto de políticas, procedimientos y controles para garantizar la seguridad de la información en el desarrollo de las actividades del Organismo.



¿Qué es el SGSI?



¿Qué fundamentos se utilizan?

¿Qué fundamentos se utilizan?

De acuerdo con la norma ISO/IEC 27001:2022, la seguridad de la información se basa en la preservación de los siguientes conceptos:

- **Confidencialidad:** La información no se pone a disposición de nadie, ni se revela a individuos o a entidades no autorizados
- **Integridad:** Mantener de forma completa y exacta la información y los métodos de procesamiento
- **Disponibilidad:** Acceder y utilizar la información y los sistemas de procesamiento por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base a estos pilares se hace un análisis y una evaluación de los activos de información con un enfoque en las amenazas y vulnerabilidades (los riesgos), que nos permitirán implementar políticas, procedimientos y controles para proteger la información, y cumplir con las normas de legalidad y de protección de datos.

¿Qué elementos incluye?

Manual de Seguridad - Guía de como se debe implementar y seguir el SGSI

- Incluye:
 - Objetivos
 - Alcance
 - Responsables
 - Políticas
 - Directrices

Procedimientos, se relacionan con las actividades operativas, nos dan los parámetros que se deben seguir para que la gestión sea eficaz, lo que permitirá tener una adecuada:

- Planificación
- Operación
- Control

Registros, es la evidencia de la información que ha sido documentada durante toda la gestión.



¿Qué elementos incluye?



Utilización



Utilización

- La información, junto a los procesos y los sistemas que hacen uso de ella, son los activos que tienen valor para el Organismo.
- La confidencialidad, integridad y disponibilidad de dicha información es esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen del Organismo, necesarios para conseguir los objetivos y asegurarse de que haya beneficios económicos.
- El modelo de gestión de la seguridad contempla los procedimientos adecuados y planifica e implementa controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de estos.
- El SGSI, ayuda a establecer la política de seguridad y los procedimientos con relación a los objetivos de negocio, con el objetivo de mantener un nivel de exposición siempre menor al nivel de riesgo que se desea asumir.



Beneficios



Beneficios

- Establecer una metodología estructurada y clara.
- Reducir el riesgo de pérdida, robo o corrupción de la información sensible.
- Los accesos a la información se dan mediante medidas de seguridad.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los clientes y los socios de la organización.
- Las auditorías externas ayudan de forma cíclica a identificar las debilidades del SGSI y las áreas que se deben mejorar.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.



Otros elementos a tener en cuenta

Otros elementos a tener en cuenta



Teniendo claro la función de un SGSI y sus tres principios básicos, otros elementos que no se pueden perder de vista en el proceso de implementación son:

- Compromiso y apoyo de la dirección – Es el área más comprometida a la hora de la difusión, la gestión y el seguimiento del proceso.
- Definición del alcance - Es preciso definir qué objetivos tendrá el SGSI; qué beneficios supondrá y por cuánto tiempo queremos aplicarlo
- Formación del personal – Los colaboradores son parte activa del proceso y por ello es necesario que reciban la formación necesaria que les permita estar a la altura del mismo.
- Evaluación de riesgos – Un SGSI se enfoca sobre todo en la gestión de riesgos asociados al manejo y la gestión de la información.
- Compromiso de mejora continua – Al igual que otros sistemas de gestión interno, un SGSI supone la adopción de la mejora continua como elemento de identidad corporativa.



Alcance



Alcance

Todos los servicios brindados por el Organismo que incluyen:

- Aplicaciones administrativas
- Aplicaciones de soporte
- Aplicaciones varias
- Infraestructura
- Soporte a Usuarios
- Mantenimiento de software
- Desarrollo de software
- Gestión de Proyectos
- Asesoría en Seguridad



¿Roles involucrados?



¿Roles involucrados?

Comisión de Seguridad de la Información (CSI): Es responsable de la definición, aprobación, comunicación y revisión de las Políticas de Seguridad, procedimientos, e implementación de controles, así como de la supervisión del SGSI.

Oficial de Seguridad de la Información (OSI): Es responsable de la coordinación y seguimiento de la implementación del sistema de gestión.

Departamento de Personal: Es responsable de la coordinación de la capacitación en temas de seguridad.

Gerentes / Líderes: Son responsables de implementar los controles que sean requeridos.

Colaboradores

- Todos somos responsables de cumplir con los controles y medidas de seguridad establecidas.
- Todos tenemos la obligación de la formación en temas de seguridad de la información.



Objetivos de la formación



Objetivos de la formación

- Permitir mejorar el conocimiento, educación y capacitación del personal en materia de seguridad de la información.
- Conocer las normas, políticas, procedimientos y controles de seguridad de la información.
- Capacitar a los empleados en el uso correcto de los medios de procesamiento de la información, procedimiento de registro, utilización de aplicaciones y herramientas, etc.
- Concientizar a todos los empleados sobre las posibles amenazas, vulnerabilidades, riesgos y problemas que pueden afectar a los sistemas del Organismo y cómo actuar ante ellos.
- Formación en torno a las normativas o leyes aplicables en materia de seguridad de la información..



Políticas



Políticas

- En conjunto con el Comité de Seguridad de la Información, se han desarrollado un conjunto de políticas de seguridad, las que establecen el marco normativo en los temas de seguridad de la información.
- Se ha confeccionado un Manual de Políticas, el que resume el objetivo de cada política.
- Se está definiendo un plan de concientización y capacitación en temas de seguridad.
- Se realizará una campaña de divulgación y explicación de cada una de las políticas que serán implementadas.
- Es responsabilidad de todos nosotros, conocer todas las políticas y aplicar sus lineamientos.



Algunas definiciones



Algunas definiciones

- **Activo** – son todos los elementos, tangibles o intangibles, que tienen valor para el Organismo.
- **Amenaza** – son las acciones que pueden afectar una vulnerabilidad de un activo causando un daño al mismo.
- **Vulnerabilidad** – es una deficiencia de diseño o estructural de un activo.
- **Riesgo** – es la probabilidad de que una amenaza se aproveche de una vulnerabilidad causando un daño en el activo y por ende en la organización.
- **Probabilidad de ocurrencia** – es el valor que representa la oportunidad de ocurrencia de la amenaza.
- **Impacto** – es el resultado de que la amenaza, de materializarse, aproveche una vulnerabilidad para causar un daño en el activo.
- **Exposición** – es el grado o la posibilidad de que se produzca un impacto.



Riesgos y Controles



Riesgos y Controles

- En función de los Riesgos identificados para cada Activo, se identificarán e implementarán un conjunto de Controles, los cuales tendrán como objetivo, disminuir la Probabilidad de Ocurrencia o el Impacto producido sobre el Activo.
- Control – Cualquier tipo de protección o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros archivos.
- Los controles pueden ser:
 - Preventivos
 - Detectivos
 - Correctivos
 - Disuasivos
 - Compensatorios
- Los controles son ejecutados con una determinada frecuencia que puede variar de un control a otro.



Revisión



Revisión

- En forma periódica, se deberá analizar el resultado de la ejecución de los controles, a los efectos de poder medir la efectividad, eficiencia y eficacia de los mismos.
- De igual forma, se deberá realizar una actualización de la evaluación de los riesgos de los activos, por lo menos con una frecuencia anual.
- En función de la revisión de los riesgos, de deberán actualizar los controles que así lo requieran.



Auditorías



Auditorías

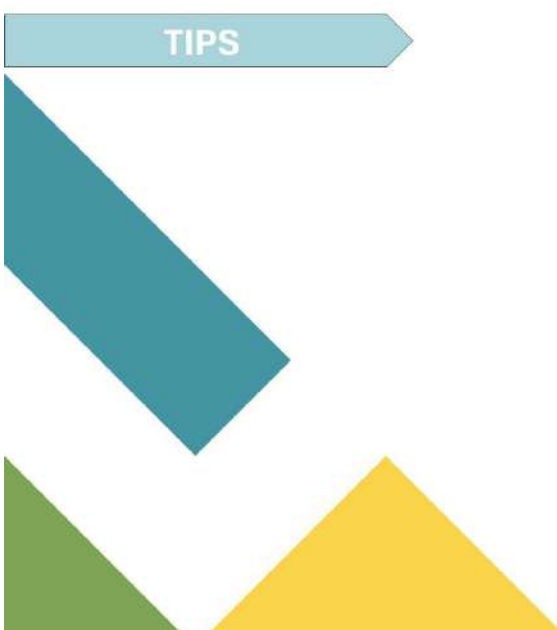
- El SGSI será **auditado** periódicamente (anualmente), tanto internamente por un auditor independiente, como **externamente por la entidad certificadora**.
- De los **hallazgos** que surjan de ambas **revisiones**, se implementarán las mejoras **recomendadas**, a los efectos de mantener **el SGSI actualizado**.



Muchas Gracias

Capacitación con Tips en puntos claves

Como complemento a la capacitación, se creó este material denominado “TIPS”, diseñado para abordar de manera sencilla y accesible temas clave como la concienciación en seguridad, el uso adecuado de medios de almacenamiento y las buenas prácticas en redes sociales. El material, elaborado en formatos visuales y de fácil comprensión, refuerza hábitos seguros en el uso de la información dentro del organismo y fomenta una cultura de seguridad alineada con los principios del SGSI.



TIPS

Puntos Claves



Puntos Claves - Concientización

- 
- No utilices tus credenciales de acceso al Organismo en aplicaciones de uso personal.
 - NO accedas a enlaces (links) sospechosos. Mejor escribe la dirección en la barra del navegador.
 - Protege la información impresa utilizando mobiliario con cerradura, cajas fuertes o armarios ignífugos.
 - Procura no transportar información sensible en dispositivos extraíbles. Si lo haces cifra la información previamente.
 - Aprende a detectar los ataques de ingeniería social y como defenderte.
 - Avisa si ves o detectas un comportamiento anómalo.

Puntos Claves - Concientización

- Bloquee la sesión de tu equipo cuando abandones tu puesto de trabajo.
- No modifiques la configuración de tus dispositivos móviles ni instales aplicaciones no autorizadas.
- Evita el uso de equipos no corporativos para acceder a servicios de la empresa.
- Si accedes al correo corporativo desde tu equipo personal, no descargues ficheros al equipo.
- Destruya la información sensible en formato papel, no te limites a tirarla a la papelera, evita una fuga de información.

TIPS

Medios de Almacenamiento

Medios de Almacenamiento



- Los medios de almacenamiento sirven para respaldar la información.
- Centraliza y agrupa tu información en al menos un dispositivo de almacenamiento.
- Organiza tus datos, carpetas, accesos y usuarios.
- Crea primero la nueva copia de respaldo, antes de borrar la copia del respaldo anterior.
- No lles información sensible en un medio de almacenamiento externo, si no se encuentra cifrado.
- Los medios de almacenamiento se pueden romper o averiar. Haz una segunda copia de seguridad en otro medio de almacenamiento.
- No almacenes información de la empresa en la nube sin autorización.

TIPS



Redes Sociales

Redes Sociales



- Configura tu privacidad con las opciones que te ofrece la red social, elige el nivel adecuado de privacidad.
- No publiques datos del Organismo en tus redes sociales.
- No utilices las mismas contraseñas de acceso que la que utilizas para acceder a los recursos del Organismo.
- No emitas opiniones en nombre del Organismo.
- Protege tu información personal y la del Organismo.

Muchas Gracias



ANEXO 5 - Listado de actividades pendientes

Este anexo contiene un listado detallado de todas las actividades pendientes necesarias para alcanzar el nivel máximo de madurez del MCS de AGESIC. El listado se encuentra ordenado por el nivel de prioridad de las actividades, e incluye: la prioridad de cada tarea, su descripción, los responsables de su ejecución y la evidencia resultante de su cumplimiento. Dichas actividades deberán ser desarrolladas por el organismo, cuando este lo entienda pertinente.

Listado de actividades pendientes

Prioridad	Tareas pendientes para alcanzar nivel de madurez	Responsable	Evidencia
P1	T009 - Documentar los procesos y procedimientos para la actualización del inventario de dispositivos físicos y sistemas.	Director de Desarrollo	E009 - Manual documentado de procesos y procedimientos de actualización del inventario.
P1	T010 - Implementar un software de inventario para gestionar y actualizar el inventario de manera centralizada.	Director de Desarrollo	E010 - Registros de implementación del software de inventario.
P1	T011 - Automatizar el proceso de actualización del inventario cuando sea posible.	Director de Desarrollo	E011 - Logs del sistema que evidencien la automatización de actualizaciones.
P1	T012 - Definir un control para verificar la precisión del inventario.	Director de TIC	E012 - Documentación de las auditorías realizadas utilizadas como evidencia de cumplimiento o desviaciones encontradas.
P1	T013 - Realizar actividades periódicas de control interno para verificar el cumplimiento de los procedimientos de inventario.	Auditoría Interna	E013 - Informes de actividades de control interno realizadas.
P1	T014 - Alinear el inventario con los procedimientos establecidos mediante revisiones periódicas.	Auditoría Interna	E014 - Registros de revisiones y ajustes al inventario en alineación con los procedimientos establecidos.
P1	T025 - Identificar y registrar el licenciamiento de software de equipos personales.	Director de Soporte	E025 - Registro de licenciamiento de software de equipos personales.
P1	T029 - Designar rol de responsable de la seguridad de la información (RSI).	CSI	E029 - Resolución con designación del RSI.
P1	T030 - Difusión del rol de RSI a todo el organismo.	CSI	E030 - Plan de difusión del rol RSI en el organismo.
P1	T031 - Identificar y designar a los integrantes del CSI.	Directorio	E031 - Documento de designación de los miembros del CSI.
P1	T032 - Establecer un registro oficial de los propietarios de los activos y comunicarles sus responsabilidades en la protección de dichos activos.	Alta Dirección	E032 - Registro de propietarios de activos con sus responsabilidades asignadas.
P1	T033 - Documentar los nombramientos y responsabilidades del CSI en un documento.	Director de RRHH	E033 - Documento que refleje los roles asignados del CSI.
P1	T034 - Establecer un cronograma de reuniones periódicas del CSI.	CSI	E034 - Cronograma de reuniones del CSI.
P1	T035 - Designar un secretario para documentar las reuniones del CSI.	CSI	E035 - Minutas o actas de reuniones del CSI firmadas por los participantes.
P1	T036 - Registrar las decisiones, acuerdos y acciones tomadas en cada sesión.	CSI	E036 - Registro de acciones derivadas de las reuniones, con responsables asignados y fechas de cumplimiento.
P1	T037 - Crear un documento formal que describa las funciones y responsabilidades del RSI, CSI y otros roles relacionados con la seguridad de la información.	CSI	E037 - Documento formal que describa roles y responsabilidades del RSI, CSI y roles relacionados.
P1	T038 - Designar un rol responsable de la gestión de riesgos (RGR).	RSI	E038 - Resolución con designación del RGR.
P1	T039 - Designar un rol responsable de la gestión de incidentes (RGI).	RSI	E039 - Resolución con designación del RGI.
P1	T040 - Designar un rol responsable de monitoreo (RM).	RSI	E040 - Resolución con designación del RM.
P1	T041 - Designar un rol responsable de la gestión de vulnerabilidades y parches (RGV).	RSI	E041 - Resolución con designación del RGV.
P1	T042 - Diseñar e implementar controles internos que evalúen posibles conflictos entre roles y áreas de responsabilidad.	CSI	E042 - Registro del diseño de controles internos para conflictos entre roles y áreas de responsabilidad.
P1	T043 - Preparar reportes con los resultados de las actividades de control interno y compartirlos con el RSI y partes interesadas.	CSI	E043 - Reportes enviados al RSI e interesados con los resultados de las revisiones.
P1	T044 - Establecer los objetivos anuales de seguridad de la información.	CSI	E044 - Documento oficial con los objetivos anuales de SI.
P1	T045 - Convocar reuniones del CSI para discutir los objetivos y aprobar las acciones necesarias.	CSI	E045 - Actas de reuniones del CSI con la discusión y aprobación de los objetivos.
P1	T046 - Definir acciones específicas para lograr los objetivos anuales, asignando responsables y fechas de cumplimiento.	CSI	E046 - Plan de acciones iniciales para cumplir con los objetivos.
P1	T047 - Diseñar un plan de acción detallado para cada objetivo establecido para alcanzar los objetivos anuales de seguridad de la información (Incluyendo: actividades específicas, cronogramas y recursos necesarios).	RSI y Director de TIC	E047 - Documento formal con el plan de acción detallado, que incluye actividades específicas, cronogramas y recursos necesarios.
P1	T048 - Establecer indicadores de desempeño (KPIs) para medir el avance del plan de acción alcanzar los objetivos anuales de seguridad de la información.	RSI y Director de TIC	E048 - Lista de indicadores de desempeño (KPIs) definidos, con sus fórmulas de cálculo y metas asociadas.
P1	T049 - Asignar responsables para cada actividad dentro del plan de acción para alcanzar los objetivos anuales de seguridad de la información .	RSI	E049 - Registro oficial de responsables asignados para cada actividad dentro del plan, con fechas y firmas de aceptación.
P1	T050 - Comunicar el plan de acción alcanzar de los objetivos anuales de seguridad de la información a las áreas involucradas.	RSI	E050 - Evidencia de comunicación del plan de acción, como correos electrónicos, actas de reuniones o presentaciones compartidas con las áreas involucradas.

P1	T051 - Crear materiales de comunicación (presentaciones, boletines, infografías) que expliquen los objetivos de seguridad y su importancia.	Comunicaciones	E051 - Materiales de difusión sobre los objetivos de SI.
P1	T052 - Realizar reuniones o capacitaciones con el personal y partes interesadas para comunicar los objetivos anuales de seguridad de la información.	RSI y Capacitación	E052 - Registro de sesiones de comunicación con el personal y partes interesadas.
P1	T053 - Implementar un sistema de seguimiento y reporte periódico del avance del plan de acción de los objetivos anuales de seguridad de la información.	RSI	E053 - Informes periódicos sobre el avance del plan de acción
P1	T054 - Diseñar una estrategia formal de seguridad de la información y ciberseguridad a mediano y largo plazo.	RSI	E054 - Estrategia de SI y ciberseguridad documentada
P1	T055 - Implementar proyectos basados en la estrategia seguridad de la información, con presupuesto asignado y aprobación del Directorio.	CSI y Directorio	E055 - Proyectos formales aprobados y con presupuesto asignado
P1	T056 - Difundir la estrategia de seguridad de la información a todos los niveles del organismo, utilizando todos los canales de comunicación disponibles.	Comunicaciones	E056 - Materiales de comunicación interna y externa para difundir la estrategia
P1	T057 - Evaluar periódicamente el impacto de la estrategia de seguridad de la información y realizar ajustes en función de las lecciones aprendidas.	CSI	E057 - Informes de evaluación del impacto de la estrategia
P1	T061 - Identificar áreas clave que requieren políticas específicas y desarrollarlas.	CSI	E061 - Lista de áreas clave identificadas y sus políticas desarrolladas.
P1	T063 - Aprobación del Directorio todas las políticas pendientes.	CSI	E063 - Acta de Resolución de aprobación de políticas.
P1	T064 - Establecer una periodicidad de revisión de las políticas para determinar su vigencia y, si corresponde, actualizarlas.	CSI	E064 - Acta de revisión de las políticas.
P1	T065 - Difusión de políticas actualizadas a todo el organismo.	CSI y Comunicaciones	E065 - Plan de difusión de políticas actualizadas
P1	T066 - Diseñar y documentar un SGSI alineado al Marco de Ciberseguridad.	CSI	E066 - Documento del SGSI alineado al marco de Ciberseguridad.
P1	T067 - Definir procedimientos específicos para cada componente del SGSI.	CSI	E067 - Procedimientos específicos documentados.
P1	T068 - Establecer indicadores clave de desempeño (KPIs) para medir la efectividad del SGSI.	RSI	E068 - KPIs definidos y reportados periódicamente para medir la efectividad del SGSI.
P1	T069 - Planificar y ejecutar revisiones periódicas formales del SGSI.	RSI	E069 - Plan de ejecución de revisión del SGSI.
P1	T070 - Presentar los resultados de las revisiones al CSI para toma de decisiones.	RSI	E070 - Informes de revisión del SGSI y planes de mejora.
P1	T073 - Documentar los roles y responsabilidades del RSI como referente ante el organismo y como referente ante CERTuy.	CSI	E073 - Documento con roles y responsabilidades del RSI.
P1	T074 - Capacitar al RSI en gestión de riesgos e incidentes de seguridad.	CSI	E074 - Plan de capacitación del RSI.
P1	T075 - Establecer un proceso formal para la gestión de incidentes de seguridad, incluyendo el reporte y la respuesta.	RSI y RGI	E075 - Documento de proceso formal para la gestión de incidentes.
P1	T077 - Desarrollar un procedimiento formal para la gestión de riesgos en conjunto con los propietarios de activos.	RSI	E077 - Documento con procedimientos para la gestión de riesgos.
P1	T078 - Realizar un seguimiento formal y periódico del cumplimiento del plan anual.	CSI	E078 - Plan de actividades y reuniones.
P1	T079 - Documentar y reportar los resultados de las actividades del plan anual a la dirección.	CSI	E079 - Reportes periódicos sobre el avance del plan anual.
P1	T084 - Crear un procedimiento de cumplimiento de la normativa (Según Decreto 092/014).	RSI y RDP	E084 - Procedimiento documentado de revisión normativa.
P1	T085 - Realizar auditorías internas para detectar posibles desvíos de cumplimiento y comunicar los resultados al CSI.	RSI	E085 - Reportes de auditoría interna.
P1	T086 - Diseñar y ejecutar controles internos que evalúen periódicamente el cumplimiento del SGSI.	RSI	E086 - Documento de controles a ejecutar para la evaluación del cumplimiento del SGSI.
P1	T087 - Documentar los resultados de las revisiones para identificar áreas de mejora.	RSI	E087 - Resultados documentados de los controles internos.
P1	T088 - Incorporar los hallazgos en un plan de acción que impulse la mejora continua.	RSI	E088 - Plan de acción para la mejora continua.
P1	T089 - Presentar los resultados y el plan de acción al Directorio para su consideración.	RSI	E089 - Presentación de resultados al Directorio
P1	T093 - Disponer de un inventario de riesgos identificados	R093 - RSI y RGR	E093 - Inventario de riesgos actualizado.
P1	T095 - Realizar el seguimiento periódico del inventario de riesgos identificados y documentar.	R095 - RGR	E095 - Plan e informe de revisión periódica de riesgos.
P1	T096 - Comunicar los resultados de la revisión al CSI y otras partes interesadas.	RSI	E096 - Comunicación formal de los resultados al CSI.
P1	T097 - Formalizar el resultado de la revisión de los riesgos frente al CSI y al directorio.	RSI	E097 - Informe elevado al CSI y al directorio del organismo.
P1	T098 - Establecer y realizar actividades de control interno para verificar el cumplimiento con la política establecida.	RSI	E098 - Informes de actividades de control interno.
P1	T100 - Desarrollar un inventario de riesgos identificados que incluya el impacto potencial al funcionamiento del organismo.	RSI y RGR	E100 - Inventario de riesgos documentado con clasificación cualitativa del impacto al funcionamiento del organismo.

P1	T101 - Establecer una frecuencia semestral para la revisión de riesgos, realizar la revisión y documentarla formalmente.	RSI y RGR	E101 - Plan de revisión semestral de riesgos e Informe de revisión de riesgos.
P1	T102 - Desarrollar un análisis de impacto en el negocio (BIA) inicial.	RSI	E102 - Documento de BIA en desarrollo.
P1	T103 - Identificar los procesos críticos y los sistemas de información que los soportan.	CSI	E103 - Documento de identificación de procesos críticos y sistemas de información.
P1	T104 - Disponer de un repositorio de lecciones aprendidas de los riesgos.	RSI y RGR	E104 - Documento de lecciones aprendidas sobre riesgos.
P1	T105 - Definir el BIA considerando los impactos a nivel de imagen, económico y en los usuarios.	RSI	E105 - Documento de BIA formalizado con diferentes tipos de impactos.
P1	T106 - Identificar todos los riesgos de seguridad de la información de todos los activos de información del organismo.	RSI y RGR	E106 - Documento actualizado con la identificación de riesgos para todos los activos de información.
P1	T107 - Elevar los resultados de la revisión de los riesgos al CSI, al Directorio y a las partes interesadas.	RSI	E107 - Informe sobre resultados de elevación de riesgos al CSI, al Directorio y otras partes interesadas.
P1	T108 - Utilizar la revisión periódica de riesgos y del BIA para la toma de decisiones.	Directorio	E108 - Actas o decisiones basadas en la revisión periódica de riesgos y BIA.
P1	T120 - Implementar modelos de identificación para abordar la gestión de riesgo asociado a proveedores de los activos y servicios críticos del organismo.	RGR	E120 - Modelo de identificación de riesgos implementado para proveedores.
P1	T121 - Definir métricas e indicadores para el seguimiento y control de los riesgos asociados a proveedores.	RGR	E121 - Documento que define las métricas e indicadores de control de proveedores.
P1	T123 - Establecer procedimientos formales para la gestión de riesgos con proveedores.	RSI y RGR	E123 - Procedimiento de gestión de riesgos de proveedores.
P1	T124 - Definir la periodicidad de las evaluaciones de los proveedores.	RSI y RGR	E124 - Documento que establece la periodicidad de las evaluaciones de los proveedores.
P1	T125 - Aplicar los procesos de gestión de riesgos en la adquisición de productos y servicios.	Director de TIC y RGR	E125 - Documentación de los procesos de gestión de riesgos aplicados en adquisiciones.
P1	T126 - Mantener los procesos de gestión de riesgos a lo largo de todo el ciclo de vida de los productos y servicios adquiridos.	RGR	E126 - Registros de mantenimiento de los procesos de gestión de riesgos en el ciclo de vida de productos y servicios.
P1	T127 - Evaluar a los proveedores basándose en el servicio brindado en relación con las necesidades del organismo.	Director de TIC	E127 - Informe de evaluación de proveedores en relación con las necesidades del organismo.
P1	T128 - Incorporar los resultados de las evaluaciones de proveedores en las actualizaciones de contratos y futuras adquisiciones.	Director de TIC	E128 - Contratos actualizados y documentación de futuras adquisiciones que reflejan los resultados de las evaluaciones de proveedores.
P1	T129 - Identificar a los proveedores y partes externas vinculadas al centro de datos.	Director de Infraestructura y RGR	E129 - Documento que identifica a los proveedores y partes externas del centro de datos.
P1	T130 - Priorizar los proveedores según su impacto en el organismo y su relación con los servicios críticos.	Director de TIC	E130 - Documento que muestra la priorización de proveedores críticos.
P1	T131 - Evaluar a los proveedores en el análisis de riesgos, considerando su impacto en el organismo.	Director de TIC y RGR	E131 - Informe del análisis de riesgos que incluye la evaluación de proveedores.
P1	T132 - Identificar todos los proveedores de servicios críticos del organismo.	CSI	E132 - Lista completa de proveedores de servicios críticos identificados.
P1	T133 - Priorizar a todos los proveedores según su impacto en el organismo.	Alta Dirección y RSI	E133 - Documento con la priorización de proveedores.
P1	T134 - Definir aspectos de seguridad de la información y ciberseguridad para los proveedores, incluyendo acciones permitidas y no permitidas.	Alta Dirección y RSI	E134 - Documento que define los aspectos de seguridad y ciberseguridad para los proveedores.
P1	T136 - Establecer procedimiento para la gestión de riesgos que contemple la evaluación de los proveedores críticos	RGR	E136 - Procedimiento formal para la gestión de riesgos de proveedores críticos.
P1	T137 - Integrar la evaluación de seguridad de la información y ciberseguridad en los procesos de adquisición de servicios y sistemas.	Alta Dirección y RSI	E137 - Documento que demuestra la integración de la evaluación de seguridad en los procesos de adquisición.
P1	T138 - Asegurar que el proceso de gestión de riesgos evalúe cada fase del ciclo de vida de los productos y servicios adquiridos, desde su contratación hasta su culminación.	RGR	E138 - Documentación del proceso de gestión de riesgos que evalúa todas las fases del ciclo de vida de productos y servicios adquiridos.
P1	T139 - Realizar la evaluación de riesgos en función de los cambios de entorno o la obsolescencia de los sistemas y servicios.	RGR	E139 - Registros de evaluaciones de riesgos realizadas por cambios de entorno u obsolescencia.
P1	T146 - Implementar un sistema centralizado para gestionar identidades y credenciales, al menos en forma administrativa.	Director de Desarrollo	E146 - Sistema centralizado de gestión de identidades y credenciales.
P1	T147 - Realizar revisiones reactivas de privilegios frente a cambios o bajas en los sistemas críticos.	RSI	E147 - Registros de revisiones reactivas documentadas.
P1	T148 - Definir un procedimiento formal para la revisión periódica de privilegios de acceso.	RSI y Director de Desarrollo	E148 - Procedimiento para revisión periódica de privilegios de acceso.
P1	T149 - Realizar revisiones proactivas periódicas de privilegios, incluyendo usuarios privilegiados.	RSI y Director de Desarrollo	E149 - Registros de revisiones proactivas periódicas de privilegios.
P1	T150 - Comunicar los resultados de las revisiones de privilegios de acceso a las partes interesadas.	RSI	E150 - Informes de resultados revisiones de privilegios de acceso enviados a las partes interesadas.

P1	T151 - Realizar actividades de control interno para verificar la realización y efectividad de las revisiones de privilegios.	RSI	E151 - Informes de auditorías internas sobre la revisión de privilegios.
P1	T154- Identificar los activos adicionales (más allá del centro de datos) que requieren controles físicos específicos.	CSI	E154 - Documento de identificación y clasificación de activos.
P1	T155 - Implementar controles de acceso físico en las áreas seguras asociadas a estos activos.	RSI	E155 - Configuración del sistema de control de acceso físico en las áreas seguras.
P1	T156 - Actualizar y gestionar las autorizaciones de acceso para todas las áreas seguras.	RSI	E156 - Registro actualizado de personas autorizadas para cada área segura.
P1	T158 - Definir y establecer perímetros de seguridad físicos alrededor de los activos críticos.	Director de Infraestructura	E158 - Documentación del diseño y medidas implementadas para proteger los activos críticos.
P1	T159 - Realizar revisiones reactivas de los registros de acceso en caso de incidentes.	Director de Infraestructura	E159 - Informes de revisiones reactivas documentadas.
P1	T160 - Definir y aprobar un procedimiento formal para la revisión periódica de accesos a los activos físicos.	CSI	E160 - Procedimiento formal de revisión de accesos a áreas seguras.
P1	T161 - Implementar revisiones periódicas de registros de acceso físico en las áreas seguras y para activos críticos.	CSI y RSI	E161 - Informes periódicos de revisiones de acceso físico a áreas seguras.
P1	T162 - Actualizar las políticas y procedimientos de acceso físico basados en los resultados de las revisiones.	CSI	E162 - Cambios documentados en las políticas y procedimientos en función de los hallazgos.
P1	T163 - Realizar auditorías internas para verificar el cumplimiento de los procedimientos establecidos.	RSI	E163 - Informes de auditoría interna sobre acceso físico.
P1	T171 - Implementar un procedimiento formal para el ABM de usuarios, incluyendo autorizaciones y registros de cambios.	RSI y Director de Desarrollo	E171 - Procedimiento formal de alta/baja/modificación.
P1	T172 - Establecer y realizar revisiones periódicas de los derechos de acceso y registrar los resultados.	RSI	E172 - Plan de revisiones e Informes documentados.
P1	T173 - Diseñar e implementar un procedimiento para la revisión periódica de derechos de acceso, priorizando usuarios privilegiados.	RSI y Director de TIC	E173 - Procedimiento para la revisión periódica de derechos de acceso.
P1	T174 - Comunicar formalmente el resultado de las revisiones de derechos de acceso a las divisiones y otras partes interesadas el resultado de las revisiones para toma de decisiones.	Director de TIC	E174 - Informes con el resultado de las revisiones de derechos de acceso enviados a las divisiones y otras partes interesadas para toma de decisiones.
P1	T175 - Coordinar entre RRHH y TIC para integrar procesos de altas, bajas y modificaciones de derechos de acceso.	Director de TIC y RRHH	E175 - Actas de reuniones de coordinación entre RRHH y TIC para la integración de procesos de altas, bajas y modificaciones de derechos de acceso.
P1	T179 - Notificar formalmente a usuarios con acceso a información sensible sobre las medidas de auditoría y sus responsabilidades.	RRHH	E179 - Notificaciones firmadas por los usuarios con acceso a información sensible.
P1	T180 - Implementar un registro de usuarios con acceso a información sensible.	RRHH	E180 - Registro de notificaciones de usuarios con acceso a información sensible.
P1	T181 - Verificar que los usuarios con acceso a información sensible sin notificar.	RRHH y Director de Desarrollo	E181 - Informe de revisiones de usuarios con acceso a información sensible.
P1	T182 - Diseñar e implementar procedimientos formales para la gestión del ciclo de vida de usuarios (alta, baja, modificación).	RSI y Director de Desarrollo	E182 - Procedimientos documentados de ABM de usuarios.
P1	T183 - Establecer un sistema centralizado para la gestión de permisos de usuarios nominados y genéricos.	Director de Desarrollo	E183 - Registros de gestión centralizada de usuarios y permisos.
P1	T184 - Realizar revisiones regulares del ciclo de vida de usuarios para asegurar el cumplimiento del procedimiento.	RSI	E184 - Informes de revisiones de ciclo de vida de usuarios.
P1	T192 - Implementar controles específicos para la gestión de usuarios privilegiados en sistemas y aplicaciones críticas.	Director de Desarrollo	E192 - Listado de usuarios privilegiados con permisos asignados.
P1	T193 - Establecer autenticación multifactor para accesos remotos a aplicaciones críticas.	Director de Infraestructura	E193 - Configuración de autenticación multifactor implementada y activa.
P1	T194 - Inventariar dispositivos externos utilizados para el acceso y asignar responsables.	Director de Infraestructura	E194 - Inventario actualizado de dispositivos externos.
P1	T195 - Diseñar e implementar un procedimiento formal de acceso lógico a redes, sistemas, recursos y dispositivos.	RSI	E195 - Procedimiento de acceso lógico a redes, sistemas, recursos y dispositivos documentado.
P1	T196 - Implementar controles de autenticación diferenciados según la clasificación de la información.	Director de Infraestructura	E196 - Configuración de controles según clasificación de información.
P1	T197 - Realizar análisis de riesgos asociados al acceso a la información para determinar las medidas de autenticación necesarias.	RGR y Director de TIC	E197 - Informe de análisis de riesgos asociados al acceso a la información.
P1	T198 - Aplicar el principio de menor privilegio en la asignación de permisos.	Director de Infraestructura	E198 - Registro de permisos asignados conforme al principio de menor privilegio.
P1	T199 - Definir y ejecutar procesos de revisión continua para validar la autenticación y configuración de los sistemas.	Director de Infraestructura	E199 - Informes de auditorías periódicas para validar la autenticación y configuración de los sistemas.

P1	T200 - Garantizar que los procedimientos de revisión consideran las políticas, normas y regulaciones aplicables.	RSI	E200 - Comparativa entre políticas internas y regulaciones externas.
P1	T201 - Comunicar los resultados de las revisiones y auditorías a las divisiones y partes interesadas.	RSI	E201 - Registro de envíos con los resultados de las revisiones de autenticación a las divisiones y partes interesadas.
P1	T202 - Realizar controles internos para verificar que los procedimientos definidos se cumplen.	RSI	E202 - Resultados de controles internos para verificar que los procedimientos de autenticación se cumplen.
P1	T204 - Diseñar campañas de concientización para el personal, definiendo objetivos específicos.	RSI y Comunicaciones	E204 - Documento con el diseño de la campaña, incluyendo objetivos, mensajes clave y formato de las actividades.
P1	T205 - Asignar y gestionar los recursos necesarios para la ejecución de las campañas de concientización.	Comunicaciones	E205 - Presupuesto aprobado para las campañas y registro de recursos asignados (equipo, herramientas, personal).
P1	T206 - Definir un cronograma para la realización de las campañas, detallando las fechas, actores críticos, objetivos, estrategias, tácticas y audiencia.	RSI y Comunicaciones	E206 - Cronograma aprobado con los detalles mencionados y validación del CSI.
P1	T207 - Elaborar el material educativo necesario para las campañas de concientización.	RSI y Comunicaciones	E207 - Copias de los materiales educativos creados (presentaciones, videos, infografías, guías).
P1	T208 - Definir métricas e indicadores para medir el éxito de las campañas de concientización.	RSI	E208 - Documento con las métricas e indicadores definidos, como porcentaje de asistencia, encuestas de satisfacción y resultados de evaluaciones.
P1	T209 - Realizar actividades de control interno para verificar el desarrollo de las campañas y su alineación con los objetivos establecidos.	RSI	E209 - Informes de auditoría interna que evalúen la ejecución de las campañas y cumplan con los objetivos establecidos.
P1	T210 - Diseñar y ejecutar actividades de evaluación periódicas para medir el nivel de conocimiento adquirido por el personal.	RSI y Capacitación	E210 - Resultados de las evaluaciones realizadas, con análisis de datos y comparaciones entre períodos.
P1	T211 - Presentar los resultados de las actividades de evaluación y las campañas al CSI y obtener su aprobación.	RSI	E211 - Actas del CSI con los resultados presentados y aprobaciones documentadas.
P1	T212 - Obtener el respaldo formal del Directorio para las campañas de concientización y sus actividades relacionadas.	CSI	E212 - Acta del Directorio confirmando el apoyo formal y continuo a las campañas y actividades de concientización.
P1	T215 - Diseñar e implementar un programa de concientización específico para usuarios privilegiados, estableciendo periodicidad.	RSI	E215 - Programa de concientización documentado, con periodicidad establecida y objetivos claros.
P1	T216 - Ejecutar actividades de concientización (charlas, boletines, simulaciones) para reforzar el conocimiento.	RSI y Comunicaciones	E216 - Registro de actividades realizadas (presentaciones, correos enviados, listas de asistencia).
P1	T217 - Coordinar y planificar cursos o talleres relevantes para usuarios privilegiados sobre seguridad de la información.	RSI y Capacitación	E217 - Cronograma de cursos o talleres con agendas detalladas.
P1	T218 - Evaluar el nivel de comprensión de los usuarios privilegiados al finalizar los cursos o talleres.	RSI y Capacitación	E218 - Resultados de evaluaciones a usuarios con privilegios tras los cursos o talleres.
P1	T219 - Diseñar un plan integral de capacitación y entrenamiento en seguridad de la información, segmentado por perfiles estratégicos.	RSI y Capacitación	E219 - Plan integral de capacitación con detalles de perfiles, objetivos y cronograma.
P1	T220 - Obtener la aprobación del plan por parte del Directorio y compromiso para su ejecución.	CSI	E220 - Resolución o acta de aprobación del plan de capacitación por el Directorio.
P1	T221 - Implementar el plan y realizar revisiones periódicas incorporando lecciones aprendidas.	RSI y Capacitación	E221 - Informes de revisiones periódicas y acciones de mejora implementadas para los planes de capacitación.
P1	T224 - Diseñar e implementar una iniciativa de concientización específica para interesados externos (ej., reuniones, boletines, talleres).	RSI y Capacitaciones	E224 - Plan de iniciativas de concientización para los interesados externos.
P1	T225 - Ejecutar las actividades de concientización en seguridad de la información planificadas para los interesados externos.	RSI y Capacitaciones	E225 - Registro de las actividades de concientización en seguridad de la información realizadas con los interesados externos.
P1	T226 - Implementar mecanismos de verificación para evaluar si los interesados externos comprenden sus roles y responsabilidades (ej., encuestas, entrevistas).	RSI y Director de TIC	E226 - Encuestas aplicadas o registros de entrevistas realizadas.
P1	T227 - Generar reportes que consoliden los resultados de la evaluación de comprensión de roles y responsabilidades.	RSI	E227 - Reportes con análisis de resultados de las evaluaciones realizadas a los interesados externos.
P1	T233 - Ampliar la difusión de riesgos de seguridad de la información al Directorio.	RSI	E233 - Registro de actividades de difusión realizadas al Directorio.
P1	T234 - Implementar una iniciativa de concientización dirigida específicamente a la Alta Dirección y al Directorio.	RSI	E234 - Material utilizado en las iniciativas de concientización.
P1	T235 - Planificar y ejecutar reuniones periódicas de concientización con la participación activa de la Alta Dirección.	RSI y Alta Dirección	E235 - Cronograma instancias de concientización planificadas para la Alta Dirección.
P1	T236 - Generar reportes de las reuniones y registrar los compromisos adquiridos por la Alta Dirección.	RSI y Alta Dirección	E236 - Actas de las reuniones y reportes de compromisos adquiridos por la Alta Dirección.
P1	T246 - Elaborar y mantener listas de software autorizado y prohibido.	Director de TIC	E246 - Listas de software autorizado y prohibido.
P1	T247 - Implementar y gestionar una solución centralizada de antivirus, asignando un responsable.	Director de TIC	E247 - Informe de gestión de la solución centralizada de antivirus.

P1	T249 - Configurar mecanismos de control para bloquear acceso a sitios web maliciosos o no autorizados.	Director de Infraestructura	E249 - Registro de configuración de mecanismos de control de acceso a sitios web maliciosos.
P1	T250 - Revisar y mantener actualizadas las listas de software autorizado y prohibido, asegurando su aprobación por el RSI.	Director de TIC	E250 - Listas de software revisadas y actualizadas con la aprobación del RSI.
P1	T251 - Verificar que todos los servidores cuentan con protección o detección de malware.	Director de Infraestructura	E251 - Informe de verificación del estado de protección de los servidores.
P1	T252 - Realizar controles internos sobre la solución antivirus y software instalado para verificar cumplimiento con políticas y procedimientos.	RSI y Director de TIC	E252 - Informes de control interno sobre la solución antivirus y software instalado.
P1	T253 - Documentar resultados de las revisiones y enviarlos al RSI y partes interesadas, proponiendo acciones correctivas en caso de desvíos.	Director de TIC	E253 - Registro de resultados de revisiones y propuestas de acciones correctivas.
P1	T260 - Realizar pruebas periódicas de restauración de respaldos.	Director de Infraestructura	E260 - Informes de pruebas de recuperación realizadas.
P1	T261 - Incorporar almacenamiento externo para respaldos de contingencia.	Director de Infraestructura	E261 - Informe de almacenamiento externo contratado para respaldos.
P1	T263 - Elaborar un plan de respaldos con detalle del grado y requisitos de retención.	RSI y Director de Infraestructura	E263 - Registro de ajustes realizados al procedimiento de respaldos.
P1	T264 - Actualizar el procedimiento de respaldos cuando existan cambios en la infraestructura o requerimientos del negocio.	RSI y Director de Infraestructura	E264 - Documento de alineación de la política de respaldos con el plan de contingencia y recuperación.
P1	T265 - Alinear la política y procedimiento de respaldos con el plan de contingencia y recuperación.	RSI y Director de Infraestructura	E265 - Registro de revisiones periódicas de la política de respaldos.
P1	T266 - Revisar periódicamente la política y procedimiento de respaldos.	RSI	E266 - Informes de mejora continua en los procedimientos de respaldos.
P1	T285 - Establecer cifrado obligatorio para la comunicación entre MTAs de dominios gubernamentales.	Director de Infraestructura	E285 - Reporte de cifrado obligatorio entre MTAs gubernamentales.
P1	T286 - Enviar reportes mensuales al CERTuy con estadísticas de actividad detectada en el WAF.	RSI	E286 - Informes mensuales enviados al CERTuy con estadísticas del WAF.
P1	T287 - Colaborar con el CERTuy en la centralización de registros del WAF a nivel nacional.	RSI	E287 - Documentación de colaboración con el CERTuy en la centralización de registros del WAF.
P1	T288 - Implementar automatismos para el análisis de registros del WAF que favorezcan actividades de revisión.	Director de Infraestructura	E288 - Automatismos implementados para análisis de registros del WAF.
P1	T289 - Establecer un procedimiento documentado para la preservación y gestión de registros del WAF.	RSI	E289 - Procedimiento documentado para la preservación y gestión de registros del WAF.
P1	T296 - Documentar procedimientos específicos para la gestión de infecciones por malware.	RSI y Director de Infraestructura	E296 - Procedimientos documentados para gestionar infecciones.
P1	T297 - Implementar una solución centralizada de antivirus.	Director de TIC	E297 - Informe técnico sobre la implementación de la solución centralizada de antivirus.
P1	T298 - Configurar controles técnicos para bloquear el acceso a sitios web maliciosos y no autorizados.	Director de Infraestructura	E298 - Capturas de pantalla y configuraciones de los controles técnicos implementados.
P1	T299 - Extender la protección contra malware a dispositivos móviles del organismo.	Director de Soporte	E299 - Lista de dispositivos móviles protegidos y configurados con antivirus.
P1	T300 - Documentar procedimientos para identificar y solucionar equipos desprotegidos.	RSI	E300 - Documento con los procedimientos de detección y solución de equipos desprotegidos.
P1	T301 - Crear un sistema de registro estadístico de infecciones por malware para análisis y mejora continua.	RSI y Director de Soporte	E301 - Base de datos e informe con estadísticas de infecciones y análisis de tendencias.
P1	T305 - Crear mecanismos para la respuesta a incidentes, especificando roles, responsabilidades, tiempos de respuesta, y acciones a seguir.	RSI	E305 - Documento de mecanismos de respuesta a incidentes.
P1	T306 - Crear un plan de difusión de los mecanismos de respuestas a incidentes a los interesados.	RSI y Comunicaciones	E306 - plan de difusión de los mecanismos de respuestas a incidentes.
P1	T307 - Establecer un protocolo para informar a los responsables de la toma de decisiones sobre los incidentes.	RSI	E307 - Informes enviados a los responsables sobre incidentes.
P1	T309 - Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E309 - Plan de respuesta a incidentes de seguridad de la información.
P1	T311 - Ajustes al plan de respuesta a incidentes de seguridad de la información.	RSI	E311 - Actualizaciones al plan de respuesta a incidentes de seguridad de la información.
P1	T312 - Establecer un plan de mejora de los procesos post incidentes que se reflejen en la política y los procedimientos.	RSI	E312 - Plan de mejora de los procesos post incidentes.
P1	T313 - Diseñar y documentar un procedimiento de revisión periódica de los planes y procedimientos de respuesta a incidentes.	RSI	E313 - Procedimiento de revisión periódica de los planes y procedimientos de respuesta a incidentes.
P1	T314 - Implementar un sistema de reportes periódicos de incidentes al Directorio que incluya métricas clave que apoyen la toma de decisiones.	RSI y RGI	E314 - Informes periódicos con métricas y análisis de incidentes y listado de indicadores de rendimiento (KPIs) utilizados.

P1	T315 - Generar un informe con las revisiones internas y las lecciones aprendidas para actualizar los planes y procedimientos de respuesta.	RSI	E315 - Informe con revisiones internas y lecciones aprendidas.
P2	T316 - Inventariar los equipos portátiles y móviles usados fuera de las instalaciones, junto con las aplicaciones y sistemas instalados.	Director de Soporte	E316 - Inventario actualizado de equipos portátiles y móviles.
P2	T317 - Implementar al menos un factor de autenticación para acceder a la información en los dispositivos.	Director de Infraestructura	E317 - Configuración documentada de los factores de autenticación aplicados en los dispositivos.
P2	T318 - Configurar sistemas de borrado remoto para dispositivos móviles en caso de extravío o robo.	Director de Soporte	E318 - Registro de configuraciones de borrado remoto activadas.
P2	T319 - Implementar medidas mínimas de protección física en los equipos portátiles (ejemplo: lingas de seguridad).	Director de Soporte	E319 - Documento de adquisición y distribución de medidas físicas de protección.
P2	T320 - Identificar responsables para los activos informáticos utilizados fuera de las instalaciones.	Director de Soporte	E320 - Registro de responsables asignados para cada activo informático.
P2	T321 - Limitar el almacenamiento de información sensible en los activos o aplicar controles adicionales como el cifrado.	Director de Infraestructura	E321 - Documentación sobre la limitación de almacenamiento sensible y detalle de las configuraciones de cifrado aplicadas a los activos.
P2	T323 - Establecer un programa de capacitación para usuarios que utilizan activos fuera de las instalaciones.	RSI y Capacitación	E323 - Materiales de capacitación y Lista de asistencia a las capacitaciones realizadas.
P2	T324 - Realizar controles periódicos de activos con información sensible y definir un plan de respuesta en caso de pérdida o robo.	RSI	E324 - Informes de los controles realizados y Documento del plan de respuesta ante pérdida o robo.
P2	T325 - Implementar doble factor de autenticación en los activos críticos.	Director de Infraestructura	E325 - Registro de configuración del doble factor de autenticación en activos críticos.
P2	T326 - Monitorear proactivamente 7x24 las medidas de protección implementadas en los activos informáticos.	RSI y Director de Infraestructura	E326 - Informes del monitoreo continuo (logs, alertas, reportes de actividades).
P2	T327 - Configurar sistemas de cifrado en los activos con claves únicas a nivel de organización y claves personales.	RSI y Director de Infraestructura	E327 - Registro de implementación de sistemas de cifrado y detalle de las configuraciones de clave única y personal.
P2	T328 - Identificar los activos (servidores, PC, dispositivos móviles o de almacenamiento) que contienen la información más crítica del organismo.	Director de Soporte y Director de Infraestructura	E328 - Inventario inicial de activos que contienen información crítica.
P2	T329 - Clasificar los activos según los criterios de clasificación de la información establecidos, alineados a la normativa vigente (Ley 18.381 y Ley 18.331).	RSI y Director de TIC	E329 - Clasificación de activos documentada y actualizada en el inventario de activos y procedimiento de clasificación alineado a normativa y criterios de valoración
P2	T334 - Gestionar la clasificación de la información contenida en los activos en el software de inventario.	RSI	E334 - Clasificación de la información de los activos en el software de inventario.
P2	T335 - Integrar la clasificación de la información como parte fundamental de la gestión de activos.	RSI	E335 - Procedimiento que describe la integración de la clasificación en la gestión de activos.
P2	T336 - Realizar actividades periódicas de control interno para verificar que el inventario de activos esté clasificado y actualizado, o cuando el organismo lo requiera.	RSI	E336 - Informes de los controles internos realizados y registros que muestran actualizaciones en el inventario de activos.
P2	T337 - Definir y realizar actividades de gestión de riesgo en el centro de datos basadas en la experiencia y apreciación del equipo sobre ciberseguridad.	Director de TIC	E337 - Registro de actividades de gestión de riesgo realizadas y documentos con la identificación y evaluación de riesgos específicos del centro de datos.
P2	T339 - Desarrollar una metodología unificada para la evaluación de riesgos de ciberseguridad en todo el organismo.	RGR	E339 - Metodología documentada de gestión de riesgos (identificación, evaluación, tratamiento, seguimiento y comunicación).
P2	T340 - Evaluar los riesgos de ciberseguridad en todas las áreas del organismo e incorporar actores críticos para la implementación de controles definidos.	CSI	E340 - Informes de evaluación de riesgos y lista de actores críticos y roles asignados en el proceso de implementación de controles.
P2	T342 - Centralizar los procedimientos de gestión de riesgos para analizar de forma integral los riesgos de ciberseguridad.	RGR	E342 - Procedimientos centralizados de gestión de riesgos e informes integrales de análisis de riesgos.
P2	T343 - Definir proyectos de seguridad de la información."	RSI	E343 - Listado de proyectos relacionados a la seguridad de la información.
P2	T344 - Alinear la gestión de riesgos con los objetivos del organismo, definiendo métricas e indicadores de cumplimiento organizacional.	CSI y Directorio	E344- Indicadores de seguimiento de riesgos alineados con los objetivos del organismo e informes de métricas y seguimiento del cumplimiento.
P2	T345 - Retroalimentar el proceso de gestión de riesgos mediante auditorías internas o externas para evitar desviaciones.	RSI y RGR	E345 - Informes de auditoría (interna y externa) y documentación de acciones correctivas implementadas a partir de las auditorías.
P2	T346 - Identificar y actualizar el software de base y aplicaciones críticas con los últimos parches disponibles.	Director de Infraestructura y RGV	E346 - Registro de actualizaciones realizadas en el software y aplicaciones críticas.
P2	T347 - Elaborar un inventario de activos que no pueden ser actualizados, detallando las razones y los controles compensatorios implementados."	Director de Infraestructura y RGR	E347 - Inventario de activos no actualizables con detalles de controles compensatorios.
P2	T348 - Implementar y mantener un ambiente de pruebas para verificar los parches antes de su puesta en producción.	Director de Infraestructura y RGV	E348 - Documentación del ambiente de pruebas y su configuración.
P2	T349 - Realizar pruebas de intrusión (ethical hacking) y evaluaciones de vulnerabilidades en sistemas críticos.	RSI y Consultor de Seguridad Externo	E349 - Informe de pruebas de intrusión y evaluación de vulnerabilidades.
P2	T350 - Elaborar y comunicar un informe con los resultados de las pruebas y el plan de acción a las partes interesadas.	RSI	E350 - Plan de acción y registro de comunicación con las partes interesadas.

P2	T351 - Documentar un procedimiento formal para la gestión de vulnerabilidades y parches, incluyendo los roles y responsabilidades.	RGV	E351 - Procedimiento documentado de gestión de vulnerabilidades y parches.
P2	T352 - Establecer un calendario para la realización periódica de pruebas de intrusión y escaneos de vulnerabilidades.	Director de Infraestructura y RSI	E352 - Cronograma de escaneos de vulnerabilidades y pruebas de intrusión.
P2	T353 - Realizar escaneos de vulnerabilidades semestrales y pruebas de intrusión anuales en sistemas críticos.	Director de Infraestructura y RGV	E353 - Informes de escaneos de vulnerabilidades y pruebas de intrusión.
P2	T354 - Contratar auditorías independientes periódicas para evaluar el estado de las vulnerabilidades y la efectividad de los controles implementados.	Director de TIC	E354 - Informes de auditorías independientes del estado de las vulnerabilidades.
P2	T355 - Utilizar los resultados de las auditorías para mejorar el Sistema de Gestión de Seguridad de la Información SGSI.	RSI	E355 - Registro de acciones de mejora aplicadas al SGSI.
P2	T356 - Mantenerse actualizado sobre las últimas amenazas y vulnerabilidades relacionadas con los sistemas y plataformas utilizadas en el organismo.	RSI y Director de Infraestructura	E356 - Registro de las fuentes de información consultadas regularmente.
P2	T357 - Establecer una suscripción a boletines informativos o fuentes confiables sobre ciberseguridad.	RSI y Director de Infraestructura	E357 - Lista de suscripciones activas a boletines informativos o alertas de seguridad.
P2	T358 - Organizar entrenamientos periódicos para el personal de seguridad de la información y TI sobre amenazas y vulnerabilidades.	RSI y Director de Infraestructura	E358 - Calendario de entrenamientos periódicos en seguridad al personal de TI.
P2	T359 - Identificar proveedores de formación en temas de ciberseguridad para la capacitación.	RSI y Director de Infraestructura	E359 - Lista de proveedores de formación en temas de ciberseguridad.
P2	T360 - Implementar un procedimiento de contacto con autoridades internas y externas relevantes (DCSIRT, CERTuy, CSIRT Antel, etc.).	RSI	E360 - Procedimiento de contacto con autoridades de centro de respuesta.
P2	T361 - Incorporar al personal de seguridad de la información en grupos especializados y fomentar su participación en eventos o conferencias de seguridad al menos una vez por año."	RSI y Director de TIC	E361 - Registro de participación en eventos de seguridad del RSI.
P2	T362 - Organizar reuniones periódicas entre el personal de seguridad de la información, el punto de contacto con autoridades, y el equipo de respuesta a incidentes para discutir temas actuales sobre amenazas y vulnerabilidades.	RSI y Director de TIC	E362 - Actas de reuniones periódicas del personal de seguridad con autoridades.
P2	T363 - Establecer un mecanismo de comunicación formal para compartir información relevante de manera periódica.	RSI y Director de TIC	E363 - Informes de seguridad compartidas con las partes interesadas.
P2	T364 - Identificar las principales amenazas para el organismo y definir controles para mitigarlas.	RSI	E364 - Documento que detalla los controles definidos para mitigar riesgos.
P2	T365 - Clasificar los controles implementados como físicos, lógicos o administrativos.	RSI y Director de TIC	E365 - Clasificación de los controles por tipo (físico, lógico o administrativo).
P2	T366 - Incorporar las respuestas a los riesgos en el inventario de riesgos de seguridad de la información.	RSI y RGR	E366 - Inventario de riesgos actualizado con las respuestas a los riesgos identificados.
P2	T367 - Identificar riesgos de seguridad de la información fuera del alcance del centro de datos y documentar las respuestas correspondientes.	RGR	E367 - Documentación de los riesgos fuera del alcance del centro de datos y las medidas implementadas.
P2	T368 - Revisar las respuestas a los riesgos con una frecuencia semestral.	RGR	E368 - Informes semestrales de revisión de respuestas a riesgos.
P2	T369 - Documentar formalmente las revisiones realizadas y comunicarlas al CSI y otras partes interesadas.	RSI	E369 - Registro de comunicación de las revisiones al CSI y partes interesadas.
P2	T370 - Asegurar que la implementación de controles se realice según las prioridades establecidas por el Directorio.	RSI y Directorio	E370 - Registro de prioridades formales establecidas por la Dirección.
P2	T371 - Coordinar la gestión de riesgos con el RSI, los propietarios de activos de información, y el CSI.	RSI y RGR	E371 - Actas de coordinación entre RSI, propietarios de activos y el CSI.
P2	T372 - Identificar los riesgos inherentes para los activos en el centro de datos que soportan servicios críticos.	RSI y RGR	E372 - Documento que describe los riesgos inherentes identificados, alineados a los activos del centro de datos.
P2	T373 - Realizar un análisis de impacto del negocio (BIA) enfocado en el área de TIC.	RSI y Director de TIC	E373 - Informe BIA específico para TIC que incluye identificación de umbrales de tolerancia.
P2	T374 - Establecer los umbrales de tolerancia al riesgo para los servicios tecnológicos.	CSI	E374 - Documento con los umbrales de tolerancia definidos para TIC.
P2	T375 - Ajustar los acuerdos de nivel de servicio (SLAs) con los proveedores según la gestión de riesgo definida.	Director de TIC	E375 - Contratos actualizados con SLAs ajustados a los parámetros de riesgo.
P2	T376 - Definir tolerancia al riesgo para los procesos críticos de todo el organismo.	CSI	E376 - Documento consolidado con tolerancia al riesgo para procesos críticos.
P2	T377 - Actualizar la metodología de gestión de riesgo para incluir criterios de RTO y RPO.	CSI	E377 - Metodología de gestión de riesgos con criterios de RTO y RPO.
P2	T378 - Implementar un proceso de revisión periódica de la tolerancia al riesgo.	RGR y Alta Dirección	E378 - Registros de revisiones de tolerancia al riesgo.
P2	T379 - Asegurar la aprobación de la tolerancia establecida por todas las partes interesadas.	CSI	E379 - Resolución de aprobación de la tolerancia establecida.
P2	T380 - Identificar los servicios críticos que puedan afectar a otras organizaciones interconectadas con evaluación de riesgos.	CSI y RGR	E380 - Documento que identifica servicios críticos, su interdependencia con otras organizaciones y evaluación de riesgos.

P2	T388 - Crear un inventario de proveedores, identificando su rol en la cadena de suministro de servicios críticos.	Alta Dirección	E388 - Lista de proveedores con descripción de su participación en los servicios críticos.
P2	T389 - Establecer un proceso de adquisición que incluya requisitos mínimos de seguridad de la información.	CSI	E389 - Documentación del proceso de adquisición con requisitos mínimos de seguridad.
P2	T390 - Comunicar a los proveedores su participación en los objetivos del organismo, definiendo roles y responsabilidades.	Director de TIC	E390 - Notificaciones enviadas a los proveedores con roles y responsabilidades definidos.
P2	T391 - Actualizar los contratos y SLA con los proveedores para incluir políticas y medidas de seguridad pertinentes.	RSI y Director de TIC	E391 - Contratos actualizados y acuerdos SLA con cláusulas de seguridad incluidas.
P2	T393 - Implementar un proceso para gestionar cambios de proveedores conforme a las necesidades del organismo.	RSI y Director de Desarrollo	E393 - Registros de gestión de cambios de proveedores.
P2	T394 - Realizar revisiones periódicas de los SLA y gestionar cualquier desvío detectado.	RSI y Director de Desarrollo	E394 - Registro de revisiones regulares y reportes de desvíos gestionados.
P2	T395 - Planificar y ejecutar auditorías periódicas a los proveedores para evaluar su cumplimiento con los SLA y las políticas de seguridad.	RSI y Director de Desarrollo	E395 - Informes de auditoría de proveedores.
P2	T396 - Ajustar los servicios de los proveedores en función de los resultados de las auditorías y las necesidades del organismo.	Director de TIC	E396 - Documentación de ajustes realizados a los servicios de los proveedores.
P2	T397 - Diseñar e implementar un proceso de evaluación del desempeño de proveedores críticos basado en los contratos establecidos.	CSI	E397 - Documento del proceso de evaluación de proveedores y registros de evaluaciones realizadas.
P2	T398 - Establecer un calendario de reuniones periódicas con proveedores para evaluar su desempeño.	RSI y Director de TIC	E398 - Agenda de reuniones periódicas y actas de reuniones realizadas.
P2	T399 - Registrar desvíos identificados en el desempeño de los proveedores y proponer acciones correctivas.	RSI y Director de TIC	E399 - Reporte de desvíos y plan de acciones correctivas con seguimiento.
P2	T400 - Actualizar la política de seguridad de la información para incluir auditorías externas independientes a proveedores críticos.	CSI	E400 - Ajustes en Política de seguridad de la información para incluir auditorías externas.
P2	T401 - Implementar auditorías externas a proveedores críticos, identificando desvíos y generando planes de acción correctivos.	RSI	E401 - Informes de auditoría externa y planes de acción correctivos priorizados.
P2	T402 - Priorizar y asignar plazos a las acciones correctivas, alineados a las necesidades del organismo.	RGR	E402 - Registro de acciones correctivas priorizadas con plazos definidos.
P2	T403 - Establecer un cronograma regular de auditorías externas basado en el apetito de riesgo.	CSI	E403 - Cronograma de auditorías aprobado y cumplido.
P2	T404 - Implementar un sistema de monitoreo permanente de servicios críticos de los proveedores.	Director de TIC	E404 - Reportes periódicos generados por el sistema de monitoreo.
P2	T405 - Revisar la efectividad de los planes de acción correctivos y ajustar los SLA conforme a los resultados y necesidades del organismo.	RSI y RGR	E405 - Informes de seguimiento de planes de acción y documentación de ajustes realizados a los SLA.
P2	T406 - Implementar comunicaciones seguras para el acceso remoto (por ejemplo, VPN con cifrado).	Director de Infraestructura	E406 - Configuración activa de comunicaciones seguras para acceso remoto.
P2	T407 - Establecer mecanismos de autenticación seguros para el acceso remoto.	Director TIC	E407 - Documentación de los mecanismos de autenticación utilizados para el acceso remoto.
P2	T408 - Implementar acuerdos de no divulgación para el personal y proveedores con acceso remoto.	Director TIC y RRHH	E408 - Acuerdos de no divulgación firmados para personal y proveedores con acceso remoto.
P2	T409 - Crear y mantener una lista blanca de recursos disponibles para acceso remoto.	Director TIC	E409 - Listado actualizado de recursos autorizados para acceso remoto.
P2	T410 - Revisar periódicamente los acuerdos de no divulgación para garantizar su vigencia y adecuación.	RSI	E410 - Evidencia de revisiones realizadas de acuerdos de no divulgación.
P2	T411 - Documentar y publicar un procedimiento formal para solicitar acceso remoto.	RSI	E411 - Procedimiento documentado y aprobado para solicitar acceso remoto.
P2	T412 - Designar un responsable para la gestión y asignación de permisos de acceso remoto.	Director de TIC	E412 - Registro del responsable asignado para gestión de acceso remoto y de sus actividades.
P2	T413 - Configurar permisos temporales para proveedores con acceso remoto.	Director de Infraestructura	E413 - Registro de accesos remoto temporales otorgados y su vencimiento.
P2	T414 - Implementar doble factor de autenticación para el acceso remoto.	Director de Infraestructura	E414 - Configuración activa de doble factor de autenticación.
P2	T415 - Centralizar la gestión del acceso remoto, al menos desde el punto de vista administrativo.	Director de TIC	E415 - Documentación que detalle la centralización del acceso remoto.
P2	T416 - Establecer y ejecutar revisiones periódicas de los usuarios con acceso remoto y sus registros de actividad.	Director de Infraestructura	E416 - Informes de revisiones periódicas realizadas de acceso remoto y registro de actividad.
P2	T417 - Definir actividades de control para verificar el cumplimiento de los procedimientos de acceso remoto.	RSI	E417 - Resultados documentados de controles internos para verificar el cumplimiento de los procedimientos de acceso remoto.
P2	T418 - Segmentar la red en al menos dos dominios básicos: red privada y red externa.	Director de Infraestructura	E418 - Configuración activa que demuestre la segmentación de red básica.

P2	T419 - Actualizar y mantener un diagrama de red detallado que refleje la segmentación existente.	Director de Infraestructura	E419 - Diagrama actualizado de la red que refleje la segmentación de red.
P2	T420 - Identificar y documentar los dominios de red según las necesidades del organismo (por ejemplo, redes de usuarios, redes de servidores, redes críticas).	Director de Infraestructura	E420 - Documento que detalle los dominios de red definidos.
P2	T421 - Definir e implementar reglas de manejo de tráfico entre segmentos (permitir, denegar, registrar).	Director de Infraestructura	E421 - Configuraciones de manejo de tráfico documentadas.
P2	T422 - Alinear el organigrama y roles del organismo con la segregación de redes, destacando las funciones críticas.	RSI y Director de Infraestructura	E422 - Organigrama actualizado con funciones relacionadas con la segmentación de red.
P2	T423 - Configurar monitoreo del tráfico en los diferentes dominios de red para análisis continuo.	Director de Infraestructura	E423 - Registros de tráfico analizados periódicamente.
P2	T424 - Implementar controles de detección de amenazas en los diferentes segmentos de red.	Director de Infraestructura	E424 - Configuración activa de controles de detección de amenazas.
P2	T425 - Definir y configurar alertas automáticas cuando se detecte tráfico no autorizado.	Director de Infraestructura	E425 - Logs y configuraciones de alertas generadas de tráfico no autorizado.
P2	T426 - Documentar un procedimiento de contención de incidentes en los segmentos de red.	RGI y Director de Infraestructura	E426 - Procedimiento aprobado de contención de incidentes en segmentos de red.
P2	T427 - Establecer un procedimiento formal de monitoreo continuo de los segmentos de red, apoyado por herramientas automatizadas.	Director de Infraestructura	E427 - Procedimiento formalizado y configuraciones de herramientas automatizadas para monitoreo de red.
P2	T428 - Alinear el procedimiento de contención de incidentes con la política general de gestión de incidentes.	RGI	E428 - Procedimiento de contención de incidentes de red con la política general de gestión de incidentes.
P2	T429 - Registrar incidentes detectados en los segmentos de red y documentar lecciones aprendidas.	RGI y Director de Infraestructura	E429 - Base de datos de incidentes en los segmentos de red y reportes de mejora continua.
P2	T430 - Realizar controles internos para garantizar que las revisiones y contenciones de incidentes se realicen según lo planificado.	RGI y Director de Infraestructura	E430 - Informes de auditoría y cumplimiento de controles internos de segmentos de red.
P2	T431 - Identificar y clasificar los datos históricos y respaldos críticos para el organismo.	Director de Infraestructura	E431 - Listado de datos históricos y respaldos clasificados como críticos.
P2	T432 - Implementar mecanismos básicos de control de acceso físico y lógico para proteger los respaldos.	Director de Infraestructura	E432 - Registros de acceso físico (bitácoras) y configuraciones de acceso lógico.
P2	T433 - Implementar cifrado para el almacenamiento de datos históricos y respaldos offline.	Director de Infraestructura	E433 - Configuración de las soluciones de respaldo que incluye cifrado y listado de respaldos cifrados.
P2	T434 - Verificar la implementación del cifrado mediante una prueba de restauración de datos cifrados.	Director de Infraestructura	E434 - Informe de prueba de restauración exitosas de datos cifrados.
P2	T436 - Crear procedimientos para la gestión de claves criptográficas para respaldos.	RSI y Director de Infraestructura	E436 - Procedimiento para la gestión de claves criptográficas para respaldos.
P2	T437 - Designar responsables en cada etapa del ciclo de vida de las claves criptográficas para respaldos.	RSI y Director de Infraestructura	E437 - Lista de responsables designados en la gestión de las claves criptográficas para respaldos.
P2	T438 - Planificar y ejecutar revisiones periódicas sobre los respaldos y datos históricos almacenados.	RSI y Director de Infraestructura	E438 - Cronograma de revisiones sobre los respaldos y datos históricos.
P2	T439 - Registrar los resultados de las revisiones, incluyendo hallazgos y acciones correctivas en caso de incumplimientos.	Director de Infraestructura	E439 - Registros de resultados de revisiones sobre los respaldos y plan de acciones correctivas en caso de desvíos.
P2	T440 - Informar los resultados de las revisiones al RSI.	Director de Infraestructura	E440 - Reportes de revisiones sobre respaldos enviados al RSI.
P2	T441 - Implementar controles básicos de cifrado en la transferencia de datos (como el uso de HTTPS, SFTP o VPN seguras).	Director de Infraestructura	E441 - Configuraciones de sistemas y redes que implementan cifrado, registro del uso de HTTPS/SFTP/VPN.
P2	T442 - Configurar reglas de seguridad en los sistemas de correo electrónico para proteger la información transmitida.	Director de Infraestructura	E442 - Detalle técnico de la configuración del correo electrónico.
P2	T443 - Estandarizar las tecnologías y prácticas criptográficas para proteger los datos en tránsito en todas las aplicaciones y sistemas.	Director de Infraestructura	E443 - Detalle del uso de criptografía estandarizada, listado de aplicaciones/sistemas protegidos.
P2	T444 - Actualizar los procedimientos internos para reflejar las tecnologías y prácticas estándar adoptadas.	RSI y Director de Infraestructura	E444 - Procedimientos actualizados que describan el uso estandarizado de criptografía.
P2	T446 - Crear procedimientos para la gestión de claves criptográficas de la información en tránsito.	RSI y Director de Infraestructura	E446 - Procedimiento para la gestión de claves criptográficas para la información en tránsito.
P2	T447 - Designar responsables en cada etapa del ciclo de vida de las claves criptográficas para la información en tránsito.	RSI y Director de Infraestructura	E447 - Lista de responsables designados en la gestión de las claves criptográficas para la información en tránsito.
P2	T448 - Planificar y ejecutar revisiones periódicas de los controles criptográficos implementados para proteger datos en tránsito.	RSI y Director de Infraestructura	E448 - Cronograma de controles criptográficos e informes de resultados de revisiones.

P2	T449 - Registrar los hallazgos de las revisiones, incluyendo los desvíos y las acciones correctivas necesarias.	Director de Infraestructura	E449 - Registros de hallazgos en controles criptográficos y planes de acción correctiva.
P2	T450 - Informar los resultados de controles criptográficos al RSI.	Director de Infraestructura	E450 - Reportes de resultados de controles criptográficos enviados al RSI.
P2	T461 - Establecer pautas iniciales para la eliminación y borrado seguro de medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E461 - Documento con pautas iniciales sobre borrado seguro de medios de almacenamiento.
P2	T462 - Informar al personal sobre la importancia de la eliminación segura de medios para proteger la confidencialidad de la información.	Director de Soporte y Director de Infraestructura	E462 - Listado de asistentes a capacitación sobre la importancia de la eliminación segura de medios de almacenamiento.
P2	T463 - Establecer puntos designados para la disposición y eliminación de medios de almacenamiento.	RSI y Director de Infraestructura	E463 - Listado de puntos designados para la eliminación de medios de almacenamiento.
P2	T464 - Implementar actividades coordinadas para el borrado seguro o disposición de los medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E464 - Registros de actividades realizadas sobre borrado seguro de medios de almacenamiento.
P2	T466 - Elaborar un procedimiento para la eliminación segura de medios de almacenamiento alineado con la política.	Director de Soporte y Director de Infraestructura	E466 - Procedimiento sobre eliminación segura de medios de almacenamiento.
P2	T467 - Capacitar al personal involucrado en la aplicación del procedimiento para eliminación segura de medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E467 - Capacitaciones de procedimiento sobre eliminación segura de medios de almacenamiento.
P2	T468 - Realizar auditorías internas periódicas para verificar el cumplimiento de los procedimientos de eliminación de medios y los puntos de disposición definidos.	RSI	E468 - Informes de auditorías realizadas para el cumplimiento de los procedimientos sobre eliminación segura de medios de almacenamiento.
P2	T469 - Registrar desvíos identificados en las auditorías y definir acciones correctivas.	RSI	E469 - Registro de desvíos detectados en la eliminación segura de medios de almacenamiento y planes de acción correctiva documentados.
P2	T470 - Informar los resultados de las auditorías y acciones correctivas al RSI.	RSI	E470 - Reportes de desvíos detectados en eliminación segura de medios de almacenamiento enviados al RSI.
P2	T471 - Implementar acuerdos de no divulgación básicos para nuevos proveedores y personal.	Director de Legales y RRHH	E471 - Plantillas de Acuerdos de no divulgación para personal y proveedores.
P2	T472 - Garantizar la firma de los acuerdos como parte del proceso de incorporación.	RRHH	E472 - Lista de personal con Acuerdos de no divulgación firmados.
P2	T473 - Identificar y categorizar el personal que no han firmado acuerdos de no divulgación.	RRHH	E473 - Listado completo de personal que no tenga firmado Acuerdos no divulgación.
P2	T474 - Identificar y categorizar los proveedores que no han firmado acuerdos de no divulgación.	Director de TIC	E474 - Listado completo de proveedores que no tenga firmado Acuerdos no divulgación.
P2	T475 - Plan para que el personal que no cuenta con Acuerdos de no divulgación firmado lo firme.	RRHH	E475 - Cronograma de implementación del plan para que el personal firme el Acuerdo de no divulgación.
P2	T476 - Plan para que los proveedores que no cuenta con Acuerdos de no divulgación firmado lo firmen.	Director de TIC	E476 - Cronograma de implementación del plan para que los proveedores firmen el Acuerdo de no divulgación.
P2	T477 - Realizar campañas de concientización sobre la importancia de los Acuerdos de no divulgación .	RSI y Capacitación	E477 - Materiales de comunicación utilizados. Registros de participación en sesiones informativas.
P2	T478 - Actualizar acuerdos contractuales para reflejar responsabilidades según roles específicos.	RRHH y Director de Legales	E478 - Nuevos modelos de contratos que incluyan responsabilidades de seguridad para roles críticos.
P2	T479 - Documentar un procedimiento de desvinculación robusto.	RRHH y Director de Legales	E479 - Procedimiento documentado que incluya revocación de accesos físicos y lógicos.
P2	T480 - Implementar un sistema DLP (Data Loss Prevention) para proteger los datos sensibles.	Director de TIC	E480 - Detalles técnicos del sistema DLP (Data Loss Prevention) implementado.
P2	T481 - Establecer un cronograma de revisión periódica de contratos y procedimientos de desvinculación.	Director de TIC	E481 - Cronograma de revisiones de procedimientos de desvinculación.
P2	T482 - Implementar un sistema de registro para monitorear y reportar desvíos e incumplimientos.	RSI	E482 - Registros de desvíos detectados en procedimientos de desvinculación y acciones correctivas implementadas.
P2	T483 - Incorporar resultados de revisiones en planes de mejora continua.	RSI y Director de TIC	E483 - Documentación de mejoras en procedimientos de procedimientos de desvinculación.
P2	T484 - Reportar hallazgos y resultados de revisiones a partes interesadas.	RSI	E484 - Reportes enviados a las áreas interesadas sobre procedimientos de desvinculación.
P2	T485 - Verificar la separación de los entornos de producción y no producción.	Director de Infraestructura	E485 - Documentación de los ambientes existentes (diagramas de arquitectura, descripción de la infraestructura).
P2	T486 - Confirmar que los entornos de producción solo se utilizan para aplicaciones críticas.	Director de Infraestructura	E486 - Listado de sistemas en producción y aplicaciones críticas.

P2	T487 - Definir plataformas separadas para cada fase del ciclo de vida de desarrollo.	Director de Infraestructura	E487 - Documentación de las plataformas de desarrollo, pruebas y producción, detallando sus características.
P2	T488 - Establecer controles para la transición entre ambientes (desarrollo, pruebas, producción).	Director de Infraestructura y Director de Desarrollo	E488 - Procedimiento para el pasaje a producción y listado de solicitudes de cambio aprobadas con su impacto en los ambientes.
P2	T489 - Implementar un procedimiento de pruebas para asegurar el control del ciclo de vida de los entornos.	Director de Desarrollo	E489 - Procedimiento o metodología de pruebas y registro de cambios realizados.
P2	T491 - Crear un procedimiento documentado para la gestión de los entornos y los pasajes entre ellos.	Director de Desarrollo	E491 - Procedimientos para el pasaje a producción.
P2	T492 - Designar responsables para la gestión de entornos y pasajes a producción.	Director de Desarrollo	E492 - Documento de asignación de responsabilidades y funciones.
P2	T493 - Mantener la información registrada durante las pruebas para asegurar la calidad y replicabilidad.	Director de Desarrollo	E493 - Registro de información de los entornos de pruebas.
P2	T494 - Involucrar a los responsables de la gestión de entornos en la planificación y ejecución de los proyectos desde el inicio.	Director de TIC	E494 - Actas de reuniones de planificación de proyectos donde se documenta la participación de los responsables de entornos.
P2	T495 - Asegurar que la clasificación de la información se maneje adecuadamente durante las pruebas.	RSI y Director de Desarrollo	E495 - Documentación sobre la clasificación y manejo de la información durante las pruebas de separación de entorno.
P2	T496 - Implementar auditorías de cumplimiento sobre la política de separación de entornos y procedimientos relacionados.	RSI	E496 - Informes de auditoría interna sobre cumplimiento de la política de separación de entornos.
P2	T497 - Reportes de seguimiento de la implementación de acciones correctivas para el cumplimiento sobre la política de separación de entornos.	RSI y Director de Desarrollo	E497 - Registro de acciones correctivas derivadas de auditorías sobre cumplimiento de la política de separación de entornos.
P2	T498 - Definir lineamientos generales de desarrollo seguro.	RSI y Director de Desarrollo	E498 - Pautas iniciales de desarrollo seguro.
P2	T499 - Establecer un proceso básico de gestión de proyectos con principios de seguridad.	RSI y Director de Desarrollo	E499 - Documentación de la metodología básica de gestión de proyectos.
P2	T500 - Involucrar a los usuarios en el ciclo de vida de los sistemas, ya sea directamente o a través de un rol representante.	Alta dirección	E500 - Actas o registros de la participación de usuarios en proyectos específicos.
P2	T501 - Incorporar requisitos de seguridad en la especificación de los proyectos.	RSI y Director de Desarrollo	E501 - Metodología de desarrollo que contemple seguridad y evidencia de su revisión periódica.
P2	T502 - Establecer principios de desarrollo seguro en los sistemas.	RSI y Director de Desarrollo	E502 - Listado de proyectos y aplicaciones desarrolladas o adquiridas.
P2	T503 - Implementar un sistema de control de versiones para el software.	Director de Desarrollo	E503 - Muestras de versionado de archivos.
P2	T504 - Sistematizar las actividades de prueba en el desarrollo.	Director de Desarrollo	E504 - Listado de actividades sistematizadas de pruebas de desarrollo.
P2	T505 - Definir un procedimiento documentado de pruebas que involucre a los usuarios.	Director TIC	E505 - Procedimiento documentado de pruebas.
P2	T506 - Establecer criterios de aceptación para los productos desarrollados o adquiridos.	Director TIC	E506 - Criterios de aceptación definidos para proyectos seleccionados.
P2	T507 - Realizar actividades de control interno para evaluar el cumplimiento de la metodología y los procedimientos definidos.	Director de Desarrollo	E507 - Informes de auditorías internas sobre cumplimiento de metodología y procedimientos de desarrollo.
P2	T508 - Implementar acciones correctivas frente a desvíos identificados en la metodología de desarrollo.	Director de Desarrollo	E508 - Registro de acciones correctivas implementadas para cumplimiento de la metodología y los procedimientos en el desarrollo.
P2	T509 - Comunicar los resultados de las evaluaciones de cumplimiento de la metodología y los procedimientos al RSI.	Director de Desarrollo	E509 - Comunicación al RSI los resultados de las evaluaciones de cumplimiento de la metodología y los procedimientos en el desarrollo.
P2	T510 - Establecer medidas básicas para comunicar y autorizar los cambios en el ámbito tecnológico.	RSI y Director de Desarrollo	E510 - Documentos o registros de comunicación y autorización de cambios.
P2	T511 - Asegurar que los cambios sean registrados y documentados de manera general.	Director de Desarrollo	E511 - Listado inicial de cambios realizados durante el período.
P2	T512 - Definir procesos formales de versionado para los productos de software.	Director de Desarrollo	E512 - Procedimiento formal para el versionado.
P2	T513 - Establecer líneas base de configuración para permitir la trazabilidad de los cambios.	Director de Desarrollo y RSI	E513 - Registros de líneas base de configuración y trazabilidad de cambios. Herramientas utilizadas para el control de versiones.
P2	T515 - Definir un procedimiento de gestión de cambios y asegurar su implementación.	RSI y Director de Desarrollo	E515 - Listado (muestra) de cambios en el período auditado y listado de cambios de emergencia.
P2	T516 - Registrar todos los cambios realizados a las líneas base.	Director de Desarrollo	E516 - Evidencia de análisis de riesgos, autorización, aprobación y registro de cambios.
P2	T517 - Implementar herramientas automatizadas que apoyen la gestión de los cambios.	Director de Desarrollo	E517 - Herramientas utilizadas para la gestión de cambios.
P2	T518 - Realizar actividades de control interno para revisar el cumplimiento de los procedimientos de gestión de cambios.	Director de Desarrollo	E518 - Resultados de revisiones internas sobre cumplimiento de procedimientos.
P2	T519 - Comunicar los resultados de las revisiones al RSI y partes interesadas.	Director de Desarrollo	E519 - Comunicaciones dirigidas al RSI y partes interesadas.

P2	T520 - Tomar medidas correctivas frente a desvíos y utilizar los resultados para mejora continua.	RSI y Director de Desarrollo	E520 - Registro de acciones correctivas y lecciones aprendidas.
P2	T521 - Implementar medidas básicas de control del medio ambiente físico en los centros de datos y áreas relacionadas.	Director de Infraestructura.	E521 - Habilitación de bomberos, cContratos con proveedores (alarmas, aire acondicionado, etc.).
P2	T522 - Asegurar que las áreas críticas cuenten con protecciones ambientales mínimas (alarmas, extintores, aire acondicionado, etc.).	Director de Infraestructura.	E522 - Protección ambiental (alarma, extintores, sistemas de extinción, aire acondicionado, etc.), ubicación de la sala de cómputo y la sala de energía.
P2	T523 - Implementar herramientas automatizadas para el monitoreo de los controles relacionados al medio ambiente físico.	Director de Infraestructura	E523 - Herramientas utilizadas para el monitoreo. Procedimiento de monitoreo.
P2	T524 - Asegurar que las herramientas permitan la detección de fallas en componentes críticos.	Director de Infraestructura	E524 - Plan de mantenimiento de componentes críticos. Reportes de fallas y alertas dentro del período auditado.
P2	T526 - Desarrollar un procedimiento de monitoreo que contemple el uso de herramientas automatizadas.	Director de Infraestructura y RM	E526 - Procedimiento de monitoreo que contemple herramientas automatizadas.
P2	T527 - Implementar controles de cambio para las actividades de mantenimiento en componentes críticos.	Director de Infraestructura	E527 - Registro del mantenimiento histórico de los valores monitoreados dentro del período auditado. Documentación de controles de cambio relacionados con el mantenimiento.
P2	T528 - Realizar actividades de control interno para verificar el cumplimiento de la política de seguridad del equipamiento y procedimientos de monitoreo.	RSI y Director de Infraestructura	E528 - Evidencia de revisión de fallas y alertas dentro del período auditado.
P2	T529 - Analizar los resultados del monitoreo para mejorar los procedimientos y retroalimentar con lecciones aprendidas.	RSI y Director de Infraestructura	E529 - Acciones correctivas implementadas basadas en resultados del monitoreo y registro de lecciones aprendidas para mejora continua.
P2	T530 - Establecer procesos para reportar los resultados a las partes interesadas.	RSI	E530 - Reportes de resultados de monitoreo enviados a partes interesadas.
P2	T541 - Instruir al personal sobre los mecanismos de reporte de incidentes.	RSI y Capacitación	E541 - Registros de capacitaciones sobre mecanismos de reporte de incidentes.
P2	T542 - Establecer lineamientos para el reporte interno de incidentes.	RSI y RGI	E542 - Documentación de lineamientos para el reporte interno de incidentes.
P2	T543 - Registrar los incidentes de seguridad reportados.	RGI	E543 - Listado de incidentes reportados y registrados.
P2	T544 - Implementar medidas básicas de contingencia y recuperación para sistemas que soportan servicios críticos.	RGI y Director de Infraestructura	E544 - Documentación de medidas básicas de contingencia y recuperación para servicios críticos.
P2	T545 - Identificar los procesos críticos del organismo.	RSI	E545 - Listado de procesos críticos del organismo.
P2	T546 - Establecer herramientas básicas para apoyar la gestión de incidentes.	Director de TIC	E546 - Herramientas implementadas para la gestión de incidentes.
P2	T547 - Implementar medidas adicionales de contingencia y recuperación.	RSI	E547 - Documentación de medidas de contingencia adicionales.
P2	T550 - Diseñar un plan de contingencia y de recuperación para los sistemas críticos.	RSI y Director de Infraestructura	E550 - Plan de contingencia y recuperación documentado.
P2	T551 - Realizar pruebas puntuales de los planes diseñados.	RSI	E551 - Resultados de las pruebas puntuales realizadas.
P2	T552 - Designar responsables específicos para la respuesta a incidentes y el mantenimiento de los planes de contingencia y recuperación.	CSI	E552 - Listado de responsables designados para la respuesta a incidentes y el mantenimiento de los planes de contingencia y recuperación.
P2	T553 - Realizar pruebas anuales de los planes de respuesta, contingencia y recuperación.	RSI y Director de TIC	E553 - Registros de pruebas anuales de los planes de respuesta, contingencia y recuperación.
P2	T554 - Llevar a cabo actividades de control interno para verificar el cumplimiento de políticas y procedimientos relacionados.	RSI y Director de TIC	E554 - Registro de actividades de control interno para verificar el cumplimiento de políticas y procedimientos relacionados.
P2	T555 - Informar los resultados de los controles y tomar acciones correctivas frente a desvíos.	RSI	E555 - Informes de controles internos realizados y acciones correctivas aplicadas.
P2	T556 - Documentar lecciones aprendidas y ajustar los procedimientos de manera continua.	RSI	E556 - Documentación de lecciones aprendidas y mejoras a los procedimientos.
P2	T571 - Implementar la gestión de parches como medida para abordar vulnerabilidades técnicas.	Director de Infraestructura	E571 - Registro de vulnerabilidades y parches gestionados.
P2	T572 - Mantener un registro de los parches aplicados y las vulnerabilidades gestionadas.	RGV	E572 - Comparativa entre las actualizaciones críticas requeridas y las realmente realizadas.
P2	T573 - Definir y documentar un plan para la gestión de vulnerabilidades y parches.	RGV	E571 - Plan documentado de gestión de vulnerabilidades y parches.
P2	T574 - Establecer mecanismos para recibir notificaciones de vulnerabilidades desde fuentes externas, como el CERTuy u otras organizaciones y analizar las notificaciones de vulnerabilidades recibidas y priorizar su tratamiento.	RGV	E572 - Registro de notificaciones de vulnerabilidades recibidas y análisis realizado.
P2	T575 - Establecer responsabilidades claras para la gestión de vulnerabilidades.	RSI	E575 - Registro de responsables de la gestión de vulnerabilidades.
P2	T576 - Incorporar escaneos de infraestructura y aplicaciones como fuentes de notificación de vulnerabilidades.	RGV	E576 - Escaneos de infraestructura y aplicaciones con vulnerabilidades detectadas.
P2	T577 - Implementar un ambiente para pruebas de parches antes de su puesta en producción y documentar los resultados de las pruebas de parches realizadas en el ambiente de pruebas.	RGV y Director de Infraestructura	E577 - Registro de pruebas realizadas en el ambiente de pruebas.

P2	T578 - Realizar revisiones de control interno sobre el plan de gestión de vulnerabilidades y comunicar los resultados de las revisiones al RSI.	RSI y RGV	E578 - Informes de revisiones de control interno realizadas.
P2	T579 - Documentar las lecciones aprendidas para mejorar la gestión de vulnerabilidades en futuras resoluciones.	RGV	E579 - Registros de lecciones aprendidas y su aplicación.
P2	T580 - Implementar mejoras al plan y procedimientos de gestión de vulnerabilidades con base en las lecciones aprendidas y revisiones internas.	RGV	E580 - Plan actualizado con mejoras basadas en las revisiones.
P2	T581 - Configurar los registros de auditoría para todos los sistemas críticos definidos.	RSI y Director de TIC	E581 - Configuración documentada de los registros en sistemas críticos.
P2	T582 - Utilizar los registros únicamente para tratar situaciones puntuales.	RSI y Director de TIC	E582 - Evidencia del uso de registros en situaciones específicas.
P2	T583 - Crear repositorio de auditoría para todos los registros de auditoría.	Director de Infraestructura	E583 - Repositorio de registros de auditoría.
P2	T584 - Proteger el repositorio de auditoría contra accesos no autorizados y alteraciones.	Director de Infraestructura	E584 - Registro de medidas de seguridad aplicadas.
P2	T585 - Definir rutinas para centralizar todos los registros de auditoría.	Director de Infraestructura	E585 - Listado de rutinas para centralización de registros de auditoría.
P2	T586 - Garantizar la confidencialidad y privacidad de los datos en los registros.	RSI	E586 - Evidencia de configuraciones que protejan la privacidad.
P2	T588 - Respalidar los registros de auditoría y revisar periódicamente los registros con herramientas automatizadas.	Director de Infraestructura	E588 - Evidencia de respaldos de registros de auditoría y revisiones periódicas con herramientas automatizadas.
P2	T589 - Sincronizar los relojes de todos los sistemas críticos.	Director de Infraestructura	E589 - Registro de sincronización de relojes en sistemas críticos.
P2	T590 - Establecer requisitos de retención de registros según normativa y políticas internas.	RSI	E590 - Documento que define los requisitos de retención.
P2	T591 - Implementar herramientas avanzadas para el análisis de grandes volúmenes de datos.	Director de Infraestructura	E591 - Configuración y evidencia del uso de herramientas de análisis.
P2	T592 - Crear mecanismos específicos para revisar las actividades de administradores de sistemas.	Director de Infraestructura	E592 - Informes de revisión de actividades de administradores.
P2	T593 - Realizar controles internos para verificar el cumplimiento de la política y procedimientos de auditoría.	Director de Infraestructura	E593 - Resultados de controles internos documentados.
P2	T594 - Comunicar los resultados de las revisiones al RSI y partes interesadas.	Director de Infraestructura	E594 - Evidencia de comunicación de resultados (ejemplo: correos o informes enviados).
P2	T595 - Configurar mecanismos básicos para registrar eventos de sistemas y redes críticos.	Director de Infraestructura	E595 - Configuración de registros de eventos de sistemas y redes.
P2	T596 - Establecer un procedimiento inicial para analizar eventos irregulares puntuales y contactar al CERTuy o CSIRT.	RSI	E596 - Listado de eventos irregulares analizados y registro de interacciones con CERTuy o CSIRT.
P2	T597 - Adquirir e implementar herramientas automatizadas para monitorear eventos, excepciones y fallas.	RM	E597 - Configuración y logs de herramientas automatizadas.
P2	T598 - Configurar y utilizar WAF en sitios web vinculados a trámites en línea.	Director de Infraestructura	E598 - Configuración del WAF implementado.
P2	T599 - Definir procedimientos para la revisión de eventos y uso de herramientas automatizadas.	RSI	E599 - Procedimientos documentados para la revisión de eventos y configuración del WAF.
P2	T601 - Establecer procedimientos para la revisión y gestión de eventos en sistemas y redes y uso de WAF.	RSI y Director de Infraestructura	E601 - Procedimientos documentados de revisión y gestión de eventos y uso de WAF.
P2	T602 - Alinear los procedimientos de gestión de eventos con los de gestión de incidentes.	RSI y RGI	E602 - Listado de eventos gestionados según los procedimientos.
P2	T603 - Establecer una periodicidad formal para la revisión de eventos y actividad anormal.	RSI	E603 - Informe de revisiones periódicas de eventos.
P2	T604 - Diseñar mecanismos para analizar patrones de ataque y documentar lecciones aprendidas.	RSI y Director de Infraestructura	E604 - Informe de análisis de patrones de ataque.
P2	T605 - Generar informes periódicos de revisiones y compartirlos con las partes interesadas.	Director de Infraestructura	E605 - Registro de reuniones y comunicaciones con partes interesadas.
P2	T606 - Implementar controles internos para evaluar el cumplimiento de los procedimientos y políticas.	RSI y Director de Infraestructura	E606 - Resultados de controles internos realizados.
P2	T607 - Identificar los sistemas y servicios más críticos.	CSI	E607 - Listado de sistemas y servicios críticos.
P2	T608 - Establecer un procedimiento básico para realizar monitoreos reactivos o esporádicos.	RM	E608 - Registro de monitoreos realizados de manera reactiva.
P2	T609 - Documentar los resultados de los monitoreos realizados y las acciones correctivas.	RM	E609 - Informe de acciones correctivas aplicadas.
P2	T610 - Implementar herramientas de monitoreo automatizadas para los activos críticos.	RM y Director de Infraestructura	E610 - Configuración de herramientas de monitoreo automatizadas.

P2	T611 - Configurar las alertas en las herramientas de monitoreo.	RM y Director de Infraestructura	E611 - Registro de alertas generadas.
P2	T612 - Documentar un procedimiento para el monitoreo automatizado y la gestión de alertas.	RM	E612 - Procedimiento documentado para el monitoreo automatizado.
P2	T613 - Ajustar las herramientas de monitoreo para identificar patrones de anomalías.	RM y Director de Infraestructura	E613 - Configuración avanzada de herramientas de monitoreo para patrones de anomalías.
P2	T614 - Establecer un procedimiento para la revisión y análisis de anomalías detectadas.	Director de Infraestructura	E614 - Procedimiento documentado para la revisión de anomalías.
P2	T615 - Ampliar el monitoreo a todos los activos de información del centro de datos.	RM y Director de Infraestructura	E615 - Registro del monitoreo de todos los activos de información.
P2	T616 - Implementar un sistema que permita cruzar información de diversas fuentes para generar alertas más precisas.	RM y Director de Infraestructura	E616 - Configuración del sistema de cruzamiento de información.
P2	T617 - Diseñar e implementar un mecanismo alternativo de monitoreo manual.	RM y Director de Infraestructura	E617 - Documentación del mecanismo alternativo de monitoreo.
P2	T618 - Documentar lecciones aprendidas y oportunidades de mejora a partir de los resultados del monitoreo.	RM	E618 - Informes de lecciones aprendidas y oportunidades de mejora.
P2	T620 - Establecer alertas reactivas para dispositivos críticos del centro de datos.	Director de Infraestructura y RM	E620 - Configuración de alertas reactivas.
P2	T621 - Realizar monitoreos esporádicos de dispositivos para identificar amenazas físicas.	Director de Infraestructura y RM	E621 - Informe de monitoreos esporádicos realizados.
P2	T622 - Configurar las funciones de monitoreo integradas en los dispositivos críticos.	Director de Infraestructura y RM	E622 - Configuración de dispositivos para monitoreo de amenazas típicas.
P2	T623 - Establecer mecanismos de notificación automatizada de alertas.	Director de Infraestructura y RM	E623 - Registro de notificaciones enviadas al personal designado.
P2	T624 - Documentar los procedimientos para la gestión de alertas.	Director de Infraestructura y RM	E624 - Procedimiento documentado para la gestión de alertas.
P2	T626 - Instalar y configurar sensores para amenazas físicas específicas.	Director de Infraestructura y RM	E626 - Registro de instalación y configuración de sensores.
P2	T627 - Establecer una estrategia de almacenamiento redundante para datos de sensores.	Director de Infraestructura y RM	E627 - Estrategia documentada para almacenamiento redundante de datos.
P2	T628 - Documentar los procedimientos de gestión y análisis de datos recolectados.	RM	E628 - Procedimiento documentado para análisis de datos recolectados.
P2	T629 - Implementar un sistema de monitoreo inteligente con capacidades de análisis histórico.	Director de Infraestructura y RM	E629 - Configuración y reportes generados por el sistema de monitoreo inteligente.
P2	T630 - Establecer procedimientos para la generación y análisis de informes de monitoreo.	Director de Infraestructura y RM	E630 - Procedimientos documentados para análisis de informes.
P2	T631 - Realizar evaluaciones periódicas del centro de datos basadas en los informes generados.	RM	E631 - Registro de evaluaciones periódicas realizadas.
P2	T632 - Definir un plan de acciones correctivas y preventivas basado en las evaluaciones realizadas.	Director de Infraestructura y RM	E632 - Plan de acciones correctivas y preventivas documentado.
P2	T633 - Identificar los sistemas y aplicaciones críticas donde se registrarán eventos relevantes de los usuarios.	CSI	E633 - Listado de sistemas y aplicaciones críticas identificadas.
P2	T634 - Configurar el registro de eventos de usuarios en los sistemas críticos.	Director de Infraestructura	E634 - Configuración de registro de eventos de usuarios en los sistemas críticos.
P2	T635 - Establecer procedimientos para revisiones reactivas de eventos registrados.	RM	E635 - Procedimiento documentado para revisiones reactivas de eventos.
P2	T636 - Documentar los resultados de las revisiones y evaluar incidentes potenciales.	RM	E636 - Registro de evaluaciones de incidentes basadas en los resultados de las revisiones.
P2	T637 - Asignar responsabilidades específicas para el monitoreo de eventos de los usuarios.	RSI	E637 - Documento que define las responsabilidades del monitoreo.
P2	T638 - Establecer un procedimiento de revisión periódica de registros que incluya inicios de sesión fallidos y acceso a Internet.	Director de Infraestructura y RM	E638 - Procedimiento documentado de revisión periódica de registros.
P2	T639 - Generar reportes para el Directorio y partes interesadas basados en la información monitoreada.	RSI y Director de TIC	E639 - Reportes generados para el Directorio y partes interesadas.
P2	T640 - Diseñar e implementar actividades de control interno para verificar el cumplimiento del procedimiento de monitoreo.	RSI	E640 - Registro de actividades de control interno realizadas para verificar cumplimiento del procedimiento de monitoreo.
P2	T641 - Generar y analizar estadísticas basadas en la información monitoreada.	RM	E641 - Estadísticas generadas a partir del monitoreo de eventos.
P2	T642 - Revisar y actualizar el procedimiento de monitoreo basado en las lecciones aprendidas.	Director de Infraestructura y RM	E642 - Procedimiento de monitoreo actualizado con las lecciones aprendidas.

P2	T643 - Identificar desvíos detectados en los proveedores de servicios críticos del centro de datos.	Director de Infraestructura	E643 - Listado de proveedores y desvíos detectados.
P2	T644 - Tomar acciones correctivas ante desvíos detectados de proveedores.	Director de Infraestructura	E644 - Registro de desvíos y acciones correctivas realizadas.
P2	T645 - Definir y documentar SLA con proveedores críticos que incluyan cláusulas de seguridad.	Director de TIC	E645 - Documentos de SLA y cláusulas con proveedores.
P2	T646 - Formalizar los acuerdos con proveedores mediante contratos.	RSI y Director de TIC	E646 - Contratos con SLA y cláusulas de seguridad de la información.
P2	T647 - Establecer un régimen de cobertura en los SLA y contratos para servicios críticos.	RSI y Director de TIC	E648 - SLA actualizados con régimen de cobertura definido.
P2	T648 - Implementar un procedimiento para la revisión de contratos cuando cambien los servicios.	RSI y Director de TIC	E649 - Procedimiento documentado para la revisión de contratos.
P2	T649 - Establecer un cronograma de revisiones periódicas de contratos y SLA.	RSI y Director de TIC	E649 - Cronograma de revisiones periódicas de contratos SLA.
P2	T650 - Generar reportes de evaluación y recomendaciones basadas en las revisiones de acuerdos SLA.	RSI	E650 - Reportes de revisiones periódicas de contratos y SLA.
P2	T651 - Configurar el monitoreo de logs de control de acceso físico y lógico.	RM	E651 - Configuración del sistema de monitoreo de logs.
P2	T652 - Establecer un sistema básico de almacenamiento y análisis de logs.	Director de Infraestructura y RM	E652 - Logs generados por los sistemas de control de acceso.
P2	T653 - Configurar reglas de monitoreo para conexiones externas y dispositivos no autorizados.	Director de Infraestructura y RM	E653 - Configuración de reglas de monitoreo.
P2	T654 - Implementar alertas automáticas ante violaciones detectadas.	RM	E654 - Registro de alertas generadas por el sistema.
P2	T655 - Desarrollar procedimientos para el monitoreo.	Director de Infraestructura y RM	E655 - Políticas y procedimientos documentados.
P2	T656 - Configurar sistemas para monitorear todos los equipos del organismo.	Director de Infraestructura y RM	E656 - Configuración del sistema de monitoreo ampliado.
P2	T657 - Implementar un sistema centralizado para la recolección de logs y emisión de alertas.	Director de Infraestructura y RM	E657 - Configuración del sistema centralizado de recolección de logs.
P2	T658 - Analizar y documentar las acciones no permitidas detectadas.	RM	E658 - Informes de análisis de acciones no permitidas.
P2	T659 - Realizar escaneos puntuales utilizando herramientas disponibles (propias o contratadas).	Director de Infraestructura	E659 - Registro de revisiones puntuales realizadas.
P2	T660 - Documentar los hallazgos de las revisiones realizadas.	Director de Infraestructura	E660 - Informes de escaneos de vulnerabilidades.
P2	T661 - Establecer un cronograma periódico para los escaneos de vulnerabilidades.	Director de Infraestructura y RGV	E661 - Cronograma de revisiones de vulnerabilidades.
P2	T662 - Realizar escaneos adicionales en caso de cambios significativos en los sistemas.	RGV	E662 - Informes de escaneos periódicos.
P2	T663 - Analizar los resultados de los escaneos para identificar vulnerabilidades críticas.	RGV	E663 - Registro de cambios significativos y escaneos asociados.
P2	T665 - Documentar el procedimiento para realizar escaneos internos y externos.	RSI	E665 - Informes de revisiones internas y externas.
P2	T666 - Contratar servicios de ethical hacking para revisiones externas.	RSI	E666 - Contrato de ethical hacking.
P2	T667 - Desarrollar un plan de acción basado en los hallazgos de las revisiones.	RSI	E667 - Plan de acción para corregir vulnerabilidades detectadas.
P2	T668 - Incorporar el procedimiento de revisión de vulnerabilidades en las actividades rutinarias de seguridad.	RSI y RGV	E668 - Registros de control interno que validen la ejecución de las revisiones.
P2	T669 - Establecer controles internos para verificar el cumplimiento del procedimiento.	RSI	E669 - Informes de mejora continua basados en las revisiones realizadas.
P2	T670 - Ajustar la frecuencia de las revisiones según análisis de riesgo o cambios significativos en los sistemas.	RSI	E670 - Análisis de riesgo asociados a cambios significativos en los sistemas.
P2	T671 - Implementar mecanismos para medir la efectividad de las correcciones realizadas.	RIS	E671 - Registros de medición de efectividad en la resolución de vulnerabilidades.
P2	T672 - Identificar personal responsable y asignar tareas específicas relacionadas con la detección de eventos en sistemas base y protección perimetral.	Director de TIC	E672 - Listado de personal asignado a tareas de detección.
P2	T673 - Documentar las asignaciones de tareas en un registro formal.	Director de TIC	E673 - Registro de las tareas asignadas.
P2	T674 - Implementar herramientas automatizadas para la detección y monitoreo de eventos.	RSI y Director de Infraestructura	E674 - Configuración de herramientas de monitoreo automatizado.
P2	T675 - Establecer un proceso para la revisión periódica de registros de eventos generados por las herramientas.	RSI y Director de Infraestructura	E675 - Procedimientos para la revisión de eventos y registros de revisión de eventos.
P2	T676 - Asignar un responsable formal y documentar un procedimiento detallado para las actividades de monitoreo.	RSI y Director de TIC	E676 - Procedimiento documentado de monitoreo.
P2	T677 - Diseñar y ejecutar pruebas periódicas del procedimiento, incluyendo diferentes escenarios y ambientes.	RSI y Director de TIC	E677 - Registro de pruebas realizadas al procedimiento.

P2	T678 - Definir y documentar actividades de comunicación formal asociadas al monitoreo.	RSI y Director de TIC	E678 - Informes de comunicación formal relacionados con el monitoreo.
P2	T679 - Establecer controles internos para verificar el cumplimiento del procedimiento de monitoreo.	RSI	E679 - Informes de control interno sobre el cumplimiento del procedimiento.
P2	T680 - Implementar un proceso de retroalimentación basado en las lecciones aprendidas de las actividades de monitoreo.	RSI y Director de Infraestructura	E680 - Documentación de lecciones aprendidas y retroalimentación.
P2	T681 - Comunicar los resultados de las actividades al RSI y otras partes interesadas.	Director de Infraestructura	E681 - Registro de comunicaciones a partes interesadas.
P2	T682 - Incorporar mejoras continuas al procedimiento de monitoreo y pruebas.	RSI y Director de Infraestructura	E682 - Procedimiento actualizado con mejoras derivadas de las actividades de monitoreo.
P2	T683 - Identificar referentes o autoridades responsables de recibir la comunicación sobre eventos anómalos.	Director de Infraestructura	E683 - Registro de eventos anómalos detectados.
P2	T684 - Establecer un proceso básico para la notificación manual de eventos anómalos detectados.	Director de Infraestructura	E684 - Proceso básico para la notificación de eventos anómalos detectados.
P2	T685 - Documentar mecanismos de comunicación estándar ante eventos anómalos.	Director de Infraestructura	E685 - Procedimientos documentados para la comunicación de eventos.
P2	T686 - Implementar registros de las comunicaciones realizadas ante eventos anómalos.	Director de Infraestructura	E686 - Registros de comunicaciones realizadas ante eventos detectados.
P2	T687 - Revisar y documentar un procedimiento completo de monitoreo, incluyendo actividades de comunicación específicas.	RSI	E687 - Procedimiento documentado de monitoreo con actividades de comunicación.
P2	T688 - Diseñar pruebas para evaluar las actividades de comunicación en escenarios de detección de eventos.	Director de Infraestructura y RM	E688 - Informes de pruebas realizadas, incluyendo resultados de las actividades de comunicación.
P2	T689 - Ejecutar pruebas periódicas del procedimiento, incluyendo las actividades de comunicación.	Director de Infraestructura y RM	E689 - Retroalimentación de las pruebas realizadas.
P2	T690 - Implementar un sistema de coordinación formal entre el RM y el RSI.	RM y RSI	E690 - Informes de coordinación entre el RM y el RSI.
P2	T691 - Realizar revisiones de control interno para evaluar el cumplimiento de los procedimientos de monitoreo y comunicación.	RSI	E691 - Resultados de las revisiones de control interno.
P2	T692 - Documentar las lecciones aprendidas y utilizarlas para mejorar los procedimientos y pruebas.	RM	E692 - Registro de lecciones aprendidas y mejoras implementadas.
P2	T693 - Mantener actualizados los procedimientos y pruebas basados en la retroalimentación obtenida.	RM	E693 - Procedimientos actualizados con mejoras basadas en la retroalimentación.
P2	T699 - Difundir la política de gestión de incidentes a todo el personal.	CSI	E699 - Distribución y firma de recepción por parte del personal.
P2	T700 - Incluir el procedimiento de reporte de incidentes en las actividades de concientización.	RSI y Comunicaciones	E700 - Materiales de formación que incluyan el procedimiento de reporte.
P2	T701 - Revisar y actualizar el plan de respuesta a incidentes y sus procedimientos.	RSI	E701 - Acta de revisión y actualización del plan de respuesta a incidentes.
P2	T702 - Realizar simulacros de respuesta a incidentes, incluyendo usuarios clave.	RSI	E702 - Resultados de simulacros de pruebas de respuesta a incidentes.
P2	T703 - Implementar un sistema de control interno para verificar el cumplimiento del plan de respuesta.	RSI	E703 - Informes de control interno sobre el cumplimiento del plan de respuesta de incidentes.
P2	T708 - Nombrar un punto de contacto único para los incidentes de seguridad.	RSI	E708 - Documento que asigna el punto de contacto.
P2	T709 - Establecer los criterios de reporte al CERTuy o equipo de respuesta.	RSI	E709 - Documento con los criterios establecidos para la notificación de incidentes.
P2	T712 - Implementar herramientas automatizadas para el reporte de eventos y gestión de incidentes.	RSI	E712 - Herramientas de automatización para el reporte de eventos y gestión de incidentes.
P2	T713 - Implementar controles internos para verificar el cumplimiento del procedimiento de reporte y gestión de incidentes.	RSI	E713 - Informes de auditoría de cumplimiento.
P2	T714 - Utilizar los resultados de los controles internos para mejorar el procedimiento de reporte y gestión de incidentes.	RSI	E714 - Actas de revisión y actualización de los procedimientos .
P2	T715 - Realizar análisis de lecciones aprendidas tras cada incidente y ajustarlos al procedimiento.	RSI	E715 - Informe de lecciones aprendidas documentado.
P2	T732 - Mantener contacto con actores clave internos y externos durante la gestión de incidentes.	RSI	E732 - Registro de comunicaciones con actores clave.
P2	T733 - Escalar las necesidades puntuales a actores externos relevantes, como CERTuy o CSIRT del sector.	RSI	E733 - Evidencia de incidentes escalados a CERTuy o CSIRT.
P2	T734 - Identificar los actores internos y externos relevantes para la gestión de incidentes.	RSI	E734 - Listado de actores internos y externos identificados.
P2	T735 - Registrar y mantener actualizados los datos de contacto de los actores identificados.	RSI	E735 - Base de datos o registro de contactos actualizados.
P2	T736 - Documentar el mecanismo de escalamiento de incidentes.	RSI	E736 - Documento con el mecanismo de escalamiento de incidentes.
P2	T740 - Realizar actividades de control interno para verificar el cumplimiento del procedimiento de reporte y gestión de incidentes, y del plan de respuesta.	RSI	E740 - Informes de control interno realizados.

P2	T741 - Utilizar los resultados de las actividades de control interno para mejorar el procedimiento y los planes.	RSI	E741 - Documentación con mejoras aplicadas al procedimiento y planes.
P2	T742 - Documentar las lecciones aprendidas y retroalimentar los procedimientos y planes de respuesta.	RSI	E742 - Registro de lecciones aprendidas y ajustes realizados.
P2	T743 - Registrar eventos de seguridad en los sistemas.	RSI y Director de Infraestructura	E743 - Registros de eventos de seguridad generados por los sistemas.
P2	T744 - Analizar reactivamente las notificaciones de seguridad generadas por los sistemas.	RSI	E744 - Informes de análisis reactivo realizados.
P2	T745 - Escalar los eventos que correspondan según su naturaleza.	RSI	E745 - Registro de eventos escalados.
P2	T746 - Definir pautas generales para el registro de eventos de seguridad.	RSI y Director de Infraestructura	E746 - Documento con pautas generales de registro de eventos.
P2	T747 - Asegurar que los nuevos sistemas se desplieguen siguiendo las pautas definidas.	Director de TIC	E747 - Registros de cumplimiento en el despliegue de nuevos sistemas.
P2	T748 - Determinar cuándo un evento o notificación constituye un incidente.	RSI y Director de TIC	E748 - Criterios definidos para la determinación de incidentes.
P2	T749 - Clasificar los incidentes según su criticidad y severidad.	RSI	E749 - Listado o base de datos con incidentes clasificados por criticidad y severidad.
P2	T752 - Determinar criterios para escalar un incidente considerando los activos afectados, criticidad y severidad.	RSI	E752 - Documentación de criterios para el escalamiento de incidentes.
P2	T753 - Incorporar mejores prácticas al procedimiento para la revisión y gestión de eventos, incluyendo análisis forense y custodia de la información.	RSI	E753 - Procedimiento de revisión y gestión de eventos con mejores prácticas.
P2	T754 - Realizar actividades de control interno para verificar el cumplimiento del procedimiento.	RSI	E754 - Informes de actividades de control interno realizadas.
P2	T755 - Utilizar los resultados de las actividades de control interno para la mejora continua del procedimiento.	RSI	E755 - Registro de mejoras aplicadas al procedimiento.
P2	T756 - Realizar análisis de impacto en forma ad-hoc durante la gestión de incidentes.	RSI	E756 - Registros de análisis de impacto realizados.
P2	T757 - Llevar a cabo actividades de respuesta a los incidentes detectados en forma ad-hoc.	RSI	E757 - Documentación de actividades de respuesta realizadas.
P2	T758 - Informar al CERTuy o CSIRT correspondiente sobre los incidentes detectados.	RSI	E758 - Reportes enviados al CERTuy o CSIRT.
P2	T759 - Definir y documentar pautas para la clasificación de incidentes.	RSI y RGI	E759 - Documento con las pautas para la clasificación de incidentes.
P2	T760 - Utilizar las pautas definidas en la gestión de todos los incidentes reportados.	RGI	E760 - Registros de incidentes clasificados siguiendo las pautas definidas.
P2	T761 - Implementar un plan y/o procedimiento de respuesta alineado a la política de gestión de incidentes.	RSI y RGI	E761 - Plan y/o procedimiento de respuesta documentado y aprobado.
P2	T762 - Incluir tareas de análisis de impacto dentro del procedimiento de gestión de incidentes.	RSI y RGI	E762 - Procedimiento de gestión de incidentes con tareas de análisis de impacto incluidas.
P2	T763 - Implementar herramientas automatizadas para el registro y seguimiento de incidentes, alineadas al plan y/o procedimiento de respuesta definido.	RSI y RGI	E763 - Registros generados por las herramientas automatizadas implementadas.
P2	T764 - Incorporar mejores prácticas en el procedimiento, incluyendo análisis forense y custodia de la información.	RSI Y RGI	E764 - Procedimiento actualizado con mejores prácticas incluidas.
P2	T765 - Realizar actividades post incidente para evaluar y mejorar la respuesta.	RSI y RGI	E765 - Informes de actividades post incidente realizadas.
P2	T766 - Sistematizar las lecciones aprendidas para mejorar procedimientos, procesos y estrategias de mitigación y respuesta.	RSI y RGI	E766 - Registro de lecciones aprendidas y mejoras aplicadas.
P2	T767 - Realizar análisis forense ante un incidente de seguridad de la información o contactar al CSIRT de referencia para que lo realice.	RSI	E767 - Registros de análisis forenses realizados o de contacto con CSIRT.
P2	T768 - Asegurar la participación de un equipo calificado o contactar al CSIRT de referencia.	RSI	E768 - Documentación de los incidentes en los que se ha solicitado análisis forense al CSIRT.
P2	T769 - Establecer pautas para garantizar la cadena de custodia durante el análisis forense.	RSI	E769 - Documento de pautas para la cadena de custodia.
P2	T770 - Generar los informes pertinentes del análisis forense y distribuirlos a las partes interesadas.	RSI	E770 - Informes de análisis forense generados y distribuidos a las partes interesadas.
P2	T771 - Documentar todos los procedimientos vinculados al análisis forense.	RSI	E771 - Procedimientos documentados vinculados al análisis forense.
P2	T772 - Asegurar que la documentación del análisis forense sea realizada por personal calificado.	RSI	E772 - Registros de capacitación del personal calificado en análisis forense.
P2	T773 - Utilizar el resultado del análisis forense para la mejora continua del SGSI del organismo.	CSI	E773 - Informe sobre las mejoras implementadas basadas en los resultados del análisis forense.
P2	T774 - Incorporar el análisis forense en la mejora de la gestión de riesgos de seguridad de la información.	RSI y RGI	E774 - Registros de ajustes y mejoras aplicadas en la gestión de riesgos a partir del análisis forense.
P2	T775 - Definir lineamientos para la categorización de los incidentes según su tipo y criticidad.	RSI y RGI	E775 - Documento con los lineamientos para la categorización de incidentes.
P2	T776 - Establecer un proceso para clasificar los incidentes según estos lineamientos.	RGI	E776 - Registros de incidentes categorizados según los lineamientos establecidos.

P2	T777 - Determinar las acciones y tiempos de respuesta asociados a cada categoría según la severidad del incidente.	RSI	E777 - Documento con las acciones y tiempos de respuesta según la severidad.
P2	T778 - Comunicar a los involucrados las acciones y tiempos de respuesta establecidos para cada categoría.	RSI y RGI	E778 - Registros de comunicación de acciones y tiempos de respuesta.
P2	T781 - Alinear las acciones asociadas a cada categoría con el plan de respuesta.	RGI	E781 - Registros de acciones alineadas con el plan de respuesta.
P2	T782 - Implementar herramientas que apoyen la gestión de los incidentes.	RGI	E782 - Informes de implementación de herramientas para la gestión de incidentes.
P2	T783 - Revisar periódicamente la categorización de incidentes y los planes de respuesta, considerando las necesidades del organismo y las tendencias de amenazas.	RSI y RGI	E783 - Informe de revisión periódica de categorización de incidentes y planes de respuesta.
P2	T784 - Realizar estadísticas utilizando las categorizaciones de incidentes y utilizar los resultados para mejorar o incrementar los controles existentes.	RSI y RGI	E784 - Estadísticas generadas a partir de las categorizaciones y resultados de mejoras en los controles.
P2	T785 - Establecer canales de comunicación para alertar sobre posibles vulnerabilidades que puedan afectar los activos y servicios críticos del centro de datos.	RSI y Director de Infraestructura	E785 - Registros de los canales de comunicación establecidos.
P2	T786 - Identificar y definir fuentes de información relevantes para recibir alertas sobre vulnerabilidades.	RSI y Director de Infraestructura	E786 - Listado de fuentes de información utilizadas para alertas de vulnerabilidades.
P2	T787 - Ampliar los canales de comunicación para incluir alertas sobre vulnerabilidades que puedan afectar los activos y servicios críticos del organismo.	RSI y Director de Infraestructura	E787 - Documentación de los canales de comunicación extendidos.
P2	T788 - Establecer un mecanismo de acción basado en la criticidad de las vulnerabilidades.	RSI y Director de Infraestructura	E788 - Procedimiento documentado de respuesta basado en la criticidad de las vulnerabilidades.
P2	T789 - Definir una metodología para la gestión de vulnerabilidades, con procedimientos detallados para su implementación.	RSI y Director de Infraestructura	E789 - Documento que define la metodología para la gestión de vulnerabilidades.
P2	T790 - Implementar herramientas que apoyen la gestión de vulnerabilidades.	RSI y Director de Infraestructura	E790 - Registros de implementación de herramientas de gestión de vulnerabilidades.
P2	T791 - Revisar periódicamente las fuentes de datos utilizadas para recibir alertas sobre vulnerabilidades.	RSI, RGI y Director de Infraestructura	E791 - Informe de revisión periódica de fuentes de datos de vulnerabilidades.
P2	T792 - Adecuar la metodología de gestión de vulnerabilidades conforme a las necesidades del organismo y su contexto.	RSI y RGI	E792 - Documentación de la adecuación de la metodología a las necesidades del organismo.
P2	T793 - Utilizar la gestión de vulnerabilidades para la mejora continua del SGSI.	RSI y RGI	E793 - Registros de actividades de mejora continua implementadas en el SGSI.
P2	T794 - Establecer mecanismos para responder y contener los incidentes detectados.	RSI	E794 - Registro de los mecanismos implementados para responder y contener incidentes.
P2	T795 - Mitigar las consecuencias de los incidentes ocurridos.	RSI y Director de Infraestructura	E795 - Reportes de mitigación de consecuencias de incidentes.
P2	T796 - Mantener un registro detallado de todos los incidentes.	RGI	E796 - Registro actualizado de incidentes.
P2	T797 - Informar sobre los incidentes detectados al CERTuy o CSIRT correspondiente y a otras partes interesadas.	RSI	E797 - Notificaciones enviadas al CERTuy o CSIRT correspondiente.
P2	T798 - Definir pautas claras para contener el daño y minimizar riesgos en el entorno operativo.	RSI y RGI	E798 - Documento con pautas para contención de daños.
P2	T799 - Informar a las gerencias sobre los incidentes detectados y sus impactos.	RSI	E799 - Informes de incidentes enviados a las gerencias.
P2	T800 - Elaborar planes de remediación para cada tipo de incidente identificado.	RGI	E800 - Planes de remediación documentados para incidentes.
P2	T833 - Revisar periódicamente las estrategias de respuesta del centro de datos.	RSI y Director de Infraestructura	E833 - Registro de revisiones realizadas a las estrategias de respuesta del centro de datos.
P2	T834 - Actualizar las estrategias de respuesta en función de los cambios en las necesidades del organismo.	RSI	E834 - Documentación de actualizaciones realizadas en respuesta a cambios en las necesidades del organismo.
P2	T835 - Revisar periódicamente las estrategias de respuesta relacionadas con los procesos del organismo que afecten los servicios críticos.	RSI y Director de TIC	E835 - Informes de revisiones de estrategias de respuesta de los procesos críticos.
P2	T836 - Coordinar las revisiones con las áreas responsables de los procesos críticos.	RSI	E836 - Actas de reuniones de coordinación con las áreas responsables.
P2	T837 - Elaborar pautas o políticas documentadas para la revisión de estrategias de respuesta.	RSI	E837 - Políticas o pautas documentadas para la revisión de estrategias de respuesta.
P2	T838 - Difundir las pautas o políticas al personal involucrado.	RSI	E838 - Registro de la difusión de pautas o políticas al personal involucrado.
P2	T839 - Supervisar el cumplimiento de las pautas o políticas documentadas.	RSI	E839 - Informes de cumplimiento de las pautas documentadas.
P2	T840 - Incorporar mejoras identificadas en las revisiones de estrategia para ajustar las estrategias de respuesta.	RSI	E840 - Registro de mejoras implementadas en las estrategias de respuesta.
P2	T841 - Utilizar las mejoras para optimizar el SGSI y fortalecer la gestión de riesgos de seguridad de la información.	RSI y RGR	E841 - Documentación de ajustes realizados en el SGSI y en la gestión de riesgos.
P2	T842 - Definir e implementar indicadores para el seguimiento y control de las estrategias de respuesta.	RSI	E842 - Indicadores definidos e informes de seguimiento y control.

P2	T843 - Implementar y mantener medidas de continuidad en el centro de datos, incluyendo alimentación redundante de energía eléctrica, control ambiental y redundancia en telecomunicaciones.	Director de Infraestructura	E843 - Documentación de medidas de continuidad en el centro de datos.
P2	T844 - Establecer un procedimiento para informar incidentes detectados al CERTuy o CSIRT correspondiente.	RSI	E844 - Registro de incidentes informados al CERTuy o CSIRT.
P2	T845 - Elaborar un plan y/o procedimiento inicial de respuesta a incidentes.	RSI y RGI	E845 - Plan o procedimiento inicial de respuesta a incidentes.
P2	T846 - Definir lineamientos para la ejecución de actividades de recuperación ante incidentes.	RSI	E846 - Lineamientos establecidos para actividades de recuperación ante incidentes.
P2	T848 - Realizar pruebas del plan de contingencia y recuperación, asegurando que se registren los resultados.	RSI y Director de Infraestructura	E848 - Registros de pruebas realizadas al plan de contingencia y recuperación.
P2	T849 - Designar un responsable de respuesta a incidentes para coordinar tareas de recuperación con los actores involucrados.	Director de TIC	E849 - Acta de designación del Responsable de Respuesta a Incidentes.
P2	T850 - Ejecutar pruebas anuales del plan de respuesta a incidentes y del plan de contingencia y recuperación.	RSI y RGI	E850 - Reportes de pruebas anuales del plan de recuperación y contingencia.
P2	T851 - Comunicar los resultados de las pruebas a la Dirección y partes interesadas.	RSI	E851 - Informe de resultados de pruebas comunicados a la Dirección.
P2	T852 - Utilizar las lecciones aprendidas de las pruebas para mejorar continuamente los planes y procedimientos.	RSI y Director de TIC	E852 - Documento con lecciones aprendidas y mejoras implementadas en los planes y procedimientos.
P2	T853 - Revisar periódicamente las estrategias de recuperación del centro de datos.	RSI y Director de Infraestructura	E853 - Registros de revisiones de las estrategias de recuperación del centro de datos.
P2	T854 - Realizar revisiones adicionales cuando existan cambios en las necesidades del organismo.	RSI y Director de TIC	E854- Registros de revisiones de las estrategias de recuperación del centro de datos.
P2	T855 - Revisar periódicamente las estrategias de recuperación de los procesos organizacionales, especialmente los servicios críticos.	CSI	E855 - Informes de revisiones periódicas de estrategias de recuperación de servicios críticos.
P2	T856 - Comunicar las estrategias de recuperación a todo el organismo, enfatizando las relacionadas con servicios críticos.	RSI	E856 - Comunicaciones internas sobre estrategias de recuperación.
P2	T858 - Asegurar que las revisiones de estrategias se basen en los cambios identificados por el Análisis de Impacto al Negocio (BIA).	RSI y Director de TIC	E858 - Informes que relacionan cambios detectados por el BIA con actualizaciones en estrategias de recuperación.
P3	T862 - Identificar los servicios críticos del organismo.	CSI	E862 - Informe de identificación de servicios críticos.
P3	T863 - Identificar los componentes prioritarios del centro de datos para la entrega de los servicios críticos.	Director de Infraestructura	E863 - Inventario de componentes prioritarios del centro de datos.
P3	T864 - Definir el tratamiento proactivo para atender eventos e incidentes de ciberseguridad.	RGI y RSI	E864 - Documento de estrategias de tratamiento proactivo para eventos e incidentes de ciberseguridad.
P3	T865 - Identificar las dependencias de los componentes prioritarios.	CSI	E865 - Documento de dependencias de los componentes prioritarios.
P3	T866 - Establecer planes de mantenimiento para los componentes prioritarios.	RSI	E866 - Planes de mantenimiento aprobados.
P3	T867 - Determinar los niveles de capacidad mínima para garantizar la entrega de los servicios críticos.	CSI	E867 - Informe de niveles de capacidad mínima definidos.
P3	T868 - Implementar la gestión de capacidad.	Director de TIC y RSI	E868 - Registro de ejecución de la gestión de capacidad.
P3	T869 - Documentar, aprobar y gestionar los cambios en los componentes prioritarios y sus dependencias.	Director de TIC y RSI	E869 - Registro de aprobación y documentación de cambios en componentes prioritarios.
P3	T870 - Realizar notificaciones a las partes interesadas sobre los cambios en los componentes prioritarios.	RSI	E870 - Reportes de notificaciones enviadas a las partes interesadas.
P3	T871 - Validar periódicamente la gestión de capacidad.	Director de TIC y RSI	E871 -Informe de validación periódica de gestión de capacidad.
P3	T872 - Documentar y priorizar el manejo de los servicios críticos de toda la infraestructura tecnológica.	Director de Infraestructura y RSI	E872 - Documento de priorización y manejo de servicios críticos.
P3	T873 - Implementar monitoreo automatizado de los componentes prioritarios.	RM y Director de Infraestructura	E873 - Registro de implementación del monitoreo automatizado.
P3	T874 - Configurar alertas del estado de los componentes ante cambios en el entorno.	RM y Director de Infraestructura	E874 - Reportes de alertas generadas por cambios en el entorno.
P3	T875 - Realizar una gestión de capacidad a largo plazo (más de 3 años).	Director de TIC y RSI	E875 - Plan de gestión de capacidad a largo plazo.
P3	T876 - Verificar la existencia de UPS y componentes redundantes en el centro de datos.	Director de Infraestructura	E876 - Informe de verificación de UPS y componentes redundantes.
P3	T877 - Garantizar redundancia en la conexión eléctrica, acondicionamiento térmico e infraestructura de comunicaciones.	Director de Infraestructura	E877 - Registro de auditoría de redundancia en conexiones eléctricas, térmicas y de comunicaciones.
P3	T878 - Definir las ventanas de tiempo máximo soportadas por el organismo sin operar.	CSI	E878 - Documento de definición de ventanas de tiempo máximo de inactividad.

P3	T879 - Implementar un generador eléctrico capaz de alimentar todos los componentes críticos del centro de datos.	Director de Infraestructura	E879 - Registro de instalación y pruebas del generador eléctrico.
P3	T880 - Diseñar y aprobar un plan de contingencia y recuperación para los procesos críticos del organismo.	CSI	E880 - Plan de contingencia y recuperación aprobado.
P3	T881 - Realizar pruebas iniciales del plan en uno o varios procesos críticos.	RSI y Director de TIC	E881 - Informe de ejecución de pruebas iniciales del plan en procesos críticos.
P3	T882 - Ejecutar pruebas del plan de contingencia y recuperación de forma periódica.	Director de Infraestructura y RSI	E882 - Reportes de ejecución y resultados de pruebas del plan de contingencia.
P3	T883 - Capacitar a todos los involucrados en el plan y su ejecución.	RSI y Director de Infraestructura	E883 - Registro de capacitaciones realizadas.
P3	T884 - Analizar los resultados de las pruebas y generar lecciones aprendidas para mejorar el plan.	RSI y Director de TIC	E884 - Documento de lecciones aprendidas y acciones de mejora implementadas.
P3	T885 - Establecer un proceso para la gestión de riesgos de los componentes del centro de datos.	Director de Infraestructura	E885 - Documento del proceso de gestión de riesgos de los componentes del centro de datos.
P3	T886 - Identificar y gestionar de forma independiente los riesgos asociados a los servicios críticos.	RGR	E886 - Registro de identificación y mitigación de riesgos en servicios críticos.
P3	T887 - Implementar una metodología para la gestión de riesgos de ciberseguridad.	RGR	E887 - Documento de metodología de gestión de riesgos de ciberseguridad.
P3	T888 - Establecer un plan de trabajo para el tratamiento de los riesgos identificados.	RGR	E888 - Plan de trabajo para tratamiento de riesgos.
P3	T906 - Evaluar y documentar la capacidad actual instalada para la prestación de los servicios críticos.	Director de Infraestructura	E906 - Informe de capacidad instalada de los servicios críticos.
P3	T907 - Considerar las necesidades de capacidad al dimensionar los servicios críticos de acuerdo a las necesidades del organismo.	Director de Infraestructura	E907 - Documento de criterios para dimensionamiento de servicios críticos.
P3	T908 - Implementar mediciones objetivas para detectar problemas de capacidad en los servicios críticos.	RM y Director de Infraestructura	E908 - Reportes de medición de capacidad y detección de problemas.
P3	T909 - Definir y documentar el proceso de gestión de la capacidad actual.	Director de Infraestructura	E909 - Documento del proceso de gestión de la capacidad.
P3	T910 - Identificar y asignar un responsable del proceso de gestión de la capacidad.	Director de Infraestructura	E910 - Acta de designación del responsable de la gestión de la capacidad.
P3	T911 - Establecer roles y responsabilidades dentro del proceso de gestión de la capacidad.	Director de Infraestructura	E911 - Matriz de roles y responsabilidades en la gestión de la capacidad.
P3	T912 - Elaborar y aprobar un plan formal de capacidad.	RSI y Director de TIC	E912 - Plan de capacidad aprobado.
P3	T913 - Definir un proceso de estimación de la capacidad alineado con el plan.	RSI y Director de Infraestructura	E913 - Procedimiento de estimación de capacidad.
P3	T914 - Utilizar la información obtenida para generar pronósticos de capacidad.	Director de TIC	E914 - Informes de pronósticos de capacidad.
P3	T915 - Establecer revisiones periódicas del plan de capacidad.	Director de TIC	E915 - Registro de revisiones del plan de capacidad.
P3	T916 - Implementar acciones de mejora continua en la gestión de capacidad.	Director de Infraestructura	E916 - Reporte de mejoras implementadas en la gestión de capacidad.
P3	T941 - Realizar revisiones periódicas de los procesos de protección de los activos críticos del centro de datos.	Director de Infraestructura	E941 - Informes de revisión de los procesos de protección en el centro de datos.
P3	T942 - Ampliar la revisión de los procesos de protección a los activos y servicios del organismo.	Director de Infraestructura y RSI	E942 - Registro de revisión de procesos de protección en todo el organismo.
P3	T943 - Comunicar los resultados de las revisiones a todas las partes interesadas.	RSI	E943 - Evidencia de comunicación a las partes interesadas.
P3	T944 - Registrar los cambios realizados a los procesos de protección, incluyendo configuraciones de seguridad.	Director de Infraestructura	E944 - Registro de cambios en configuraciones de seguridad.
P3	T945 - Implementar una gestión formal de cambios en los procesos de protección.	Director de Infraestructura	E945 - Documentación del proceso de gestión de cambios en protección.
P3	T946 - Incorporar los resultados de las revisiones a la mejora continua del SGSI.	RSI	E946 - Informes de impacto y mejora continua en el SGSI.
P3	T947 - Evaluar el impacto de los cambios en la protección y definir mejoras estratégicas.	CSI	E947 - Actas de la comisión de seguridad con decisiones sobre mejoras.
P3	T948 - Establecer una metodología para documentar lecciones aprendidas de incidentes de seguridad en el centro de datos.	Director de Infraestructura	E948 - Documentos con registros de lecciones aprendidas.
P3	T949 - Registrar las lecciones aprendidas en una base de datos o repositorio accesible para el equipo de seguridad.	RGI	E949 - Repositorio de lecciones aprendidas en el centro de datos.
P3	T950 - Extender la sistemática de aprendizaje de incidentes a todo el organismo.	RSI	E950 - Registro de incidentes y aprendizajes a nivel organizacional.
P3	T951 - Difundir las lecciones aprendidas a todas las partes interesadas mediante informes o reuniones periódicas.	RSI	E951 - Evidencia de comunicaciones o reuniones con partes interesadas

P3	T952 - Incorporar las lecciones aprendidas en los planes de respuesta a incidentes.	RGI	E952 - Plan de respuesta actualizado con lecciones aprendidas.
P3	T953 - Ajustar y mejorar los canales de comunicación y los procesos de escalamiento en base a incidentes pasados.	RGI	E953 - Documentación de mejoras en comunicación y escalamiento.
P3	T954 - Analizar las lecciones aprendidas para mejorar el SGSI y el análisis de riesgos.	RSI	E954 - Informe de mejoras en el SGSI basado en lecciones aprendidas.
P3	T955 - Definir indicadores para medir la efectividad de los controles implementados.	Director de TIC y RSI	E955 - Reporte de indicadores de efectividad de controles.
P3	T956 - Capacitar al personal en las actividades básicas a realizar en caso de detectar o sospechar un incidente.	RSI y Capacitación	E956 - Registro de capacitaciones sobre respuesta a incidentes.
P3	T957 - Identificar y documentar a los proveedores que brindan soporte a los servicios críticos.	Director de Infraestructura	E957 - Listado actualizado de proveedores de soporte a servicios críticos.
P3	T959 - Establecer un plan básico de recuperación.	RSI y Director de Infraestructura	E959 - Plan básico de recuperación
P3	T960 - Capacitar a los involucrados en los mecanismos de respuesta y plan básico de recuperación.	RSI Y Director de Infraestructura	E960 - Registro de capacitaciones realizadas en mecanismos de respuesta y plan básico de recuperación.
P3	T962 - Desarrollar un plan de recuperación ante desastres (DRP).	RSI y Director de Infraestructura	E962 - Plan de recuperación ante desastres (DRP).
P3	T963 - Registrar los resultados de la ejecución de los planes de respuesta a incidentes y DRP.	Director de Infraestructura	E963 - Registros de pruebas de respuesta a incidentes y DRP.
P3	T964 - Alinear el plan de respuesta a incidentes con DRP.	RGI y RSI	E964 - Documentación del alineamiento entre plan respuesta a incidentes y DRP.
P3	T965 - Realizar pruebas anuales del plan de respuesta a incidentes y DRP.	RSI	E965 - Planificación anual de plan respuesta a incidentes y DRP.
P3	T966 - Utilizar como insumo los resultados de las pruebas de plan de respuesta a incidentes y DRP para mejora continua.	RSI	E966 - Informe de lecciones aprendidas y mejoras aplicadas al plan de respuesta a incidentes y DRP.
P3	T967 - Realizar el mantenimiento de los activos del centro de datos según los requerimientos técnicos.	Director de Infraestructura	E967 - Registro de mantenimiento de activos tecnológicos.
P3	T968 - Registrar las tareas de mantenimiento realizadas en los activos.	Director de Infraestructura	E968 - Reportes de intervenciones en los equipos del centro de datos.
P3	T969 - Definir y documentar planes anuales de mantenimiento.	Director de Infraestructura	E969 - Documento de planes anuales de mantenimiento.
P3	T970 - Gestionar accesos a los usuarios autorizados para realizar tareas de mantenimiento programado.	Director de Infraestructura	E970 - Registros de acceso para mantenimiento.
P3	T971 - Registrar el mantenimiento, fallos y cambios realizados sobre los activos.	Director de Infraestructura	E971 - Reportes de fallos y cambios en los activos.
P3	T972 - Desarrollar un procedimiento de mantenimiento preventivo y correctivo para la plataforma tecnológica.	Director de Infraestructura y RSI	E972 - Documento de procedimiento de mantenimiento.
P3	T973 - Implementar el procedimiento en la planificación del mantenimiento de los activos.	Director de Infraestructura y RSI	E973 - Informes de cumplimiento del procedimiento.
P3	T974 - Evaluar periódicamente la efectividad del procedimiento.	Director de Infraestructura y RSI	E974 - Evaluaciones de efectividad del mantenimiento.
P3	T975 - Implementar procesos de control de cambio para el mantenimiento de los activos.	RSI	E975 - Registros de control de cambios en mantenimiento.
P3	T976 - Documentar y gestionar aprobaciones del CSI para las tareas de mantenimiento.	RSI	E976 - Documentación de aprobaciones del CSI.
P3	T977 - Implementar un proceso de control interno para verificar el cumplimiento del mantenimiento del equipamiento.	Director de Infraestructura y RSI	E977 - Informes de control interno sobre el cumplimiento de mantenimiento.
P3	T978 - Aprobar la alta y baja de usuarios (internos o externos) que realizan mantenimiento remoto.	Director de infraestructura	E978 - Registros de aprobación y baja de usuarios remotos.
P3	T979 - Documentar las aprobaciones y bajas de accesos remotos en los activos informáticos del centro de datos.	Director de infraestructura	E979 - Listado actualizado de usuarios con acceso remoto.
P3	T980 - Implementar un proceso de gestión de aprobación de usuarios para conexión remota.	Director de infraestructura y RSI	E980 - Documento de plan anual de mantenimiento aprobado.
P3	T981 - Registrar todos los eventos de acceso remoto de cada usuario.	Director de infraestructura	E981 - Registros de accesos remotos detallados.
P3	T982 - Garantizar el cumplimiento de cláusulas de confidencialidad, integridad y disponibilidad de la información.	Director de infraestructura	E982 - Acuerdos de confidencialidad firmados.
P3	T983 - Desarrollar un procedimiento que genere alertas automáticas en cada evento de conexión remota.	Director de infraestructura y RSI	E983 - Procedimiento documentado para generación de alertas automáticas.

P3	T984 - Implementar un sistema de monitoreo para identificar y trazar actividades de usuarios conectados.	RM	E984 - Informes de trazabilidad de actividades en accesos remotos.
P3	T985 - Evaluar las alertas y detectar posibles desviaciones en las acciones de mantenimiento.	RM	E985 - Reportes de análisis de alertas generadas
P3	T986 - Realizar revisiones periódicas de logs de acceso remoto y actividades de usuarios.	RSI	E986 - Informes de auditoría de accesos remotos.
P3	T987 - Implementar controles internos para detectar accesos no autorizados o actividades sospechosas.	Director de Infraestructura y RSI	E987 - Registros de revisiones periódicas de logs.
P3	T988 - Generar informes y reportes para retroalimentar el proceso de mantenimiento remoto.	Director de Infraestructura y RSI	E988 - Reportes de control de accesos y actividades sospechosas.
P3	T989 - Difundir la importancia de la protección y uso seguro de medios extraíbles.	RSI y Capacitación	E989 - Materiales de difusión y registros de capacitaciones realizadas.
P3	T990 - Identificar y documentar los tipos de medios extraíbles autorizados.	Director de TIC	E990 - Documento de medios extraíbles autorizados.
P3	T991 - Definir y comunicar pautas para el uso de medios extraíbles.	RSI	E991 - Registro de comunicaciones enviadas sobre las pautas de uso.
P3	T992 - Implementar un proceso de reporte de hurto, pérdida o daño de medios extraíbles.	Director de Infraestructura	E992 - Registros de reportes de incidentes de medios extraíbles.
P3	T993 - Definir e implementar el procedimiento de eliminación segura de medios extraíbles al final de su vida útil.	Director de Infraestructura	E993 - Registros de eliminación segura de medios extraíbles.
P3	T994 - Realizar revisiones de control interno sobre el cumplimiento de las pautas de uso y el procedimiento de medios extraíbles.	Director de Infraestructura y RSI	E994 - Informes de revisión interna sobre cumplimiento de pautas.
P3	T995 - Analizar los resultados de las revisiones para mejorar el procedimiento y comunicar los hallazgos al RSI y partes interesadas.	Director de Infraestructura y RSI	E995 - Documento de mejora del procedimiento basado en los hallazgos.
P3	T996 - Implementar redundancia en los componentes críticos del centro de datos para asegurar la entrega de servicios y tolerar fallos.	Director de Infraestructura	E996 - Registro de los componentes con redundancia y sus configuraciones.
P3	T997 - Implementar y configurar un centro de datos alternativo para asegurar la resiliencia y prolongación operativa en caso de fallas.	Director de Infraestructura y RSI	E998 - Documentación del centro de datos alternativo y su capacidad operativa.
P3	T998 - Documentar la implementación y pruebas de los mecanismos de tolerancia a fallos en el centro de datos principal.	Director de Infraestructura y RSI	E998 - Informe de implementación y pruebas de tolerancia a fallos.
P3	T999 - Realizar pruebas periódicas en el centro de datos alternativo para verificar la correcta configuración de los sistemas.	Director de Infraestructura y RSI	E999 - Registro de resultados de pruebas periódicas en el centro de datos alternativo.
P3	T1000 - Garantizar que todos los componentes de soporte a los servicios críticos cuenten con redundancia.	Director de Infraestructura y RSI	E1000 - Reporte de la redundancia implementada en todos los componentes críticos.
P3	T1001 - Mejorar continuamente los procesos de resiliencia basado en pruebas periódicas, ajustando la calibración de activos según las necesidades del organismo.	Director de Infraestructura y RSI	E1001 - Documentación de ajustes y calibraciones realizadas con base en las pruebas.
P3	T1002 - Definir parámetros esperables para usuarios privilegiados.	RSI	E1002 - Documento con los parámetros definidos para usuarios privilegiados.
P3	T1003 - Gestionar parámetros esperables para sistemas críticos del centro de datos.	Director de Infraestructura	E1003 - Registro de parámetros configurados para sistemas críticos.
P3	T1004 - Definir parámetros esperables para todos los usuarios asociados a servicios críticos del organismo.	RSI	E1004 - Inventario de parámetros esperables para usuarios y sistemas críticos.
P3	T1005 - Gestionar parámetros esperables para sistemas de soporte u otros que deban ser monitoreados.	Director de Infraestructura	E1005 - Registro de configuraciones para sistemas de soporte y otros sistemas monitoreados.
P3	T1006 - Reportar desvíos al RSI.	Director de Infraestructura	E1006 - Informes de desvíos registrados y enviados al RSI.
P3	T1007 - Documentar la línea base de operaciones de red y flujos de datos esperados.	RSI	E1007 - Documento oficial de la línea base de operaciones de red y flujos de datos.
P3	T1008 - Definir el procedimiento de monitoreo y actuación ante desvíos.	RM	E1008 - Procedimiento documentado para monitoreo y actuación ante desvíos.
P3	T1009 - Generar indicadores y métricas sobre los eventos monitoreados.	RM y RSI	E1009 - Reportes periódicos con indicadores y métricas generados.
P3	T1010 - Revisar periódicamente la configuración de la línea base.	RSI	E1010 - Actas de revisiones periódicas de la configuración de la línea base.
P3	T1011 - Realizar revisiones de la línea base ante cambios tecnológicos o de objetivos del organismo.	RM y RSI	E1011 - Documentación de revisiones realizadas ante cambios tecnológicos u organizacionales.
P3	T1012 - Utilizar los indicadores para la mejora continua de la línea base.	RM y RGI	E1012 - Análisis de indicadores utilizados para mejoras continuas.
P3	T1013 - Apoyar la gestión de la línea base con las métricas generadas.	RM y RGI	E1013 - Reportes consolidados de métricas aplicadas a la gestión de la línea base.
P3	T1014 - Revisar los eventos locales generados por el equipamiento y activos del centro de datos.	RM y Director de Infraestructura	E1014 - Listado de eventos locales revisados.
P3	T1015 - Registrar las revisiones realizadas sobre los eventos locales.	RM y Director de Infraestructura	E1015 - Registro documentado de las revisiones realizadas.

P3	T1016 - Configurar los sistemas que soportan los servicios críticos para emitir alertas de eventos según las pautas establecidas por el apetito de riesgo del organismo.	RM y Director de Infraestructura	E1016 - Registro de configuración de alertas en los sistemas críticos.
P3	T1017 - Implementar un sistema de centralización de logs para los sistemas críticos.	Director de Infraestructura y RM	E1017 - Documentación técnica del sistema de centralización de logs implementado.
P3	T1018 - Documentar procesos y procedimientos para la centralización de logs.	RM y RSI	E1018 - Procedimientos documentados para la centralización de logs.
P3	T1019 - Configurar herramientas para la emisión de alertas basadas en los logs centralizados.	RM y Director de Infraestructura	E1019 - Configuración registrada de las herramientas de emisión de alertas.
P3	T1020 - Realizar pruebas de los procedimientos y herramientas para asegurar su efectividad.	Director de Infraestructura y RM	E1020 - Resultados de las pruebas realizadas.
P3	T1021 - Implementar procesos automatizados para correlacionar información desde múltiples fuentes.	Director de Infraestructura y RM	E1021 - Registro de procesos automatizados implementados.
P3	T1022 - Configurar sistemas automatizados para la ejecución de acciones basadas en correlaciones.	Director de Infraestructura y RM	E1022 - Configuración documentada de sistemas automatizados.
P3	T1023 - Revisar periódicamente los procedimientos implementados.	RM y Director de Infraestructura	E1023 - Informes de revisión periódica de procedimientos.
P3	T1024 - Actualizar los procedimientos y herramientas basados en los resultados de la revisión.	Director de Infraestructura y RM	E1024 - Procedimientos y herramientas actualizados según los resultados de la revisión.
P3	T1025 - Analizar el impacto de los eventos que afectan a los sistemas y servicios más críticos.	CSI	E1025 - Informe de análisis de impacto para eventos críticos.
P3	T1026 - Registrar los eventos analizados y sus impactos.	Director de Infraestructura y RSI	R1026 - Director de Infraestructura y RSI
P3	T1027 - Identificar los activos afectados utilizando el inventario de activos críticos del centro de datos.	CSI	E1027 - Inventario actualizado con los activos afectados identificados.
P3	T1028 - Definir y documentar los umbrales tolerables para los activos críticos (por ejemplo, tiempo de espera tolerable para aplicaciones).	CSI	E1028 - Documento que detalla los umbrales tolerables definidos para activos críticos.
P3	T1029 - Configurar y automatizar algunas alertas ante incidentes relacionados con los activos críticos.	Director de Infraestructura y RM	E1029 - Registro de configuración de alertas automatizadas.
P3	T1030 - Incorporar las actividades de identificación de impacto y determinación de umbrales en el procedimiento de detección y monitoreo.	RSI y RM	E1030 - Procedimiento documentado que incluye actividades de identificación de impacto y umbrales.
P3	T1031 - Automatizar las alertas relacionadas con los umbrales de tolerancia definidos para los activos críticos del centro de datos.	RM y Director de Infraestructura	E1031 - Registro de alertas automatizadas basadas en umbrales definidos.
P3	T1032 - Clasificar las alertas según el riesgo asociado al incidente.	RM	E1032 - Reporte de clasificación de alertas por nivel de riesgo.
P3	T1033 - Realizar actividades de control interno para verificar el cumplimiento con el procedimiento de detección y monitoreo.	RSI y RM	E1033 - Informe de control interno sobre cumplimiento del procedimiento de detección y monitoreo.
P3	T1034 - Analizar los resultados de las actividades de control interno y generar recomendaciones para la mejora del procedimiento de detección y monitoreo.	RSI	E1034 - Documento con recomendaciones generadas para la mejora del procedimiento.
P3	T1035 - Incorporar las lecciones aprendidas en el procedimiento de detección y monitoreo.	RM	E1035 - Procedimiento actualizado con las lecciones aprendidas.
P3	T1059 - Identificar los requisitos legales aplicables al uso de los logs.	RSI y Director de Legales	E1059 - Listado de requisitos legales aplicables identificados.
P3	T1060 - Configurar los sistemas de generación de logs para garantizar que cumplan con los requisitos aplicables.	Director de Infraestructura y RSI	E1060 - Configuración documentada de los sistemas de generación de logs.
P3	T1061 - Definir un procedimiento para el uso de los logs en cumplimiento con los requisitos legales.	RSI	E1061 - Procedimiento documentado para el uso de los logs en cumplimiento con los requisitos legales.
P3	T1062 - Revisar la normativa sectorial aplicable a la recolección y uso de logs.	RSI y Director de Legales	E1062 - Informe de normativa sectorial aplicable revisada.
P3	T1063 - Actualizar los procedimientos existentes para incluir las regulaciones sectoriales.	RSI	E1063 - Procedimientos actualizados con las regulaciones sectoriales.
P3	T1064 - Capacitar al personal responsable sobre las normativas de protección de datos aplicables a los logs.	RSI y Capacitación	E1064 - Registro de las capacitaciones realizadas, incluyendo lista de asistencia.
P3	T1065 - Establecer un proceso para monitorear cambios en los requisitos legales y normativos.	RSI y Director de Legales	E1065 - Registro de monitoreo de cambios normativos y legales.
P3	T1066 - Revisar los procedimientos de detección y actualizar conforme a los nuevos requisitos legales y normativos.	RSI y Director de Legales	E1066 - Procedimientos actualizados y versionados.
P3	T1067 - Documentar los cambios realizados en los procedimientos legales y normativos y comunicar a las partes involucradas.	RSI	E1067 - Comunicaciones enviadas sobre los cambios realizados.
P3	T1068 - Diseñar un plan de auditorías internas para verificar el cumplimiento de los requisitos legales y normativos aplicables.	Auditoría Interna	E1068 - Plan de auditorías internas para verificar cumplimiento de los requisitos legales y normativos aplicables.

P3	T1069 - Realizar auditorías periódicas sobre el uso de los logs y actividades relacionadas.	Auditoria Interna y RSI	E1069 - Informes de auditorías realizadas de cumplimiento de los requisitos legales y normativos aplicables
P3	T1070 - Analizar los resultados de las auditorías sobre los requisitos legales y normativos respecto a los logs y definir acciones de mejora continua.	RSI	E1070 - Registro de acciones de mejora implementadas basadas en los resultados de las auditorías para cumplimiento de los requisitos legales y normativos aplicables
P3	T1071 - Identificar los activos físicos y lógicos del centro de datos sujetos a detección y monitoreo.	Director de Infraestructura	E1071 - Listado de activos físicos y lógicos del centro de datos.
P3	T1072 - Definir las pruebas necesarias para validar los procesos de detección y monitoreo de los activos del centro de datos.	RSI	E1072 - Documento con el diseño de las pruebas de detección y monitoreo.
P3	T1073 - Ejecutar pruebas de detección y monitoreo de activos del centro de datos.	Director de Infraestructura	E1073 - Informes de resultados de las pruebas realizadas.
P3	T1074 - Identificar los activos y usuarios críticos del organismo para ser incluidos en las pruebas de detección.	CSI	E1074 - Listado de activos y usuarios críticos de la organización.
P3	T1075 - Definir y actualizar las pruebas para incluir activos y usuarios críticos del organismo.	RSI	E1075 - Documento actualizado con las pruebas diseñadas para activos y usuarios críticos.
P3	T1076 - Ejecutar pruebas de detección y monitoreo en activos y usuarios críticos.	Director de Infraestructura y RSI	E1076 - Informes de resultados de las pruebas realizadas.
P3	T1077 - Diseñar y documentar un procedimiento que establezca periodicidad y criterios para pruebas de detección.	RSI	E1077 - Procedimiento documentado con periodicidad y criterios para pruebas de detección.
P3	T1078 - Implementar herramientas de automatización para la detección de desvíos en las pruebas.	Director de Infraestructura y RM	E1078 - Registro de configuraciones y reportes generados por herramientas de automatización.
P3	T1079 - Documentar los resultados de las pruebas de detección de desvío.	Director de Infraestructura	E1079 - Informe con resultados documentados y registro de gestión de cambios.
P3	T1080 - Analizar las lecciones aprendidas para identificar mejoras aplicables al SGSI y la gestión de riesgos.	RSI	E1080 - Informe con análisis de lecciones aprendidas aplicadas al SGSI.
P3	T1081 - Actualizar el SGSI y las políticas de gestión de riesgos con base en las lecciones aprendidas.	RSI	E1081 - Actualización de políticas y procedimientos del SGSI.
P3	T1082 - Monitorear el impacto de las mejoras implementadas en el SGSI.	RSI	E1082 - Informes de auditoría sobre el impacto de las mejoras en el SGSI.
P3	T1083 - Identificar incorporaciones o modificaciones realizadas en los sistemas críticos e infraestructuras del centro de datos.	Director de Infraestructura	E1083 - Registro de cambios realizados en los sistemas críticos e infraestructuras del centro de datos.
P3	T1084 - Actualizar las configuraciones del monitoreo para reflejar cambios en los sistemas críticos e infraestructuras.	RM y Director de Infraestructura	E1084 - Configuraciones actualizadas del sistema de monitoreo.
P3	T1085 - Validar que las actualizaciones de monitoreo incluyan las modificaciones realizadas.	RSI	E1085 - Informe de validación de monitoreo actualizado.
P3	T1086 - Identificar las incorporaciones o modificaciones realizadas en los sistemas del organismo.	Director de TIC y RSI	E1086 - Registro de cambios realizados en los sistemas del negocio.
P3	T1087 - Actualizar las configuraciones del monitoreo para reflejar cambios en los sistemas del organismo.	RM y RSI	E1087 - Configuraciones actualizadas del sistema de monitoreo para los sistemas del organismo.
P3	T1088 - Validar que las actualizaciones de monitoreo incluyan las modificaciones realizadas en los sistemas del organismo.	Director de Infraestructura y RSI	E1088 - Informe de validación de monitoreo actualizado para los sistemas del organismo.
P3	T1089 - Diseñar y documentar el procedimiento de monitoreo de los activos de información del organismo.	RSI y RM	E1089 - Procedimiento documentado de monitoreo de activos de información.
P3	T1090 - Configurar sistemas para correlacionar eventos de los distintos sistemas de monitoreo.	RM y Director de Infraestructura	E1090 - Configuraciones de correlación de eventos en sistemas de monitoreo.
P3	T1091 - Implementar y configurar alertas automatizadas para detectar desvíos.	RM y Director de Infraestructura	E1091 - Configuraciones de alertas automatizadas.
P3	T1092 - Validar el funcionamiento de las alertas automatizadas y de la correlación de eventos.	Director de Infraestructura y RM	E1092 - Informe de validación de las alertas y correlación de eventos.
P3	T1108 - Identificar las lecciones aprendidas de los incidentes de seguridad de la información relacionados con el centro de datos.	RGI y RSI	E1108 - Informe de lecciones aprendidas de los incidentes vinculados al centro de datos.
P3	T1109 - Registrar las lecciones aprendidas en un repositorio centralizado.	RGI	E1109 - Registro de lecciones aprendidas en el repositorio centralizado.
P3	T1110 - Identificar las lecciones aprendidas de los incidentes de seguridad de la información en todo el organismo.	RSI y RGI	E1110 - Informe consolidado de lecciones aprendidas de los incidentes de seguridad de la información a nivel organizacional.
P3	T1111 - Consolidar las lecciones aprendidas de los incidentes de seguridad de la información en un registro único para la organización.	RGI	E1111 - Registro único de lecciones aprendidas de los incidentes de seguridad de la información actualizado.
P3	T1112 - Implementar herramientas para el registro y gestión de lecciones aprendidas de incidentes de seguridad de la información.	Director de Desarrollo y RGI	E1112 - Documentación sobre la implementación de herramientas de registro y gestión.

P3	T1113 - Comunicar las lecciones aprendidas sobre incidentes de seguridad de la información a todas las partes interesadas mediante los canales definidos.	RSI y RGI	E1113 - Actas o registros de las comunicaciones realizadas.
P3	T1114 - Establecer un proceso formal para compartir las lecciones aprendidas sobre incidentes de seguridad de la información	RSI y RGI	E1114 - Procedimiento formal para compartir lecciones aprendidas .
P3	T1115 - Analizar las lecciones aprendidas de los incidentes de seguridad de la información para identificar oportunidades de mejora en el SGSI.	RGI y RSI	E1115 - Informe de análisis de lecciones aprendidas con recomendaciones de mejora.
P3	T1116 - Incorporar las lecciones aprendidas de los incidentes de seguridad de la información en la gestión de riesgos de seguridad de la información.	RGI y RSI	E1116 - Actualización del mapa de riesgos con base en lecciones aprendidas.
P3	T1117 - Definir y monitorear indicadores relacionados con la implementación de lecciones aprendidas de los incidentes de seguridad de la información.	RGI y RSI	E1117 - Indicadores definidos y reportes de monitoreo.
P3	T1128 - Determinar a la persona o grupo responsable de la comunicación externa durante crisis o incidentes mayores.	Directorio	E1128 - Documento oficial de designación del responsable de la comunicación externa.
P3	T1129 - Establecer la autorización expresa para que las áreas técnicas puedan comunicar externamente en situaciones específicas.	Directorio	E1129 - Registro de autorización de comunicación externa para áreas técnicas.
P3	T1130 - Definir y designar un vocero oficial para situaciones de crisis relacionadas con ciberseguridad y seguridad de la información.	Directorio	E1130 - Documento de designación oficial del vocero.
P3	T1131 - Difundir al personal la identidad del vocero y los canales oficiales de contacto en caso de incidentes.	Directorio y Comunicaciones	E1131 - Comunicación interna difundida al personal sobre el vocero y los canales de contacto.
P3	T1132 - Elaborar un plan de comunicaciones para situaciones de crisis, incluyendo evaluación, notificaciones y monitoreo.	CSI y Comunicaciones	E1132 - Plan de comunicaciones ante crisis documentado.
P3	T1133 - Establecer un procedimiento detallado para gestionar la comunicación durante crisis, desde la evaluación hasta la entrega de mensajes a la audiencia correspondiente.	CSI y Comunicaciones	E1133 - Procedimiento de gestión de comunicación en crisis aprobado.
P3	T1134 - Difundir el plan y procedimiento a los actores involucrados, asegurando que todos los responsables estén informados.	Comunicaciones	E1134 - Confirmación de difusión del plan y procedimiento a los actores relevantes.
P3	T1135 - Realizar ensayos prácticos de crisis para poner a prueba el plan y procedimiento de comunicación.	Comunicaciones y RSI	E1135 - Informe de los ensayos de crisis realizados con el plan de comunicación.
P3	T1136 - Realizar revisiones periódicas de control interno para evaluar el cumplimiento del plan de comunicación ante crisis.	RSI y Comunicaciones	E1136 - Informe de revisión interna de control de cumplimiento con el plan de comunicación.
P3	T1137 - Documentar los resultados de las revisiones de control y utilizarlos para la mejora continua del plan.	RSI	E1137 - Documento de actualización y mejora del plan basado en resultados de las revisiones
P3	T1138 - Involucrar al Directorio en las actualizaciones del plan de comunicación, con un enfoque especial en la aprobación y difusión de los mensajes.	RSI	E1138 - Acta de aprobación del Directorio del plan de comunicación y difusión.

ANEXO 6 - Listado completo de actividades

Este anexo contiene un listado detallado de todas las actividades que se deben realizar para dar cumplimiento a los máximos niveles de madurez de cada una de las subcategorías, de acuerdo con la estructura del MCS de AGESIC.

Cabe destacar que algunas actividades se repiten en el modelo, ya que su ejecución contribuye al cumplimiento de más de una subcategoría. Para facilitar su identificación, las actividades duplicadas están sombreadas en el siguiente listado y, además, incluyen una referencia a la tarea original junto al número de tarea, esta referencia también se encuentra en la evidencia resultante de su cumplimiento.

Función	Cat	Cat_Nombre	Subcat	Nivel Madurez	Prio	Tareas para alcanzar nivel de madurez	Responsable	Evidencia
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	1	P1	T001 - Crear un inventario inicial que registre todos los dispositivos físicos del centro de datos.	Director de Infraestructura	E001 - Inventario documentado y actualizado de dispositivos físicos del centro de datos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	1	P1	T002 - Implementar un mecanismo para mantener el inventario actualizado (por ejemplo, revisiones periódicas o automatización básica).	Director de Infraestructura	E002 - Procedimiento para mantener el inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	1	P1	T003 - Asegurar que el inventario incluya información clave como ubicación, estado, y fecha de última revisión.	Director de Infraestructura	E003 - Registro de actualizaciones al inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	2	P1	T004 - Ampliar el inventario existente para incluir dispositivos de todas las áreas del organismo.	Director de Desarrollo	E004 - Inventario consolidado que incluya dispositivos de todas las áreas del organismo.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	2	P1	T005 - Establecer un sistema unificado de registro que permita integrar información de todos los dispositivos físicos y sistemas.	Director de Desarrollo	E005 - Procedimientos documentados para la gestión del inventario ampliado.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	2	P1	T006 - Implementar revisiones regulares del inventario para asegurar su precisión y vigencia.	Director de Desarrollo	E006 - Registros de revisiones periódicas del inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	2	P1	T007 - Capacitar al personal de las áreas involucradas sobre la importancia del inventario y cómo reportar cambios.	Director de Desarrollo	E007 - Evidencia de capacitaciones realizadas al personal de áreas involucradas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	3	P1	T008 - Desarrollar una política de Uso Aceptable de los Activos Móviles.	CSI	E008 - Política de Uso Aceptable de Dispositivos Móviles.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	3	P1	T009 - Documentar los procesos y procedimientos para la actualización del inventario de dispositivos físicos y sistemas.	Director de Desarrollo	E009 - Manual documentado de procesos y procedimientos de actualización del inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	3	P1	T010 - Implementar un software de inventario para gestionar y actualizar el inventario de manera centralizada.	Director de Desarrollo	E010 - Registros de implementación del software de inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	3	P1	T011 - Automatizar el proceso de actualización del inventario cuando sea posible.	Director de Desarrollo	E011 - Logs del sistema que evidencien la automatización de actualizaciones.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	4	P1	T012 - Definir un control para verificar la precisión del inventario.	Director de TIC	E012 - Documentación de las auditorías realizadas utilizadas como evidencia de cumplimiento o desviaciones encontradas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	4	P1	T013 - Realizar actividades periódicas de control interno para verificar el cumplimiento de los procedimientos de inventario.	Auditoría Interna	E013 - Informes de actividades de control interno realizadas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-1	4	P1	T014 - Alinear el inventario con los procedimientos establecidos mediante revisiones periódicas.	Auditoría Interna	E014 - Registros de revisiones y ajustes al inventario en alineación con los procedimientos establecidos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	1	P1	T015 - Identificar y registrar el software de base (sistemas operativos, bases de datos, middleware) y software de aplicación utilizado en el centro de datos.	Director de TIC	E015 - Inventario documentado y actualizado del software de base y de aplicación del centro de datos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	1	P1	T016 - Establecer un procedimiento para mantener actualizado el inventario de software.	Director de Infraestructura	E016 - Procedimientos documentados para la gestión del inventario de software.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	1	P1	T017 - Asegurar que el inventario incluya información relevante como nombre del software, versión, fecha de instalación, y estado actual.	Director de Infraestructura	E017 - Registros de actualizaciones o revisiones del inventario de software.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	2	P1	T018 - Ampliar el inventario existente para abarcar plataformas de software y aplicaciones utilizadas en todas las áreas del organismo.	Director de TIC	E018 - Inventario consolidado de plataformas de software y aplicaciones de todas las áreas del organismo.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	2	P1	T019 - Implementar un sistema centralizado para registrar y gestionar el inventario de software de todo el organismo.	Director de Desarrollo	E019 - Registros de licencias del software utilizado en servidores y otros equipos críticos.

IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	2	P1	T020 - Registrar las licencias asociadas al software utilizado, incluyendo información como tipo de licencia, proveedor, fecha de expiración y cumplimiento de términos.	Director de Soporte y Director de Infraestructura	E020 - Resultados de auditorías periódicas de licenciamiento.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	3	P1	T021 - (REF. T008) Desarrollar una política de Uso Aceptable de los Activos Móviles.	CSI	E021 - (REF. E008) Política de Uso Aceptable de Dispositivos Móviles.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	3	P1	T022 - (REF. T009) Documentar los procesos y procedimientos para la actualización del inventario de dispositivos físicos y sistemas.	Director de Infraestructura	E022 - (REF. E009) Manual documentado de procesos y procedimientos de actualización del inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	3	P1	T023 - (REF. T010) Implementar un software de inventario para gestionar y actualizar el inventario de manera centralizada.	Director de Infraestructura	E023 - (REF. E010) Registros de implementación del software de inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	3	P1	T024 - (REF. T011) Automatizar el proceso de actualización del inventario cuando sea posible.	Director de Infraestructura	E024 - (REF. E011) Logs del sistema que evidencien la automatización de actualizaciones.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	3	P1	T025 - Identificar y registrar el licenciamiento de software de equipos personales.	Director de Soporte	E025 - Registro de licenciamiento de software de equipos personales.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	4	P1	T026 - (REF. T012) Definir un control para verificar la precisión del inventario.	Director de TIC	E026 - (REF. E012) Documentación de las auditorías realizadas utilizadas como evidencia de cumplimiento o desviaciones encontradas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	4	P1	T027 - (REF. T013) Realizar actividades periódicas de control interno para verificar el cumplimiento de los procedimientos de inventario.	Auditoría Interna	E027 - (REF. E013) Informes de actividades de control interno realizadas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-2	4	P1	T028 - (REF. T014) Alinear el inventario con los procedimientos establecidos mediante revisiones periódicas.	Auditoría Interna	E028 - (REF. E014) Registros de revisiones y ajustes al inventario en alineación con los procedimientos establecidos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	1	P1	T029 - Designar rol de responsable de la seguridad de la información (RSI).	CSI	E029 - Resolución con designación del RSI.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	1	P1	T030 - Difusión del rol de RSI a todo el organismo.	CSI	E030 - Plan de difusión del rol RSI en el organismo.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	1	P1	T031 - Identificar y designar a los integrantes del CSI.	Directorio	E031 - Documento de designación de los miembros del CSI.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	1	P1	T032 - Establecer un registro oficial de los propietarios de los activos y comunicarles sus responsabilidades en la protección de dichos activos.	Alta Dirección	E032 - Registro de propietarios de activos con sus responsabilidades asignadas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	1	P1	T033 - Documentar los nombramientos y responsabilidades del CSI en un documento.	Director de RRHH	E033 - Documento que refleje los roles asignados del CSI.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	2	P1	T034 - Establecer un cronograma de reuniones periódicas del CSI.	CSI	E034 - Cronograma de reuniones del CSI.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	2	P1	T035 - Designar un secretario para documentar las reuniones del CSI.	CSI	E035 - Minutas o actas de reuniones del CSI firmadas por los participantes.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	2	P1	T036 - Registrar las decisiones, acuerdos y acciones tomadas en cada sesión.	CSI	E036 - Registro de acciones derivadas de las reuniones, con responsables asignados y fechas de cumplimiento.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	3	P1	T037 - Crear un documento formal que describa las funciones y responsabilidades del RSI, CSI y otros roles relacionados con la seguridad de la información.	CSI	E037 - Documento formal que describa roles y responsabilidades del RSI, CSI y roles relacionados.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	3	P1	T038 - Designar un rol responsable de la gestión de riesgos (RGR).	RSI	E038 - Resolución con designación del RGR.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	3	P1	T039 - Designar un rol responsable de la gestión de incidentes (RGI).	RSI	E039 - Resolución con designación del RGI.

IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	3	P1	T040 - Designar un rol responsable de monitoreo (RM).	RSI	E040 - Resolución con designación del RM.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	3	P1	T041 - Designar un rol responsable de la gestión de vulnerabilidades y parches (RGV).	RSI	E041 - Resolución con designación del RGV.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	4	P1	T042 - Diseñar e implementar controles internos que evalúen posibles conflictos entre roles y áreas de responsabilidad.	CSI	E042 - Registro del diseño de controles internos para conflictos entre roles y áreas de responsabilidad.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-6	4	P1	T043 - Preparar reportes con los resultados de las actividades de control interno y compartirlos con el RSI y partes interesadas.	CSI	E043 - Reportes enviados al RSI e interesados con los resultados de las revisiones.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	1	P1	T044 - Establecer los objetivos anuales de seguridad de la información.	CSI	E044 - Documento oficial con los objetivos anuales de SI.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	1	P1	T045 - Convocar reuniones del CSI para discutir los objetivos y aprobar las acciones necesarias.	CSI	E045 - Actas de reuniones del CSI con la discusión y aprobación de los objetivos.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	1	P1	T046 - Definir acciones específicas para lograr los objetivos anuales, asignando responsables y fechas de cumplimiento.	CSI	E046 - Plan de acciones iniciales para cumplir con los objetivos.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	2	P1	T047 - Diseñar un plan de acción detallado para cada objetivo establecido para alcanzar los objetivos anuales de seguridad de la información (Incluyendo: actividades específicas, cronogramas y recursos necesarios).	RSI y Director de TIC	E047 - Documento formal con el plan de acción detallado, que incluye actividades específicas, cronogramas y recursos necesarios.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	2	P1	T048 - Establecer indicadores de desempeño (KPIs) para medir el avance del plan de acción alcanzar los objetivos anuales de seguridad de la información.	RSI y Director de TIC	E048 - Lista de indicadores de desempeño (KPIs) definidos, con sus fórmulas de cálculo y metas asociadas.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	2	P1	T049 - Asignar responsables para cada actividad dentro del plan de acción para alcanzar los objetivos anuales de seguridad de la información.	RSI	E049 - Registro oficial de responsables asignados para cada actividad dentro del plan, con fechas y firmas de aceptación.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	2	P1	T050 - Comunicar el plan de acción alcanzar de los objetivos anuales de seguridad de la información a las áreas involucradas.	RSI	E050 - Evidencia de comunicación del plan de acción, como correos electrónicos, actas de reuniones o presentaciones compartidas con las áreas involucradas.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	3	P1	T051 - Crear materiales de comunicación (presentaciones, boletines, infografías) que expliquen los objetivos de seguridad y su importancia.	Comunicaciones	E051 - Materiales de difusión sobre los objetivos de SI.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	3	P1	T052 - Realizar reuniones o capacitaciones con el personal y partes interesadas para comunicar los objetivos anuales de seguridad de la información.	RSI y Capacitación	E052 - Registro de sesiones de comunicación con el personal y partes interesadas.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	3	P1	T053 - Implementar un sistema de seguimiento y reporte periódico del avance del plan de acción de los objetivos anuales de seguridad de la información.	RSI	E053 - Informes periódicos sobre el avance del plan de acción
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	4	P1	T054 - Diseñar una estrategia formal de seguridad de la información y ciberseguridad a mediano y largo plazo.	RSI	E054 - Estrategia de SI y ciberseguridad documentada
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	4	P1	T055 - Implementar proyectos basados en la estrategia seguridad de la información, con presupuesto asignado y aprobación del Directorio.	CSI y Directorio	E055 - Proyectos formales aprobados y con presupuesto asignado
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	4	P1	T056 - Difundir la estrategia de seguridad de la información a todos los niveles del organismo, utilizando todos los canales de comunicación disponibles.	Comunicaciones	E056 - Materiales de comunicación interna y externa para difundir la estrategia
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-3	4	P1	T057 - Evaluar periódicamente el impacto de la estrategia de seguridad de la información y realizar ajustes en función de las lecciones aprendidas.	CSI	E057 - Informes de evaluación del impacto de la estrategia
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	1	P1	T058 - Desarrollar una Política de seguridad de la información (PSI).	CSI	E058 - Política de seguridad de la información.

IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	1	P1	T059 - Disponer del acta de Resolución con la aprobación y adopción de la PSI.	RSI y Comunicaciones	E059 - Acta de Resolución con la aprobación de la PSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	1	P1	T060 - Comunicar la PSI a todo el organismo.	CSI	E060 - Plan de comunicación de la PSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	2	P1	T061 - Identificar áreas clave que requieren políticas específicas y desarrollarlas.	CSI	E061 - Lista de áreas clave identificadas y sus políticas desarrolladas.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	2	P1	T062 - Desarrollar políticas adicionales alineadas con la política general y manual de políticas asociadas.	CSI	E062 - Políticas adicionales alineadas con la política general y Manual de Políticas.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	2	P1	T063 - Aprobación del Directorio todas las políticas pendientes.	CSI	E063 - Acta de Resolución de aprobación de políticas.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	3	P1	T064 - Establecer una periodicidad de revisión de las políticas para determinar su vigencia y, si corresponde, actualizarlas.	CSI	E064 - Acta de revisión de las políticas.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	3	P1	T065 - Difusión de políticas actualizadas a todo el organismo.	CSI y Comunicaciones	E065 - Plan de difusión de políticas actualizadas
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	4	P1	T066 - Diseñar y documentar un SGSI alineado al Marco de Ciberseguridad.	CSI	E066 - Documento del SGSI alineado al marco de Ciberseguridad.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	4	P1	T067 - Definir procedimientos específicos para cada componente del SGSI.	CSI	E067 - Procedimientos específicos documentados.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	4	P1	T068 - Establecer indicadores clave de desempeño (KPIs) para medir la efectividad del SGSI.	RSI	E068 - KPIs definidos y reportados periódicamente para medir la efectividad del SGSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	4	P1	T069 - Planificar y ejecutar revisiones periódicas formales del SGSI.	RSI	E069 - Plan de ejecución de revisión del SGSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-1	4	P1	T070 - Presentar los resultados de las revisiones al CSI para toma de decisiones.	RSI	E070 - Informes de revisión del SGSI y planes de mejora.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	1	P1	T071 - (REF. T029) Designar rol de Responsable de la Seguridad de la Información.	CSI	E071 - (REF. E029) - Resolución con designación del RSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	1	P1	T072 - (REF. T030) - Difusión del rol de RSI a todo el organismo.	CSI	E072 - (REF. E030) - Plan de difusión del rol RSI en el organismo.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	2	P1	T073 - Documentar los roles y responsabilidades del RSI como referente ante el organismo y como referente ante CERTuy.	CSI	E073 - Documento con roles y responsabilidades del RSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	2	P1	T074 - Capacitar al RSI en gestión de riesgos e incidentes de seguridad.	CSI	E074 - Plan de capacitación del RSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	2	P1	T075 - Establecer un proceso formal para la gestión de incidentes de seguridad, incluyendo el reporte y la respuesta.	RSI y RGI	E075 - Documento de proceso formal para la gestión de incidentes.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	3	P1	T076 - (REF. T038) Designar un rol responsable de la gestión de riesgos (RGR).	RSI	E076 - (REF. E038) Resolución con designación del RGR.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	3	P1	T077 - Desarrollar un procedimiento formal para la gestión de riesgos en conjunto con los propietarios de activos.	RSI	E077 - Documento con procedimientos para la gestión de riesgos.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	4	P1	T078 - Realizar un seguimiento formal y periódico del cumplimiento del plan anual.	CSI	E078 - Plan de actividades y reuniones.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-2	4	P1	T079 - Documentar y reportar los resultados de las actividades del plan anual a la dirección.	CSI	E079 - Reportes periódicos sobre el avance del plan anual.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	1	P1	T080 - Designar rol de responsable de datos personales (RDP).	Directorio	R080 - Resolución con designación del RDP.

IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	1	P1	T081 - Identificar y listar los requisitos normativos aplicables a el organismo relacionados con seguridad de la información y ciberseguridad.	CSI	R081 - Listado documentado de normativas aplicables.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	2	P1	T082 - Revisar las pautas internas del organismo para asegurarse de que están alineadas con las normativas legales identificadas.	CSI	E082 - Informe de revisión y cumplimiento de las pautas internas.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	2	P1	T083 - Modificar o actualizar las pautas organizacionales para reflejar la normativa vigente.	CSI	E083 - Documento actualizado de pautas organizacionales.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	3	P1	T084 - Crear un procedimiento de cumplimiento de la normativa (Según Decreto 092/014).	RSI y RDP	E084 - Procedimiento documentado de revisión normativa.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	3	P1	T085 - Realizar auditorías internas para detectar posibles desvíos de cumplimiento y comunicar los resultados al CSI.	RSI	E085 - Reportes de auditoría interna.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	4	P1	T086 - Diseñar y ejecutar controles internos que evalúen periódicamente el cumplimiento del SGSI.	RSI	E086 - Documento de controles a ejecutar para la evaluación del cumplimiento del SGSI.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	4	P1	T087 - Documentar los resultados de las revisiones para identificar áreas de mejora.	RSI	E087 - Resultados documentados de los controles internos.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	4	P1	T088 - Incorporar los hallazgos en un plan de acción que impulse la mejora continua.	RSI	E088 - Plan de acción para la mejora continua.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-3	4	P1	T089 - Presentar los resultados y el plan de acción al Directorio para su consideración.	RSI	E089 - Presentación de resultados al Directorio
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	1	P1	T090 - Identificar las amenazas y vulnerabilidades de los activos de información del centro de datos.	Director de Infraestructura	E090 - Documento con la lista de amenazas y vulnerabilidades identificadas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	1	P1	T091 - Realizar una primera revisión de los riesgos de manera ad-hoc.	Director de Infraestructura	E091 - Informe de la revisión ad-hoc de riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	2	P1	T092 - (REF. T038) Designar un rol responsable de la gestión de riesgos (RGR).	RSI	E092 - (REF. E038) Resolución con designación del RGR.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	2	P1	T093 - Disponer de un inventario de riesgos identificados	RSI y RGR	E093 - Inventario de riesgos actualizado.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	3	P1	T094 - Definir una política de gestión de riesgos.	RSI	E094 - Política de gestión de riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	3	P1	T095 - Realizar el seguimiento periódico del inventario de riesgos identificados y documentar.	RGR	E095 - Plan e informe de revisión periódica de riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	3	P1	T096 - Comunicar los resultados de la revisión al CSI y otras partes interesadas.	RSI	E096 - Comunicación formal de los resultados al CSI.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	4	P1	T097 - Formalizar el resultado de la revisión de los riesgos frente al CSI y al directorio.	RSI	E097 - Informe elevado al CSI y al directorio del organismo.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-3	4	P1	T098 - Establecer y realizar actividades de control interno para verificar el cumplimiento con la política establecida.	RSI	E098 - Informes de actividades de control interno.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	1	P1	T099 - Identificar los principales riesgos de seguridad de la información para el organismo.	CSI	E099 - Documento con identificación de riesgos y su clasificación (cualitativa por impacto y probabilidad).
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	2	P1	T100 - Desarrollar un inventario de riesgos identificados que incluya el impacto potencial al funcionamiento del organismo.	RSI y RGR	E100 - Inventario de riesgos documentado con clasificación cualitativa del impacto al funcionamiento del organismo.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	3	P1	T101 - Establecer una frecuencia semestral para la revisión de riesgos, realizar la revisión y documentarla formalmente.	RSI y RGR	E101 - Plan de revisión semestral de riesgos e Informe de revisión de riesgos.

IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	3	P1	T102 - Desarrollar un análisis de impacto en el negocio (BIA) inicial.	RSI	E102 - Documento de BIA en desarrollo.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	3	P1	T103 - Identificar los procesos críticos y los sistemas de información que los soportan.	CSI	E103 - Documento de identificación de procesos críticos y sistemas de información.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	4	P1	T104 - Disponer de un repositorio de lecciones aprendidas de los riesgos.	RSI y RGR	E104 - Documento de lecciones aprendidas sobre riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	4	P1	T105 - Definir el BIA considerando los impactos a nivel de imagen, económico y en los usuarios.	RSI	E105 - Documento de BIA formalizado con diferentes tipos de impactos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	4	P1	T106 - Identificar todos los riesgos de seguridad de la información de todos los activos de información del organismo.	RSI y RGR	E106 - Documento actualizado con la identificación de riesgos para todos los activos de información.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	4	P1	T107 - Elevar los resultados de la revisión de los riesgos al CSI, al Directorio y a las partes interesadas.	RSI	E107 - Informe sobre resultados de elevación de riesgos al CSI, al Directorio y otras partes interesadas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-4	4	P1	T108 - Utilizar la revisión periódica de riesgos y del BIA para la toma de decisiones.	Directorio	E108 - Actas o decisiones basadas en la revisión periódica de riesgos y BIA.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	1	P1	T109 - (REF. T099) Identificar los principales riesgos de seguridad de la información para el organismo.	CSI	E109 - (REF. E099) Documento con identificación de riesgos y su clasificación (cualitativa por impacto y probabilidad).
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	2	P1	T110 - (REF. T100) Desarrollar un inventario de riesgos identificados que incluya el impacto potencial al funcionamiento del organismo.	RSI y RGR	E110 - (REF. E100) Inventario de riesgos documentado con clasificación cualitativa del impacto al funcionamiento del organismo.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	3	P1	T111 - (REF. T101) Establecer una frecuencia semestral para la revisión de riesgos, realizar la revisión y documentarla formalmente.	RSI y RGR	E111 - (REF. E101) Plan de revisión semestral de riesgos e Informe de revisión de riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	3	P1	T112 - (REF. T102) Desarrollar un análisis de impacto en el negocio (BIA) inicial.	RSI	E112 - (REF. E102) Documento de BIA en desarrollo.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	3	P1	T113 - (REF. T103) Identificar los procesos críticos y los sistemas de información que los soportan.	CSI	E113 - (REF. E103) Documento de identificación de procesos críticos y sistemas de información.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	4	P1	T114 - (REF. T104) Disponer de un repositorio de lecciones aprendidas de los riesgos	RSI y RGR	E114 - (REF. E104) Documento de lecciones aprendidas sobre riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	4	P1	T115 - (REF. T105) Definir el BIA considerando los impactos a nivel de imagen, económico y en los usuarios.	RSI	E115 - (REF. E105) Documento de BIA formalizado con diferentes tipos de impactos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	4	P1	T116 - (REF. T106) Identificar todos los riesgos de seguridad de la información de todos los activos de información del organismo.	RSI y RGR	E116 - (REF. E106) Documento actualizado con la identificación de riesgos para todos los activos de información.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	4	P1	T117 - (REF. T107) Elevar los resultados de la revisión de los riesgos al CSI, al Directorio y a las partes interesadas.	RSI	E117 - (REF. E107) Informe sobre resultados de elevación de riesgos al CSI, al Directorio y otras partes interesadas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-5	4	P1	T118 - (REF. T108) Utilizar la revisión periódica de riesgos y del BIA para la toma de decisiones.	Directorio	E118 - (REF. E108) Actas o decisiones basadas en la revisión periódica de riesgos y BIA.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	1	P1	T119 - Identificar proveedores de los activos y servicios críticos del centro de datos.	Director de TIC y CSI	E119 - Lista de proveedores de los activos y servicios críticos del centro de datos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	2	P1	T120 - Implementar modelos de identificación para abordar la gestión de riesgo asociado a proveedores de los activos y servicios críticos del organismo.	RGR	E120 - Modelo de identificación de riesgos implementado para proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la	ID.CS-1	2	P1	T121 - Definir métricas e indicadores para el seguimiento y control de los riesgos asociados a proveedores.	RGR	E121 - Documento que define las métricas e indicadores de control de proveedores.

		cadena de suministros						
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	3	P1	T122 - Desarrollar una política de gestión de riesgos de proveedores.	CSI	E122 - Política de gestión de riesgos de proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	3	P1	T123 - Establecer procedimientos formales para la gestión de riesgos con proveedores.	RSI y RGR	E123 - Procedimiento de gestión de riesgos de proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	3	P1	T124 - Definir la periodicidad de las evaluaciones de los proveedores.	RSI y RGR	E124 - Documento que establece la periodicidad de las evaluaciones de los proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	4	P1	T125 - Aplicar los procesos de gestión de riesgos en la adquisición de productos y servicios.	Director de TIC y RGR	E125 - Documentación de los procesos de gestión de riesgos aplicados en adquisiciones.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	4	P1	T126 - Mantener los procesos de gestión de riesgos a lo largo de todo el ciclo de vida de los productos y servicios adquiridos.	RGR	E126 - Registros de mantenimiento de los procesos de gestión de riesgos en el ciclo de vida de productos y servicios.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	4	P1	T127 - Evaluar a los proveedores basándose en el servicio brindado en relación con las necesidades del organismo.	Director de TIC	E127 - Informe de evaluación de proveedores en relación con las necesidades del organismo.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-1	4	P1	T128 - Incorporar los resultados de las evaluaciones de proveedores en las actualizaciones de contratos y futuras adquisiciones.	Director de TIC	E128 - Contratos actualizados y documentación de futuras adquisiciones que reflejan los resultados de las evaluaciones de proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	1	P1	T129 - Identificar a los proveedores y partes externas vinculadas al centro de datos.	Director de Infraestructura y RGR	E129 - Documento que identifica a los proveedores y partes externas del centro de datos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	1	P1	T130 - Priorizar los proveedores según su impacto en el organismo y su relación con los servicios críticos.	Director de TIC	E130 - Documento que muestra la priorización de proveedores críticos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	1	P1	T131 - Evaluar a los proveedores en el análisis de riesgos, considerando su impacto en el organismo.	Director de TIC y RGR	E131 - Informe del análisis de riesgos que incluye la evaluación de proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	2	P1	T132 - Identificar todos los proveedores de servicios críticos del organismo.	CSI	E132 - Lista completa de proveedores de servicios críticos identificados.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	2	P1	T133 - Priorizar a todos los proveedores según su impacto en el organismo.	Alta Dirección y RSI	E133 - Documento con la priorización de proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	2	P1	T134 - Definir aspectos de seguridad de la información y ciberseguridad para los proveedores, incluyendo acciones permitidas y no permitidas.	Alta Dirección y RSI	E134 - Documento que define los aspectos de seguridad y ciberseguridad para los proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la	ID.CS-2	3	P1	T135 - (REF. T122) - Desarrollar una política de gestión de riesgos de proveedores.	CSI	E135 - (REF. E122) - Política de gestión de riesgos de proveedores.

		cadena de suministros						
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	3	P1	T136 - Establecer procedimiento para la gestión de riesgos que contemple la evaluación de los proveedores críticos	RGR	E136 - Procedimiento formal para la gestión de riesgos de proveedores críticos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	4	P1	T137 - Integrar la evaluación de seguridad de la información y ciberseguridad en los procesos de adquisición de servicios y sistemas.	Alta Dirección y RSI	E137 - Documento que demuestra la integración de la evaluación de seguridad en los procesos de adquisición.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	4	P1	T138 - Asegurar que el proceso de gestión de riesgos evalúe cada fase del ciclo de vida de los productos y servicios adquiridos, desde su contratación hasta su culminación.	RGR	E138 - Documentación del proceso de gestión de riesgos que evalúa todas las fases del ciclo de vida de productos y servicios adquiridos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-2	4	P1	T139 - Realizar la evaluación de riesgos en función de los cambios de entorno o la obsolescencia de los sistemas y servicios.	RGR	E139 - Registros de evaluaciones de riesgos realizadas por cambios de entorno u obsolescencia.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	1	P1	T140 - Configurar controles de acceso lógico basados en usuarios nominados.	Director de TIC	E140 - Configuración de acceso lógico documentada que muestra la asociación entre usuarios y accesos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	1	P1	T141 - Establecer un registro inicial de usuarios nominados que tienen acceso a redes, recursos y sistemas.	Director de TIC	E141 - Lista de usuarios con acceso a redes, recursos y sistemas con permisos asignados.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	2	P1	T142 - Definir pautas para gestionar altas, bajas y modificaciones de acceso lógico.	Director de TIC	E142 - Documento de pautas para la gestión de accesos lógicos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	2	P1	T143 - Establecer un flujo de aprobaciones para gestionar cambios en los accesos lógicos.	Director de TIC	E143 - Registro de aprobaciones para modificaciones de acceso lógico.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	2	P1	T144 - Implementar un sistema para registrar y monitorear las altas, bajas y modificaciones realizadas.	RSI y Director de TIC	E144 - Registro histórico de cambios en accesos lógicos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	3	P1	T145 - Desarrollar una política de acceso lógico.	CSI	E145 - Política de acceso lógico.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	3	P1	T146 - Implementar un sistema centralizado para gestionar identidades y credenciales, al menos en forma administrativa.	Director de Desarrollo	E146 - Sistema centralizado de gestión de identidades y credenciales.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	3	P1	T147 - Realizar revisiones reactivas de privilegios frente a cambios o bajas en los sistemas críticos.	RSI	E147 - Registros de revisiones reactivas documentadas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	4	P1	T148 - Definir un procedimiento formal para la revisión periódica de privilegios de acceso.	RSI y Director de Desarrollo	E148 - Procedimiento para revisión periódica de privilegios de acceso.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	4	P1	T149 - Realizar revisiones proactivas periódicas de privilegios, incluyendo usuarios privilegiados.	RSI y Director de Desarrollo	E149 - Registros de revisiones proactivas periódicas de privilegios.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	4	P1	T150 - Comunicar los resultados de las revisiones de privilegios de acceso a las partes interesadas.	RSI	E150 - Informes de resultados revisiones de privilegios de acceso enviados a las partes interesadas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-1	4	P1	T151 - Realizar actividades de control interno para verificar la realización y efectividad de las revisiones de privilegios.	RSI	E151 - Informes de auditorías internas sobre la revisión de privilegios.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	1	P1	T152 - Implementar controles básicos de acceso físico a los activos críticos del centro de datos.	Director de Infraestructura	E152 - Configuración inicial de sistemas de control de acceso físico y su documentación.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	1	P1	T153 - Crear un registro de autorizaciones para acceder a los activos físicos del centro de datos.	Director de Infraestructura	E153 - Registro con el listado de personas autorizadas.

PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	2	P1	T154- Identificar los activos adicionales (más allá del centro de datos) que requieren controles físicos específicos.	CSI	E154 - Documento de identificación y clasificación de activos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	2	P1	T155 - Implementar controles de acceso físico en las áreas seguras asociadas a estos activos.	RSI	E155 - Configuración del sistema de control de acceso físico en las áreas seguras.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	2	P1	T156 - Actualizar y gestionar las autorizaciones de acceso para todas las áreas seguras.	RSI	E156 - Registro actualizado de personas autorizadas para cada área segura.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	3	P1	T157 - Desarrollar una política de control de acceso físico que abarque todos los activos críticos.	CSI	E157 - Política de control de acceso físico.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	3	P1	T158 - Definir y establecer perímetros de seguridad físicos alrededor de los activos críticos.	Director de Infraestructura	E158 - Documentación del diseño y medidas implementadas para proteger los activos críticos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	3	P1	T159 - Realizar revisiones reactivas de los registros de acceso en caso de incidentes.	Director de Infraestructura	E159 - Informes de revisiones reactivas documentadas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	4	P1	T160 - Definir y aprobar un procedimiento formal para la revisión periódica de accesos a los activos físicos.	CSI	E160 - Procedimiento formal de revisión de accesos a áreas seguras.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	4	P1	T161 - Implementar revisiones periódicas de registros de acceso físico en las áreas seguras y para activos críticos.	CSI y RSI	E161 - Informes periódicos de revisiones de acceso físico a áreas seguras.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	4	P1	T162 - Actualizar las políticas y procedimientos de acceso físico basados en los resultados de las revisiones.	CSI	E162 - Cambios documentados en las políticas y procedimientos en función de los hallazgos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-2	4	P1	T163 - Realizar auditorías internas para verificar el cumplimiento de los procedimientos establecidos.	RSI	E163 - Informes de auditoría interna sobre acceso físico.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	1	P1	T164 - Implementar credenciales nominadas para todos los usuarios con acceso a la red y sistemas.	Director de Infraestructura	E164 - Listado de usuarios nominados con accesos de red otorgados.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	1	P1	T165 - Definir controles básicos para el uso de usuarios privilegiados.	Director de Infraestructura	E165 - Listado de controles básicos para usuarios privilegiados.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	1	P1	T166 - Eliminar el uso de cuentas genéricas o compartidas, reemplazándolas por usuarios nominados con permisos controlados.	Director de Infraestructura	E166 - Listado de bajas de usuarios genéricos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	2	P1	T167 - Establecer roles y permisos basados en los principios de menor privilegio y segregación de funciones.	Director de Infraestructura	E167 - Documentación de roles y permisos asignados.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	2	P1	T168 - Implementar autenticación fuerte para usuarios críticos mediante métodos como doble factor de autenticación.	Director de Infraestructura	E168 - Configuración de doble factor de autenticación y listado de usuarios críticos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	2	P1	T169 - Centralizar la administración de usuarios y permisos mediante herramientas específicas.	Director de Infraestructura	E169 - Herramienta centralizada para la gestión de usuarios.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	3	P1	T170 - (REF. T145) Desarrollar una política de acceso lógico.	CSI	E170 - (REF. E145) Política de gestión de acceso lógico.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	3	P1	T171 - Implementar un procedimiento formal para el ABM de usuarios, incluyendo autorizaciones y registros de cambios.	RSI y Director de Desarrollo	E171 - Procedimiento formal de alta/baja/modificación.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	3	P1	T172 - Establecer y realizar revisiones periódicas de los derechos de acceso y registrar los resultados.	RSI	E172 - Plan de revisiones e Informes documentados.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	4	P1	T173 - Diseñar e implementar un procedimiento para la revisión periódica de derechos de acceso, priorizando usuarios privilegiados.	RSI y Director de TIC	E173 - Procedimiento para la revisión periódica de derechos de acceso.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	4	P1	T174 - Comunicar formalmente el resultado de las revisiones de derechos de acceso a las divisiones y otras partes interesadas el resultado de las revisiones para toma de decisiones.	Director de TIC	E174 - Informes con el resultado de las revisiones de derechos de acceso enviados a las divisiones y otras partes interesadas para toma de decisiones.

PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-4	4	P1	T175 - Coordinar entre RRHH y TIC para integrar procesos de altas, bajas y modificaciones de derechos de acceso.	Director de TIC y RRHH	E175 - Actas de reuniones de coordinación entre RRHH y TIC para la integración de procesos de altas, bajas y modificaciones de derechos de acceso.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	1	P1	T176 - Definir roles y perfiles específicos para el personal con acceso al centro de datos.	Director de Infraestructura	E176 - Listado de roles y perfiles segregados al centro de datos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	1	P1	T177 - Implementar un registro de actividades realizadas en el centro de datos.	Director de Infraestructura	E177 - Logs de actividades realizadas en el centro de datos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	1	P1	T178 - Revisar esporádicamente los registros de actividades para detectar anomalías.	Director de Infraestructura	E178 - Informes de revisiones de acceso al centro de datos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	2	P1	T179 - Notificar formalmente a usuarios con acceso a información sensible sobre las medidas de auditoría y sus responsabilidades.	RRHH	E179 - Notificaciones firmadas por los usuarios con acceso a información sensible.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	2	P1	T180 - Implementar un registro de usuarios con acceso a información sensible.	RRHH	E180 - Registro de notificaciones de usuarios con acceso a información sensible.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	2	P1	T181 - Verificar que los usuarios con acceso a información sensible sin notificar.	RRHH y Director de Desarrollo	E181 - Informe de revisiones de usuarios con acceso a información sensible.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	3	P1	T182 - Diseñar e implementar procedimientos formales para la gestión del ciclo de vida de usuarios (alta, baja, modificación).	RSI y Director de Desarrollo	E182 - Procedimientos documentados de ABM de usuarios.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	3	P1	T183 - Establecer un sistema centralizado para la gestión de permisos de usuarios nominados y genéricos.	Director de Desarrollo	E183 - Registros de gestión centralizada de usuarios y permisos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	3	P1	T184 - Realizar revisiones regulares del ciclo de vida de usuarios para asegurar el cumplimiento del procedimiento.	RSI	E184 - Informes de revisiones de ciclo de vida de usuarios.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	4	P1	T185 - (REF. T148) Definir un procedimiento formal para la revisión periódica de privilegios de acceso.	RSI y Director de Desarrollo	E185 - (REF. E148) Procedimiento para revisión periódica de privilegios de acceso.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	4	P1	T186 - (REF. T149) Realizar revisiones proactivas periódicas de privilegios, incluyendo usuarios privilegiados.	RSI y Director de Desarrollo	E186 - (REF. E149) Registros de revisiones proactivas periódicas de privilegios.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	4	P1	T187 - (REF. T150) Comunicar los resultados de las revisiones de privilegios de acceso a las partes interesadas.	RSI	E187 - (REF. E150) Informes de resultados revisiones de privilegios de acceso enviados a las partes interesadas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-6	4	P1	T188 - (REF. T151) Realizar actividades de control interno para verificar la realización y efectividad de las revisiones de privilegios.	RSI	E188 - (REF. E151) Informes de auditorías internas sobre la revisión de privilegios.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	1	P1	T189 - Implementar autenticación obligatoria en todos los sistemas del organismo.	Director de Desarrollo	E189 - Registros de autenticación habilitada en los sistemas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	1	P1	T190 - Garantizar que todos los usuarios sean nominados y cumplan con la política de control de acceso.	Director de Desarrollo	E190 - Listado de usuarios nominados con roles asignados.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	1	P1	T191 - Autorizar y registrar dispositivos que se conecten a la red del organismo.	Director de Infraestructura	E191 - Registro de dispositivos autorizados para conexión.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	2	P1	T192 - Implementar controles específicos para la gestión de usuarios privilegiados en sistemas y aplicaciones críticas.	Director de Desarrollo	E192 - Listado de usuarios privilegiados con permisos asignados.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	2	P1	T193 - Establecer autenticación multifactor para accesos remotos a aplicaciones críticas.	Director de Infraestructura	E193 - Configuración de autenticación multifactor implementada y activa.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	2	P1	T194 - Inventariar dispositivos externos utilizados para el acceso y asignar responsables.	Director de Infraestructura	E194 - Inventario actualizado de dispositivos externos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	3	P1	T195 - Diseñar e implementar un procedimiento formal de acceso lógico a redes, sistemas, recursos y dispositivos.	RSI	E195 - Procedimiento de acceso lógico a redes, sistemas, recursos y dispositivos documentado.

PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	3	P1	T196 - Implementar controles de autenticación diferenciados según la clasificación de la información.	Director de Infraestructura	E196 - Configuración de controles según clasificación de información.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	3	P1	T197 - Realizar análisis de riesgos asociados al acceso a la información para determinar las medidas de autenticación necesarias.	RGR y Director de TIC	E197 - Informe de análisis de riesgos asociados al acceso a la información.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	3	P1	T198 - Aplicar el principio de menor privilegio en la asignación de permisos.	Director de Infraestructura	E198 - Registro de permisos asignados conforme al principio de menor privilegio.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	4	P1	T199 - Definir y ejecutar procesos de revisión continua para validar la autenticación y configuración de los sistemas.	Director de Infraestructura	E199 - Informes de auditorías periódicas para validar la autenticación y configuración de los sistemas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	4	P1	T200 - Garantizar que los procedimientos de revisión consideran las políticas, normas y regulaciones aplicables.	RSI	E200 - Comparativa entre políticas internas y regulaciones externas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	4	P1	T201 - Comunicar los resultados de las revisiones y auditorías a las divisiones y partes interesadas.	RSI	E201 - Registro de envíos con los resultados de las revisiones de autenticación a las divisiones y partes interesadas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-7	4	P1	T202 - Realizar controles internos para verificar que los procedimientos definidos se cumplen.	RSI	E202 - Resultados de controles internos para verificar que los procedimientos de autenticación se cumplen.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	1	P1	T203 - Iniciar actividades de difusión de información relacionada con seguridad de la información, incluyendo la difusión de políticas y mecanismos de protección.	RSI y Comunicaciones	E203 - Registro de las actividades realizadas (presentaciones, correos electrónicos, boletines informativos) y lista de distribución o participantes.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	2	P1	T204 - Diseñar campañas de concientización para el personal, definiendo objetivos específicos.	RSI y Comunicaciones	E204 - Documento con el diseño de la campaña, incluyendo objetivos, mensajes clave y formato de las actividades.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	2	P1	T205 - Asignar y gestionar los recursos necesarios para la ejecución de las campañas de concientización.	Comunicaciones	E205 - Presupuesto aprobado para las campañas y registro de recursos asignados (equipo, herramientas, personal).
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	3	P1	T206 - Definir un cronograma para la realización de las campañas, detallando las fechas, actores críticos, objetivos, estrategias, tácticas y audiencia.	RSI y Comunicaciones	E206 - Cronograma aprobado con los detalles mencionados y validación del CSI.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	3	P1	T207 - Elaborar el material educativo necesario para las campañas de concientización.	RSI y Comunicaciones	E207 - Copias de los materiales educativos creados (presentaciones, videos, infografías, guías).
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	3	P1	T208 - Definir métricas e indicadores para medir el éxito de las campañas de concientización.	RSI	E208 - Documento con las métricas e indicadores definidos, como porcentaje de asistencia, encuestas de satisfacción y resultados de evaluaciones.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	4	P1	T209 - Realizar actividades de control interno para verificar el desarrollo de las campañas y su alineación con los objetivos establecidos.	RSI	E209 - Informes de auditoría interna que evalúen la ejecución de las campañas y cumplan con los objetivos establecidos.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	4	P1	T210 - Diseñar y ejecutar actividades de evaluación periódicas para medir el nivel de conocimiento adquirido por el personal.	RSI y Capacitación	E210 - Resultados de las evaluaciones realizadas, con análisis de datos y comparaciones entre períodos.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	4	P1	T211 - Presentar los resultados de las actividades de evaluación y las campañas al CSI y obtener su aprobación.	RSI	E211 - Actas del CSI con los resultados presentados y aprobaciones documentadas.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-1	4	P1	T212 - Obtener el respaldo formal del Directorio para las campañas de concientización y sus actividades relacionadas.	CSI	E212 - Acta del Directorio confirmando el apoyo formal y continuo a las campañas y actividades de concientización.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	1	P1	T213 - Identificar a los usuarios privilegiados y comunicarles la importancia de sus roles y responsabilidades.	RSI y Comunicaciones	E213 - Lista de usuarios privilegiados identificados y correo o registro de comunicación oficial.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	1	P1	T214 - Realizar una reunión inicial para explicar las implicancias y riesgos asociados a sus roles.	RSI	E214 - Cada Director de División explica los riesgos asociados a sus roles
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	2	P1	T215 - Diseñar e implementar un programa de concientización específico para usuarios privilegiados, estableciendo periodicidad.	RSI	E215 - Programa de concientización documentado, con periodicidad establecida y objetivos claros.

PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	2	P1	T216 - Ejecutar actividades de concientización (charlas, boletines, simulaciones) para reforzar el conocimiento.	RSI y Comunicaciones	E216 - Registro de actividades realizadas (presentaciones, correos enviados, listas de asistencia).
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	3	P1	T217 - Coordinar y planificar cursos o talleres relevantes para usuarios privilegiados sobre seguridad de la información.	RSI y Capacitación	E217 - Cronograma de cursos o talleres con agendas detalladas.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	3	P1	T218 - Evaluar el nivel de comprensión de los usuarios privilegiados al finalizar los cursos o talleres.	RSI y Capacitación	E218 - Resultados de evaluaciones a usuarios con privilegios tras los cursos o talleres.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	4	P1	T219 - Diseñar un plan integral de capacitación y entrenamiento en seguridad de la información, segmentado por perfiles estratégicos.	RSI y Capacitación	E219 - Plan integral de capacitación con detalles de perfiles, objetivos y cronograma.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	4	P1	T220 - Obtener la aprobación del plan por parte del Directorio y compromiso para su ejecución.	CSI	E220 - Resolución o acta de aprobación del plan de capacitación por el Directorio.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-2	4	P1	T221 - Implementar el plan y realizar revisiones periódicas incorporando lecciones aprendidas.	RSI y Capacitación	E221 - Informes de revisiones periódicas y acciones de mejora implementadas para los planes de capacitación.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	1	P1	T222 - Identificar a los interesados externos clave y documentar sus roles y responsabilidades en relación con la seguridad de la información.	CSI	E222 - Listado de interesados externos con roles y responsabilidades en relación con la seguridad de la información.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	1	P1	T223 - Comunicar las pautas definidas a los interesados externos mediante un canal formal (ej., contrato, acta o correo oficial).	Alta Dirección	E223 - Registro de pautas de seguridad con a los interesados externos que detalle su rol y responsabilidad.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	2	P1	T224 - Diseñar e implementar una iniciativa de concientización específica para interesados externos (ej., reuniones, boletines, talleres).	RSI y Capacitación	E224 - Plan de iniciativas de concientización para los interesados externos.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	2	P1	T225 - Ejecutar las actividades de concientización en seguridad de la información planificadas para los interesados externos.	RSI y Capacitación	E225 - Registro de las actividades de concientización en seguridad de la información realizadas con los interesados externos.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	3	P1	T226 - Implementar mecanismos de verificación para evaluar si los interesados externos comprenden sus roles y responsabilidades (ej., encuestas, entrevistas).	RSI y Director de TIC	E226 - Encuestas aplicadas o registros de entrevistas realizadas.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	3	P1	T227 - Generar reportes que consoliden los resultados de la evaluación de comprensión de roles y responsabilidades.	RSI	E227 - Reportes con análisis de resultados de las evaluaciones realizadas a los interesados externos.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	4	P1	T228 - (REF. T219) Diseñar un plan integral de capacitación y entrenamiento en seguridad de la información, segmentado por perfiles estratégicos.	RSI y Capacitación	E228 - (REF. E219) Plan integral de capacitación con detalles de perfiles, objetivos y cronograma.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	4	P1	T229 - (REF. T220) Obtener la aprobación del plan por parte del Directorio y compromiso para su ejecución.	CSI	E229 - (REF. E220) Resolución o acta de aprobación del plan de capacitación por el Directorio.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-3	4	P1	T230 - (REF. T221) Implementar el plan y realizar revisiones periódicas incorporando lecciones aprendidas.	RSI y Capacitación	E230 - (REF. E221) Informes de revisiones periódicas y acciones de mejora implementadas para los planes de capacitación.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	1	P1	T231 - Realizar una sesión informativa inicial a la Alta Dirección sobre los riesgos de seguridad de la información relevantes para el organismo.	CSI	E231 - Acta de la sesión informativa sobre riesgos de seguridad de la información realizada con la Alta Dirección.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	1	P1	T232 - Documentar los principales riesgos de seguridad de la información y compartirlo con el Directorio.	CSI	E232 - Documento con los principales riesgos de seguridad de la información, firmado por los asistentes.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	2	P1	T233 - Ampliar la difusión de riesgos de seguridad de la información al Directorio.	RSI	E233 - Registro de actividades de difusión realizadas al Directorio.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	2	P1	T234 - Implementar una iniciativa de concientización dirigida específicamente a la Alta Dirección y al Directorio.	RSI	E234 - Material utilizado en las iniciativas de concientización.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	3	P1	T235 - Planificar y ejecutar reuniones periódicas de concientización con la participación activa de la Alta Dirección.	RSI y Alta Dirección	E235 - Cronograma instancias de concientización planificadas para la Alta Dirección.

PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	3	P1	T236 - Generar reportes de las reuniones y registrar los compromisos adquiridos por la Alta Dirección.	RSI y Alta Dirección	E236 - Actas de las reuniones y reportes de compromisos adquiridos por la Alta Dirección.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	4	P1	T237 - (REF. T219) Diseñar un plan integral de capacitación y entrenamiento en seguridad de la información, segmentado por perfiles estratégicos.	RSI y Capacitación	E237 - (REF. E219) Plan integral de capacitación con detalles de perfiles, objetivos y cronograma.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	4	P1	T238 - (REF. T220) Obtener la aprobación del plan por parte del Directorio y compromiso para su ejecución.	CSI	E238 - (REF. E220) Resolución o acta de aprobación del plan de capacitación por el Directorio.
PROTEGER (PR)	PR.CF	Concientización y formación	PR.CF-4	4	P1	T239 - (REF. T221) Implementar el plan y realizar revisiones periódicas incorporando lecciones aprendidas.	RSI y Capacitación	E239 - (REF. E221) Informes de revisiones periódicas y acciones de mejora implementadas para los planes de capacitación.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	1	P1	T240 - Definir pautas estándar para la instalación de software en los equipos del personal.	Director de Soporte	E240 - Documento con pautas estándar para la instalación de software.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	1	P1	T241 - Instalar software antivirus en los equipos del personal.	Director de Soporte	E241 - Informe de implementación del software antivirus en los equipos del personal.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	1	P1	T242 - Realizar tareas de concientización sobre prevención ante software malicioso.	Director de Soporte y Capacitación	E242 - Registro de actividades de concientización realizadas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	2	P1	T243 - Restringir la instalación de software en los equipos a usuarios autorizados.	Director de Soporte	E243 - Registro de usuarios autorizados para instalar software en los equipos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	2	P1	T244 - Desarrollar un procedimiento para la instalación de software en producción, asignando responsables.	Director de Infraestructura	E244 - Procedimiento para la instalación de software en producción.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	2	P1	T245 - Instalar soluciones antivirus en servidores de archivos y correo electrónico.	Director de Infraestructura	E245 - Informe de implementación de soluciones antivirus en servidores.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	3	P1	T246 - Elaborar y mantener listas de software autorizado y prohibido.	Director de TIC	E246 - Listas de software autorizado y prohibido.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	3	P1	T247 - Implementar y gestionar una solución centralizada de antivirus, asignando un responsable.	Director de TIC	E247 - Informe de gestión de la solución centralizada de antivirus.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	3	P1	T248 - Desarrollar una política de protección contra software malicioso.	CSI	E248 - Política de protección contra software malicioso.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	3	P1	T249 - Configurar mecanismos de control para bloquear acceso a sitios web maliciosos o no autorizados.	Director de Infraestructura	E249 - Registro de configuración de mecanismos de control de acceso a sitios web maliciosos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	4	P1	T250 - Revisar y mantener actualizadas las listas de software autorizado y prohibido, asegurando su aprobación por el RSI.	Director de TIC	E250 - Listas de software revisadas y actualizadas con la aprobación del RSI.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	4	P1	T251 - Verificar que todos los servidores cuentan con protección o detección de malware.	Director de Infraestructura	E251 - Informe de verificación del estado de protección de los servidores.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	4	P1	T252 - Realizar controles internos sobre la solución antivirus y software instalado para verificar cumplimiento con políticas y procedimientos.	RSI y Director de TIC	E252 - Informes de control interno sobre la solución antivirus y software instalado.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-6	4	P1	T253 - Documentar resultados de las revisiones y enviarlos al RSI y partes interesadas, proponiendo acciones correctivas en caso de desvíos.	Director de TIC	E253 - Registro de resultados de revisiones y propuestas de acciones correctivas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	1	P1	T254 - Realizar respaldos periódicos de los activos del centro de datos.	Director de Infraestructura	E254 - Cronogramas documentados de respaldos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la	PR.PI-4	1	P1	T255 - Documentar los activos críticos de información que requieren respaldo.	Director de Infraestructura	E255 - Registro de activos respaldados.

		protección de la información						
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	1	P1	T256 - Almacenar los respaldos en una ubicación inicial definida.	Director de Infraestructura	E256 - Logs del sistema que evidencien la realización de respaldos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	2	P1	T257 - Implementar una solución automatizada para respaldos.	Director de Infraestructura	E257 - Logs y reportes generados por las soluciones automatizadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	2	P1	T258 - Definir ubicaciones seguras para respaldos con acceso restringido.	RSI y Director de Infraestructura	E258 - Documento de políticas de acceso a los respaldos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	2	P1	T259 - Documentar medidas de seguridad asociadas a los respaldos.	RSI y Director de Infraestructura	E259 - Registro de ubicaciones seguras y medidas de seguridad implementadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	3	P1	T260 - Realizar pruebas periódicas de restauración de respaldos.	Director de Infraestructura	E260 - Informes de pruebas de recuperación realizadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	3	P1	T261 - Incorporar almacenamiento externo para respaldos de contingencia.	Director de Infraestructura	E261 - Informe de almacenamiento externo contratado para respaldos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	3	P1	T262 - Desarrollar una política de respaldo de información.	CSI	E262 - Política de respaldo de información.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	3	P1	T263 - Elaborar un plan de respaldos con detalle del grado y requisitos de retención.	RSI y Director de Infraestructura	E263 - Registro de ajustes realizados al procedimiento de respaldos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	3	P1	T264 - Actualizar el procedimiento de respaldos cuando existan cambios en la infraestructura o requerimientos del organismo.	RSI y Director de Infraestructura	E264 - Documento de alineación de la política de respaldos con el plan de contingencia y recuperación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	4	P1	T265 - Alinear la política y procedimiento de respaldos con el plan de contingencia y recuperación.	RSI y Director de Infraestructura	E265 - Registro de revisiones periódicas de la política de respaldos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-4	4	P1	T266 - Revisar periódicamente la política y procedimiento de respaldos.	RSI	E266 - Informes de mejora continua en los procedimientos de respaldos.

PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	1	P1	T267 - (REF. T164) Implementar credenciales nominadas para todos los usuarios con acceso a la red y sistemas.	Director de Infraestructura	E267 - (REF. E164) Listado de usuarios nominados con accesos de red otorgados.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	1	P1	T268 - (REF. T165) Definir controles básicos para el uso de usuarios privilegiados.	Director de Infraestructura	E268 - (REF. E165) Listado de controles básicos para usuarios privilegiados.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	1	P1	T269 - (REF. T166) Eliminar el uso de cuentas genéricas o compartidas, reemplazándolas por usuarios nominados con permisos controlados.	Director de Infraestructura"	E269 - (REF. E166) Listado de bajas de usuarios genéricos.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	2	P1	T270 - (REF. T167) Establecer roles y permisos basados en los principios de menor privilegio y segregación de funciones.	Director de Infraestructura	E267 - (REF. E164) Documentación de roles y permisos asignados.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	2	P1	T271 - (REF. T168) Implementar autenticación fuerte para usuarios críticos mediante métodos como doble factor de autenticación.	Director de Infraestructura	E268 - (REF. E165) Configuración de doble factor de autenticación y listado de usuarios críticos.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	2	P1	T272 - (REF. T169) Centralizar la administración de usuarios y permisos mediante herramientas específicas.	Director de Infraestructura"	E269 - (REF. E166) Herramienta centralizada para la gestión de usuarios.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	3	P1	T273 - (REF. T145) Desarrollar una política de acceso lógico.	CSI	E273 - (REF. E145) Política de gestión de acceso lógico.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	3	P1	T274 - (REF. T171) Implementar un procedimiento formal para el ABM de usuarios, incluyendo autorizaciones y registros de cambios.	RSI y Director de Desarrollo	E274 - (REF. E171) Procedimiento formal de alta/baja/modificación.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	3	P1	T275 - (REF. T172) Establecer y realizar revisiones periódicas de los derechos de acceso y registrar los resultados.	RSI	E275 - (REF. E172) Plan de revisiones e Informes documentados.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	4	P1	T276 - (REF. T173) Diseñar e implementar un procedimiento para la revisión periódica de derechos de acceso, priorizando usuarios privilegiados.	RSI y Dirección TIC	E276 - (REF. E173) Procedimiento para la revisión periódica de derechos de acceso.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	4	P1	T277 - (REF. T174) Comunicar formalmente el resultado de las revisiones de derechos de acceso a las divisiones y otras partes interesadas el resultado de las revisiones para toma de decisiones.	Director TIC	E277 - (REF. E174) Informes con el resultado de las revisiones de derechos de acceso enviados a las divisiones y otras partes interesadas para toma de decisiones.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-3	4	P1	T278 - (REF. T175) Coordinar entre RRHH y TIC para integrar procesos de altas, bajas y modificaciones de derechos de acceso.	Director TIC y RRHH	E278 - (REF. E175) Actas de reuniones de coordinación entre RRHH y TIC para la integración de procesos de altas, bajas y modificaciones de derechos de acceso.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	1	P1	T279 - Implementar el cifrado de comunicación entre MTAs como método preferido.	Director de Infraestructura	E279 - Configuración de cifrado entre MTAs completada.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	1	P1	T280 - Configurar los servicios de Web mail con HTTPS utilizando certificados válidos.	Director de Infraestructura	E280 - Certificados válidos configurados en servicios de Web mail.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	2	P1	T281 - Proteger todas las aplicaciones Web disponibles en Internet mediante WAF configurado en modo detección.	Director de Infraestructura	E281 - Configuración de WAF en modo detección para aplicaciones Web.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	3	P1	T282 - Evolucionar el WAF de producción de modo detección a modo bloqueo.	Director de Infraestructura	E282 - Configuración de WAF en modo bloqueo en ambiente de producción.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	3	P1	T283 - Implementar un WAF en ambiente de prueba para realizar pruebas funcionales.	Director de Infraestructura	E283 - Instalación y pruebas funcionales documentadas en ambiente de prueba del WAF.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	3	P1	T284 - Centralizar los registros del WAF en un repositorio único.	Director de Infraestructura	E284 - Centralización de registros del WAF en repositorio de logs.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	4	P1	T285 - Establecer cifrado obligatorio para la comunicación entre MTAs de dominios gubernamentales.	Director de Infraestructura	E285 - Reporte de cifrado obligatorio entre MTAs gubernamentales.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	4	P1	T286 - Enviar reportes mensuales al CERTuy con estadísticas de actividad detectada en el WAF.	RSI	E286 - Informes mensuales enviados al CERTuy con estadísticas del WAF.

PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	4	P1	T287 - Colaborar con el CERTuy en la centralización de registros del WAF a nivel nacional.	RSI	E287 - Documentación de colaboración con el CERTuy en la centralización de registros del WAF.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	4	P1	T288 - Implementar automatismos para el análisis de registros del WAF que favorezcan actividades de revisión.	Director de Infraestructura	E288 - Automatismos implementados para análisis de registros del WAF.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-4	4	P1	T289 - Establecer un procedimiento documentado para la preservación y gestión de registros del WAF.	RSI	E289 - Procedimiento documentado para la preservación y gestión de registros del WAF.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	1	P1	T290 - (REF. T241) Instalar software antivirus en los equipos del personal.	Director de Soporte	E290 - (REF. E241) Registro de instalación del antivirus en todos los equipos del personal.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	1	P1	T291 - Establecer un procedimiento básico para resolver problemas de malware de forma ad-hoc.	Director de Soporte	E291 - Documento con el procedimiento básico para resolver problemas de malware.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	2	P1	T292 - (REF. T245) Instalar soluciones antivirus en servidores de archivos y correo electrónico.	Director de Soporte	E292 - (REF. E245) E245 - Informe de implementación de soluciones antivirus en servidores.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	2	P1	T293 - Configurar chequeos periódicos automáticos en los equipos del personal.	Director de Soporte	E293 - Logs de chequeos periódicos en las estaciones de trabajo.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	2	P1	T294 - Diseñar y realizar actividades de concientización sobre riesgos de software malicioso para el personal.	RSI y Capacitación	E294 - Material utilizado en las actividades de concientización sobre software malicioso.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	3	P1	T295 - (REF. T248) Definir una política de protección contra software malicioso.	RSI	E295 - (REF. E248) Política de protección contra software malicioso.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	3	P1	T296 - Documentar procedimientos específicos para la gestión de infecciones por malware.	RSI y Director de Infraestructura	E296 - Procedimientos documentados para gestionar infecciones.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	3	P1	T297 - Implementar una solución centralizada de antivirus.	Director de TIC	E297 - Informe técnico sobre la implementación de la solución centralizada de antivirus.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	4	P1	T298 - Configurar controles técnicos para bloquear el acceso a sitios web maliciosos y no autorizados.	Director de Infraestructura	E298 - Capturas de pantalla y configuraciones de los controles técnicos implementados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	4	P1	T299 - Extender la protección contra malware a dispositivos móviles del organismo.	Director de Soporte	E299 - Lista de dispositivos móviles protegidos y configurados con antivirus.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	4	P1	T300 - Documentar procedimientos para identificar y solucionar equipos desprotegidos.	RSI	E300 - Documento con los procedimientos de detección y solución de equipos desprotegidos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-4	4	P1	T301 - Crear un sistema de registro estadístico de infecciones por malware para análisis y mejora continua.	RSI y Director de Soporte	E301 - Base de datos e informe con estadísticas de infecciones y análisis de tendencias.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	1	P1	T302 - Definir los mecanismos de respuestas a incidentes.	RSI	E302 - Documento con los mecanismos de respuesta de incidentes.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	1	P1	T303 - Implementar las herramientas para detectar y reportar incidentes.	RSI	E303 - Herramienta de reporte de incidentes.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	1	P1	T304 - Establecer los pasos para informar al CERTuy cuando se detecte un incidente.	RSI	E304 - Documento con los pasos para informar incidentes al CERTuy, incluyendo tiempos de respuesta y contenido de la información a compartir.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	2	P1	T305 - Crear mecanismos para la respuesta a incidentes, especificando roles, responsabilidades, tiempos de respuesta, y acciones a seguir.	RSI	E305 - Documento de mecanismos de respuesta a incidentes.

RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	2	P1	T306 - Crear un plan de difusión de los mecanismos de respuestas a incidentes a los interesados.	RSI y Comunicaciones	E306 - plan de difusión de los mecanismos de respuestas a incidentes.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	2	P1	T307 - Establecer un protocolo para informar a los responsables de la toma de decisiones sobre los incidentes.	RSI	E307 - Informes enviados a los responsables sobre incidentes.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	3	P1	T308 - Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E308 - Política de gestión de incidentes de seguridad de la información.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	3	P1	T309 - Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E309 - Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	3	P1	T310 - (REF. T039) Designar un rol responsable de la gestión de incidentes (RGI).	RSI	E310 - (REF. E039) Resolución con designación del RGI.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	3	P1	T311 - Ajustes al plan de respuesta a incidentes de seguridad de la información.	RSI	E311 - Actualizaciones al plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	3	P1	T312 - Establecer un plan de mejora de los procesos post incidentes que se reflejen en la política y los procedimientos.	RSI	E312 - Plan de mejora de los procesos post incidentes.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	4	P1	T313 - Diseñar y documentar un procedimiento de revisión periódica de los planes y procedimientos de respuesta a incidentes.	RSI	E313 - Procedimiento de revisión periódica de los planes y procedimientos de respuesta a incidentes.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	4	P1	T314 - Implementar un sistema de reportes periódicos de incidentes al Directorio que incluya métricas clave que apoyen la toma de decisiones.	RSI y RGI	E314 - Informes periódicos con métricas y análisis de incidentes y listado de indicadores de rendimiento (KPIs) utilizados.
RESPONDER (RE)	RE.PR	Planificación de la respuesta	RE.PR-1	4	P1	T315 - Generar un informe con las revisiones internas y las lecciones aprendidas para actualizar los planes y procedimientos de respuesta.	RSI	E315 - Informe con revisiones internas y lecciones aprendidas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	1	P2	T451 - (REF. T441) Implementar controles básicos de cifrado en la transferencia de datos (como el uso de HTTPS, SFTP o VPN seguras).	Director de Infraestructura	E451 - (REF. E441) Configuraciones de sistemas y redes que implementan cifrado, registro del uso de HTTPS/SFTP/VPN.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	1	P2	T452 - (REF. T442) Configurar reglas de seguridad en los sistemas de correo electrónico para proteger la información transmitida.	Director de Infraestructura	E452 - (REF. E442) Detalle técnico de la configuración del correo electrónico.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	2	P2	T453 - (REF. T443) Estandarizar las tecnologías y prácticas criptográficas para proteger los datos en tránsito en todas las aplicaciones y sistemas.	Director de Infraestructura	E453 - (REF. E443) Detalle del uso de criptografía estandarizada, listado de aplicaciones/sistemas protegidos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	2	P2	T454 - (REF. T444) Actualizar los procedimientos internos para reflejar las tecnologías y prácticas estándar adoptadas.	Director de Infraestructura	E454 - (REF. E444) Procedimientos actualizados que describan el uso estandarizado de criptografía.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	3	P2	T455 - (REF. T435) Desarrollar una política de uso de controles criptográficos.	CSI	E455 - (REF. E435) Política de uso de controles criptográficos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	3	P2	T456 - (REF. T446) Crear procedimientos para la gestión de claves criptográficas de la información en tránsito.	RSI y Director de Infraestructura	E456 - (REF. E446) Procedimiento para la gestión de claves criptográficas para la información en tránsito.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	3	P2	T457 - (REF. T447) Designar responsables en cada etapa del ciclo de vida de las claves criptográficas para la información en tránsito.	RSI y Director de Infraestructura	E457 - (REF. E447) Lista de responsables designados en la gestión de las claves criptográficas para la información en tránsito.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	4	P2	T458 - (REF. T448) Planificar y ejecutar revisiones periódicas de los controles criptográficos implementados para proteger datos en tránsito.	RSI y Director de Infraestructura	E458 - (REF. E448) Cronograma de controles criptográficos e informes de resultados de revisiones.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	4	P2	T459 - (REF. T449) Registrar los hallazgos de las revisiones, incluyendo los desvíos y las acciones correctivas necesarias.	Director de Infraestructura	E459 - (REF. E449) Registros de hallazgos en controles criptográficos y planes de acción correctiva.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-3	4	P2	T460 - (REF. T450) Informar los resultados de controles criptográficos al RSI.	Director de Infraestructura	E460 - (REF. E450) Reportes de resultados de controles criptográficos enviados al RSI.

IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	1	P2	T316 - Inventariar los equipos portátiles y móviles usados fuera de las instalaciones, junto con las aplicaciones y sistemas instalados.	Director de Soporte	E316 - Inventario actualizado de equipos portátiles y móviles.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	1	P2	T317 - Implementar al menos un factor de autenticación para acceder a la información en los dispositivos.	Director de Infraestructura	E317 - Configuración documentada de los factores de autenticación aplicados en los dispositivos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	1	P2	T318 - Configurar sistemas de borrado remoto para dispositivos móviles en caso de extravío o robo.	Director de Soporte	E318 - Registro de configuraciones de borrado remoto activadas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	1	P2	T319 - Implementar medidas mínimas de protección física en los equipos portátiles (ejemplo: lingas de seguridad).	Director de Soporte	E319 - Documento de adquisición y distribución de medidas físicas de protección.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	2	P2	T320 - Identificar responsables para los activos informáticos utilizados fuera de las instalaciones.	Director de Soporte	E320 - Registro de responsables asignados para cada activo informático.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	2	P2	T321 - Limitar el almacenamiento de información sensible en los activos o aplicar controles adicionales como el cifrado.	Director de Infraestructura	E321 - Documentación sobre la limitación de almacenamiento sensible y detalle de las configuraciones de cifrado aplicadas a los activos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	3	P2	T322 - Desarrollar una política para el uso adecuado de activos.	CSI	E322 - Política de uso aceptable de activos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	3	P2	T323 - Establecer un programa de capacitación para usuarios que utilizan activos fuera de las instalaciones.	RSI y Capacitación	E323 - Materiales de capacitación y Lista de asistencia a las capacitaciones realizadas.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	3	P2	T324 - Realizar controles periódicos de activos con información sensible y definir un plan de respuesta en caso de pérdida o robo.	RSI	E324 - Informes de los controles realizados y Documento del plan de respuesta ante pérdida o robo.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	3	P2	T325 - Implementar doble factor de autenticación en los activos críticos.	Director de Infraestructura	E325 - Registro de configuración del doble factor de autenticación en activos críticos.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	4	P2	T326 - Monitorear proactivamente 7x24 las medidas de protección implementadas en los activos informáticos.	RSI y Director de Infraestructura	E326 - Informes del monitoreo continuo (logs, alertas, reportes de actividades).
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-4	4	P2	T327 - Configurar sistemas de cifrado en los activos con claves únicas a nivel del organismo y claves personales.	RSI y Director de Infraestructura	E327 - Registro de implementación de sistemas de cifrado y detalle de las configuraciones de clave única y personal.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	1	P2	T328 - Identificar los activos (servidores, PC, dispositivos móviles o de almacenamiento) que contienen la información más crítica del organismo.	Director de Soporte y Director de Infraestructura	E328 - Inventario inicial de activos que contienen información crítica.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	2	P2	T329 - Clasificar los activos según los criterios de clasificación de la información establecidos, alineados a la normativa vigente (Ley 18.381 y Ley 18.331).	RSI y Director de TIC	E329 - Clasificación de activos documentada y actualizada en el inventario de activos y procedimiento de clasificación alineado a normativa y criterios de valoración
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	3	P2	T330 - (REF. T008) Desarrollar una política de Uso Aceptable de los Activos Móviles.	CSI	E330 - (REF. E008) Política de Uso Aceptable de Dispositivos Móviles.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	3	P2	T331 - (REF. T009) Documentar los procesos y procedimientos para la actualización del inventario de dispositivos físicos y sistemas.	Director de Desarrollo	E331 - (REF. E009) Manual documentado de procesos y procedimientos de actualización del inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	3	P2	T332 - (REF. T010) Implementar un software de inventario para gestionar y actualizar el inventario de manera centralizada.	Director de Desarrollo	E332 - (REF. E010) Registros de implementación del software de inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	3	P2	T333 - (REF. T011) Automatizar el proceso de actualización del inventario cuando sea posible.	Director de Desarrollo	E333 - (REF. E011) Logs del sistema que evidencien la automatización de actualizaciones.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	3	P2	T334 - Gestionar la clasificación de la información contenida en los activos en el software de inventario.	RSI	E334 - Clasificación de la información de los activos en el software de inventario.
IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	4	P2	T335 - Integrar la clasificación de la información como parte fundamental de la gestión de activos.	RSI	E335 - Procedimiento que describe la integración de la clasificación en la gestión de activos.

IDENTIFICAR (ID)	ID.GA	Gestión de activos	ID.GA-5	4	P2	T336 - Realizar actividades periódicas de control interno para verificar que el inventario de activos esté clasificado y actualizado, o cuando el organismo lo requiera.	RSI	E336 - Informes de los controles internos realizados y registros que muestran actualizaciones en el inventario de activos.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	1	P2	T337 - Definir y realizar actividades de gestión de riesgo en el centro de datos basadas en la experiencia y apreciación del equipo sobre ciberseguridad.	Director de TIC	E337 - Registro de actividades de gestión de riesgo realizadas y documentos con la identificación y evaluación de riesgos específicos del centro de datos.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	2	P2	T338 - (REF. T038) Designar un rol responsable de la gestión de riesgos (RGR).	RSI	E338 - (REF. E038) Resolución con designación del RGR.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	2	P2	T339 - Desarrollar una metodología unificada para la evaluación de riesgos de ciberseguridad en toda el organismo.	RGR	E339 - Metodología documentada de gestión de riesgos (identificación, evaluación, tratamiento, seguimiento y comunicación).
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	2	P2	T340 - Evaluar los riesgos de ciberseguridad en todas las áreas del organismo e incorporar actores críticos para la implementación de controles definidos.	CSI	E340 - Informes de evaluación de riesgos y lista de actores críticos y roles asignados en el proceso de implementación de controles.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	3	P2	T341 - Desarrollar una política de gestión de riesgos de seguridad de la información.	CSI	E341 - Política de Gestión de Riesgos de Seguridad de la Información.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	3	P2	T342 - Centralizar los procedimientos de gestión de riesgos para analizar de forma integral los riesgos de ciberseguridad.	RGR	E342 - Procedimientos centralizados de gestión de riesgos e informes integrales de análisis de riesgos.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	3	P2	T343 - Definir proyectos de seguridad de la información."	RSI	E343 - Listado de proyectos relacionados a la seguridad de la información.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	4	P2	T344 - Alinear la gestión de riesgos con los objetivos del organismo, definiendo métricas e indicadores de cumplimiento organizacional.	CSI y Directorio	E344- Indicadores de seguimiento de riesgos alineados con los objetivos del organismo e informes de métricas y seguimiento del cumplimiento.
IDENTIFICAR (ID)	ID.GO	Gobernanza	ID.GO-4	4	P2	T345 - Retroalimentar el proceso de gestión de riesgos mediante auditorías internas o externas para evitar desviaciones.	RSI y RGR	E345 - Informes de auditoría (interna y externa) y documentación de acciones correctivas implementadas a partir de las auditorías.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	1	P2	T346 - Identificar y actualizar el software de base y aplicaciones críticas con los últimos parches disponibles.	Director de Infraestructura y RGV	E346 - Registro de actualizaciones realizadas en el software y aplicaciones críticas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	1	P2	T347 - Elaborar un inventario de activos que no pueden ser actualizados, detallando las razones y los controles compensatorios implementados."	Director de Infraestructura y RGR	E347 - Inventario de activos no actualizables con detalles de controles compensatorios.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	2	P2	T348 - Implementar y mantener un ambiente de pruebas para verificar los parches antes de su puesta en producción.	Director de Infraestructura y RGV	E348 - Documentación del ambiente de pruebas y su configuración.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	2	P2	T349 - Realizar pruebas de intrusión (ethical hacking) y evaluaciones de vulnerabilidades en sistemas críticos.	RSI y Consultor de Seguridad Externo	E349 - Informe de pruebas de intrusión y evaluación de vulnerabilidades.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	2	P2	T350 - Elaborar y comunicar un informe con los resultados de las pruebas y el plan de acción a las partes interesadas.	RSI	E350 - Plan de acción y registro de comunicación con las partes interesadas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	3	P2	T351 - Documentar un procedimiento formal para la gestión de vulnerabilidades y parches, incluyendo los roles y responsabilidades.	RGV	E351 - Procedimiento documentado de gestión de vulnerabilidades y parches.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	3	P2	T352 - Establecer un calendario para la realización periódica de pruebas de intrusión y escaneos de vulnerabilidades.	Director de Infraestructura y RSI	E352 - Cronograma de escaneos de vulnerabilidades y pruebas de intrusión.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	3	P2	T353 - Realizar escaneos de vulnerabilidades semestrales y pruebas de intrusión anuales en sistemas críticos.	Director de Infraestructura y RGV	E353 - Informes de escaneos de vulnerabilidades y pruebas de intrusión.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	4	P2	T354 - Contratar auditorías independientes periódicas para evaluar el estado de las vulnerabilidades y la efectividad de los controles implementados.	Director de TIC	E354 - Informes de auditorías independientes del estado de las vulnerabilidades.

IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-1	4	P2	T355 - Utilizar los resultados de las auditorías para mejorar el Sistema de Gestión de Seguridad de la Información SGSI.	RSI	E355 - Registro de acciones de mejora aplicadas al SGSI.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	1	P2	T356 - Mantenerse actualizado sobre las últimas amenazas y vulnerabilidades relacionadas con los sistemas y plataformas utilizadas en el organismo.	RSI y Director de Infraestructura	E356 - Registro de las fuentes de información consultadas regularmente.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	1	P2	T357 - Establecer una suscripción a boletines informativos o fuentes confiables sobre ciberseguridad.	RSI y Director de Infraestructura	E357 - Lista de suscripciones activas a boletines informativos o alertas de seguridad.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	2	P2	T358 - Organizar entrenamientos periódicos para el personal de seguridad de la información y TI sobre amenazas y vulnerabilidades.	RSI y Director de Infraestructura	E358 - Calendario de entrenamientos periódicos en seguridad al personal de TI.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	2	P2	T359 - Identificar proveedores de formación en temas de ciberseguridad para la capacitación.	RSI y Director de Infraestructura	E359 - Lista de proveedores de formación en temas de ciberseguridad.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	3	P2	T360 - Implementar un procedimiento de contacto con autoridades internas y externas relevantes (DCSIRT, CERTuy, CSIRT Antel, etc.).	RSI	E360 - Procedimiento de contacto con autoridades de centro de respuesta.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	3	P2	T361 - Incorporar al personal de seguridad de la información en grupos especializados y fomentar su participación en eventos o conferencias de seguridad al menos una vez por año."	RSI y Director de TIC	E361 - Registro de participación en eventos de seguridad del RSI.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	4	P2	T362 - Organizar reuniones periódicas entre el personal de seguridad de la información, el punto de contacto con autoridades, y el equipo de respuesta a incidentes para discutir temas actuales sobre amenazas y vulnerabilidades.	RSI y Director de TIC	E362 - Actas de reuniones periódicas del personal de seguridad con autoridades.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-2	4	P2	T363 - Establecer un mecanismo de comunicación formal para compartir información relevante de manera periódica.	RSI y Director de TIC	E363 - Informes de seguridad compartidas con las partes interesadas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	1	P2	T364 - Identificar las principales amenazas para el organismo y definir controles para mitigarlas.	RSI	E364 - Documento que detalla los controles definidos para mitigar riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	1	P2	T365 - Clasificar los controles implementados como físicos, lógicos o administrativos.	RSI y Director de TIC	E365 - Clasificación de los controles por tipo (físico, lógico o administrativo).
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	2	P2	T366 - Incorporar las respuestas a los riesgos en el inventario de riesgos de seguridad de la información.	RSI y RGR	E366 - Inventario de riesgos actualizado con las respuestas a los riesgos identificados.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	2	P2	T367 - Identificar riesgos de seguridad de la información fuera del alcance del centro de datos y documentar las respuestas correspondientes.	RGR	E367 - Documentación de los riesgos fuera del alcance del centro de datos y las medidas implementadas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	3	P2	T368 - Revisar las respuestas a los riesgos con una frecuencia semestral.	RGR	E368 - Informes semestrales de revisión de respuestas a riesgos.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	3	P2	T369 - Documentar formalmente las revisiones realizadas y comunicarlas al CSI y otras partes interesadas.	RSI	E369 - Registro de comunicación de las revisiones al CSI y partes interesadas.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	4	P2	T370 - Asegurar que la implementación de controles se realice según las prioridades establecidas por el Directorio.	RSI y Directorio	E370 - Registro de prioridades formales establecidas por la Dirección.
IDENTIFICAR (ID)	ID.ER	Evaluación de riesgos	ID.ER-6	4	P2	T371 - Coordinar la gestión de riesgos con el RSI, los propietarios de activos de información, y el CSI.	RSI y RGR	E371 - Actas de coordinación entre RSI, propietarios de activos y el CSI.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	1	P2	T372 - Identificar los riesgos inherentes para los activos en el centro de datos que soportan servicios críticos.	RSI y RGR	E372 - Documento que describe los riesgos inherentes identificados, alineados a los activos del centro de datos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	2	P2	T373 - Realizar un análisis de impacto del negocio (BIA) enfocado en el área de TIC.	RSI y Director de TIC	E373 - Informe BIA específico para TIC que incluye identificación de umbrales de tolerancia.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	2	P2	T374 - Establecer los umbrales de tolerancia al riesgo para los servicios tecnológicos.	CSI	E374 - Documento con los umbrales de tolerancia definidos para TIC.

IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	3	P2	T375 - Ajustar los acuerdos de nivel de servicio (SLAs) con los proveedores según la gestión de riesgo definida.	Director de TIC	E375 - Contratos actualizados con SLAs ajustados a los parámetros de riesgo.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	3	P2	T376 - Definir tolerancia al riesgo para los procesos críticos de todo el organismo.	CSI	E376 - Documento consolidado con tolerancia al riesgo para procesos críticos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	3	P2	T377 - Actualizar la metodología de gestión de riesgo para incluir criterios de RTO y RPO.	CSI	E377 - Metodología de gestión de riesgos con criterios de RTO y RPO.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	4	P2	T378 - Implementar un proceso de revisión periódica de la tolerancia al riesgo.	RGR y Alta Dirección	E378 - Registros de revisiones de tolerancia al riesgo.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-2	4	P2	T379 - Asegurar la aprobación de la tolerancia establecida por todas las partes interesadas.	CSI	E379 - Resolución de aprobación de la tolerancia establecida.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	1	P2	T380 - Identificar los servicios críticos que puedan afectar a otras organizaciones interconectadas con evaluación de riesgos.	CSI y RGR	E380 - Documento que identifica servicios críticos, su interdependencia con otras organizaciones y evaluación de riesgos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	2	P2	T381 - (REF. T373) Realizar un análisis de impacto del negocio (BIA) enfocado en el área de TIC.	RSI y Director de TIC	E381 - (REF. E373) Informe BIA específico para TIC que incluye identificación de umbrales de tolerancia.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	2	P2	T382 - (REF. T374) Establecer los umbrales de tolerancia al riesgo para los servicios tecnológicos.	CSI	E382 - (REF. E374) Documento con los umbrales de tolerancia definidos para TIC.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	3	P2	T383 - (REF. T375) Ajustar los acuerdos de nivel de servicio (SLAs) con los proveedores según la gestión de riesgo definida.	Director de TIC	E383 - (REF. E375) Contratos actualizados con SLAs ajustados a los parámetros de riesgo.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	3	P2	T384 - (REF. T376) Definir tolerancia al riesgo para los procesos críticos de todo el organismo.	CSI	E384 - (REF. E376) Documento consolidado con tolerancia al riesgo para procesos críticos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	3	P2	T385 - (REF. T377) Actualizar la metodología de gestión de riesgo para incluir criterios de RTO y RPO.	CSI	E385 - (REF. E377) Metodología de gestión de riesgos con criterios de RTO y RPO.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	4	P2	T386 - (REF. T378) Implementar un proceso de revisión periódica de la tolerancia al riesgo.	RGR y Alta Dirección	E386 - (REF. E378) Registros de revisiones de tolerancia al riesgo.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-3	4	P2	T387 - (REF. T379) Asegurar la aprobación de la tolerancia establecida por todas las partes interesadas.	CSI	E387 - (REF. E379) Resolución de aprobación de la tolerancia establecida.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	1	P2	T388 - Crear un inventario de proveedores, identificando su rol en la cadena de suministro de servicios críticos.	Alta Dirección	E388 - Lista de proveedores con descripción de su participación en los servicios críticos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	1	P2	T389 - Establecer un proceso de adquisición que incluya requisitos mínimos de seguridad de la información.	CSI	E389 - Documentación del proceso de adquisición con requisitos mínimos de seguridad.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	2	P2	T390 - Comunicar a los proveedores su participación en los objetivos del organismo, definiendo roles y responsabilidades.	Director de TIC	E390 - Notificaciones enviadas a los proveedores con roles y responsabilidades definidos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	2	P2	T391 - Actualizar los contratos y SLA con los proveedores para incluir políticas y medidas de seguridad pertinentes.	RSI y Director de TIC	E391 - Contratos actualizados y acuerdos SLA con cláusulas de seguridad incluidas.

IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	3	P2	T392 - Desarrollar una política de gestión de proveedores.	CSI	E392 - Política de Gestión de Proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	3	P2	T393 - Implementar un proceso para gestionar cambios de proveedores conforme a las necesidades del organismo.	RSI y Director de Desarrollo	E393 - Registros de gestión de cambios de proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	3	P2	T394 - Realizar revisiones periódicas de los SLA y gestionar cualquier desvío detectado.	RSI y Director de Desarrollo	E394 - Registro de revisiones regulares y reportes de desvíos gestionados.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	4	P2	T395 - Planificar y ejecutar auditorías periódicas a los proveedores para evaluar su cumplimiento con los SLA y las políticas de seguridad.	RSI y Director de Desarrollo	E395 - Informes de auditoría de proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-3	4	P2	T396 - Ajustar los servicios de los proveedores en función de los resultados de las auditorías y las necesidades del organismo.	Director de TIC	E396 - Documentación de ajustes realizados a los servicios de los proveedores.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	1	P2	T397 - Diseñar e implementar un proceso de evaluación del desempeño de proveedores críticos basado en los contratos establecidos.	CSI	E397 - Documento del proceso de evaluación de proveedores y registros de evaluaciones realizadas.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	2	P2	T398 - Establecer un calendario de reuniones periódicas con proveedores para evaluar su desempeño.	RSI y Director de TIC	E398 - Agenda de reuniones periódicas y actas de reuniones realizadas.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	2	P2	T399 - Registrar desvíos identificados en el desempeño de los proveedores y proponer acciones correctivas.	RSI y Director de TIC	E399 - Reporte de desvíos y plan de acciones correctivas con seguimiento.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	3	P2	T400 - Actualizar la política de seguridad de la información para incluir auditorías externas independientes a proveedores críticos.	CSI	E400 - Ajustes en Política de seguridad de la información para incluir auditorías externas.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	3	P2	T401 - Implementar auditorías externas a proveedores críticos, identificando desvíos y generando planes de acción correctivos.	RSI	E401 - Informes de auditoría externa y planes de acción correctivos priorizados.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	3	P2	T402 - Priorizar y asignar plazos a las acciones correctivas, alineados a las necesidades del organismo.	RGR	E402 - Registro de acciones correctivas priorizadas con plazos definidos.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	4	P2	T403 - Establecer un cronograma regular de auditorías externas basado en el apetito de riesgo.	CSI	E403 - Cronograma de auditorías aprobado y cumplido.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	4	P2	T404 - Implementar un sistema de monitoreo permanente de servicios críticos de los proveedores.	Director de TIC	E404 - Reportes periódicos generados por el sistema de monitoreo.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-4	4	P2	T405 - Revisar la efectividad de los planes de acción correctivos y ajustar los SLA conforme a los resultados y necesidades del organismo.	RSI y RGR	E405 - Informes de seguimiento de planes de acción y documentación de ajustes realizados a los SLA.

PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	1	P2	T406 - Implementar comunicaciones seguras para el acceso remoto (por ejemplo, VPN con cifrado).	Director de Infraestructura	E406 - Configuración activa de comunicaciones seguras para acceso remoto.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	1	P2	T407 - Establecer mecanismos de autenticación seguros para el acceso remoto.	Director TIC	E407 - Documentación de los mecanismos de autenticación utilizados para el acceso remoto.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	2	P2	T408 - Implementar acuerdos de no divulgación para el personal y proveedores con acceso remoto.	Director TIC y RRHH	E408 - Acuerdos de no divulgación firmados para personal y proveedores con acceso remoto.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	2	P2	T409 - Crear y mantener una lista blanca de recursos disponibles para acceso remoto.	Director TIC	E409 - Listado actualizado de recursos autorizados para acceso remoto.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	2	P2	T410 - Revisar periódicamente los acuerdos de no divulgación para garantizar su vigencia y adecuación.	RSI	E410 - Evidencia de revisiones realizadas de acuerdos de no divulgación.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	3	P2	T411 - Documentar y publicar un procedimiento formal para solicitar acceso remoto.	RSI	E411 - Procedimiento documentado y aprobado para solicitar acceso remoto.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	3	P2	T412 - Designar un responsable para la gestión y asignación de permisos de acceso remoto.	Director de TIC	E412 - Registro del responsable asignado para gestión de acceso remoto y de sus actividades.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	3	P2	T413 - Configurar permisos temporales para proveedores con acceso remoto.	Director de Infraestructura	E413 - Registro de accesos remoto temporales otorgados y su vencimiento.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	3	P2	T414 - Implementar doble factor de autenticación para el acceso remoto.	Director de Infraestructura	E414 - Configuración activa de doble factor de autenticación.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	3	P2	T415 - Centralizar la gestión del acceso remoto, al menos desde el punto de vista administrativo.	Director de TIC	E415 - Documentación que detalle la centralización del acceso remoto.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	4	P2	T416 - Establecer y ejecutar revisiones periódicas de los usuarios con acceso remoto y sus registros de actividad.	Director de Infraestructura	E416 - Informes de revisiones periódicas realizadas de acceso remoto y registro de actividad.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-3	4	P2	T417 - Definir actividades de control para verificar el cumplimiento de los procedimientos de acceso remoto.	RSI	E417 - Resultados documentados de controles internos para verificar el cumplimiento de los procedimientos de acceso remoto.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	1	P2	T418 - Segmentar la red en al menos dos dominios básicos: red privada y red externa.	Director de Infraestructura	E418 - Configuración activa que demuestre la segmentación de red básica.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	1	P2	T419 - Actualizar y mantener un diagrama de red detallado que refleje la segmentación existente.	Director de Infraestructura	E419 - Diagrama actualizado de la red que refleje la segmentación de red.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	2	P2	T420 - Identificar y documentar los dominios de red según las necesidades del organismo (por ejemplo, redes de usuarios, redes de servidores, redes críticas).	Director de Infraestructura	E420 - Documento que detalle los dominios de red definidos.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	2	P2	T421 - Definir e implementar reglas de manejo de tráfico entre segmentos (permitir, denegar, registrar).	Director de Infraestructura	E421 - Configuraciones de manejo de tráfico documentadas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	2	P2	T422 - Alinear el organigrama y roles del organismo con la segregación de redes, destacando las funciones críticas.	RSI y Director de Infraestructura	E422 - Organigrama actualizado con funciones relacionadas con la segmentación de red.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	3	P2	T423 - Configurar monitoreo del tráfico en los diferentes dominios de red para análisis continuo.	Director de Infraestructura	E423 - Registros de tráfico analizados periódicamente.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	3	P2	T424 - Implementar controles de detección de amenazas en los diferentes segmentos de red.	Director de Infraestructura	E424 - Configuración activa de controles de detección de amenazas.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	3	P2	T425 - Definir y configurar alertas automáticas cuando se detecte tráfico no autorizado.	Director de Infraestructura	E425 - Logs y configuraciones de alertas generadas de tráfico no autorizado.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	3	P2	T426 - Documentar un procedimiento de contención de incidentes en los segmentos de red.	RGI y Director de Infraestructura	E426 - Procedimiento aprobado de contención de incidentes en segmentos de red.

PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	4	P2	T427 - Establecer un procedimiento formal de monitoreo continuo de los segmentos de red, apoyado por herramientas automatizadas.	Director de Infraestructura	E427 - Procedimiento formalizado y configuraciones de herramientas automatizadas para monitoreo de red.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	4	P2	T428 - Alinear el procedimiento de contención de incidentes con la política general de gestión de incidentes.	RGI	E428 - Procedimiento de contención de incidentes de red con la política general de gestión de incidentes.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	4	P2	T429 - Registrar incidentes detectados en los segmentos de red y documentar lecciones aprendidas.	RGI y Director de Infraestructura	E429 - Base de datos de incidentes en los segmentos de red y reportes de mejora continua.
PROTEGER (PR)	PR.CA	Control de acceso	PR.CA-5	4	P2	T430 - Realizar controles internos para garantizar que las revisiones y contenciones de incidentes se realicen según lo planificado.	RGI y Director de Infraestructura	E430 - Informes de auditoría y cumplimiento de controles internos de segmentos de red.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	1	P2	T431 - Identificar y clasificar los datos históricos y respaldos críticos para el organismo.	Director de Infraestructura	E431 - Listado de datos históricos y respaldos clasificados como críticos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	1	P2	T432 - Implementar mecanismos básicos de control de acceso físico y lógico para proteger los respaldos.	Director de Infraestructura	E432 - Registros de acceso físico (bitácoras) y configuraciones de acceso lógico.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	2	P2	T433 - Implementar cifrado para el almacenamiento de datos históricos y respaldos offline.	Director de Infraestructura	E433 - Configuración de las soluciones de respaldo que incluye cifrado y listado de respaldos cifrados.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	2	P2	T434 - Verificar la implementación del cifrado mediante una prueba de restauración de datos cifrados.	Director de Infraestructura	E434 - Informe de prueba de restauración exitosas de datos cifrados.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	3	P2	T435 - Desarrollar una política de uso de controles criptográficos.	CSI	E435 - Política de uso de controles criptográficos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	3	P2	T436 - Crear procedimientos para la gestión de claves criptográficas para respaldos.	RSI y Director de Infraestructura	E436 - Procedimiento para la gestión de claves criptográficas para respaldos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	3	P2	T437 - Designar responsables en cada etapa del ciclo de vida de las claves criptográficas para respaldos.	RSI y Director de Infraestructura	E437 - Lista de responsables designados en la gestión de las claves criptográficas para respaldos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	4	P2	T438 - Planificar y ejecutar revisiones periódicas sobre los respaldos y datos históricos almacenados.	RSI y Director de Infraestructura	E438 - Cronograma de revisiones sobre los respaldos y datos históricos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	4	P2	T439 - Registrar los resultados de las revisiones, incluyendo hallazgos y acciones correctivas en caso de incumplimientos.	Director de Infraestructura	E439 - Registros de resultados de revisiones sobre los respaldos y plan de acciones correctivas en caso de desvíos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-1	4	P2	T440 - Informar los resultados de las revisiones al RSI.	Director de Infraestructura	E440 - Reportes de revisiones sobre respaldos enviados al RSI.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	1	P2	T441 - Implementar controles básicos de cifrado en la transferencia de datos (como el uso de HTTPS, SFTP o VPN seguras).	Director de Infraestructura	E441 - Configuraciones de sistemas y redes que implementan cifrado, registro del uso de HTTPS/SFTP/VPN.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	1	P2	T442 - Configurar reglas de seguridad en los sistemas de correo electrónico para proteger la información transmitida.	Director de Infraestructura	E442 - Detalle técnico de la configuración del correo electrónico.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	2	P2	T443 - Estandarizar las tecnologías y prácticas criptográficas para proteger los datos en tránsito en todas las aplicaciones y sistemas.	Director de Infraestructura	E443 - Detalle del uso de criptografía estandarizada, listado de aplicaciones/sistemas protegidos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	2	P2	T444 - Actualizar los procedimientos internos para reflejar las tecnologías y prácticas estándar adoptadas.	RSI y Director de Infraestructura	E444 - Procedimientos actualizados que describan el uso estandarizado de criptografía.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	3	P2	T445 - (REF. R435) - Desarrollar una política de uso de controles criptográficos.	CSI	E445 - (REF. E435) Política de uso de controles criptográficos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	3	P2	T446 - Crear procedimientos para la gestión de claves criptográficas de la información en tránsito.	RSI y Director de Infraestructura	E446 - Procedimiento para la gestión de claves criptográficas para la información en tránsito.

PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	3	P2	T447 - Designar responsables en cada etapa del ciclo de vida de las claves criptográficas para la información en tránsito.	RSI y Director de Infraestructura	E447 - Lista de responsables designados en la gestión de las claves criptográficas para la información en tránsito.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	4	P2	T448 - Planificar y ejecutar revisiones periódicas de los controles criptográficos implementados para proteger datos en tránsito.	RSI y Director de Infraestructura	E448 - Cronograma de controles criptográficos e informes de resultados de revisiones.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	4	P2	T449 - Registrar los hallazgos de las revisiones, incluyendo los desvíos y las acciones correctivas necesarias.	Director de Infraestructura	E449 - Registros de hallazgos en controles criptográficos y planes de acción correctiva.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-2	4	P2	T450 - Informar los resultados de controles criptográficos al RSI.	Director de Infraestructura	E450 - Reportes de resultados de controles criptográficos enviados al RSI.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	1	P2	T461 - Establecer pautas iniciales para la eliminación y borrado seguro de medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E461 - Documento con pautas iniciales sobre borrado seguro de medios de almacenamiento.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	1	P2	T462 - Informar al personal sobre la importancia de la eliminación segura de medios para proteger la confidencialidad de la información.	Director de Soporte y Director de Infraestructura	E462 - Listado de asistentes a capacitación sobre la importancia de la eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	2	P2	T463 - Establecer puntos designados para la disposición y eliminación de medios de almacenamiento.	RSI y Director de Infraestructura	E463 - Listado de puntos designados para la eliminación de medios de almacenamiento.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	2	P2	T464 - Implementar actividades coordinadas para el borrado seguro o disposición de los medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E464 - Registros de actividades realizadas sobre borrado seguro de medios de almacenamiento.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	3	P2	T465 - Desarrollar una política de destrucción de la información.	CSI	E465 - Política de destrucción de información.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	3	P2	T466 - Elaborar un procedimiento para la eliminación segura de medios de almacenamiento alineado con la política.	Director de Soporte y Director de Infraestructura	E466 - Procedimiento sobre eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	3	P2	T467 - Capacitar al personal involucrado en la aplicación del procedimiento para eliminación segura de medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E467 - Capacitaciones de procedimiento sobre eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	4	P2	T468 - Realizar auditorías internas periódicas para verificar el cumplimiento de los procedimientos de eliminación de medios y los puntos de disposición definidos.	RSI	E468 - Informes de auditorías realizadas para el cumplimiento de los procedimientos sobre eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	4	P2	T469 - Registrar desvíos identificados en las auditorías y definir acciones correctivas.	RSI	E469 - Registro de desvíos detectados en la eliminación segura de medios de almacenamiento y planes de acción correctiva documentados.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-3	4	P2	T470 - Informar los resultados de las auditorías y acciones correctivas al RSI.	RSI	E470 - Reportes de desvíos detectados en eliminación segura de medios de almacenamiento enviados al RSI.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	1	P2	T471 - Implementar acuerdos de no divulgación básicos para nuevos proveedores y personal.	Director de Legales y RRHH	E471 - Plantillas de Acuerdos de no divulgación para personal y proveedores.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	1	P2	T472 - Garantizar la firma de los acuerdos como parte del proceso de incorporación.	RRHH	E472 - Lista de personal con Acuerdos de no divulgación firmados.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	2	P2	T473 - Identificar y categorizar el personal que no han firmado acuerdos de no divulgación.	RRHH	E473 - Listado completo de personal que no tenga firmado Acuerdos no divulgación.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	2	P2	T474 - Identificar y categorizar los proveedores que no han firmado acuerdos de no divulgación.	Director de TIC	E474 - Listado completo de proveedores que no tenga firmado Acuerdos no divulgación.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	2	P2	T475 - Plan para que el personal que no cuenta con Acuerdos de no divulgación firmado lo firme.	RRHH	E475 - Cronograma de implementación del plan para que el personal firme el Acuerdo de no divulgación.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	2	P2	T476 - Plan para que los proveedores que no cuenta con Acuerdos de no divulgación firmado lo firmen.	Director de TIC	E476 - Cronograma de implementación del plan para que los proveedores firmen el Acuerdo de no divulgación.

PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	2	P2	T477 - Realizar campañas de concientización sobre la importancia de los Acuerdos de no divulgación .	RSI y Capacitación	E477 - Materiales de comunicación utilizados. Registros de participación en sesiones informativas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	3	P2	T478 - Actualizar acuerdos contractuales para reflejar responsabilidades según roles específicos.	RRHH y Director de Legales	E478 - Nuevos modelos de contratos que incluyan responsabilidades de seguridad para roles críticos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	3	P2	T479 - Documentar un procedimiento de desvinculación robusto.	RRHH y Director de Legales	E479 - Procedimiento documentado que incluya revocación de accesos físicos y lógicos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	3	P2	T480 - Implementar un sistema DLP (Data Loss Prevention) para proteger los datos sensibles.	Director de TIC	E480 - Detalles técnicos del sistema DLP (Data Loss Prevention) implementado.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	4	P2	T481 - Establecer un cronograma de revisión periódica de contratos y procedimientos de desvinculación.	Director de TIC	E481 - Cronograma de revisiones de procedimientos de desvinculación.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	4	P2	T482 - Implementar un sistema de registro para monitorear y reportar desvíos e incumplimientos.	RSI	E482 - Registros de desvíos detectados en procedimientos de desvinculación y acciones correctivas implementadas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	4	P2	T483 - Incorporar resultados de revisiones en planes de mejora continua.	RSI y Director de TIC	E483 - Documentación de mejoras en procedimientos de procedimientos de desvinculación.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-5	4	P2	T484 - Reportar hallazgos y resultados de revisiones a partes interesadas.	RSI	E484 - Reportes enviados a las áreas interesadas sobre procedimientos de desvinculación.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	1	P2	T485 - Verificar la separación de los entornos de producción y no producción.	Director de Infraestructura	E485 - Documentación de los ambientes existentes (diagramas de arquitectura, descripción de la infraestructura).
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	1	P2	T486 - Confirmar que los entornos de producción solo se utilizan para aplicaciones críticas.	Director de Infraestructura	E486 - Listado de sistemas en producción y aplicaciones críticas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	2	P2	T487 - Definir plataformas separadas para cada fase del ciclo de vida de desarrollo.	Director de Infraestructura	E487 - Documentación de las plataformas de desarrollo, pruebas y producción, detallando sus características.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	2	P2	T488 - Establecer controles para la transición entre ambientes (desarrollo, pruebas, producción).	Director de Infraestructura y Director de Desarrollo	E488 - Procedimiento para el pasaje a producción y listado de solicitudes de cambio aprobadas con su impacto en los ambientes.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	2	P2	T489 - Implementar un procedimiento de pruebas para asegurar el control del ciclo de vida de los entornos.	Director de Desarrollo	E489 - Procedimiento o metodología de pruebas y registro de cambios realizados.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	3	P2	T490 - Desarrollar una política de separación de entornos.	CSI	E490 - Política de separación de entornos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	3	P2	T491 - Crear un procedimiento documentado para la gestión de los entornos y los pasajes entre ellos.	Director de Desarrollo	E491 - Procedimientos para el pasaje a producción.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	3	P2	T492 - Designar responsables para la gestión de entornos y pasajes a producción.	Director de Desarrollo	E492 - Documento de asignación de responsabilidades y funciones.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	3	P2	T493 - Mantener la información registrada durante las pruebas para asegurar la calidad y replicabilidad.	Director de Desarrollo	E493 - Registro de información de los entornos de pruebas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	4	P2	T494 - Involucrar a los responsables de la gestión de entornos en la planificación y ejecución de los proyectos desde el inicio.	Director de TIC	E494 - Actas de reuniones de planificación de proyectos donde se documenta la participación de los responsables de entornos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	4	P2	T495 - Asegurar que la clasificación de la información se maneje adecuadamente durante las pruebas.	RSI y Director de Desarrollo	E495 - Documentación sobre la clasificación y manejo de la información durante las pruebas de separación de entorno.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	4	P2	T496 - Implementar auditorías de cumplimiento sobre la política de separación de entornos y procedimientos relacionados.	RSI	E496 - Informes de auditoría interna sobre cumplimiento de la política de separación de entornos.

PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-7	4	P2	T497 - Reportes de seguimiento de la implementación de acciones correctivas para el cumplimiento sobre la política de separación de entornos.	RSI y Director de Desarrollo	E497 - Registro de acciones correctivas derivadas de auditorías sobre cumplimiento de la política de separación de entornos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	1	P2	T498 - Definir lineamientos generales de desarrollo seguro.	RSI y Director de Desarrollo	E498 - Pautas iniciales de desarrollo seguro.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	1	P2	T499 - Establecer un proceso básico de gestión de proyectos con principios de seguridad.	RSI y Director de Desarrollo	E499 - Documentación de la metodología básica de gestión de proyectos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	1	P2	T500 - Involucrar a los usuarios en el ciclo de vida de los sistemas, ya sea directamente o a través de un rol representante.	Alta dirección	E500 - Actas o registros de la participación de usuarios en proyectos específicos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	2	P2	T501 - Incorporar requisitos de seguridad en la especificación de los proyectos.	RSI y Director de Desarrollo	E501 - Metodología de desarrollo que contemple seguridad y evidencia de su revisión periódica.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	2	P2	T502 - Establecer principios de desarrollo seguro en los sistemas.	RSI y Director de Desarrollo	E502 - Listado de proyectos y aplicaciones desarrolladas o adquiridas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	2	P2	T503 - Implementar un sistema de control de versiones para el software.	Director de Desarrollo	E503 - Muestras de versionado de archivos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	2	P2	T504 - Sistematizar las actividades de prueba en el desarrollo.	Director de Desarrollo	E504 - Listado de actividades sistematizadas de pruebas de desarrollo.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	3	P2	T505 - Definir un procedimiento documentado de pruebas que involucre a los usuarios.	Director TIC	E505 - Procedimiento documentado de pruebas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	3	P2	T506 - Establecer criterios de aceptación para los productos desarrollados o adquiridos.	Director TIC	E506 - Criterios de aceptación definidos para proyectos seleccionados.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	4	P2	T507 - Realizar actividades de control interno para evaluar el cumplimiento de la metodología y los procedimientos definidos.	Director de Desarrollo	E507 - Informes de auditorías internas sobre cumplimiento de metodología y procedimientos de desarrollo.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la	PR.PI-2	4	P2	T508 - Implementar acciones correctivas frente a desvíos identificados en la metodología de desarrollo.	Director de Desarrollo	E508 - Registro de acciones correctivas implementadas para cumplimiento de la metodología y los procedimientos en el desarrollo.

		protección de la información						
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-2	4	P2	T509 - Comunicar los resultados de las evaluaciones de cumplimiento de la metodología y los procedimientos al RSI.	Director de Desarrollo	E509 - Comunicación al RSI los resultados de las evaluaciones de cumplimiento de la metodología y los procedimientos en el desarrollo.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	1	P2	T510 - Establecer medidas básicas para comunicar y autorizar los cambios en el ámbito tecnológico.	RSI y Director de Desarrollo	E510 - Documentos o registros de comunicación y autorización de cambios.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	1	P2	T511 - Asegurar que los cambios sean registrados y documentados de manera general.	Director de Desarrollo	E511 - Listado inicial de cambios realizados durante el período.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	2	P2	T512 - Definir procesos formales de versionado para los productos de software.	Director de Desarrollo	E512 - Procedimiento formal para el versionado.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	2	P2	T513 - Establecer líneas base de configuración para permitir la trazabilidad de los cambios.	Director de Desarrollo y RSI	E513 - Registros de líneas base de configuración y trazabilidad de cambios. Herramientas utilizadas para el control de versiones.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	3	P2	T514 - Desarrollar una política de gestión de cambios.	CSI	E514 - Política de Gestión de Cambio.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	3	P2	T515 - Definir un procedimiento de gestión de cambios y asegurar su implementación.	RSI y Director de Desarrollo	E515 - Listado (muestra) de cambios en el período auditado y listado de cambios de emergencia.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	3	P2	T516 - Registrar todos los cambios realizados a las líneas base.	Director de Desarrollo	E516 - Evidencia de análisis de riesgos, autorización, aprobación y registro de cambios.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	4	P2	T517 - Implementar herramientas automatizadas que apoyen la gestión de los cambios.	Director de Desarrollo	E517 - Herramientas utilizadas para la gestión de cambios.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	4	P2	T518 - Realizar actividades de control interno para revisar el cumplimiento de los procedimientos de gestión de cambios.	Director de Desarrollo	E518 - Resultados de revisiones internas sobre cumplimiento de procedimientos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	4	P2	T519 - Comunicar los resultados de las revisiones al RSI y partes interesadas.	Director de Desarrollo	E519 - Comunicaciones dirigidas al RSI y partes interesadas.

PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-3	4	P2	T520 - Tomar medidas correctivas frente a desvíos y utilizar los resultados para mejora continua.	RSI y Director de Desarrollo	E520 - Registro de acciones correctivas y lecciones aprendidas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	1	P2	T521 - Implementar medidas básicas de control del medio ambiente físico en los centros de datos y áreas relacionadas.	Director de Infraestructura	E521 - Habilitación de bomberos, cContratos con proveedores (alarmas, aire acondicionado, etc.).
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	1	P2	T522 - Asegurar que las áreas críticas cuenten con protecciones ambientales mínimas (alarmas, extintores, aire acondicionado, etc.).	Director de Infraestructura	E522 - Protección ambiental (alarma, extintores, sistemas de extinción, aire acondicionado, etc.), ubicación de la sala de cómputo y la sala de energía.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	2	P2	T523 - Implementar herramientas automatizadas para el monitoreo de los controles relacionados al medio ambiente físico.	Director de Infraestructura	E523 - Herramientas utilizadas para el monitoreo. Procedimiento de monitoreo.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	2	P2	T524 - Asegurar que las herramientas permitan la detección de fallas en componentes críticos.	Director de Infraestructura	E524 - Plan de mantenimiento de componentes críticos. Reportes de fallas y alertas dentro del período auditado.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	3	P2	T525 - Desarrollar una política de seguridad del equipamiento.	CSI	E525 - Política de seguridad del equipamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	3	P2	T526 - Desarrollar un procedimiento de monitoreo que contemple el uso de herramientas automatizadas.	Director de Infraestructura y RM	E526 - Procedimiento de monitoreo que contemple herramientas automatizadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	3	P2	T527 - Implementar controles de cambio para las actividades de mantenimiento en componentes críticos.	Director de Infraestructura	E527 - Registro del mantenimiento histórico de los valores monitoreados dentro del período auditado. Documentación de controles de cambio relacionados con el mantenimiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	4	P2	T528 - Realizar actividades de control interno para verificar el cumplimiento de la política de seguridad del equipamiento y procedimientos de monitoreo.	RSI y Director de Infraestructura	E528 - Evidencia de revisión de fallas y alertas dentro del período auditado.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	4	P2	T529 - Analizar los resultados del monitoreo para mejorar los procedimientos y retroalimentar con lecciones aprendidas.	RSI y Director de Infraestructura	E529 - Acciones correctivas implementadas basadas en resultados del monitoreo y registro de lecciones aprendidas para mejora continua.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-5	4	P2	T530 - Establecer procesos para reportar los resultados a las partes interesadas.	RSI	E530 - Reportes de resultados de monitoreo enviados a partes interesadas.

PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	1	P2	T531 - (REF. T461) Establecer pautas iniciales para la eliminación y borrado seguro de medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E531 - (REF. E461) Documento con pautas iniciales sobre borrado seguro de medios de almacenamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	1	P2	T532 - (REF. T462) Informar al personal sobre la importancia de la eliminación segura de medios para proteger la confidencialidad de la información.	Director de Soporte y Director de Infraestructura	E532 - (REF. E462) Listado de asistentes a capacitación sobre la importancia de la eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	2	P2	T533 - (REF. T463) Establecer puntos designados para la disposición y eliminación de medios de almacenamiento.	RSI y Director de Infraestructura	E533 - (REF. E463) Listado de puntos designados para la eliminación de medios de almacenamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	2	P2	T534 - (REF. T464) Implementar actividades coordinadas para el borrado seguro o disposición de los medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E534 - (REF. E464) Registros de actividades realizadas sobre borrado seguro de medios de almacenamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	3	P2	T535 - (REF. T465) Desarrollar una política de destrucción de la información.	CSI	E535 - (REF. E465) Política de destrucción de información.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	3	P2	T536 - (REF. T466) Elaborar un procedimiento para la eliminación segura de medios de almacenamiento alineado con la política.	Director de Soporte y Director de Infraestructura	E536 - (REF. E466) Procedimiento sobre eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	3	P2	T537 - (REF. T467) Capacitar al personal involucrado en la aplicación del procedimiento para eliminación segura de medios de almacenamiento.	Director de Soporte y Director de Infraestructura	E537 - (REF. E467) Capacitaciones de procedimiento sobre eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	4	P2	T538 - (REF. T468) Realizar auditorías internas periódicas para verificar el cumplimiento de los procedimientos de eliminación de medios y los puntos de disposición definidos.	RSI	E538 - (REF. E468) Informes de auditorías realizadas para el cumplimiento de los procedimientos sobre eliminación segura de medios de almacenamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	4	P2	T539 - (REF. T469) Registrar desvíos identificados en las auditorías y definir acciones correctivas.	RSI	E539 - (REF. E469) Registro de desvíos detectados en la eliminación segura de medios de almacenamiento y planes de acción correctiva documentados.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-6	4	P2	T540 - (REF. T470) Informar los resultados de las auditorías y acciones correctivas al RSI.	RSI	E540 - (REF. E470) Reportes de desvíos detectados en eliminación segura de medios de almacenamiento enviados al RSI.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	1	P2	T541 - Instruir al personal sobre los mecanismos de reporte de incidentes.	RSI y Capacitación	E541 - Registros de capacitaciones sobre mecanismos de reporte de incidentes.
PROTEGER (PR)	PR.PI	Procesos y procedimientos	PR.PI-9	1	P2	T542 - Establecer lineamientos para el reporte interno de incidentes.	RSI y RGI	E542 - Documentación de lineamientos para el reporte interno de incidentes.

		para la protección de la información						
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	1	P2	T543 - Registrar los incidentes de seguridad reportados.	RGI	E543 - Listado de incidentes reportados y registrados.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	1	P2	T544 - Implementar medidas básicas de contingencia y recuperación para sistemas que soportan servicios críticos.	RGI y Director de Infraestructura	E544 - Documentación de medidas básicas de contingencia y recuperación para servicios críticos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	2	P2	T545 - Identificar los procesos críticos del organismo.	RSI	E545 - Listado de procesos críticos del organismo.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	2	P2	T546 - Establecer herramientas básicas para apoyar la gestión de incidentes.	Director de TIC	E546 - Herramientas implementadas para la gestión de incidentes.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	2	P2	T547 - Implementar medidas adicionales de contingencia y recuperación.	RSI	E547 - Documentación de medidas de contingencia adicionales.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	3	P2	T548 - (REF. T308) Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E548 - (REF. E308) Política de gestión de incidentes.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	3	P2	T549 - (REF. T309) Ajustar el plan de respuesta a la política de gestión de incidentes.	RGI	E549 - (REF. E309) Plan de respuesta a incidentes.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	3	P2	T550 - Diseñar un plan de contingencia y de recuperación para los sistemas críticos.	RSI y Director de Infraestructura	E550 - Plan de contingencia y recuperación documentado.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	3	P2	T551 - Realizar pruebas puntuales de los planes diseñados.	RSI	E551 - Resultados de las pruebas puntuales realizadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	4	P2	T552 - Designar responsables específicos para la respuesta a incidentes y el mantenimiento de los planes de contingencia y recuperación.	CSI	E552 - Listado de responsables designados para la respuesta a incidentes y el mantenimiento de los planes de contingencia y recuperación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la	PR.PI-9	4	P2	T553 - Realizar pruebas anuales de los planes de respuesta, contingencia y recuperación.	RSI y Director de TIC	E553 - Registros de pruebas anuales de los planes de respuesta, contingencia y recuperación.

		protección de la información						
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	4	P2	T554 - Llevar a cabo actividades de control interno para verificar el cumplimiento de políticas y procedimientos relacionados.	RSI y Director de TIC	E554 - Registro de actividades de control interno para verificar el cumplimiento de políticas y procedimientos relacionados.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	4	P2	T555 - Informar los resultados de los controles y tomar acciones correctivas frente a desvíos.	RSI	E555 - Informes de controles internos realizados y acciones correctivas aplicadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-9	4	P2	T556 - Documentar lecciones aprendidas y ajustar los procedimientos de manera continua.	RSI	E556 - Documentación de lecciones aprendidas y mejoras a los procedimientos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	1	P2	T557 - (REF. T471) Implementar acuerdos de no divulgación básicos para nuevos proveedores y personal.	Director de Legales y RRHH	E557 - (REF. E471) Plantillas de Acuerdos de no divulgación para personal y proveedores.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	1	P2	T558 - (REF. T472) Garantizar la firma de los acuerdos como parte del proceso de incorporación.	RRHH	E558 - (REF. E472) Lista de personal con Acuerdos de no divulgación firmados.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	2	P2	T559 - (REF. T473) Identificar y categorizar el personal que no han firmado acuerdos de no divulgación.	RRHH	E559 - (REF. E473) Listado completo de personal que no tenga firmado Acuerdos no divulgación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	2	P2	T560 - (REF. T474) Identificar y categorizar los proveedores que no han firmado acuerdos de no divulgación.	Director de TIC	E560 - (REF. E474) Listado completo de proveedores que no tenga firmado Acuerdos no divulgación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	2	P2	T561 - (REF. T475) Plan para que el personal que no cuenta con Acuerdos de no divulgación firmado lo firme.	RRHH	E561 - (REF. E475) Cronograma de implementación del plan para que el personal firme el Acuerdo de no divulgación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	2	P2	T562 - (REF. T476) Plan para que los proveedores que no cuenta con Acuerdos de no divulgación firmado lo firmen.	Director de TIC	E562 - (REF. E476) Cronograma de implementación del plan para que los proveedores firmen el Acuerdo de no divulgación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	2	P2	T563 - (REF. T477) Realizar campañas de concientización sobre la importancia de los Acuerdos de no divulgación .	RSI y Capacitación	E563 - (REF. E477) Materiales de comunicación utilizados. Registros de participación en sesiones informativas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	3	P2	T564 - (REF. T478) Actualizar acuerdos contractuales para reflejar responsabilidades según roles específicos.	RRHH y Director de Legales	E564 - (REF. E478) Nuevos modelos de contratos que incluyan responsabilidades de seguridad para roles críticos.

PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	3	P2	T565 - (REF. T479) Documentar un procedimiento de desvinculación robusto.	RRHH y Director de Legales	E565 - (REF. E479) Procedimiento documentado que incluya revocación de accesos físicos y lógicos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	3	P2	T566 - (REF. T480) Implementar un sistema DLP (Data Loss Prevention) para proteger los datos sensibles.	Director de TIC	E566 - (REF. E480) Detalles técnicos del sistema DLP (Data Loss Prevention) implementado.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	4	P2	T567 - (REF. T481) Establecer un cronograma de revisión periódica de contratos y procedimientos de desvinculación.	Director de TIC	E567 - (REF. E481) Cronograma de revisiones e informes de revisiones realizadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	4	P2	T568 - (REF. T482) Implementar un sistema de registro para monitorear y reportar desvíos e incumplimientos.	RSI	E568 - (REF. E482) Registros de desvíos detectados e informes con acciones correctivas implementadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	4	P2	T569 - (REF. T483) Incorporar resultados de revisiones en planes de mejora continua.	RSI y Director de TIC	E569 - (REF. E483) Documentación de mejoras en procedimientos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-11	4	P2	T570 - (REF. T484) Reportar hallazgos y resultados de revisiones a partes interesadas.	RSI	E570 - (REF. E484) Reportes enviados a las áreas interesadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	1	P2	T571 - Implementar la gestión de parches como medida para abordar vulnerabilidades técnicas.	Director de Infraestructura	E571 - Registro de vulnerabilidades y parches gestionados.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	1	P2	T572 - Mantener un registro de los parches aplicados y las vulnerabilidades gestionadas.	RGV	E572 - Comparativa entre las actualizaciones críticas requeridas y las realmente realizadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	2	P2	T573 - Definir y documentar un plan para la gestión de vulnerabilidades y parches.	RGV	E571 - Plan documentado de gestión de vulnerabilidades y parches.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	2	P2	T574 - Establecer mecanismos para recibir notificaciones de vulnerabilidades desde fuentes externas, como el CERTuy u otras organizaciones y analizar las notificaciones de vulnerabilidades recibidas y priorizar su tratamiento.	RGV	E572 - Registro de notificaciones de vulnerabilidades recibidas y análisis realizado.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	3	P2	T575 - Establecer responsabilidades claras para la gestión de vulnerabilidades.	RSI	E575 - Registro de responsables de la gestión de vulnerabilidades.
PROTEGER (PR)	PR.PI	Procesos y procedimientos	PR.PI-12	3	P2	T576 - Incorporar escaneos de infraestructura y aplicaciones como fuentes de notificación de vulnerabilidades.	RGV	E576 - Escaneos de infraestructura y aplicaciones con vulnerabilidades detectadas.

		para la protección de la información						
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	3	P2	T577 - Implementar un ambiente para pruebas de parches antes de su puesta en producción y documentar los resultados de las pruebas de parches realizadas en el ambiente de pruebas.	RGV y Director de Infraestructura	E577 - Registro de pruebas realizadas en el ambiente de pruebas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	4	P2	T578 - Realizar revisiones de control interno sobre el plan de gestión de vulnerabilidades y comunicar los resultados de las revisiones al RSI.	RSI y RGV	E578 - Informes de revisiones de control interno realizadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	4	P2	T579 - Documentar las lecciones aprendidas para mejorar la gestión de vulnerabilidades en futuras resoluciones.	RGV	E579 - Registros de lecciones aprendidas y su aplicación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-12	4	P2	T580 - Implementar mejoras al plan y procedimientos de gestión de vulnerabilidades con base en las lecciones aprendidas y revisiones internas.	RGV	E580 - Plan actualizado con mejoras basadas en las revisiones.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	1	P2	T581 - Configurar los registros de auditoría para todos los sistemas críticos definidos.	RSI y Director de TIC	E581 - Configuración documentada de los registros en sistemas críticos.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	1	P2	T582 - Utilizar los registros únicamente para tratar situaciones puntuales.	RSI y Director de TIC	E582 - Evidencia del uso de registros en situaciones específicas.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	2	P2	T583 - Crear repositorio de auditoría para todos los registros de auditoría.	Director de Infraestructura	E583 - Repositorio de registros de auditoría.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	2	P2	T584 - Proteger el repositorio de auditoría contra accesos no autorizados y alteraciones.	Director de Infraestructura	E584 - Registro de medidas de seguridad aplicadas.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	2	P2	T585 - Definir rutinas para centralizar todos los registros de auditoría.	Director de Infraestructura	E585 - Listado de rutinas para centralización de registros de auditoría.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	2	P2	T586 - Garantizar la confidencialidad y privacidad de los datos en los registros.	RSI	E586 - Evidencia de configuraciones que protejan la privacidad.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	3	P2	T587 - Desarrollar una política de registro y auditoría de eventos de sistemas de información.	CSI	E587 - política de registro y auditoría de eventos de sistemas de información
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	3	P2	T588 - Respalidar los registros de auditoría y revisar periódicamente los registros con herramientas automatizadas.	Director de Infraestructura	E588 - Evidencia de respaldos de registros de auditoría y revisiones periódicas con herramientas automatizadas.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	3	P2	T589 - Sincronizar los relojes de todos los sistemas críticos.	Director de Infraestructura	E589 - Registro de sincronización de relojes en sistemas críticos.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	4	P2	T590 - Establecer requisitos de retención de registros según normativa y políticas internas.	RSI	E590 - Documento que define los requisitos de retención.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	4	P2	T591 - Implementar herramientas avanzadas para el análisis de grandes volúmenes de datos.	Director de Infraestructura	E591 - Configuración y evidencia del uso de herramientas de análisis.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	4	P2	T592 - Crear mecanismos específicos para revisar las actividades de administradores de sistemas.	Director de Infraestructura	E592 - Informes de revisión de actividades de administradores.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	4	P2	T593 - Realizar controles internos para verificar el cumplimiento de la política y procedimientos de auditoría.	Director de Infraestructura	E593 - Resultados de controles internos documentados.

PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-1	4	P2	T594 - Comunicar los resultados de las revisiones al RSI y partes interesadas.	Director de Infraestructura	E594 - Evidencia de comunicación de resultados (ejemplo: correos o informes enviados).
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	1	P2	T595 - Configurar mecanismos básicos para registrar eventos de sistemas y redes críticos.	Director de Infraestructura	E595 - Configuración de registros de eventos de sistemas y redes.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	1	P2	T596 - Establecer un procedimiento inicial para analizar eventos irregulares puntuales y contactar al CERTuy o CSIRT.	RSI	E596 - Listado de eventos irregulares analizados y registro de interacciones con CERTuy o CSIRT.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	2	P2	T597 - Adquirir e implementar herramientas automatizadas para monitorear eventos, excepciones y fallas.	RM	E597 - Configuración y logs de herramientas automatizadas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	2	P2	T598 - Configurar y utilizar WAF en sitios web vinculados a trámites en línea.	Director de Infraestructura	E598 - Configuración del WAF implementado.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	2	P2	T599 - Definir procedimientos para la revisión de eventos y uso de herramientas automatizadas.	RSI	E599 - Procedimientos documentados para la revisión de eventos y configuración del WAF.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	3	P2	T600 - (REF. T587) Desarrollar una política de registro y auditoría de eventos de sistemas de información.	CSI	E600 - (REF. E587) Política de registro y auditoría de eventos de sistemas de información.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	3	P2	T601 - Establecer procedimientos para la revisión y gestión de eventos en sistemas y redes y uso WAF.	RSI y Director de Infraestructura	E601 - Procedimientos documentados de revisión y gestión de eventos y uso de WAF.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	3	P2	T602 - Alinear los procedimientos de gestión de eventos con los de gestión de incidentes.	RSI y RGI	E602 - Listado de eventos gestionados según los procedimientos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	4	P2	T603 - Establecer una periodicidad formal para la revisión de eventos y actividad anormal.	RSI	E603 - Informe de revisiones periódicas de eventos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	4	P2	T604 - Diseñar mecanismos para analizar patrones de ataque y documentar lecciones aprendidas.	RSI y Director de Infraestructura	E604 - Informe de análisis de patrones de ataque.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	4	P2	T605 - Generar informes periódicos de revisiones y compartirlos con las partes interesadas.	Director de Infraestructura	E605 - Registro de reuniones y comunicaciones con partes interesadas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-2	4	P2	T606 - Implementar controles internos para evaluar el cumplimiento de los procedimientos y políticas.	RSI y Director de Infraestructura	E606 - Resultados de controles internos realizados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	1	P2	T607 - Identificar los sistemas y servicios más críticos.	CSI	E607 - Listado de sistemas y servicios críticos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	1	P2	T608 - Establecer un procedimiento básico para realizar monitoreos reactivos o esporádicos.	RM	E608 - Registro de monitoreos realizados de manera reactiva.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	1	P2	T609 - Documentar los resultados de los monitoreos realizados y las acciones correctivas.	RM	E609 - Informe de acciones correctivas aplicadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	2	P2	T610 - Implementar herramientas de monitoreo automatizadas para los activos críticos.	RM y Director de Infraestructura	E610 - Configuración de herramientas de monitoreo automatizadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	2	P2	T611 - Configurar las alertas en las herramientas de monitoreo.	RM y Director de Infraestructura	E611 - Registro de alertas generadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	2	P2	T612 - Documentar un procedimiento para el monitoreo automatizado y la gestión de alertas.	RM	E612 - Procedimiento documentado para el monitoreo automatizado.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	3	P2	T613 - Ajustar las herramientas de monitoreo para identificar patrones de anomalías.	RM y Director de Infraestructura	E613 - Configuración avanzada de herramientas de monitoreo para patrones de anomalías.

DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	3	P2	T614 - Establecer un procedimiento para la revisión y análisis de anomalías detectadas.	Director de Infraestructura	E614 - Procedimiento documentado para la revisión de anomalías.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	4	P2	T615 - Ampliar el monitoreo a todos los activos de información del centro de datos.	RM y Director de Infraestructura	E615 - Registro del monitoreo de todos los activos de información.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	4	P2	T616 - Implementar un sistema que permita cruzar información de diversas fuentes para generar alertas más precisas.	RM y Director de Infraestructura	E616 - Configuración del sistema de cruzamiento de información.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	4	P2	T617 - Diseñar e implementar un mecanismo alternativo de monitoreo manual.	RM y Director de Infraestructura	E617 - Documentación del mecanismo alternativo de monitoreo.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-1	4	P2	T618 - Documentar lecciones aprendidas y oportunidades de mejora a partir de los resultados del monitoreo.	RM	E618 - Informes de lecciones aprendidas y oportunidades de mejora.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	1	P2	T619 - (REF. T152) Implementar controles básicos de acceso físico a los activos críticos del centro de datos.	Director de Infraestructura y RM	E619 - (REF. E152) Configuración inicial de sistemas de control de acceso físico y su documentación.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	1	P2	T620 - Establecer alertas reactivas para dispositivos críticos del centro de datos.	Director de Infraestructura y RM	E620 - Configuración de alertas reactivas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	1	P2	T621 - Realizar monitoreos esporádicos de dispositivos para identificar amenazas físicas.	Director de Infraestructura y RM	E621 - Informe de monitoreos esporádicos realizados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	2	P2	T622 - Configurar las funciones de monitoreo integradas en los dispositivos críticos.	Director de Infraestructura y RM	E622 - Configuración de dispositivos para monitoreo de amenazas típicas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	2	P2	T623 - Establecer mecanismos de notificación automatizada de alertas.	Director de Infraestructura y RM	E623 - Registro de notificaciones enviadas al personal designado.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	2	P2	T624 - Documentar los procedimientos para la gestión de alertas.	Director de Infraestructura y RM	E624 - Procedimiento documentado para la gestión de alertas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	3	P2	T625 - (REF. T157) Desarrollar una política de control de acceso físico que abarque todos los activos críticos.	CSI	E625 - (REF. E157) Política de control de acceso físico.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	3	P2	T626 - Instalar y configurar sensores para amenazas físicas específicas.	Director de Infraestructura y RM	E626 - Registro de instalación y configuración de sensores.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	3	P2	T627 - Establecer una estrategia de almacenamiento redundante para datos de sensores.	Director de Infraestructura y RM	E627 - Estrategia documentada para almacenamiento redundante de datos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	3	P2	T628 - Documentar los procedimientos de gestión y análisis de datos recolectados.	RM	E628 - Procedimiento documentado para análisis de datos recolectados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	4	P2	T629 - Implementar un sistema de monitoreo inteligente con capacidades de análisis histórico.	Director de Infraestructura y RM	E629 - Configuración y reportes generados por el sistema de monitoreo inteligente.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	4	P2	T630 - Establecer procedimientos para la generación y análisis de informes de monitoreo.	Director de Infraestructura y RM	E630 - Procedimientos documentados para análisis de informes.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	4	P2	T631 - Realizar evaluaciones periódicas del centro de datos basadas en los informes generados.	RM	E631 - Registro de evaluaciones periódicas realizadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-2	4	P2	T632 - Definir un plan de acciones correctivas y preventivas basado en las evaluaciones realizadas.	Director de Infraestructura y RM	E632 - Plan de acciones correctivas y preventivas documentado.

DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	1	P2	T633 - Identificar los sistemas y aplicaciones críticas donde se registrarán eventos relevantes de los usuarios.	CSI	E633 - Listado de sistemas y aplicaciones críticas identificadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	1	P2	T634 - Configurar el registro de eventos de usuarios en los sistemas críticos.	Director de Infraestructura	E634 - Configuración de registro de eventos de usuarios en los sistemas críticos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	2	P2	T635 - Establecer procedimientos para revisiones reactivas de eventos registrados.	RM	E635 - Procedimiento documentado para revisiones reactivas de eventos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	2	P2	T636 - Documentar los resultados de las revisiones y evaluar incidentes potenciales.	RM	E636 - Registro de evaluaciones de incidentes basadas en los resultados de las revisiones.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	3	P2	T637 - Asignar responsabilidades específicas para el monitoreo de eventos de los usuarios.	RSI	E637 - Documento que define las responsabilidades del monitoreo.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	3	P2	T638 - Establecer un procedimiento de revisión periódica de registros que incluya inicios de sesión fallidos y acceso a Internet.	Director de Infraestructura y RM	E638 - Procedimiento documentado de revisión periódica de registros.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	3	P2	T639 - Generar reportes para el Directorio y partes interesadas basados en la información monitoreada.	RSI y Director de TIC	E639 - Reportes generados para el Directorio y partes interesadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	4	P2	T640 - Diseñar e implementar actividades de control interno para verificar el cumplimiento del procedimiento de monitoreo.	RSI	E640 - Registro de actividades de control interno realizadas para verificar cumplimiento del procedimiento de monitoreo.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	4	P2	T641 - Generar y analizar estadísticas basadas en la información monitoreada.	RM	E641 - Estadísticas generadas a partir del monitoreo de eventos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-3	4	P2	T642 - Revisar y actualizar el procedimiento de monitoreo basado en las lecciones aprendidas.	Director de Infraestructura y RM	E642 - Procedimiento de monitoreo actualizado con las lecciones aprendidas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	1	P2	T643 - Identificar desvíos detectados en los proveedores de servicios críticos del centro de datos.	Director de Infraestructura	E643 - Listado de proveedores y desvíos detectados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	1	P2	T644 - Tomar acciones correctivas ante desvíos detectados de proveedores.	Director de Infraestructura	E644 - Registro de desvíos y acciones correctivas realizadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	2	P2	T645 - Definir y documentar SLA con proveedores críticos que incluyan cláusulas de seguridad.	Director de TIC	E645 - Documentos de SLA y cláusulas con proveedores.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	2	P2	T646 - Formalizar los acuerdos con proveedores mediante contratos.	RSI y Director de TIC	E646 - Contratos con SLA y cláusulas de seguridad de la información.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	3	P2	T647 - Establecer un régimen de cobertura en los SLA y contratos para servicios críticos.	RSI y Director de TIC	E648 - SLA actualizados con régimen de cobertura definido.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	3	P2	T648 - Implementar un procedimiento para la revisión de contratos cuando cambien los servicios.	RSI y Director de TIC	E649 - Procedimiento documentado para la revisión de contratos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	4	P2	T649 - Establecer un cronograma de revisiones periódicas de contratos y SLA.	RSI y Director de TIC	E649 - Cronograma de revisiones periódicas de contratos SLA.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-6	4	P2	T650 - Generar reportes de evaluación y recomendaciones basadas en las revisiones de acuerdos SLA.	RSI	E650 - Reportes de revisiones periódicas de contratos y SLA.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	1	P2	T651 - Configurar el monitoreo de logs de control de acceso físico y lógico.	RM	E651 - Configuración del sistema de monitoreo de logs.

DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	1	P2	T652 - Establecer un sistema básico de almacenamiento y análisis de logs.	Director de Infraestructura y RM	E652 - Logs generados por los sistemas de control de acceso.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	2	P2	T653 - Configurar reglas de monitoreo para conexiones externas y dispositivos no autorizados.	Director de Infraestructura y RM	E653 - Configuración de reglas de monitoreo.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	2	P2	T654 - Implementar alertas automáticas ante violaciones detectadas.	RM	E654 - Registro de alertas generadas por el sistema.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	3	P2	T655 - Desarrollar procedimientos para el monitoreo.	Director de Infraestructura y RM	E655 - Políticas y procedimientos documentados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	3	P2	T656 - Configurar sistemas para monitorear todos los equipos del organismo.	Director de Infraestructura y RM	E656 - Configuración del sistema de monitoreo ampliado.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	4	P2	T657 - Implementar un sistema centralizado para la recolección de logs y emisión de alertas.	Director de Infraestructura y RM	E657 - Configuración del sistema centralizado de recolección de logs.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-7	4	P2	T658 - Analizar y documentar las acciones no permitidas detectadas.	RM	E658 - Informes de análisis de acciones no permitidas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	1	P2	T659 - Realizar escaneos puntuales utilizando herramientas disponibles (propias o contratadas).	Director de Infraestructura	E659 - Registro de revisiones puntuales realizadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	1	P2	T660 - Documentar los hallazgos de las revisiones realizadas.	Director de Infraestructura	E660 - Informes de escaneos de vulnerabilidades.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	2	P2	T661 - Establecer un cronograma periódico para los escaneos de vulnerabilidades.	Director de Infraestructura y RGV	E661 - Cronograma de revisiones de vulnerabilidades.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	2	P2	T662 - Realizar escaneos adicionales en caso de cambios significativos en los sistemas.	RGV	E662 - Informes de escaneos periódicos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	2	P2	T663 - Analizar los resultados de los escaneos para identificar vulnerabilidades críticas.	RGV	E663 - Registro de cambios significativos y escaneos asociados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	3	P2	T664 - (REF. T041) Designar un rol responsable de la gestión de vulnerabilidades y parches (RGV).	RSI	E664 - (REF. E041) Resolución con designación del RGV.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	3	P2	T665 - Documentar el procedimiento para realizar escaneos internos y externos.	RSI	E665 - Informes de revisiones internas y externas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	3	P2	T666 - Contratar servicios de ethical hacking para revisiones externas.	RSI	E666 - Contrato de ethical hacking.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	3	P2	T667 - Desarrollar un plan de acción basado en los hallazgos de las revisiones.	RSI	E667 - Plan de acción para corregir vulnerabilidades detectadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	4	P2	T668 - Incorporar el procedimiento de revisión de vulnerabilidades en las actividades rutinarias de seguridad.	RSI y RGV	E668 - Registros de control interno que validen la ejecución de las revisiones.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	4	P2	T669 - Establecer controles internos para verificar el cumplimiento del procedimiento.	RSI	E669 - Informes de mejora continua basados en las revisiones realizadas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	4	P2	T670 - Ajustar la frecuencia de las revisiones según análisis de riesgo o cambios significativos en los sistemas.	RSI	E670 - Análisis de riesgo asociados a cambios significativos en los sistemas.

DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-8	4	P2	T671 - Implementar mecanismos para medir la efectividad de las correcciones realizadas.	RIS	E671 - Registros de medición de efectividad en la resolución de vulnerabilidades.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	1	P2	T672 - Identificar personal responsable y asignar tareas específicas relacionadas con la detección de eventos en sistemas base y protección perimetral.	Director de TIC	E672 - Listado de personal asignado a tareas de detección.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	1	P2	T673 - Documentar las asignaciones de tareas en un registro formal.	Director de TIC	E673 - Registro de las tareas asignadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	2	P2	T674 - Implementar herramientas automatizadas para la detección y monitoreo de eventos.	RSI y Director de Infraestructura	E674 - Configuración de herramientas de monitoreo automatizado.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	2	P2	T675 - Establecer un proceso para la revisión periódica de registros de eventos generados por las herramientas.	RSI y Director de Infraestructura	E675 - Procedimientos para la revisión de eventos y registros de revisión de eventos.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	3	P2	T676 - Asignar un responsable formal y documentar un procedimiento detallado para las actividades de monitoreo.	RSI y Director de TIC	E676 - Procedimiento documentado de monitoreo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	3	P2	T677 - Diseñar y ejecutar pruebas periódicas del procedimiento, incluyendo diferentes escenarios y ambientes.	RSI y Director de TIC	E677 - Registro de pruebas realizadas al procedimiento.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	3	P2	T678 - Definir y documentar actividades de comunicación formal asociadas al monitoreo.	RSI y Director de TIC	E678 - Informes de comunicación formal relacionados con el monitoreo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	4	P2	T679 - Establecer controles internos para verificar el cumplimiento del procedimiento de monitoreo.	RSI	E679 - Informes de control interno sobre el cumplimiento del procedimiento.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	4	P2	T680 - Implementar un proceso de retroalimentación basado en las lecciones aprendidas de las actividades de monitoreo.	RSI y Director de Infraestructura	E680 - Documentación de lecciones aprendidas y retroalimentación.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	4	P2	T681 - Comunicar los resultados de las actividades al RSI y otras partes interesadas.	Director de Infraestructura	E681 - Registro de comunicaciones a partes interesadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-1	4	P2	T682 - Incorporar mejoras continuas al procedimiento de monitoreo y pruebas.	RSI y Director de Infraestructura	E682 - Procedimiento actualizado con mejoras derivadas de las actividades de monitoreo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	1	P2	T683 - Identificar referentes o autoridades responsables de recibir la comunicación sobre eventos anómalos.	Director de Infraestructura	E683 - Registro de eventos anómalos detectados.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	1	P2	T684 - Establecer un proceso básico para la notificación manual de eventos anómalos detectados.	Director de Infraestructura	E684 - Proceso básico para la notificación de eventos anómalos detectados.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	2	P2	T685 - Documentar mecanismos de comunicación estándar ante eventos anómalos.	Director de Infraestructura	E685 - Procedimientos documentados para la comunicación de eventos.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	2	P2	T686 - Implementar registros de las comunicaciones realizadas ante eventos anómalos.	Director de Infraestructura	E686 - Registros de comunicaciones realizadas ante eventos detectados.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	3	P2	T687 - Revisar y documentar un procedimiento completo de monitoreo, incluyendo actividades de comunicación específicas.	RSI	E687 - Procedimiento documentado de monitoreo con actividades de comunicación.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	3	P2	T688 - Diseñar pruebas para evaluar las actividades de comunicación en escenarios de detección de eventos.	Director de Infraestructura y RM	E688 - Informes de pruebas realizadas, incluyendo resultados de las actividades de comunicación.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	3	P2	T689 - Ejecutar pruebas periódicas del procedimiento, incluyendo las actividades de comunicación.	Director de Infraestructura y RM	E689 - Retroalimentación de las pruebas realizadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	4	P2	T690 - Implementar un sistema de coordinación formal entre el RM y el RSI.	RM y RSI	E690 - Informes de coordinación entre el RM y el RSI.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	4	P2	T691 - Realizar revisiones de control interno para evaluar el cumplimiento de los procedimientos de monitoreo y comunicación.	RSI	E691 - Resultados de las revisiones de control interno.

DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	4	P2	T692 - Documentar las lecciones aprendidas y utilizarlas para mejorar los procedimientos y pruebas.	RM	E692 - Registro de lecciones aprendidas y mejoras implementadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-4	4	P2	T693 - Mantener actualizados los procedimientos y pruebas basados en la retroalimentación obtenida.	RM	E693 - Procedimientos actualizados con mejoras basadas en la retroalimentación.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	1	P2	T694 - (REF. T302) Definir los mecanismos de respuestas a incidentes	RSI	E694 - (REF. E302) Documento con los mecanismos de respuesta de incidentes
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	1	P2	T695 - (REF. T303) Implementar las herramientas o sistemas necesarios para detectar y reportar incidentes.	RSI	E695 - (REF. E303) Herramienta de reporte de incidentes
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	1	P2	T696 - (REF. T304) Establecer los pasos claros para informar al CERTuy cuando se detecte un incidente	RSI	E696 - (REF. E304) Documento con los pasos para informar incidentes al CERTuy, incluyendo tiempos de respuesta y contenido de la información a compartir
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	2	P2	T697 - (REF. T309) Establecer un plan de respuesta a incidentes de seguridad de la información.	RSI	E697 - (REF. E309) Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	2	P2	T698 - Definir un plan de concientización y sensibilización en seguridad de la información todo el organismo.	RSI	E698 - Plan de concientización y sensibilización en seguridad de la información.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	3	P2	T699 - Difundir la política de gestión de incidentes a todo el personal.	CSI	E699 - Distribución y firma de recepción por parte del personal.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	3	P2	T700 - Incluir el procedimiento de reporte de incidentes en las actividades de concientización.	RSI y Comunicaciones	E700 - Materiales de formación que incluyan el procedimiento de reporte.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	3	P2	T701 - Revisar y actualizar el plan de respuesta a incidentes y sus procedimientos.	RSI	E701 - Acta de revisión y actualización del plan de respuesta a incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	4	P2	T702 - Realizar simulacros de respuesta a incidentes, incluyendo usuarios clave.	RSI	E702 - Resultados de simulacros de pruebas de respuesta a incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-1	4	P2	T703 - Implementar un sistema de control interno para verificar el cumplimiento del plan de respuesta.	RSI	E703 - Informes de control interno sobre el cumplimiento del plan de respuesta de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	1	P2	T704 - (REF. T541) Instruir al personal sobre los mecanismos de reporte de incidentes.	RSI y Capacitación	E704 - (REF. E541) Registros de capacitaciones sobre mecanismos de reporte de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	1	P2	T705 - (REF. T542) Establecer lineamientos para el reporte interno de incidentes.	RSI y RGI	E705 - (REF. E542) Documentación de lineamientos para el reporte interno de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	1	P2	T706 - (REF. T543) Registrar los incidentes de seguridad reportados.	RGI	E706 - (REF. E543) Listado de incidentes reportados y registrados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	1	P2	T707 - (REF. T544) Implementar medidas básicas de contingencia y recuperación para sistemas que soportan servicios críticos.	RGI y Director de Infraestructura	E707 - (REF. E544) Documentación de las medidas de contingencia aplicadas.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	2	P2	T708 - Nombrar un punto de contacto único para los incidentes de seguridad.	RSI	E708 - Documento que asigna el punto de contacto.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	2	P2	T709 - Establecer los criterios de reporte al CERTuy o equipo de respuesta.	RSI	E709 - Documento con los criterios establecidos para la notificación de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	3	P2	T710 - (REF. T308) Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E710 - (REF. E308) Política de gestión de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	3	P2	T711 - (REF. T309) Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E711 - (REF. E309) Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	3	P2	T712 - Implementar herramientas automatizadas para el reporte de eventos y gestión de incidentes.	RSI	E712 - Herramientas de automatización para el reporte de eventos y gestión de incidentes.

RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	4	P2	T713 - Implementar controles internos para verificar el cumplimiento del procedimiento de reporte y gestión de incidentes.	RSI	E713 - Informes de auditoría de cumplimiento.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	4	P2	T714 - Utilizar los resultados de los controles internos para mejorar el procedimiento de reporte y gestión de incidentes.	RSI	E714 - Actas de revisión y actualización de los procedimientos .
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-2	4	P2	T715 - Realizar análisis de lecciones aprendidas tras cada incidente y ajustarlos al procedimiento.	RSI	E715 - Informe de lecciones aprendidas documentado.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	1	P2	T716 - (REF. T541) Instruir al personal sobre los mecanismos de reporte de incidentes.	RSI y Capacitación	E716 - (REF. E541) Registros de capacitaciones sobre mecanismos de reporte de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	1	P2	T717 - (REF. T542) Establecer lineamientos para el reporte interno de incidentes.	RSI y RGI	E717 - (REF. E542) Documentación de lineamientos para el reporte interno de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	1	P2	T718 - (REF. T543) Registrar los incidentes de seguridad reportados.	RGI	E718 - (REF. E543) Listado de incidentes reportados y registrados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	1	P2	T719 - (REF. T544) Implementar medidas básicas de contingencia y recuperación para sistemas que soportan servicios críticos.	RGI y Director de Infraestructura	E719 - (REF. E544) Documentación de las medidas de contingencia aplicadas.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	2	P2	T720 - (REF. T545) Identificar los procesos críticos del organismo.	RSI	E720 - (REF. E545) Listado de procesos críticos documentados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	2	P2	T721 - (REF. T546) Establecer herramientas básicas para apoyar la gestión de incidentes.	Director de TIC	E721 - (REF. E546) Herramientas implementadas para la gestión de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	2	P2	T722 - (REF. T547) Implementar medidas adicionales de contingencia y recuperación.	RSI	E722 - (REF. E547) Documentación de medidas de contingencia adicionales.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	3	P2	T723 - (REF. T548) Desarrollar y difundir una política de gestión de incidentes de seguridad de la información.	RSI	E723 - (REF. E548) Política de gestión de incidentes aprobada y difundida.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	3	P2	T724 - (REF. T549) Definir un plan de respuesta a incidentes alineado con la política.	RSI	E724 - (REF. E549) Plan de respuesta a incidentes documentado.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	3	P2	T725 - (REF. T550) Diseñar un plan de contingencia y de recuperación para los sistemas críticos.	RSI y Director de TIC	E725 - (REF. E550) Plan de contingencia y recuperación.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	3	P2	T726 - (REF. T551) Realizar pruebas puntuales de los planes diseñados.	RSI	E726 - (REF. E551) Resultados de las pruebas puntuales realizadas.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	4	P2	T727 - (REF. T552) Designar responsables específicos para la respuesta a incidentes y el mantenimiento de los planes de contingencia y recuperación.	CSI	E727 - (REF. E552) Listado de responsables designados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	4	P2	T728 - (REF. T553) Realizar pruebas anuales de los planes de respuesta, contingencia y recuperación.	RSI y Director de TIC	E728 - (REF. E553) Registros de pruebas anuales de los planes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	4	P2	T729 - (REF. T545) Llevar a cabo actividades de control interno para verificar el cumplimiento de políticas y procedimientos relacionados.	RSI y Director de TIC	E729 - (REF. E554) Registro de actividades de control interno para verificar el cumplimiento de políticas y procedimientos relacionados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	4	P2	T730 - (REF. T555) Informar los resultados de los controles y tomar acciones correctivas frente a desvíos.	RSI	E730 - (REF. E555) Informes de controles internos realizados y acciones correctivas aplicadas.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-3	4	P2	T731 - (REF. T556) Documentar lecciones aprendidas y ajustar los procedimientos de manera continua.	RSI	E731 - (REF. E556) Documentación de lecciones aprendidas y mejoras a los procedimientos.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	1	P2	T732 - Mantener contacto con actores clave internos y externos durante la gestión de incidentes.	RSI	E732 - Registro de comunicaciones con actores clave.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	1	P2	T733 - Escalar las necesidades puntuales a actores externos relevantes, como CERTuy o CSIRT del sector.	RSI	E733 - Evidencia de incidentes escalados a CERTuy o CSIRT.

RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	2	P2	T734 - Identificar los actores internos y externos relevantes para la gestión de incidentes.	RSI	E734 - Listado de actores internos y externos identificados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	2	P2	T735 - Registrar y mantener actualizados los datos de contacto de los actores identificados.	RSI	E735 - Base de datos o registro de contactos actualizados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	2	P2	T736 - Documentar el mecanismo de escalamiento de incidentes.	RSI	E736 - Documento con el mecanismo de escalamiento de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	2	P2	T737 - (REF. T308) Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E737 - (REF. E308) Política de gestión de incidentes de seguridad de la información.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	3	P2	T738 - (REF. T309) Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E738 - (REF. E309) Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	4	P2	T739 - (REF. T310) Designar un responsable específico para la gestión de la respuesta a incidentes.	CSI	E739 - (REF. E310) Circular con la asignación formal del responsable de la respuesta.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	4	P2	T740 - Realizar actividades de control interno para verificar el cumplimiento del procedimiento de reporte y gestión de incidentes, y del plan de respuesta.	RSI	E740 - Informes de control interno realizados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	4	P2	T741 - Utilizar los resultados de las actividades de control interno para mejorar el procedimiento y los planes.	RSI	E741 - Documentación con mejoras aplicadas al procedimiento y planes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-4	4	P2	T742 - Documentar las lecciones aprendidas y retroalimentar los procedimientos y planes de respuesta.	RSI	E742 - Registro de lecciones aprendidas y ajustes realizados.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	1	P2	T743 - Registrar eventos de seguridad en los sistemas.	RSI y Director de Infraestructura	E743 - Registros de eventos de seguridad generados por los sistemas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	1	P2	T744 - Analizar reactivamente las notificaciones de seguridad generadas por los sistemas.	RSI	E744 - Informes de análisis reactivo realizados.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	1	P2	T745 - Escalar los eventos que correspondan según su naturaleza.	RSI	E745 - Registro de eventos escalados.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	2	P2	T746 - Definir pautas generales para el registro de eventos de seguridad.	RSI y Director de Infraestructura	E746 - Documento con pautas generales de registro de eventos.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	2	P2	T747 - Asegurar que los nuevos sistemas se desplieguen siguiendo las pautas definidas.	Director de TIC	E747 - Registros de cumplimiento en el despliegue de nuevos sistemas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	2	P2	T748 - Determinar cuándo un evento o notificación constituye un incidente.	RSI y Director de TIC	E748 - Criterios definidos para la determinación de incidentes.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	2	P2	T749 - Clasificar los incidentes según su criticidad y severidad.	RSI	E749 - Listado o base de datos con incidentes clasificados por criticidad y severidad.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	3	P2	T750 - (REF. T600) Desarrollar una política de registro y auditoría de eventos de sistemas de información.	CSI	E750 - (REF. E600) Política de registro y auditoría de eventos de sistemas de información.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	3	P2	T751 - (REF. T601) Documentar procedimientos para la revisión y gestión de eventos en sistemas, redes y WAF.	RSI y Director de Infraestructura	E751 - (REF. E601) Procedimientos documentados de revisión y gestión de eventos.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	3	P2	T752 - Determinar criterios para escalar un incidente considerando los activos afectados, criticidad y severidad.	RSI	E752 - Documentación de criterios para el escalamiento de incidentes.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	4	P2	T753 - Incorporar mejores prácticas al procedimiento para la revisión y gestión de eventos, incluyendo análisis forense y custodia de la información.	RSI	E753 - Procedimiento de revisión y gestión de eventos con mejores prácticas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	4	P2	T754 - Realizar actividades de control interno para verificar el cumplimiento del procedimiento.	RSI	E754 - Informes de actividades de control interno realizadas.

RESPONDER (RE)	RE.AN	Análisis	RE.AN-1	4	P2	T755 - Utilizar los resultados de las actividades de control interno para la mejora continua del procedimiento.	RSI	E755 - Registro de mejoras aplicadas al procedimiento.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	1	P2	T756 - Realizar análisis de impacto en forma ad-hoc durante la gestión de incidentes.	RSI	E756 - Registros de análisis de impacto realizados.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	1	P2	T757 - Llevar a cabo actividades de respuesta a los incidentes detectados en forma ad-hoc.	RSI	E757 - Documentación de actividades de respuesta realizadas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	1	P2	T758 - Informar al CERTuy o CSIRT correspondiente sobre los incidentes detectados.	RSI	E758 - Reportes enviados al CERTuy o CSIRT.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	2	P2	T759 - Definir y documentar pautas para la clasificación de incidentes.	RSI y RGI	E759 - Documento con las pautas para la clasificación de incidentes.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	2	P2	T760 - Utilizar las pautas definidas en la gestión de todos los incidentes reportados.	RGI	E760 - Registros de incidentes clasificados siguiendo las pautas definidas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	3	P2	T761 - Implementar un plan y/o procedimiento de respuesta alineado a la política de gestión de incidentes.	RSI y RGI	E761 - Plan y/o procedimiento de respuesta documentado y aprobado.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	3	P2	T762 - Incluir tareas de análisis de impacto dentro del procedimiento de gestión de incidentes.	RSI y RGI	E762 - Procedimiento de gestión de incidentes con tareas de análisis de impacto incluidas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	3	P2	T763 - Implementar herramientas automatizadas para el registro y seguimiento de incidentes, alineadas al plan y/o procedimiento de respuesta definido.	RSI y RGI	E763 - Registros generados por las herramientas automatizadas implementadas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	4	P2	T764 - Incorporar mejores prácticas en el procedimiento, incluyendo análisis forense y custodia de la información.	RSI Y RGI	E764 - Procedimiento actualizado con mejores prácticas incluidas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	4	P2	T765 - Realizar actividades post incidente para evaluar y mejorar la respuesta.	RSI y RGI	E765 - Informes de actividades post incidente realizadas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-2	4	P2	T766 - Sistematizar las lecciones aprendidas para mejorar procedimientos, procesos y estrategias de mitigación y respuesta.	RSI y RGI	E766 - Registro de lecciones aprendidas y mejoras aplicadas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	1	P2	T767 - Realizar análisis forense ante un incidente de seguridad de la información o contactar al CSIRT de referencia para que lo realice.	RSI	E767 - Registros de análisis forenses realizados o de contacto con CSIRT.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	1	P2	T768 - Asegurar la participación de un equipo calificado o contactar al CSIRT de referencia.	RSI	E768 - Documentación de los incidentes en los que se ha solicitado análisis forense al CSIRT.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	2	P2	T769 - Establecer pautas para garantizar la cadena de custodia durante el análisis forense.	RSI	E769 - Documento de pautas para la cadena de custodia.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	3	P2	T770 - Generar los informes pertinentes del análisis forense y distribuirlos a las partes interesadas.	RSI	E770 - Informes de análisis forense generados y distribuidos a las partes interesadas.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	3	P2	T771 - Documentar todos los procedimientos vinculados al análisis forense.	RSI	E771 - Procedimientos documentados vinculados al análisis forense.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	3	P2	T772 - Asegurar que la documentación del análisis forense sea realizada por personal calificado.	RSI	E772 - Registros de capacitación del personal calificado en análisis forense.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	4	P2	T773 - Utilizar el resultado del análisis forense para la mejora continua del SGSI del organismo.	CSI	E773 - Informe sobre las mejoras implementadas basadas en los resultados del análisis forense.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-3	4	P2	T774 - Incorporar el análisis forense en la mejora de la gestión de riesgos de seguridad de la información.	RSI y RGI	E774 - Registros de ajustes y mejoras aplicadas en la gestión de riesgos a partir del análisis forense.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	1	P2	T775 - Definir lineamientos para la categorización de los incidentes según su tipo y criticidad.	RSI y RGI	E775 - Documento con los lineamientos para la categorización de incidentes.

RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	1	P2	T776 - Establecer un proceso para clasificar los incidentes según estos lineamientos.	RGI	E776 - Registros de incidentes categorizados según los lineamientos establecidos.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	2	P2	T777 - Determinar las acciones y tiempos de respuesta asociados a cada categoría según la severidad del incidente.	RSI	E777 - Documento con las acciones y tiempos de respuesta según la severidad.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	2	P2	T778 - Comunicar a los involucrados las acciones y tiempos de respuesta establecidos para cada categoría.	RSI y RGI	E778 - Registros de comunicación de acciones y tiempos de respuesta.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	3	P2	T779 - (REF. T308) Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E779 - (REF. E308) Política de gestión de incidentes de seguridad de la información.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	3	P2	T780 - (REF. T309) Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E780 - (REF. E309) Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	3	P2	T781 - Alinear las acciones asociadas a cada categoría con el plan de respuesta.	RGI	E781 - Registros de acciones alineadas con el plan de respuesta.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	3	P2	T782 - Implementar herramientas que apoyen la gestión de los incidentes.	RGI	E782 - Informes de implementación de herramientas para la gestión de incidentes.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	4	P2	T783 - Revisar periódicamente la categorización de incidentes y los planes de respuesta, considerando las necesidades del organismo y las tendencias de amenazas.	RSI y RGI	E783 - Informe de revisión periódica de categorización de incidentes y planes de respuesta.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-4	4	P2	T784 - Realizar estadísticas utilizando las categorizaciones de incidentes y utilizar los resultados para mejorar o incrementar los controles existentes.	RSI y RGI	E784 - Estadísticas generadas a partir de las categorizaciones y resultados de mejoras en los controles.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	1	P2	T785 - Establecer canales de comunicación para alertar sobre posibles vulnerabilidades que puedan afectar los activos y servicios críticos del centro de datos.	RSI y Director de Infraestructura	E785 - Registros de los canales de comunicación establecidos.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	1	P2	T786 - Identificar y definir fuentes de información relevantes para recibir alertas sobre vulnerabilidades.	RSI y Director de Infraestructura	E786 - Listado de fuentes de información utilizadas para alertas de vulnerabilidades.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	2	P2	T787 - Ampliar los canales de comunicación para incluir alertas sobre vulnerabilidades que puedan afectar los activos y servicios críticos del organismo.	RSI y Director de Infraestructura	E787 - Documentación de los canales de comunicación extendidos.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	2	P2	T788 - Establecer un mecanismo de acción basado en la criticidad de las vulnerabilidades.	RSI y Director de Infraestructura	E788 - Procedimiento documentado de respuesta basado en la criticidad de las vulnerabilidades.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	3	P2	T789 - Definir una metodología para la gestión de vulnerabilidades, con procedimientos detallados para su implementación.	RSI y Director de Infraestructura	E789 - Documento que define la metodología para la gestión de vulnerabilidades.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	3	P2	T790 - Implementar herramientas que apoyen la gestión de vulnerabilidades.	RSI y Director de Infraestructura	E790 - Registros de implementación de herramientas de gestión de vulnerabilidades.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	4	P2	T791 - Revisar periódicamente las fuentes de datos utilizadas para recibir alertas sobre vulnerabilidades.	RGV y Director de Infraestructura	E791 - Informe de revisión periódica de fuentes de datos de vulnerabilidades.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	4	P2	T792 - Adecuar la metodología de gestión de vulnerabilidades conforme a las necesidades del organismo y su contexto.	RSI y RGI	E792 - Documentación de la adecuación de la metodología a las necesidades del organismo.
RESPONDER (RE)	RE.AN	Análisis	RE.AN-5	4	P2	T793 - Utilizar la gestión de vulnerabilidades para la mejora continua del SGSI.	RSI y RGI	E793 - Registros de actividades de mejora continua implementadas en el SGSI.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	1	P2	T794 - Establecer mecanismos para responder y contener los incidentes detectados.	RSI	E794 - Registro de los mecanismos implementados para responder y contener incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	1	P2	T795 - Mitigar las consecuencias de los incidentes ocurridos.	RSI y Director de Infraestructura	E795 - Reportes de mitigación de consecuencias de incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	1	P2	T796 - Mantener un registro detallado de todos los incidentes.	RGI	E796 - Registro actualizado de incidentes.

RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	1	P2	T797 - Informar sobre los incidentes detectados al CERTuy o CSIRT correspondiente y a otras partes interesadas.	RSI	E797 - Notificaciones enviadas al CERTuy o CSIRT correspondiente.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	2	P2	T798 - Definir pautas claras para contener el daño y minimizar riesgos en el entorno operativo.	RSI y RGI	E798 - Documento con pautas para contención de daños.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	2	P2	T799 - Informar a las gerencias sobre los incidentes detectados y sus impactos.	RSI	E799 - Informes de incidentes enviados a las gerencias.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	2	P2	T800 - Elaborar planes de remediación para cada tipo de incidente identificado.	RGI	E800 - Planes de remediación documentados para incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	3	P2	T801 - (REF. T308) Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E801 - (REF. E308) Política de gestión de incidentes de seguridad de la información.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	3	P2	T802 - (REF. T309) Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E802 - (REF. E309) Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	3	P2	T803 - (REF. T712) Implementar herramientas automatizadas para el reporte de eventos y gestión de incidentes.	RSI	E803 - (REF. E712) Herramientas de automatización para el reporte de eventos y gestión de incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	4	P2	T804 - (REF. T764) Incorporar mejores prácticas en el procedimiento, incluyendo análisis forense y custodia de la información.	RSI Y RGI	E804 - (REF. E764) Procedimiento actualizado con mejores prácticas incluidas.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	4	P2	T805 - (REF. T765) Realizar actividades post incidente para evaluar y mejorar la respuesta.	RSI y RGI	E805 - (REF. E765) Informes de actividades post incidente realizadas.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-1	4	P2	T806 - (REF. T766) Sistematizar las lecciones aprendidas para mejorar procedimientos, procesos y estrategias de mitigación y respuesta.	RSI y RGI	E806 - (REF. E766) Registro de lecciones aprendidas y mejoras aplicadas.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	1	P2	T807 - (REF. T794) Establecer mecanismos para responder y contener los incidentes detectados.	RSI	E807 - (REF. E794) Registro de los mecanismos implementados para responder y contener incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	1	P2	T808 - (REF. T795) Mitigar las consecuencias de los incidentes ocurridos.	RSI y Director de Infraestructura	E808 - (REF. E795) Reportes de mitigación de consecuencias de incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	1	P2	T809 - (REF. T796) Mantener un registro detallado de todos los incidentes.	RGI	E809 - (REF. E796) Registro actualizado de incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	1	P2	T810 - (REF. T797) Informar sobre los incidentes detectados al CERTuy o CSIRT correspondiente y a otras partes interesadas.	RSI	E810 - (REF. E797) Notificaciones enviadas al CERTuy o CSIRT correspondiente.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	2	P2	T811 - (REF. T798) Definir pautas claras para contener el daño y minimizar riesgos en el entorno operativo.	RSI y RGI	E811 - (REF. E798) Documento con pautas para contención de daños.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	2	P2	T812 - (REF. T799) Informar a las gerencias sobre los incidentes detectados y sus impactos.	RSI	E812 - (REF. E799) Informes de incidentes enviados a las gerencias.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	2	P2	T813 - (REF. T800) Elaborar planes de remediación para cada tipo de incidente identificado.	RGI	E813 - (REF. E800) Planes de remediación documentados para incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	3	P2	T814 - (REF. T801) Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E814 - (REF. E801) Política de gestión de incidentes de seguridad de la información.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	3	P2	T815 - (REF. T802) Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E815 - (REF. E802) Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	3	P2	T816 - (REF. T803) Implementar herramientas automatizadas para el reporte de eventos y gestión de incidentes.	RGI y Director de TIC	E816 - (REF. E803) Herramientas de automatización para el reporte de eventos y gestión de incidentes..
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	4	P2	T817 - (REF. T764) Incorporar mejores prácticas en el procedimiento, incluyendo análisis forense y custodia de la información.	RSI Y RGI	E817 - (REF. E764) Procedimiento actualizado con mejores prácticas incluidas.

RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	4	P2	T818 - (REF. T765) Realizar actividades post incidente para evaluar y mejorar la respuesta.	RSI y RGI	E818 - (REF. E765) Informes de actividades post incidente realizadas.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-2	4	P2	T819 - (REF. T766) Sistematizar las lecciones aprendidas para mejorar procedimientos, procesos y estrategias de mitigación y respuesta.	RSI y RGI	E819 - (REF. E766) Registro de lecciones aprendidas y mejoras aplicadas.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	1	P2	T820 - (REF. T794) Establecer mecanismos para responder y contener los incidentes detectados.	RSI	E820 - (REF. E794) Registro de los mecanismos implementados para responder y contener incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	1	P2	T821 - (REF. T795) Mitigar las consecuencias de los incidentes ocurridos.	RSI y Director de Infraestructura	E821 - (REF. E795) Reportes de mitigación de consecuencias de incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	1	P2	T822 - (REF. T796) Mantener un registro detallado de todos los incidentes.	RGI	E822 - (REF. E796) Registro actualizado de incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	1	P2	T823 - (REF. T797) Informar sobre los incidentes detectados al CERTuy o CSIRT correspondiente y a otras partes interesadas.	RSI	E823 - (REF. E797) Notificaciones enviadas al CERTuy o CSIRT correspondiente.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	2	P2	T824 - (REF. T798) Definir pautas claras para contener el daño y minimizar riesgos en el entorno operativo.	RSI y RGI	E824 - (REF. E798) Documento con pautas para contención de daños.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	2	P2	T825 - (REF. T799) Informar a las gerencias sobre los incidentes detectados y sus impactos.	RSI	E825 - (REF. E799) Informes de incidentes enviados a las gerencias.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	2	P2	T826 - (REF. T800) Elaborar planes de remediación para cada tipo de incidente identificado.	RGI	E826 - (REF. E800) Planes de remediación documentados para incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	3	P2	T827 - (REF. T801) Desarrollar una política de gestión de incidentes de seguridad de la información.	CSI	E827 - (REF. E801) Política de gestión de incidentes de seguridad de la información.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	3	P2	T828 - (REF. T802) Establecer un plan de respuesta a incidentes de seguridad de la información.	RSI	E828 - (REF. E802) Plan de respuesta a incidentes de seguridad de la información.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	3	P2	T829 - (REF. T803) Implementar herramientas automatizadas para el registro y seguimiento de incidentes	RGI y Director de TIC	E829 - (REF. E803) Herramientas de automatización para el reporte de eventos y gestión de incidentes.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	4	P2	T830 - (REF. T764) Incorporar mejores prácticas en el procedimiento, incluyendo análisis forense y custodia de la información.	RSI Y RGI	E830 - (REF. E764) Procedimiento actualizado con mejores prácticas incluidas.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	4	P2	T831 - (REF. T765) Realizar actividades post incidente para evaluar y mejorar la respuesta.	RSI y RGI	E831 - (REF. E765) Informes de actividades post incidente realizadas.
RESPONDER (RE)	RE.MI	Mitigación	RE.MI-3	4	P2	T832 - (REF. T766) Sistematizar las lecciones aprendidas para mejorar procedimientos, procesos y estrategias de mitigación y respuesta.	RSI y RGI	E832 - (REF. E766) Registro de lecciones aprendidas y mejoras aplicadas.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	1	P2	T833 - Revisar periódicamente las estrategias de respuesta del centro de datos.	RSI y Director de Infraestructura	E833 - Registro de revisiones realizadas a las estrategias de respuesta del centro de datos.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	1	P2	T834 - Actualizar las estrategias de respuesta en función de los cambios en las necesidades del organismo.	RSI	E834 - Documentación de actualizaciones realizadas en respuesta a cambios en las necesidades del organismo.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	2	P2	T835 - Revisar periódicamente las estrategias de respuesta relacionadas con los procesos del organismo que afecten los servicios críticos.	RSI y Director de TIC	E835 - Informes de revisiones de estrategias de respuesta de los procesos críticos.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	2	P2	T836 - Coordinar las revisiones con las áreas responsables de los procesos críticos.	RSI	E836 - Actas de reuniones de coordinación con las áreas responsables.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	3	P2	T837 - Elaborar pautas o políticas documentadas para la revisión de estrategias de respuesta.	RSI	E837 - Políticas o pautas documentadas para la revisión de estrategias de respuesta.

RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	3	P2	T838 - Difundir las pautas o políticas al personal involucrado.	RSI	E838 - Registro de la difusión de pautas o políticas al personal involucrado.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	3	P2	T839 - Supervisar el cumplimiento de las pautas o políticas documentadas.	RSI	E839 - Informes de cumplimiento de las pautas documentadas.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	4	P2	T840 - Incorporar mejoras identificadas en las revisiones de estrategia para ajustar las estrategias de respuesta.	RSI	E840 - Registro de mejoras implementadas en las estrategias de respuesta.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	4	P2	T841 - Utilizar las mejoras para optimizar el SGSI y fortalecer la gestión de riesgos de seguridad de la información.	RSI y RGR	E841 - Documentación de ajustes realizados en el SGSI y en la gestión de riesgos.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-2	4	P2	T842 - Definir e implementar indicadores para el seguimiento y control de las estrategias de respuesta.	RSI	E842 - Indicadores definidos e informes de seguimiento y control.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	1	P2	T843 - Implementar y mantener medidas de continuidad en el centro de datos, incluyendo alimentación redundante de energía eléctrica, control ambiental y redundancia en telecomunicaciones.	Director de Infraestructura	E843 - Documentación de medidas de continuidad en el centro de datos.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	1	P2	T844 - Establecer un procedimiento para informar incidentes detectados al CERTuy o CSIRT correspondiente.	RSI	E844 - Registro de incidentes informados al CERTuy o CSIRT.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	2	P2	T845 - Elaborar un plan y/o procedimiento inicial de respuesta a incidentes.	RSI y RGI	E845 - Plan o procedimiento inicial de respuesta a incidentes.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	2	P2	T846 - Definir lineamientos para la ejecución de actividades de recuperación ante incidentes.	RSI	E846 - Lineamientos establecidos para actividades de recuperación ante incidentes.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	3	P2	T847 - (REF. T550) Diseñar un plan de contingencia y de recuperación.	RSI y Director de Infraestructura	E847 - (REF. E550) Plan de contingencia y recuperación.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	3	P2	T848 - Realizar pruebas del plan de contingencia y recuperación, asegurando que se registren los resultados.	RSI y Director de Infraestructura	E848 - Registros de pruebas realizadas al plan de contingencia y recuperación.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	4	P2	T849 - Designar un responsable de respuesta a incidentes para coordinar tareas de recuperación con los actores involucrados.	Director de TIC	E849 - Acta de designación del Responsable de Respuesta a Incidentes.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	4	P2	T850 - Ejecutar pruebas anuales del plan de respuesta a incidentes y del plan de contingencia y recuperación.	RSI y RGI	E850 - Reportes de pruebas anuales del plan de recuperación y contingencia.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	4	P2	T851 - Comunicar los resultados de las pruebas a la Dirección y partes interesadas.	RSI	E851 - Informe de resultados de pruebas comunicados a la Dirección.
RECUPERAR (RC)	RC.PR	Planificación de la recuperación	RC.PR-1	4	P2	T852 - Utilizar las lecciones aprendidas de las pruebas para mejorar continuamente los planes y procedimientos.	RSI y Director de TIC	E852 - Documento con lecciones aprendidas y mejoras implementadas en los planes y procedimientos.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	1	P2	T853 - Revisar periódicamente las estrategias de recuperación del centro de datos.	RSI y Director de Infraestructura	E853 - Registros de revisiones de las estrategias de recuperación del centro de datos.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	1	P2	T854 - Realizar revisiones adicionales cuando existan cambios en las necesidades del organismo.	RSI y Director de TIC	E854- Registros de revisiones de las estrategias de recuperación del centro de datos.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	2	P2	T855 - Revisar periódicamente las estrategias de recuperación de los procesos organizacionales, especialmente los servicios críticos.	CSI	E855 - Informes de revisiones periódicas de estrategias de recuperación de servicios críticos.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	2	P2	T856 - Comunicar las estrategias de recuperación a todo el organismo, enfatizando las relacionadas con servicios críticos.	RSI	E856 - Comunicaciones internas sobre estrategias de recuperación.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	3	P2	T857 - Desarrollar una política de continuidad de las operaciones y recuperación ante desastres.	CSI	E857 - Política de Continuidad de las Operaciones y Recuperación ante Desastres.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	3	P2	T858 - Asegurar que las revisiones de estrategias se basen en los cambios identificados por el Análisis de Impacto al Negocio (BIA).	RSI y Director de TIC	E858 - Informes que relacionan cambios detectados por el BIA con actualizaciones en estrategias de recuperación.

RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	4	P2	T859 - (REF. T840) Incorporar mejoras identificadas en las revisiones de estrategia para ajustar las estrategias de respuesta.	RSI	E859 - (REF. E840) Registro de mejoras implementadas en las estrategias de respuesta.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	4	P2	T860 - (REF. T841) Utilizar las mejoras para optimizar el SGSI y fortalecer la gestión de riesgos de seguridad de la información.	RSI y RGR	E860 - (REF. E841) Documentación de ajustes realizados en el SGSI y en la gestión de riesgos.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-2	4	P2	T861 - (REF. T842) Definir e implementar indicadores para el seguimiento y control de las estrategias de respuesta.	RSI	E861 - (REF. E842) Indicadores definidos e informes de seguimiento y control.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	1	P3	T862 - Identificar los servicios críticos del organismo.	CSI	E862 - Informe de identificación de servicios críticos.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	1	P3	T863 - Identificar los componentes prioritarios del centro de datos para la entrega de los servicios críticos.	Director de Infraestructura	E863 - Inventario de componentes prioritarios del centro de datos.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	1	P3	T864 - Definir el tratamiento proactivo para atender eventos e incidentes de ciberseguridad.	RGI y RSI	E864 - Documento de estrategias de tratamiento proactivo para eventos e incidentes de ciberseguridad.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	2	P3	T865 - Identificar las dependencias de los componentes prioritarios.	CSI	E865 - Documento de dependencias de los componentes prioritarios.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	2	P3	T866 - Establecer planes de mantenimiento para los componentes prioritarios.	RSI	E866 - Planes de mantenimiento aprobados.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	2	P3	T867 - Determinar los niveles de capacidad mínima para garantizar la entrega de los servicios críticos.	CSI	E867 - Informe de niveles de capacidad mínima definidos.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	2	P3	T868 - Implementar la gestión de capacidad.	Director de TIC y RSI	E868 - Registro de ejecución de la gestión de capacidad.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	3	P3	T869 - Documentar, aprobar y gestionar los cambios en los componentes prioritarios y sus dependencias.	Director de TIC y RSI	E869 - Registro de aprobación y documentación de cambios en componentes prioritarios.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	3	P3	T870 - Realizar notificaciones a las partes interesadas sobre los cambios en los componentes prioritarios.	RSI	E870 - Reportes de notificaciones enviadas a las partes interesadas.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	3	P3	T871 - Validar periódicamente la gestión de capacidad.	Director de TIC y RSI	E871 - Informe de validación periódica de gestión de capacidad.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	4	P3	T872 - Documentar y priorizar el manejo de los servicios críticos de toda la infraestructura tecnológica.	Director de Infraestructura y RSI	E872 - Documento de priorización y manejo de servicios críticos.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	4	P3	T873 - Implementar monitoreo automatizado de los componentes prioritarios.	RM y Director de Infraestructura	E873 - Registro de implementación del monitoreo automatizado.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	4	P3	T874 - Configurar alertas del estado de los componentes ante cambios en el entorno.	RM y Director de Infraestructura	E874 - Reportes de alertas generadas por cambios en el entorno.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-4	4	P3	T875 - Realizar una gestión de capacidad a largo plazo (más de 3 años).	Director de TIC y RSI	E875 - Plan de gestión de capacidad a largo plazo.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	1	P3	T876 - Verificar la existencia de UPS y componentes redundantes en el centro de datos.	Director de Infraestructura	E876 - Informe de verificación de UPS y componentes redundantes.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	1	P3	T877 - Garantizar redundancia en la conexión eléctrica, acondicionamiento térmico e infraestructura de comunicaciones.	Director de Infraestructura	E877 - Registro de auditoría de redundancia en conexiones eléctricas, térmicas y de comunicaciones.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	2	P3	T878 - Definir las ventanas de tiempo máximo soportadas por el organismo sin operar.	CSI	E878 - Documento de definición de ventanas de tiempo máximo de inactividad.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	2	P3	T879 - Implementar un generador eléctrico capaz de alimentar todos los componentes críticos del centro de datos.	Director de Infraestructura	E879 - Registro de instalación y pruebas del generador eléctrico.

IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	3	P3	T880 - Diseñar y aprobar un plan de contingencia y recuperación para los procesos críticos del organismo.	CSI	E880 - Plan de contingencia y recuperación aprobado.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	3	P3	T881 - Realizar pruebas iniciales del plan en uno o varios procesos críticos.	RSI y Director de TIC	E881 - Informe de ejecución de pruebas iniciales del plan en procesos críticos.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	4	P3	T882 - Ejecutar pruebas del plan de contingencia y recuperación de forma periódica.	Director de Infraestructura y RSI	E882 - Reportes de ejecución y resultados de pruebas del plan de contingencia.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	4	P3	T883 - Capacitar a todos los involucrados en el plan y su ejecución.	RSI y Director de Infraestructura	E883 - Registro de capacitaciones realizadas.
IDENTIFICAR (ID)	ID.AN	Ambiente del negocio	ID.AN-5	4	P3	T884 - Analizar los resultados de las pruebas y generar lecciones aprendidas para mejorar el plan.	RSI y Director de TIC	E884 - Documento de lecciones aprendidas y acciones de mejora implementadas.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	1	P3	T885 - Establecer un proceso para la gestión de riesgos de los componentes del centro de datos.	Director de Infraestructura	E885 - Documento del proceso de gestión de riesgos de los componentes del centro de datos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	1	P3	T886 - Identificar y gestionar de forma independiente los riesgos asociados a los servicios críticos.	RGR	E886 - Registro de identificación y mitigación de riesgos en servicios críticos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	2	P3	T887 - Implementar una metodología para la gestión de riesgos de ciberseguridad.	RGR	E887 - Documento de metodología de gestión de riesgos de ciberseguridad.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	2	P3	T888 - Establecer un plan de trabajo para el tratamiento de los riesgos identificados.	RGR	E888 - Plan de trabajo para tratamiento de riesgos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	2	P3	T889 - (REF. T038) Designar un rol responsable de la gestión de riesgos (RGR).	RSI	E889 - (REF. E038) Resolución con designación del RGR.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	3	P3	T890 - (REF. T094) Definir una política de gestión de riesgos	RSI	E890 - (REF. E094) Política de gestión de riesgos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	3	P3	T891 - (REF. T095) Seguimiento periódico del inventario de riesgos identificados y documentar,	RSI	E891 - (REF. E095) Plan e informe de revisión periódica de riesgos.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	3	P3	T892 - (REF. T096) Comunicar los resultados de la revisión al CSI y otras partes interesadas.	RSI	E892 - (REF. E096) Comunicación formal de los resultados al CSI.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	4	P3	T893 - (REF. T097) Formalizar el resultado de la revisión de los riesgos frente al CSI y al directorio.	RSI	E893 - (REF. E097) Informe elevado al CSI y al directorio del organismo.
IDENTIFICAR (ID)	ID.GR	Estrategia para la gestión de riesgos	ID.GR-1	4	P3	T894 - (REF. T098) Establecer y realizar actividades de control interno para verificar el cumplimiento con la política establecida	RSI	E894 - (REF. E098) Informes de actividades de control interno.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	1	P3	T895 - (REF. T956) Capacitar al personal en las actividades básicas a realizar en caso de detectar o sospechar un incidente.	RSI y Capacitación	E895 - (REF. E956) Registro de capacitaciones sobre respuesta a incidentes.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	1	P3	T896 - (REF. T132) Identificar todos los proveedores de servicios críticos del organismo.	Director de Infraestructura	E896 - (REF. E132) Lista completa de proveedores de servicios críticos identificados.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	2	P3	T897 - (REF. T305) Crear mecanismos para la respuesta a incidentes, especificando roles, responsabilidades, tiempos de respuesta, y acciones a seguir.	RSI	E987 - (REF. E305) Documento de mecanismos de respuesta a incidentes.

IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	2	P3	T898 - (REF. T959) Establecer un plan básico de recuperación.	RSI y Director de Infraestructura	E959 - (REF. E959) Plan básico de recuperación.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	2	P3	T899 - (REF. T960) Capacitar a los involucrados en los mecanismos de respuesta y plan básico de recuperación.	RSI Y Director de Infraestructura	E960 - (REF. E960) Registro de capacitaciones realizadas en mecanismos de respuesta y plan básico de recuperación.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	3	P3	T900 - (REF. T309) Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E900 - (REF. E309) Plan de respuesta a incidentes de seguridad de la información.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	3	P3	T901 - (REF. T962) Desarrollar un plan de recuperación ante desastres (DRP).	RSI y Director de Infraestructura	E901 - (REF. E962) Plan de recuperación ante desastres (DRP).
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	3	P3	T902 - (REF. T963) Registrar los resultados de la ejecución de los planes de respuesta a incidentes y DRP.	Director de Infraestructura	E902 - (REF. E963) Registros de pruebas de respuesta a incidentes y DRP.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	4	P3	T903 - (REF. T964) Alinear el plan de respuesta a incidentes con el DRP.	RGI y RSI	E903 - (REF. E964) Documentación del alineamiento entre plan respuesta a incidentes y DRP.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	4	P3	T904 - (REF. T965) Realizar pruebas anuales del plan de respuesta a incidentes y DRP.	RSI	E904 - (REF. E965) Planificación anual de plan respuesta a incidentes y DRP.
IDENTIFICAR (ID)	ID.CS	Gestión de riesgos en la cadena de suministros	ID.CS-5	4	P3	T905 - (REF. T966) Utilizar como insumo los resultados de las pruebas de plan de respuesta a incidentes y DRP para mejora continua.	RSI	E905 - (REF. E966) Informe de lecciones aprendidas y mejoras aplicadas al plan de respuesta a incidentes y DRP.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	1	P3	T906 - Evaluar y documentar la capacidad actual instalada para la prestación de los servicios críticos.	Director de Infraestructura	E906 - Informe de capacidad instalada de los servicios críticos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	2	P3	T907 - Considerar las necesidades de capacidad al dimensionar los servicios críticos de acuerdo a las necesidades del organismo.	Director de Infraestructura	E907 - Documento de criterios para dimensionamiento de servicios críticos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	2	P3	T908 - Implementar mediciones objetivas para detectar problemas de capacidad en los servicios críticos.	RM y Director de Infraestructura	E908 - Reportes de medición de capacidad y detección de problemas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	3	P3	T909 - Definir y documentar el proceso de gestión de la capacidad actual.	Director de Infraestructura	E909 - Documento del proceso de gestión de la capacidad.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	3	P3	T910 - Identificar y asignar un responsable del proceso de gestión de la capacidad.	Director de Infraestructura	E910 - Acta de designación del responsable de la gestión de la capacidad.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	3	P3	T911 - Establecer roles y responsabilidades dentro del proceso de gestión de la capacidad.	Director de Infraestructura	E911 - Matriz de roles y responsabilidades en la gestión de la capacidad.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	4	P3	T912 - Elaborar y aprobar un plan formal de capacidad.	RSI y Director de TIC	E912 - Plan de capacidad aprobado.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	4	P3	T913 - Definir un proceso de estimación de la capacidad alineado con el plan.	RSI y Director de Infraestructura	E913 - Procedimiento de estimación de capacidad.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	4	P3	T914 - Utilizar la información obtenida para generar pronósticos de capacidad.	Director de TIC	E914 - Informes de pronósticos de capacidad.

PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	4	P3	T915 - Establecer revisiones periódicas del plan de capacidad.	Director de TIC	E915 - Registro de revisiones del plan de capacidad.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-4	4	P3	T916 - Implementar acciones de mejora continua en la gestión de capacidad.	Director de Infraestructura	E916 - Reporte de mejoras implementadas en la gestión de capacidad.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	1	P3	T917 - (REF. T607) Identificar los sistemas y servicios más críticos.	CSI	E917 - (REF. E607) Listado de sistemas y servicios críticos.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	1	P3	T918 - (REF. T608) Establecer un procedimiento básico para realizar monitoreos reactivos o esporádicos.	RSI y Director de TIC	E918 - (REF. E608) Registro de monitoreos realizados de manera reactiva.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	1	P3	T919 - (REF. T609) Documentar los resultados de los monitoreos realizados y las acciones correctivas.	RSI	E919 - (REF. E609) Informe de acciones correctivas aplicadas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	2	P3	T920 - (REF. T610) Implementar herramientas de monitoreo automatizadas para los activos críticos.	RM y Director de Infraestructura	E920 - (REF. E610) Configuración de herramientas de monitoreo automatizadas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	2	P3	T921 - (REF. T611) Configurar las alertas en las herramientas de monitoreo.	Director de Infraestructura	E921 - (REF. E611) Registro de alertas generadas.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	2	P3	T922 - (REF. T612) Documentar un procedimiento para el monitoreo automatizado y la gestión de alertas.	Director de TIC y RSI	E922 - (REF. E612) Procedimiento documentado para el monitoreo automatizado.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	3	P3	T923 - (REF. T613) Ajustar las herramientas de monitoreo para identificar patrones de anomalías.	Director de Infraestructura	E923 - (REF. E613) Configuración avanzada de herramientas de monitoreo para patrones de anomalías.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	3	P3	T924 - (REF. T614) Establecer un procedimiento para la revisión y análisis de anomalías detectadas.	Director de Infraestructura	E924 - (REF. E614) Procedimiento documentado para la revisión de anomalías.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	4	P3	T925 - (REF. T615) Ampliar el monitoreo a todos los activos de información del centro de datos.	Director de Infraestructura	E925 - (REF. E615) Registro del monitoreo de todos los activos de información.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	4	P3	T926 - (REF. T616) Implementar un sistema que permita cruzar información de diversas fuentes para generar alertas más precisas.	Director de Infraestructura	E926 - (REF. E616) Configuración del sistema de cruzamiento de información.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	4	P3	T927 - (REF. T617) Diseñar e implementar un mecanismo alternativo de monitoreo manual.	Director de Infraestructura	E927 - (REF. E617) Documentación del mecanismo alternativo de monitoreo.
PROTEGER (PR)	PR.SD	Seguridad de los datos	PR.SD-8	4	P3	T928 - (REF. T618) Documentar lecciones aprendidas y oportunidades de mejora a partir de los resultados del monitoreo.	Director de Infraestructura	E928 - (REF. E618) Informes de lecciones aprendidas y oportunidades de mejora.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	1	P3	T930 - (REF. T510) Establecer medidas básicas para comunicar y autorizar los cambios en el ámbito tecnológico.	RSI y Director de Desarrollo	E930 - (REF. E510) Documentos o registros de comunicación y autorización de cambios.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	1	P3	T931 - (REF. T511) Asegurar que los cambios sean registrados y documentados de manera general.	Director de Desarrollo	E931 - (REF. E511) Listado inicial de cambios realizados durante el período.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	2	P3	T932 - (REF. T512) Definir procesos formales de versionado para los productos de software.	Director de Desarrollo	E932 - (REF. E512) Procedimiento formal para el versionado.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la	PR.PI-1	2	P3	T933 - (REF. T513) Establecer líneas base de configuración para permitir la trazabilidad de los cambios.	Director de Desarrollo y RSI	E933 - (REF. E513) Registros de líneas base de configuración y trazabilidad de cambios. Herramientas utilizadas para el control de versiones.

		protección de la información						
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	3	P3	T934 - (REF. T514) - Desarrollar una política de gestión de cambios.	CSI	E934 - (REF. E514) Política de Gestión de Cambio.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	3	P3	T935 - (REF. T515) Documentar el procedimiento de gestión de cambios y asegurar su implementación.	RSI y Director de Desarrollo	E935 - (REF. E515) Listado (muestra) de cambios en el período auditado y listado de cambios de emergencia.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	3	P3	T936 - (REF. T516) Registrar todos los cambios realizados a las líneas base.	Director de Desarrollo	E936 - (REF. E516) Evidencia de análisis de riesgos, autorización, aprobación y registro de cambios.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	4	P3	T937 - (REF. T517) Implementar herramientas automatizadas que apoyen la gestión de los cambios.	Director de Desarrollo	E937 - (REF. E517) Herramientas utilizadas para la gestión de cambios.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	4	P3	T938 - (REF. T518) Realizar actividades de control interno para revisar el cumplimiento de los procedimientos de gestión de cambios.	Director de Desarrollo	E938 - (REF. E518) Resultados de revisiones internas sobre cumplimiento de procedimientos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	4	P3	T939 - (REF. T519) Comunicar los resultados de las revisiones al RSI y partes interesadas.	Director de Desarrollo	E939 - (REF. E519) Comunicaciones dirigidas al RSI y partes interesadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-1	4	P3	T940 - (REF. T520) Tomar medidas correctivas frente a desvíos y utilizar los resultados para mejora continua.	RSI y Director de Desarrollo	E940 - (REF. E520) Registro de acciones correctivas y lecciones aprendidas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-7	1	P3	T941 - Realizar revisiones periódicas de los procesos de protección de los activos críticos del centro de datos.	Director de Infraestructura	E941 - Informes de revisión de los procesos de protección en el centro de datos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-7	2	P3	T942 - Ampliar la revisión de los procesos de protección a los activos y servicios del organismo.	Director de Infraestructura y RSI	E942 - Registro de revisión de procesos de protección en todo el organismo.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-7	2	P3	T943 - Comunicar los resultados de las revisiones a todas las partes interesadas.	RSI	E943 - Evidencia de comunicación a las partes interesadas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-7	3	P3	T944 - Registrar los cambios realizados a los procesos de protección, incluyendo configuraciones de seguridad.	Director de Infraestructura	E944 - Registro de cambios en configuraciones de seguridad.

PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-7	3	P3	T945 - Implementar una gestión formal de cambios en los procesos de protección.	Director de Infraestructura	E945 - Documentación del proceso de gestión de cambios en protección.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-7	4	P3	T946 - Incorporar los resultados de las revisiones a la mejora continua del SGSI.	RSI	E946 - Informes de impacto y mejora continua en el SGSI.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-7	4	P3	T947 - Evaluar el impacto de los cambios en la protección y definir mejoras estratégicas.	CSI	E947 - Actas de la comisión de seguridad con decisiones sobre mejoras.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	1	P3	T948 - Establecer una metodología para documentar lecciones aprendidas de incidentes de seguridad en el centro de datos.	Director de Infraestructura	E948 - Documentos con registros de lecciones aprendidas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	1	P3	T949 - Registrar las lecciones aprendidas en una base de datos o repositorio accesible para el equipo de seguridad.	RGI	E949 - Repositorio de lecciones aprendidas en el centro de datos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	2	P3	T950 - Extender la sistemática de aprendizaje de incidentes a toda el organismo.	RSI	E950 - Registro de incidentes y aprendizajes a nivel organizacional.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	2	P3	T951 - Difundir las lecciones aprendidas a todas las partes interesadas mediante informes o reuniones periódicas.	RSI	E951 - Evidencia de comunicaciones o reuniones con partes interesadas
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	3	P3	T952 - Incorporar las lecciones aprendidas en los planes de respuesta a incidentes.	RGI	E952 - Plan de respuesta actualizado con lecciones aprendidas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	3	P3	T953 - Ajustar y mejorar los canales de comunicación y los procesos de escalamiento en base a incidentes pasados.	RGI	E953 - Documentación de mejoras en comunicación y escalamiento.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	4	P3	T954 - Analizar las lecciones aprendidas para mejorar el SGSI y el análisis de riesgos.	RSI	E954 - Informe de mejoras en el SGSI basado en lecciones aprendidas.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-8	4	P3	T955 - Definir indicadores para medir la efectividad de los controles implementados.	Director de TIC y RSI	E955 - Reporte de indicadores de efectividad de controles.
PROTEGER (PR)	PR.PI	Procesos y procedimientos	PR.PI-10	1	P3	T956 - Capacitar al personal en las actividades básicas a realizar en caso de detectar o sospechar un incidente.	RSI y Capacitación	E956 - Registro de capacitaciones sobre respuesta a incidentes.

		para la protección de la información						
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	1	P3	T957 - Identificar y documentar a los proveedores que brindan soporte a los servicios críticos.	Director de Infraestructura	E957 - Listado actualizado de proveedores de soporte a servicios críticos.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	2	P3	T958 - (REF. T305) Crear mecanismos para la respuesta a incidentes, especificando roles, responsabilidades, tiempos de respuesta, y acciones a seguir.	RSI	E958 - (REF. E305) Documento de mecanismos de respuesta a incidentes.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	2	P3	T959 - Establecer un plan básico de recuperación.	RSI y Director de Infraestructura	E959 - Plan básico de recuperación
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	2	P3	T960 - Capacitar a los involucrados en los mecanismos de respuesta y plan básico de recuperación.	RSI Y Director de Infraestructura	E960 - Registro de capacitaciones realizadas en mecanismos de respuesta y plan básico de recuperación.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	3	P3	T961 - (REF. T309) Establecer un plan de respuesta a incidentes de seguridad de la información.	RGI	E961 - (REF. E309) Plan de respuesta a incidentes de seguridad de la información.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	3	P3	T962 - Desarrollar un plan de recuperación ante desastres (DRP).	RSI y Director de Infraestructura	E962 - Plan de recuperación ante desastres (DRP).
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	3	P3	T963 - Registrar los resultados de la ejecución de los planes de respuesta a incidentes y DRP.	Director de Infraestructura	E963 - Registros de pruebas de respuesta a incidentes y DRP.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	4	P3	T964 - Alinear el plan de respuesta a incidentes con DRP.	RGI y RSI	E964 - Documentación del alineamiento entre plan respuesta a incidentes y DRP.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	4	P3	T965 - Realizar pruebas anuales del plan de respuesta a incidentes y DRP.	RSI	E965 - Planificación anual de plan respuesta a incidentes y DRP.
PROTEGER (PR)	PR.PI	Procesos y procedimientos para la protección de la información	PR.PI-10	4	P3	T966 - Utilizar como insumo los resultados de las pruebas de plan de respuesta a incidentes y DRP para mejora continua.	RSI	E966 - Informe de lecciones aprendidas y mejoras aplicadas al plan de respuesta a incidentes y DRP.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	1	P3	T967 - Realizar el mantenimiento de los activos del centro de datos según los requerimientos técnicos.	Director de Infraestructura	E967 - Registro de mantenimiento de activos tecnológicos.

PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	1	P3	T968 - Registrar las tareas de mantenimiento realizadas en los activos.	Director de Infraestructura	E968 - Reportes de intervenciones en los equipos del centro de datos.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	2	P3	T969 - Definir y documentar planes anuales de mantenimiento.	Director de Infraestructura	E969 - Documento de planes anuales de mantenimiento.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	2	P3	T970 - Gestionar accesos a los usuarios autorizados para realizar tareas de mantenimiento programado.	Director de Infraestructura	E970 - Registros de acceso para mantenimiento.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	2	P3	T971 - Registrar el mantenimiento, fallos y cambios realizados sobre los activos.	Director de Infraestructura	E971 - Reportes de fallos y cambios en los activos.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	3	P3	T972 - Desarrollar un procedimiento de mantenimiento preventivo y correctivo para la plataforma tecnológica.	Director de Infraestructura y RSI	E972 - Documento de procedimiento de mantenimiento.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	3	P3	T973 - Implementar el procedimiento en la planificación del mantenimiento de los activos.	Director de Infraestructura y RSI	E973 - Informes de cumplimiento del procedimiento.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	3	P3	T974 - Evaluar periódicamente la efectividad del procedimiento.	Director de Infraestructura y RSI	E974 - Evaluaciones de efectividad del mantenimiento.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	4	P3	T975 - Implementar procesos de control de cambio para el mantenimiento de los activos.	RSI	E975 - Registros de control de cambios en mantenimiento.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	4	P3	T976 - Documentar y gestionar aprobaciones del CSI para las tareas de mantenimiento.	RSI	E976 - Documentación de aprobaciones del CSI.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-1	4	P3	T977 - Implementar un proceso de control interno para verificar el cumplimiento del mantenimiento del equipamiento.	Director de Infraestructura y RSI	E977 - Informes de control interno sobre el cumplimiento de mantenimiento.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	1	P3	T978 - Aprobar la alta y baja de usuarios (internos o externos) que realizan mantenimiento remoto.	Director de infraestructura	E978 - Registros de aprobación y baja de usuarios remotos.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	1	P3	T979 - Documentar las aprobaciones y bajas de accesos remotos en los activos informáticos del centro de datos.	Director de infraestructura	E979 - Listado actualizado de usuarios con acceso remoto.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	2	P3	T980 - Implementar un proceso de gestión de aprobación de usuarios para conexión remota.	Director de infraestructura y RSI	E980 - Documento de plan anual de mantenimiento aprobado.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	2	P3	T981 - Registrar todos los eventos de acceso remoto de cada usuario.	Director de infraestructura	E981 - Registros de accesos remotos detallados.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	2	P3	T982 - Garantizar el cumplimiento de cláusulas de confidencialidad, integridad y disponibilidad de la información.	Director de infraestructura	E982 - Acuerdos de confidencialidad firmados.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	3	P3	T983 - Desarrollar un procedimiento que genere alertas automáticas en cada evento de conexión remota.	Director de infraestructura y RSI	E983 - Procedimiento documentado para generación de alertas automáticas.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	3	P3	T984 - Implementar un sistema de monitoreo para identificar y trazar actividades de usuarios conectados.	RM	E984 - Informes de trazabilidad de actividades en accesos remotos.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	3	P3	T985 - Evaluar las alertas y detectar posibles desviaciones en las acciones de mantenimiento.	RM	E985 - Reportes de análisis de alertas generadas
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	4	P3	T986 - Realizar revisiones periódicas de logs de acceso remoto y actividades de usuarios.	RSI	E986 - Informes de auditoría de accesos remotos.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	4	P3	T987 - Implementar controles internos para detectar accesos no autorizados o actividades sospechosas.	Director de Infraestructura y RSI	E987 - Registros de revisiones periódicas de logs.
PROTEGER (PR)	PR.MA	Mantenimiento	PR.MA-2	4	P3	T988 - Generar informes y reportes para retroalimentar el proceso de mantenimiento remoto.	Director de Infraestructura y RSI	E988 - Reportes de control de accesos y actividades sospechosas.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-2	1	P3	T989 - Difundir la importancia de la protección y uso seguro de medios extraíbles.	RSI y Capacitación	E989 - Materiales de difusión y registros de capacitaciones realizadas.

PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-2	2	P3	T990 - Identificar y documentar los tipos de medios extraíbles autorizados.	Director de TIC	E990 - Documento de medios extraíbles autorizados.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-2	2	P3	T991 - Definir y comunicar pautas para el uso de medios extraíbles.	RSI	E991 - Registro de comunicaciones enviadas sobre las pautas de uso.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-2	3	P3	T992 - Implementar un proceso de reporte de hurto, pérdida o daño de medios extraíbles.	Director de Infraestructura	E992 - Registros de reportes de incidentes de medios extraíbles.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-2	3	P3	T993 - Definir e implementar el procedimiento de eliminación segura de medios extraíbles al final de su vida útil.	Director de Infraestructura	E993 - Registros de eliminación segura de medios extraíbles.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-2	4	P3	T994 - Realizar revisiones de control interno sobre el cumplimiento de las pautas de uso y el procedimiento de medios extraíbles.	Director de Infraestructura y RSI	E994 - Informes de revisión interna sobre cumplimiento de pautas.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-2	4	P3	T995 - Analizar los resultados de las revisiones para mejorar el procedimiento y comunicar los hallazgos al RSI y partes interesadas.	Director de Infraestructura y RSI	E995 - Documento de mejora del procedimiento basado en los hallazgos.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-5	1	P3	T996 - Implementar redundancia en los componentes críticos del centro de datos para asegurar la entrega de servicios y tolerar fallos.	Director de Infraestructura	E996 - Registro de los componentes con redundancia y sus configuraciones.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-5	2	P3	T997 - Implementar y configurar un centro de datos alternativo para asegurar la resiliencia y prolongación operativa en caso de fallas.	Director de Infraestructura y RSI	E998 - Documentación del centro de datos alternativo y su capacidad operativa.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-5	3	P3	T998 - Documentar la implementación y pruebas de los mecanismos de tolerancia a fallos en el centro de datos principal.	Director de Infraestructura y RSI	E998 - Informe de implementación y pruebas de tolerancia a fallos.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-5	3	P3	T999 - Realizar pruebas periódicas en el centro de datos alternativo para verificar la correcta configuración de los sistemas.	Director de Infraestructura y RSI	E999 - Registro de resultados de pruebas periódicas en el centro de datos alternativo.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-5	4	P3	T1000 - Garantizar que todos los componentes de soporte a los servicios críticos cuenten con redundancia.	Director de Infraestructura y RSI	E1000 - Reporte de la redundancia implementada en todos los componentes críticos.
PROTEGER (PR)	PR.TP	Tecnología de protección	PR.TP-5	4	P3	T1001 - Mejorar continuamente los procesos de resiliencia basado en pruebas periódicas, ajustando la calibración de activos según las necesidades del negocio.	Director de Infraestructura y RSI	E1001 - Documentación de ajustes y calibraciones realizadas con base en las pruebas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	1	P3	T1002 - Definir parámetros esperables para usuarios privilegiados.	RSI	E1002 - Documento con los parámetros definidos para usuarios privilegiados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	1	P3	T1003 - Gestionar parámetros esperables para sistemas críticos del centro de datos.	Director de Infraestructura	E1003 - Registro de parámetros configurados para sistemas críticos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	2	P3	T1004 - Definir parámetros esperables para todos los usuarios asociados a servicios críticos del organismo.	RSI	E1004 - Inventario de parámetros esperables para usuarios y sistemas críticos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	2	P3	T1005 - Gestionar parámetros esperables para sistemas de soporte u otros que deban ser monitoreados.	Director de Infraestructura	E1005 - Registro de configuraciones para sistemas de soporte y otros sistemas monitoreados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	2	P3	T1006 - Reportar desvíos al RSI.	Director de Infraestructura	E1006 - Informes de desvíos registrados y enviados al RSI.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	3	P3	T1007 - Documentar la línea base de operaciones de red y flujos de datos esperados.	RSI	E1007 - Documento oficial de la línea base de operaciones de red y flujos de datos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	3	P3	T1008 - Definir el procedimiento de monitoreo y actuación ante desvíos.	RM	E1008 - Procedimiento documentado para monitoreo y actuación ante desvíos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	3	P3	T1009 - Generar indicadores y métricas sobre los eventos monitoreados.	RM y RSI	E1009 - Reportes periódicos con indicadores y métricas generados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	4	P3	T1010 - Revisar periódicamente la configuración de la línea base.	RSI	E1010 - Actas de revisiones periódicas de la configuración de la línea base.

DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	4	P3	T1011 - Realizar revisiones de la línea base ante cambios tecnológicos o de objetivos de organismo.	RM y RSI	E1011 - Documentación de revisiones realizadas ante cambios tecnológicos u organizacionales.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	4	P3	T1012 - Utilizar los indicadores para la mejora continua de la línea base.	RM y RGI	E1012 - Análisis de indicadores utilizados para mejoras continuas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-1	4	P3	T1013 - Apoyar la gestión de la línea base con las métricas generadas.	RM y RGI	E1013 - Reportes consolidados de métricas aplicadas a la gestión de la línea base.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	1	P3	T1014 - Revisar los eventos locales generados por el equipamiento y activos del centro de datos.	RM y Director de Infraestructura	E1014 - Listado de eventos locales revisados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	1	P3	T1015 - Registrar las revisiones realizadas sobre los eventos locales.	RM y Director de Infraestructura	E1015 - Registro documentado de las revisiones realizadas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	2	P3	T1016 - Configurar los sistemas que soportan los servicios críticos para emitir alertas de eventos según las pautas establecidas por el apetito de riesgo del organismo.	RM y Director de Infraestructura	E1016 - Registro de configuración de alertas en los sistemas críticos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	2	P3	T1017 - Implementar un sistema de centralización de logs para los sistemas críticos.	Director de Infraestructura y RM	E1017 - Documentación técnica del sistema de centralización de logs implementado.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	3	P3	T1018 - Documentar procesos y procedimientos para la centralización de logs.	RM y RSI	E1018 - Procedimientos documentados para la centralización de logs.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	3	P3	T1019 - Configurar herramientas para la emisión de alertas basadas en los logs centralizados.	RM y Director de Infraestructura	E1019 - Configuración registrada de las herramientas de emisión de alertas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	3	P3	T1020 - Realizar pruebas de los procedimientos y herramientas para asegurar su efectividad.	Director de Infraestructura y RM	E1020 - Resultados de las pruebas realizadas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	4	P3	T1021 - Implementar procesos automatizados para correlacionar información desde múltiples fuentes.	Director de Infraestructura y RM	E1021 - Registro de procesos automatizados implementados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	4	P3	T1022 - Configurar sistemas automatizados para la ejecución de acciones basadas en correlaciones.	Director de Infraestructura y RM	E1022 - Configuración documentada de sistemas automatizados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	4	P3	T1023 - Revisar periódicamente los procedimientos implementados.	RM y Director de Infraestructura	E1023 - Informes de revisión periódica de procedimientos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-3	4	P3	T1024 - Actualizar los procedimientos y herramientas basados en los resultados de la revisión.	Director de Infraestructura y RM	E1024 - Procedimientos y herramientas actualizados según los resultados de la revisión.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	1	P3	T1025 - Analizar el impacto de los eventos que afectan a los sistemas y servicios más críticos.	CSI	E1025 - Informe de análisis de impacto para eventos críticos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	1	P3	T1026 - Registrar los eventos analizados y sus impactos.	Director de Infraestructura y RSI	R1026 - Director de Infraestructura y RSI
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	2	P3	T1027 - Identificar los activos afectados utilizando el inventario de activos críticos del centro de datos.	CSI	E1027 - Inventario actualizado con los activos afectados identificados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	2	P3	T1028 - Definir y documentar los umbrales tolerables para los activos críticos (por ejemplo, tiempo de espera tolerable para aplicaciones).	CSI	E1028 - Documento que detalla los umbrales tolerables definidos para activos críticos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	2	P3	T1029 - Configurar y automatizar algunas alertas ante incidentes relacionados con los activos críticos.	Director de Infraestructura y RM	E1029 - Registro de configuración de alertas automatizadas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	3	P3	T1030 - Incorporar las actividades de identificación de impacto y determinación de umbrales en el procedimiento de detección y monitoreo.	RSI y RM	E1030 - Procedimiento documentado que incluye actividades de identificación de impacto y umbrales.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	3	P3	T1031 - Automatizar las alertas relacionadas con los umbrales de tolerancia definidos para los activos críticos del centro de datos.	RM y Director de Infraestructura	E1031 - Registro de alertas automatizadas basadas en umbrales definidos.

DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	3	P3	T1032 - Clasificar las alertas según el riesgo asociado al incidente.	RM	E1032 - Reporte de clasificación de alertas por nivel de riesgo.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	4	P3	T1033 - Realizar actividades de control interno para verificar el cumplimiento con el procedimiento de detección y monitoreo.	RSI y RM	E1033 - Informe de control interno sobre cumplimiento del procedimiento de detección y monitoreo.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	4	P3	T1034 - Analizar los resultados de las actividades de control interno y generar recomendaciones para la mejora del procedimiento de detección y monitoreo.	RSI	E1034 - Documento con recomendaciones generadas para la mejora del procedimiento.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-4	4	P3	T1035 - Incorporar las lecciones aprendidas en el procedimiento de detección y monitoreo.	RM	E1035 - Procedimiento actualizado con las lecciones aprendidas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	1	P3	T1036 - (REF. T1025) Analizar el impacto de los eventos que afectan a los sistemas y servicios más críticos.	CSI	E1036 - (REF E1025) Informe de análisis de impacto para eventos críticos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	1	P3	T1037 - (REF. T1026) Registrar los eventos analizados y sus impactos.	Director de Infraestructura y RSI	E1037 - (REF E1026) Registro documentado de eventos y sus impactos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	2	P3	T1038 - (REF. T1027) Identificar los activos afectados utilizando el inventario de activos críticos del centro de datos.	CSI	E1038 - (REF E1027) Inventario actualizado con los activos afectados identificados.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	2	P3	T1039 - (REF. T1028) Definir y documentar los umbrales tolerables para los activos críticos (por ejemplo, tiempo de espera tolerable para aplicaciones).	CSI	E1039 - (REF E1028) Documento que detalla los umbrales tolerables definidos para activos críticos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	2	P3	T1040 - (REF. T1029) Configurar y automatizar algunas alertas ante incidentes relacionados con los activos críticos.	Director de Infraestructura y RM	E1040 - (REF E1029) Registro de configuración de alertas automatizadas.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	3	P3	T1041 - (REF. T1030) Incorporar las actividades de identificación de impacto y determinación de umbrales en el procedimiento de detección y monitoreo.	RSI y RM	E1041 - (REF E1030) Procedimiento documentado que incluye actividades de identificación de impacto y umbrales.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	3	P3	T1042 - (REF. T1031) Automatizar las alertas relacionadas con los umbrales de tolerancia definidos para los activos críticos del centro de datos.	RM y Director de Infraestructura	E1042 - (REF E1031) Registro de alertas automatizadas basadas en umbrales definidos.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	3	P3	T1043 - (REF. T1032) Clasificar las alertas según el riesgo asociado al incidente.	RM	E1043 - (REF E1032) Reporte de clasificación de alertas por nivel de riesgo.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	4	P3	T1044 - (REF. T1033) Realizar actividades de control interno para verificar el cumplimiento con el procedimiento de detección y monitoreo.	RSI y RM	E1044 - (REF E1033) Informe de control interno sobre cumplimiento del procedimiento de detección y monitoreo.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	4	P3	T1045 - (REF. T1034) Analizar los resultados de las actividades de control interno y generar recomendaciones para la mejora del procedimiento de detección y monitoreo.	RSI	E1045 - (REF E1034) Documento con recomendaciones generadas para la mejora del procedimiento.
DETECTAR (DE)	DE.AE	Anomalías y eventos	DE.AE-5	4	P3	T1046 - (REF. T1035) Incorporar las lecciones aprendidas en el procedimiento de detección y monitoreo.	RM	E1046 - (REF E1035) Procedimiento actualizado con las lecciones aprendidas.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	1	P3	T1047 - (REF. T241) Instalar software antivirus en los equipos del personal.	Director de Soporte	E1047 - (REF. E241) Registro de instalación del antivirus en todos los equipos del personal.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	1	P3	T1048 - (REF. T291) Establecer un procedimiento básico para resolver problemas de malware de forma ad-hoc.	Director de Soporte	E1048 - (REF. E291) Documento con el procedimiento básico para resolver problemas de malware.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	2	P3	T1049 - (REF. T245) Instalar soluciones antivirus en servidores de archivos y correo electrónico.	Director de Soporte	E1049 - (REF. E245) Logs de instalación y configuración de antivirus en los servidores correspondientes.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	2	P3	T1050 - (REF. T293) Configurar chequeos periódicos automáticos en los equipos del personal.	Director de Soporte	E1050 - (REF. E293) Capturas de configuración de chequeos automáticos en las estaciones de trabajo.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	2	P3	T1051 - (REF. T294) Diseñar y realizar actividades de concientización sobre riesgos de software malicioso para el personal.	RSI y Capacitación	E1051 - (REF. E294) Material utilizado en las actividades de concientización y lista de asistentes.

DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	3	P3	T1052 - (REF. T248) Desarrollar una política de protección contra software malicioso.	CSI	E1052 - (REF. E248) Política aprobada para el manejo de software malicioso.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	3	P3	T1053 - (REF. T296) Documentar procedimientos específicos para la gestión de infecciones por malware.	RSI	E1053 - (REF. E296) Procedimientos documentados para gestionar infecciones.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	3	P3	T1054 - (REF. T297) Implementar una solución centralizada de antivirus para toda el área de TIC (luego todo el organismo)	Director de TIC	E1054 - (REF. E297) Informe técnico sobre la implementación de la solución centralizada de antivirus.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	4	P3	T1055 - (REF. T298) Configurar controles técnicos para bloquear el acceso a sitios web maliciosos y no autorizados.	Director de Infraestructura	E1055 - (REF. E298) Capturas de pantalla y configuraciones de los controles técnicos implementados.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	4	P3	T1056 - (REF. T299) Extender la protección contra malware a dispositivos móviles del organismo.	Director de Soporte	E1056 - (REF. E299) Lista de dispositivos móviles protegidos y configurados con antivirus.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	4	P3	T1057 - (REF. T300) Documentar procedimientos para identificar y solucionar equipos desprotegidos.	RSI	E1057 - (REF. E300) Documento con los procedimientos de detección y solución de equipos desprotegidos.
DETECTAR (DE)	DE.MC	Monitoreo continuo de la seguridad	DE.MC-5	4	P3	T1058 - (REF. T301) Crear un sistema de registro estadístico de infecciones por malware para análisis y mejora continua.	RSI y Director de Soporte	E1058 - (REF. E301) Base de datos e informe con estadísticas de infecciones y análisis de tendencias.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	1	P3	T1059 - Identificar los requisitos legales aplicables al uso de los logs.	RSI y Director de Legales	E1059 - Listado de requisitos legales aplicables identificados.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	1	P3	T1060 - Configurar los sistemas de generación de logs para garantizar que cumplan con los requisitos aplicables.	Director de Infraestructura y RSI	E1060 - Configuración documentada de los sistemas de generación de logs.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	1	P3	T1061 - Definir un procedimiento para el uso de los logs en cumplimiento con los requisitos legales.	RSI	E1061 - Procedimiento documentado para el uso de los logs en cumplimiento con los requisitos legales.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	2	P3	T1062 - Revisar la normativa sectorial aplicable a la recolección y uso de logs.	RSI y Director de Legales	E1062 - Informe de normativa sectorial aplicable revisada.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	2	P3	T1063 - Actualizar los procedimientos existentes para incluir las regulaciones sectoriales.	RSI	E1063 - Procedimientos actualizados con las regulaciones sectoriales.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	2	P3	T1064 - Capacitar al personal responsable sobre las normativas de protección de datos aplicables a los logs.	RSI y Capacitación	E1064 - Registro de las capacitaciones realizadas, incluyendo lista de asistencia.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	3	P3	T1065 - Establecer un proceso para monitorear cambios en los requisitos legales y normativos.	RSI y Director de Legales	E1065 - Registro de monitoreo de cambios normativos y legales.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	3	P3	T1066 - Revisar los procedimientos de detección y actualizar conforme a los nuevos requisitos legales y normativos.	RSI y Director de Legales	E1066 - Procedimientos actualizados y versionados.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	3	P3	T1067 - Documentar los cambios realizados en los procedimientos legales y normativos y comunicar a las partes involucradas.	RSI	E1067 - Comunicaciones enviadas sobre los cambios realizados.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	4	P3	T1068 - Diseñar un plan de auditorías internas para verificar el cumplimiento de los requisitos legales y normativos aplicables.	Auditoría Interna	E1068 - Plan de auditorías internas para verificar cumplimiento de los requisitos legales y normativos aplicables.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	4	P3	T1069 - Realizar auditorías periódicas sobre el uso de los logs y actividades relacionadas.	Auditoría Interna y RSI	E1069 - Informes de auditorías realizadas de cumplimiento de los requisitos legales y normativos aplicables
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-2	4	P3	T1070 - Analizar los resultados de las auditorías sobre los requisitos legales y normativos respecto a los logs y definir acciones de mejora continua.	RSI	E1070 - Registro de acciones de mejora implementadas basadas en los resultados de las auditorías para cumplimiento de los requisitos legales y normativos aplicables
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	1	P3	T1071 - Identificar los activos físicos y lógicos del centro de datos sujetos a detección y monitoreo.	Director de Infraestructura	E1071 - Listado de activos físicos y lógicos del centro de datos.

DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	1	P3	T1072 - Definir las pruebas necesarias para validar los procesos de detección y monitoreo de los activos del centro de datos.	RSI	E1072 - Documento con el diseño de las pruebas de detección y monitoreo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	1	P3	T1073 - Ejecutar pruebas de detección y monitoreo de activos del centro de datos.	Director de Infraestructura	E1073 - Informes de resultados de las pruebas realizadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	2	P3	T1074 - Identificar los activos y usuarios críticos del organismo para ser incluidos en las pruebas de detección.	CSI	E1074 - Listado de activos y usuarios críticos del organismo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	2	P3	T1075 - Definir y actualizar las pruebas para incluir activos y usuarios críticos del organismo.	RSI	E1075 - Documento actualizado con las pruebas diseñadas para activos y usuarios críticos.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	2	P3	T1076 - Ejecutar pruebas de detección y monitoreo en activos y usuarios críticos.	Director de Infraestructura y RSI	E1076 - Informes de resultados de las pruebas realizadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	3	P3	T1077 - Diseñar y documentar un procedimiento que establezca periodicidad y criterios para pruebas de detección.	RSI	E1077 - Procedimiento documentado con periodicidad y criterios para pruebas de detección.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	3	P3	T1078 - Implementar herramientas de automatización para la detección de desvíos en las pruebas.	Director de Infraestructura y RM	E1078 - Registro de configuraciones y reportes generados por herramientas de automatización.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	4	P3	T1079 - Documentar los resultados de las pruebas de detección de desvío.	Director de Infraestructura	E1079 - Informe con resultados documentados y registro de gestión de cambios.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	4	P3	T1080 - Analizar las lecciones aprendidas para identificar mejoras aplicables al SGSI y la gestión de riesgos.	RSI	E1080 - Informe con análisis de lecciones aprendidas aplicadas al SGSI.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	4	P3	T1081 - Actualizar el SGSI y las políticas de gestión de riesgos con base en las lecciones aprendidas.	RSI	E1081 - Actualización de políticas y procedimientos del SGSI.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-3	4	P3	T1082 - Monitorear el impacto de las mejoras implementadas en el SGSI.	RSI	E1082 - Informes de auditoría sobre el impacto de las mejoras en el SGSI.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	1	P3	T1083 - Identificar incorporaciones o modificaciones realizadas en los sistemas críticos e infraestructuras del centro de datos.	Director de Infraestructura	E1083 - Registro de cambios realizados en los sistemas críticos e infraestructuras del centro de datos.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	1	P3	T1084 - Actualizar las configuraciones del monitoreo para reflejar cambios en los sistemas críticos e infraestructuras.	RM y Director de Infraestructura	E1084 - Configuraciones actualizadas del sistema de monitoreo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	1	P3	T1085 - Validar que las actualizaciones de monitoreo incluyan las modificaciones realizadas.	RSI	E1085 - Informe de validación de monitoreo actualizado.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	2	P3	T1086 - Identificar las incorporaciones o modificaciones realizadas en los sistemas del organismo.	Director de TIC y RSI	E1086 - Registro de cambios realizados en los sistemas del organismo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	2	P3	T1087 - Actualizar las configuraciones del monitoreo para reflejar cambios en los sistemas del organismo.	RM y RSI	E1087 - Configuraciones actualizadas del sistema de monitoreo para los sistemas del negocio.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	2	P3	T1088 - Validar que las actualizaciones de monitoreo incluyan las modificaciones realizadas en los sistemas del organismo.	Director de Infraestructura y RSI	E1088 - Informe de validación de monitoreo actualizado para los sistemas del organismo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	3	P3	T1089 - Diseñar y documentar el procedimiento de monitoreo de los activos de información del organismo.	RSI y RM	E1089 - Procedimiento documentado de monitoreo de activos de información.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	3	P3	T1090 - Configurar sistemas para correlacionar eventos de los distintos sistemas de monitoreo.	RM y Director de Infraestructura	E1090 - Configuraciones de correlación de eventos en sistemas de monitoreo.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	3	P3	T1091 - Implementar y configurar alertas automatizadas para detectar desvíos.	RM y Director de Infraestructura	E1091 - Configuraciones de alertas automatizadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	3	P3	T1092 - Validar el funcionamiento de las alertas automatizadas y de la correlación de eventos.	Director de Infraestructura y RM	E1092 - Informe de validación de las alertas y correlación de eventos.

DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	4	P3	T1093 - (REF. T690) Implementar un sistema de coordinación formal entre el responsable del monitoreo y el RSI.	Director de TIC	E1093 - (REF. E690) Informes de coordinación entre el responsable de monitoreo y el RSI.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	4	P3	T1094 - (REF. T691) Realizar revisiones de control interno para evaluar el cumplimiento de los procedimientos de monitoreo y comunicación.	RSI	E1094 - (REF. E691) Resultados de las revisiones de control interno.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	4	P3	T1095 - (REF. T692) Documentar las lecciones aprendidas y utilizarlas para mejorar los procedimientos y pruebas.	RSI	E1095 - (REF. E692) Registro de lecciones aprendidas y mejoras implementadas.
DETECTAR (DE)	DE.PD	Procesos de detección	DE.PD-5	4	P3	T1096 - (REF. T693) Mantener actualizados los procedimientos y pruebas basados en la retroalimentación obtenida.	RSI	E1096 - (REF. E693) Procedimientos actualizados con mejoras basadas en la retroalimentación.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	1	P3	T1097 - (REF. T732) Mantener contacto con actores clave internos y externos durante la gestión de incidentes.	RSI	E1097 - (REF. E732) Registro de comunicaciones con actores clave.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	1	P3	T1098 - (REF. T733) Escalar las necesidades puntuales a actores externos relevantes, como CERTuy o CSIRT del sector.	RSI	E1098 - (REF. E733) Evidencia de incidentes escalados a CERTuy o CSIRT.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	2	P3	T1099 - (REF. T734) Identificar los actores internos y externos relevantes para la gestión de incidentes.	RSI	E1099 - (REF. E734) Listado de actores internos y externos identificados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	2	P3	T1100 - (REF. T735) Registrar y mantener actualizados los datos de contacto de los actores identificados.	RSI	E1100 - (REF. E735) Base de datos o registro de contactos actualizados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	2	P3	T1101 - (REF. T736) Documentar el mecanismo de escalamiento de incidentes.	RSI	E1101 - (REF. E736) Documento con el mecanismo de escalamiento de incidentes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	3	P3	T1102 - (REF. T737) Definir una política de gestión de incidentes que incluya actividades de comunicación con partes interesadas.	RSI	E1102 - (REF. E737) Política de gestión de incidentes aprobada.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	3	P3	T1103 - (REF. T738) Crear un plan y/o procedimiento alineado a la política de gestión de incidentes que contemple la comunicación con interesados.	RSI	E1103 - (REF. E738) Plan y/o procedimiento documentado que incluye comunicación con interesados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	4	P3	T1104 - (REF. T739) Designar un responsable que coordine la respuesta a incidentes y gestione la comunicación con las partes interesadas.	RSI	E1104 - (REF. E739) Documento de designación formal del responsable de coordinación.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	4	P3	T1105 - (REF. T740) Realizar actividades de control interno para verificar el cumplimiento del procedimiento de reporte y gestión de incidentes, y del plan de respuesta.	RSI	E1105 - (REF. E740) Informes de control interno realizados.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	4	P3	T1106 - (REF. T741) Utilizar los resultados de las actividades de control interno para mejorar el procedimiento y los planes.	RSI	E1106 - (REF. E741) Documentación con mejoras aplicadas al procedimiento y planes.
RESPONDER (RE)	RE.CO	Comunicaciones	RE.CO-5	4	P3	T1107 - (REF. T742) Documentar las lecciones aprendidas y retroalimentar los procedimientos y planes de respuesta.	RSI	E1107 - (REF. E742) Registro de lecciones aprendidas y ajustes realizados.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	1	P3	T1108 - Identificar las lecciones aprendidas de los incidentes de seguridad de la información relacionados con el centro de datos.	RGI y RSI	E1108 - Informe de lecciones aprendidas de los incidentes vinculados al centro de datos.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	1	P3	T1109 - Registrar las lecciones aprendidas en un repositorio centralizado.	RGI	E1109 - Registro de lecciones aprendidas en el repositorio centralizado.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	2	P3	T1110 - Identificar las lecciones aprendidas de los incidentes de seguridad de la información en todo el organismo.	RSI y RGI	E1110 - Informe consolidado de lecciones aprendidas de los incidentes de seguridad de la información a nivel organizacional.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	2	P3	T1111 - Consolidar las lecciones aprendidas de los incidentes de seguridad de la información en un registro único para la organización.	RGI	E1111 - Registro único de lecciones aprendidas de los incidentes de seguridad de la información actualizado.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	3	P3	T1112 - Implementar herramientas para el registro y gestión de lecciones aprendidas de incidentes de seguridad de la información.	Director de Desarrollo y RGI	E1112 - Documentación sobre la implementación de herramientas de registro y gestión.

RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	3	P3	T1113 - Comunicar las lecciones aprendidas sobre incidentes de seguridad de la información a todas las partes interesadas mediante los canales definidos.	RSI y RGI	E1113 - Actas o registros de las comunicaciones realizadas.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	3	P3	T1114 - Establecer un proceso formal para compartir las lecciones aprendidas sobre incidentes de seguridad de la información	RSI y RGI	E1114 - Procedimiento formal para compartir lecciones aprendidas.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	4	P3	T1115 - Analizar las lecciones aprendidas de los incidentes de seguridad de la información para identificar oportunidades de mejora en el SGSI.	RGI y RSI	E1115 - Informe de análisis de lecciones aprendidas con recomendaciones de mejora.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	4	P3	T1116 - Incorporar las lecciones aprendidas de los incidentes de seguridad de la información en la gestión de riesgos de seguridad de la información.	RGI y RSI	E1116 - Actualización del mapa de riesgos con base en lecciones aprendidas.
RESPONDER (RE)	RE.ME	Mejoras	RE.ME-1	4	P3	T1117 - Definir y monitorear indicadores relacionados con la implementación de lecciones aprendidas de los incidentes de seguridad de la información.	RGI y RSI	E1117 - Indicadores definidos y reportes de monitoreo.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	1	P3	T1118 - (REF. T1108) Identificar las lecciones aprendidas de los incidentes de seguridad de la información relacionados con el centro de datos.	RGI y RSI	E1118 - (REF. E1108) Informe de lecciones aprendidas de los incidentes vinculados al centro de datos.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	1	P3	T1119 - (REF. T1109) Registrar las lecciones aprendidas en un repositorio centralizado.	RGI	E1119 - (REF. E1109) Registro de lecciones aprendidas en el repositorio centralizado.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	2	P3	T1120 - (REF. T1110) Identificar las lecciones aprendidas de los incidentes de seguridad de la información en todo el organismo.	RSI y RGI	E1120 - (REF. E1110) Informe consolidado de lecciones aprendidas de los incidentes de seguridad de la información a nivel organizacional.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	2	P3	T1121 - (REF. T1111) Consolidar las lecciones aprendidas de los incidentes de seguridad de la información en un registro único para el organismo.	RGI	E1121 - (REF. E1111) Registro único de lecciones aprendidas de los incidentes de seguridad de la información actualizado.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	3	P3	T1122 - (REF. T1112) Implementar herramientas para el registro y gestión de lecciones aprendidas de incidentes de seguridad de la información.	Director de Desarrollo y RGI	E1122 - (REF. E1112) Documentación sobre la implementación de herramientas de registro y gestión.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	3	P3	T1123 - (REF. T1113) Comunicar las lecciones aprendidas sobre incidentes de seguridad de la información a todas las partes interesadas mediante los canales definidos.	RSI y RGI	E1123 - (REF. E1113) Actas o registros de las comunicaciones realizadas.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	3	P3	T1124 - (REF. T1114) Establecer un proceso formal para compartir las lecciones aprendidas sobre incidentes de seguridad de la información	RSI y RGI	E1124 - (REF. E1114) Procedimiento formal para compartir lecciones aprendidas
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	4	P3	T1125 - (REF. T1115) Analizar las lecciones aprendidas de los incidentes de seguridad de la información para identificar oportunidades de mejora en el SGSI.	RGI y RSI	E1125 - (REF. E1115) Informe de análisis de lecciones aprendidas con recomendaciones de mejora.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	4	P3	T1126 - (REF. T1116) Incorporar las lecciones aprendidas de los incidentes de seguridad de la información en la gestión de riesgos de seguridad de la información.	RGI y RSI	E1126 - (REF. E1116) Actualización del mapa de riesgos con base en lecciones aprendidas.
RECUPERAR (RC)	RC.ME	Mejoras	RC.ME-1	4	P3	T1127 - (REF. T1117) Definir y monitorear indicadores relacionados con la implementación de lecciones aprendidas de los incidentes de seguridad de la información.	RGI y RSI	E1127 - (REF. E1117) Indicadores definidos y reportes de monitoreo.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	1	P3	T1128 - Determinar a la persona o grupo responsable de la comunicación externa durante crisis o incidentes mayores.	Directorio	E1128 - Documento oficial de designación del responsable de la comunicación externa.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	1	P3	T1129 - Establecer la autorización expresa para que las áreas técnicas puedan comunicar externamente en situaciones específicas.	Directorio	E1129 - Registro de autorización de comunicación externa para áreas técnicas.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	2	P3	T1130 - Definir y designar un vocero oficial para situaciones de crisis relacionadas con ciberseguridad y seguridad de la información.	Directorio	E1130 - Documento de designación oficial del vocero.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	2	P3	T1131 - Difundir al personal la identidad del vocero y los canales oficiales de contacto en caso de incidentes.	Directorio y Comunicaciones	E1131 - Comunicación interna difundida al personal sobre el vocero y los canales de contacto.

RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	3	P3	T1132 - Elaborar un plan de comunicaciones para situaciones de crisis, incluyendo evaluación, notificaciones y monitoreo.	CSI y Comunicaciones	E1132 - Plan de comunicaciones ante crisis documentado.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	3	P3	T1133 - Establecer un procedimiento detallado para gestionar la comunicación durante crisis, desde la evaluación hasta la entrega de mensajes a la audiencia correspondiente.	CSI y Comunicaciones	E1133 - Procedimiento de gestión de comunicación en crisis aprobado.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	3	P3	T1134 - Difundir el plan y procedimiento a los actores involucrados, asegurando que todos los responsables estén informados.	Comunicaciones	E1134 - Confirmación de difusión del plan y procedimiento a los actores relevantes.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	4	P3	T1135 - Realizar ensayos prácticos de crisis para poner a prueba el plan y procedimiento de comunicación.	Comunicaciones y RSI	E1135 - Informe de los ensayos de crisis realizados con el plan de comunicación.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	4	P3	T1136 - Realizar revisiones periódicas de control interno para evaluar el cumplimiento del plan de comunicación ante crisis.	RSI y Comunicaciones	E1136 - Informe de revisión interna de control de cumplimiento con el plan de comunicación.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	4	P3	T1137 - Documentar los resultados de las revisiones de control y utilizarlos para la mejora continua del plan.	RSI	E1137 - Documento de actualización y mejora del plan basado en resultados de las revisiones
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-1	4	P3	T1138 - Involucrar al Directorio en las actualizaciones del plan de comunicación, con un enfoque especial en la aprobación y difusión de los mensajes.	RSI	E1138 - Acta de aprobación del Directorio del plan de comunicación y difusión.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	1	P3	T1139 - (REF. T1128) Determinar a la persona o grupo responsable de la comunicación externa durante crisis o incidentes mayores.	Directorio	E1139 - (REF. E1128) Documento oficial de designación del responsable de la comunicación externa.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	1	P3	T1140 - (REF. T1129) Establecer la autorización expresa para que las áreas técnicas puedan comunicar externamente en situaciones específicas.	Directorio	E1140 - (REF. E1129) Registro de autorización de comunicación externa para áreas técnicas.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	2	P3	T1141 - (REF. T1130) Definir y designar un vocero oficial para situaciones de crisis relacionadas con ciberseguridad y seguridad de la información.	Directorio	E1141 - (REF. E1130) Documento de designación oficial del vocero.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	2	P3	T1142 - (REF. T1131) Difundir al personal la identidad del vocero y los canales oficiales de contacto en caso de incidentes.	Directorio y Comunicaciones	E1142 - (REF. E1131) Comunicación interna difundida al personal sobre el vocero y los canales de contacto.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	3	P3	T1143 - (REF. T1132) Elaborar un plan de comunicaciones para situaciones de crisis, incluyendo evaluación, notificaciones y monitoreo.	CSI y Comunicaciones	E1143 - (REF. E1132) Plan de comunicaciones ante crisis documentado.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	3	P3	T1144 - (REF. T1133) Establecer un procedimiento detallado para gestionar la comunicación durante crisis, desde la evaluación hasta la entrega de mensajes a la audiencia correspondiente.	CSI y Comunicaciones	E1144 - (REF. E1133) Procedimiento de gestión de comunicación en crisis aprobado.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	3	P3	T1145 - (REF. T1134) Difundir el plan y procedimiento a los actores involucrados, asegurando que todos los responsables estén informados.	Comunicaciones	E1145 - (REF. E1134) Confirmación de difusión del plan y procedimiento a los actores relevantes.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	4	P3	T1146 - (REF. T1135) Realizar ensayos prácticos de crisis para poner a prueba el plan y procedimiento de comunicación.	Comunicaciones y RSI	E1146 - (REF. E1135) Informe de los ensayos de crisis realizados con el plan de comunicación.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	4	P3	T1147 - (REF. T1136) Realizar revisiones periódicas de control interno para evaluar el cumplimiento del plan de comunicación ante crisis.	RSI y Comunicaciones	E1147 - (REF. E1136) Informe de revisión interna de control de cumplimiento con el plan de comunicación.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	4	P3	T1148 - (REF. T1137) Documentar los resultados de las revisiones de control y utilizarlos para la mejora continua del plan.	RSI	E1148 - (REF. E1137) Documento de actualización y mejora del plan basado en resultados de las revisiones
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-2	4	P3	T1149 - (REF. T1138) Involucrar al Directorio en las actualizaciones del plan de comunicación, con un enfoque especial en la aprobación y difusión de los mensajes.	RSI	E1149 - (REF. E1138) Acta de aprobación del Directorio del plan de comunicación y difusión.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	1	P3	T1150 - (REF. T1128) Determinar a la persona o grupo responsable de la comunicación externa durante crisis o incidentes mayores.	Directorio	E1150 - (REF. E1128) Documento oficial de designación del responsable de la comunicación externa.

RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	1	P3	T1151 - (REF. T1129) Establecer la autorización expresa para que las áreas técnicas puedan comunicar externamente en situaciones específicas.	Directorio	E1151 - (REF. E1129) Registro de autorización de comunicación externa para áreas técnicas.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	2	P3	T1152 - (REF. T1130) Definir y designar un vocero oficial para situaciones de crisis relacionadas con ciberseguridad y seguridad de la información.	Directorio	E1152 - (REF. E1130) Documento de designación oficial del vocero.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	2	P3	T1153 - (REF. T1131) Difundir al personal la identidad del vocero y los canales oficiales de contacto en caso de incidentes.	Directorio y Comunicaciones	E1153 - (REF. E1131) Comunicación interna difundida al personal sobre el vocero y los canales de contacto.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	3	P3	T1154 - (REF. T1132) Elaborar un plan de comunicaciones para situaciones de crisis, incluyendo evaluación, notificaciones y monitoreo.	CSI y Comunicaciones	E1154 - (REF. E1132) Plan de comunicaciones ante crisis documentado.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	3	P3	T1155 - (REF. T1133) Establecer un procedimiento detallado para gestionar la comunicación durante crisis, desde la evaluación hasta la entrega de mensajes a la audiencia correspondiente.	CSI y Comunicaciones	E1155 - (REF. E1133) Procedimiento de gestión de comunicación en crisis aprobado.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	3	P3	T1156 - (REF. T1134) Difundir el plan y procedimiento a los actores involucrados, asegurando que todos los responsables estén informados.	Comunicaciones	E1156 - (REF. E1134) Confirmación de difusión del plan y procedimiento a los actores relevantes.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	4	P3	T1157 - (REF. T1135) Realizar ensayos prácticos de crisis para poner a prueba el plan y procedimiento de comunicación.	Comunicaciones y RSI	E1157 - (REF. E1135) Informe de los ensayos de crisis realizados con el plan de comunicación.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	4	P3	T1158 - (REF. T1136) Realizar revisiones periódicas de control interno para evaluar el cumplimiento del plan de comunicación ante crisis.	RSI y Comunicaciones	E1158 - (REF. E1136) Informe de revisión interna de control de cumplimiento con el plan de comunicación.
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	4	P3	T1159 - (REF. T1137) Documentar los resultados de las revisiones de control y utilizarlos para la mejora continua del plan.	RSI	E1159 - (REF. E1137) Documento de actualización y mejora del plan basado en resultados de las revisiones
RECUPERAR (RC)	RC.CO	Comunicaciones	RC.CO-3	4	P3	T1160 - (REF. T1138) Involucrar al Directorio en las actualizaciones del plan de comunicación, con un enfoque especial en la aprobación y difusión de los mensajes.	RSI	E1160 - (REF. E1138) Acta de aprobación del Directorio del plan de comunicación y difusión.

ANEXO 7 - Política de Seguridad de Información vigente

Este anexo se presenta la Política de Seguridad de la Información (PSI) vigente en el organismo. Con el fin de preservar la identidad del organismo, se procedió a anonimizar cualquier información que pudiera permitir su identificación, incluyendo referencias a sus actividades. Recordamos que la PSI propuesta para ser aprobada y remplazar a esta política, se encuentra en el ANEXO 3 - Entregable 2: Políticas a medida del organismo, como Pol-01 Política de Seguridad de la Información.

Política de Seguridad de Información

1.- Trámite y Revisiones

1.1.- Trámite

El documento “Política de Seguridad de la Información” fue diseñado por la Comisión de Seguridad de la Información.

La Comisión de Seguridad de la Información está conformada por representantes de Dirección General, Área de Planificación Estratégica y Presupuestal, División Tecnologías de la Información y Comunicaciones, Auditoría Interna de Gestión y División Jurídica.

1.2.- Revisiones

Fecha	N° de versión	Elaborado por	Aprobado por	Párrafos modificados	Surge de:
04/11/2022	01	Comisión de Seguridad de la Información		Documento nuevo	TIC
02/03/2023	02	Comisión de Seguridad de la Información			

2.- Objeto y Campo de Aplicación

El objeto de la presente política es proteger la información y preservar su integridad, confidencialidad y disponibilidad contra posibles amenazas. Es de aplicación en todo el ámbito del organismo y para todos los usuarios que tengan acceso a activos de información del organismo.

2.1.- Vigencia

La presente política entra en vigencia a partir de su publicación, establecida en la carátula.

La política será revisada con una periodicidad no mayor a tres años, con el objetivo de incorporar los cambios derivados de los avances tecnológicos y las modificaciones en la estructura organizacional del organismo, las regulaciones y normas externas.

3.- Referencias Normativas

3.1.- MARCOS LEGALES QUE APLICAN A ESTA POLÍTICA

- Ley N° 18.331 – Protección de Datos Personales y Acción de “HABEAS DATA”
- Ley N° 18.381 – Ley Sobre el derecho de acceso a la información pública

3.2.- RESOLUCIONES

- Res. 2526/22 – Creación de la Comisión de Seguridad de la Información.

4.- Política De Seguridad De La Información

El organismo reconoce la importancia de identificar y proteger sus activos de información. Para ello velará para evitar la destrucción, divulgación, modificación y utilización no autorizada de toda información.

La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger los activos de información. La Seguridad de la Información se caracteriza como la preservación de:

- a) su confidencialidad, asegurando que sólo quienes estén autorizados puedan acceder a la información;
- b) su integridad, asegurando que la información y sus métodos de proceso sean exactos y completos;
- c) su disponibilidad, asegurando que los usuarios autorizados tengan acceso a la información cuando lo requieran.

a seguridad de la información se consigue implantando un conjunto adecuado de controles, tales como políticas, procedimientos, estructuras organizativas, software e infraestructura.

La presente Política de Seguridad de la Información debe ser conocida y cumplida por todas las personas vinculadas al organismo, independientemente del cargo que desempeñe y de su situación contractual.

Esta Política de Seguridad de la Información se integrará a la normativa básica del organismo, incluyendo su difusión previa, y la instrumentación de las medidas correspondientes por incumplimiento de la presente política, así como de los documentos relacionados a ésta.

Las responsabilidades de todas las personas vinculadas al organismo, independientemente del cargo que desempeñe, de su vínculo laboral y de su situación contractual, se incluyen en el Anexo I.

5.- ANEXO I: Guías De Uso

Este anexo contiene las guías para el uso responsable y seguro de los activos de información institucionales conforme a la reglamentación vigente.

USO DE DISPOSITIVOS MÓVILES PROVISTOS POR EL ORGANISMO

OBJETIVO

- a- Proteger la información del organismo almacenada o accesible desde dispositivos móviles (celulares, tablets, notebooks) provistos por el organismo, a través de todo tipo de conexión.
- b- Evitar la infección y distribución de código malicioso, información reservada e información sensible.
- c- Prevenir accesos no autorizados a recursos del organismo.

ALCANCE

Todo dispositivo móvil provisto por el organismo que contenga o acceda a información del organismo.

MARCO NORMATIVO

Esta guía está alineada con la reglamentación del uso de telefonía móvil y fija institucional, Resolución de Directorio 867/19, en donde se detallan las condiciones de uso y acciones a tomar.

DESCRIPCIÓN

Los dispositivos móviles provistos por el organismo sólo deben utilizarse con fines laborales para el cumplimiento de las tareas correspondientes. Su uso, debe seguir las siguientes pautas de seguridad:

- a- Responsabilidades. El usuario es el responsable del dispositivo que se le ha entregado para el desempeño de sus tareas. Por tanto, es el usuario el que debe garantizar la integridad y seguridad tanto del dispositivo como de la información que contiene.
- b- Pérdida o robo: Tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo. En caso de hurto y extravío se debe reportar a la brevedad al superior inmediato y realizar la denuncia a la seccional policial correspondiente.

En el caso de que se trate de un teléfono celular, adicionalmente se deberá gestionar la suspensión inmediata del servicio ante el Departamento de Cuentas Oficiales a los efectos de solicitar la inhabilitación de la línea y el bloqueo del equipo.

Si el extravío o daño son consecuencia de un mal uso o negligencia, el funcionario deberá reponer los gastos surgidos de la reparación y o reposición del dispositivo y/o accesorios.

Se deberá implementar instrumentos y herramientas técnicas (hardware y software) que permitan bloquear y/o borrar la información de forma remota. Se deberá evaluar puntualmente los riesgos asociados al uso de dispositivos que no permitan el cumplimiento de este control.

- c- Funcionalidades: No está permitido realizar el desbloqueo de las limitaciones del fabricante y/o proveedor, alterar las configuraciones realizadas por el organismo o cualquier otro método de cambio de las protecciones de los dispositivos.
- d- Privacidad de los datos: Tomar las apropiadas precauciones para prevenir que otras personas externas a la organización (familia, amigos, etc.) tengan acceso a los dispositivos del organismo y los recursos asociados a los mismos.

Los dispositivos deben contar con bloqueo mediante contraseña, pin u otro medio robusto de autenticación.

- e- Acceso remoto: Utilizar los mecanismos de seguridad establecidos para acceder a los recursos del organismo mediante conexiones remotas.

Contar con un proceso formal para la administración de solicitudes de alta, baja y modificación de autorizaciones. Estos registros quedarán accesibles con motivos de auditoría durante 5 años.

- f- Notificación en caso de infección. Si se sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal técnico responsable.

- g- Gestión de Dispositivos: Todos los dispositivos deben estar inventariados.

Las aplicaciones instaladas en el dispositivo deben ser obtenidas por canales oficiales y con el licenciamiento debido.

- h- Conexión a redes. No está permitido conectarse a redes públicas (sin clave de acceso).

- i- Transporte y custodia. El dispositivo no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo. En ningún caso se debe descuidar el dispositivo si se viaja en transporte público o personal, ni dejarlo visible o fácilmente accesible. Si se trabaja en lugares donde no se garantiza la custodia del dispositivo, éste debe quedar anclado con un candado de seguridad o guardado en un armario de seguridad.

- j- Reutilización o eliminación. Se deberá contar con un proceso formal para la reutilización y/o eliminación de dispositivos (cambio de usuario, equipos en desuso, etc.) que garanticen la eliminación completa y segura de la información previa y sensible allí almacenada.

Al momento de dejar de utilizar un dispositivo, ya sea por cambio de funciones, desvinculación o cualquier otro motivo, el funcionario deberá entregar el mismo al área correspondiente:

- Celulares, al Departamento de Cuentas Oficiales.
- Notebooks o Tablets al Departamento de Soporte de la División TIC.

USO DEL CORREO ELECTRÓNICO

OBJETIVO

Establecer las responsabilidades y lineamientos que deben cumplir todos los usuarios del correo institucional con el fin de garantizar el uso seguro del mismo.

ALCANCE

Todo usuario de correo electrónico institucional del organismo.

MARCO NORMATIVO

- Comunicaciones y notificaciones electrónicas, artículos 32, 79 y 80 del Reglamento de Procedimiento administrativo del organismo.
- Artículo 18 del Reglamento de Funcionarios del organismo.
- Circulares de Dirección General número 41612/17 y 5649/18.

DESCRIPCIÓN

El organismo brinda a todas las personas vinculadas al organismo, independientemente del cargo que desempeñe o de su vínculo laboral, una casilla de correo institucional personal como herramienta de comunicación laboral. El uso de esa casilla de correo debe seguir las siguientes pautas de seguridad:

a- Responsabilidades.

- La casilla de correo electrónico institucional es para uso exclusivo de la persona para la cual fue creada. El usuario no debe transferir ni compartir su contraseña de acceso.
- Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.
- La información contenida en los correos es de propiedad del organismo. En esa medida, el organismo no se hace responsable de la información de carácter personal que los usuarios puedan almacenar en sus cuentas institucionales.

b- Definición de contraseña. La contraseña asignada inicialmente es temporal, ésta debe ser remplazada por una de conocimiento y uso exclusivo del usuario asignado.

- La contraseña seleccionada deberá cumplir con la política de contraseñas del organismo.
 - Longitud mínima de 10 caracteres.
 - Contener al menos una letra mayúscula.
 - Contener al menos una letra minúscula.
 - Contener al menos un número
 - Contener al menos un símbolo (Ej: ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | })
- Las contraseñas no deberían ser formadas por el nombre personal propio o de un familiar cercano, la dirección, fechas importantes, número de teléfono, número de documento, nombre de usuario, apodos o cualquier término que pueda ser adivinado fácilmente.
- Se debe evitar incluir en las contraseñas palabras relacionadas con el sitio (por ejemplo, si se está creando una contraseña para el correo electrónico, no se debe utilizar las palabras correo o Zimbra).
- Se debe evitar utilizar la misma contraseña en diferentes sistemas o servicios.

c- Privacidad y seguridad.

- Los usuarios no deben dejar escrita y a la vista su contraseña.
- Las cuentas de correo institucional son de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente, y no prestarla bajo ninguna circunstancia.
- Ante un incidente de seguridad de información o investigación administrativa, el organismo tiene la potestad de bloquear una cuenta de correo de un usuario. Sin embargo, no se podrá acceder a la información en ella contenida sin un debido proceso que asegure la objetividad, autenticidad, conservación e inalterabilidad de la misma, debiendo documentarse lo actuado mediante acta notarial y previa autorización del

Directorio y el contralor de la persona involucrada o un representante por él designado o, cuando esto no sea posible, un representante del personal.

- Todo correo de procedencia desconocida, correo basura, SPAM o correo no deseado que sea recibido en el correo electrónico institucional personal, debe marcado como spam y reportado a la División TIC con el fin de evitar posibles infecciones por código malicioso o virus.
- En el caso de que un usuario olvide su contraseña, o sospeche que otras personas están accediendo a su cuenta de correo electrónico, deberá notificar a la División TIC en forma inmediata.
- Se debe evitar enviar archivos adjuntos de origen desconocido o sospechoso.
- El usuario del correo electrónico institucional personal debe reportar oportunamente a la División TIC cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, pérdida de contraseñas, etc.
- La División TIC nunca solicitará información personal o de la cuenta por correo electrónico, por lo tanto, el usuario no debe brindar sus credenciales de acceso (usuario y contraseña).
- No está permitido compartir contactos o listas de distribución del organismo con personas externas al organismo, con el objetivo de propiciar el envío de propagandas, ofertas, negocios personales, avisos publicitarios, o información de otro tipo, ajena a las labores propias del cargo.

d- Uso.

- No se deberá utilizar correos personales para fines laborales, sólo se deben utilizar las herramientas provistas por el organismo para la comunicación electrónica.
- En caso de cuentas compartidas por diferentes usuarios, el usuario principal y dueño de la cuenta de correo debe otorgar dicha autorización por escrito o por correo electrónico indicando qué usuarios tendrán acceso a la cuenta de correo.
- No está permitida la propagación de correos electrónicos de procedencia desconocida, SPAM, correo basura o no deseado, hacia cuentas institucionales.

- La División Comunicaciones es la única autorizada para el envío de correos masivos, comunicados, etc., y en caso que alguna área, departamento o persona requiera enviar algún correo masivo al personal del organismo, deberá solicitarlo a la División, quienes evaluarán la pertinencia o no de dicha solicitud y realizará las comunicaciones correspondientes.

DIVULGACIÓN DE INFORMACIÓN

OBJETIVO

Prevenir la divulgación de la información clasificada como secreta, reservada o confidencial.

ALCANCE

Esta guía refiere a la protección de la información, entendiendo información como todo contenido producido, obtenido o bajo el control del organismo, cualquiera que sea su soporte (papel, electrónico o grabación sonora, visual o audiovisual), clasificada como secreta, reservada o confidencial.

MARCO NORMATIVO

- Ley N° 18.381 sobre el derecho de acceso a la información pública.
- Decreto Reglamentario N° 232/2010, que establece los principios relacionados con el derecho de acceso a la información.

DESCRIPCIÓN

Dado a la naturaleza de la información que se maneja el organismo, se debe considerar la sensibilidad de los datos que residen en los sistemas de información para el debido control y acceso. Pérdida o mal uso de esta información puede resultar en una variedad de daños, tales como pérdida de confidencialidad e incumplimiento de regulaciones y leyes aplicables (Ley N° 18.331 – Protección de Datos Personales y Acción de “HABEAS DATA”).

- a- Establecer contratos de no divulgación con todas las personas vinculadas al organismo, independientemente del cargo que desempeñe, de su vínculo laboral y de su situación contractual.
- b- Todo documento, carpeta, y otros medios de almacenamiento que contienen información sensible, restringida o confidencial debe ser ubicada en áreas protegidas. Estos medios de almacenamiento de información nunca deben ser ubicados en un lugar donde visitantes pueda tener acceso a ellos.
- c- Diversos tipos de datos presentan varios riesgos. Preste atención particular a cómo se guarda la información personal: datos personales, tarjetas de crédito o información financiera, y otros datos sensibles relativos a la información de los beneficiarios. Si no existe una necesidad legítima de información personalmente identificable, para un proceso específico no la guarde. Si existe una necesidad legítima de la información, guárdela solamente mientras sea necesario.
- d- Los datos personales deben ser utilizados solamente para propósitos requeridos o legales.
- e- Los medios de almacenamiento de información que contienen información sensible, restringida o confidencial debe ser guardada en un área segura a final de cada día laborable.
- f- Las computadoras portátiles (“laptops”) y otros dispositivos portátiles (tales como memoria USB / pendrive, etc.) que contiene información del organismo debe estar protegida con contraseña.
- g- Toda información de respaldo de datos (“backup”) enviado o almacenado en medios de datos (por ejemplo: pendrives, CD, discos ópticos, etc.) debe ser protegido y debe ser manejado según las políticas y procedimientos vigentes en la institución.
- h- Las infracciones de esta política pueden tener como resultado acciones disciplinarias conforme a políticas y procedimientos disciplinarios vigentes en la institución.

Las distintas oficinas y servicios del organismo deben seguir las siguientes prácticas:

- a- Todas las computadoras deben ser aseguradas cuando el área de trabajo está desocupada o desatendida.
- b- Todo documento, carpeta, y otros medios de almacenamiento que contienen información sensible, restringida o confidencial debe ser retirada del escritorio y asegurada al final de la jornada de trabajo.
- c- Cada usuario es responsable de asegurar todo documento y medio electrónico de almacenamiento que contenga información sensible o confidencial que esta esté ubicada en las oficinas.
- d- Las contraseñas no pueden ser dejadas en notas en el escritorio ni en una ubicación accesible, y son de uso exclusivo personal (no se pueden compartir).
- e- Los informes impresos que contienen información sensible, restringida o confidencial deben ser retirados inmediatamente de las impresoras.
- f- Al momento de desechar, los documentos sensibles o confidenciales deben ser destruidos.
- g- Controles de acceso y monitoreo deben ser aplicados en áreas de oficina e instalaciones de almacenaje donde resida información restringida o confidencial.

Notificación de eventos de divulgación no autorizada:

En eventos los cuales información sensible, restringida o confidencial es extraviada o es divulgada a entidades no autorizadas o si este acontecimiento incluye pérdida de cualquier equipo, medio electrónico de almacenamiento o componente tecnológico, se debe notificar inmediatamente al superior y realizar la denuncia correspondiente si fuese necesario.

Uso de Redes Sociales:

La organización puede crear su perfil oficial en las redes sociales para dar a conocer sus programas, actividades y otros temas de interés, y para tener un contacto directo con la ciudadanía, y de esta manera poder conocer sus necesidades y requerimientos. No obstante, se debe cumplir con los lineamientos expresados a continuación:

- La administración de las redes sociales institucionales son de uso exclusivo del área de Comunicación Institucional.
- El uso de las mismas debe cumplir con la Política de Seguridad de la Información, con especial atención en lo que refiere a la Ley N° 18.331 – Protección de Datos Personales y Acción de “HABEAS DATA”.
- Se debe tener claramente identificadas las personas (y sus correspondientes usuarios) con acceso a los perfiles en redes sociales, debiendo estos corresponder con cuentas institucionales y no personales.
- Las cuentas utilizadas para recuperación de los datos de acceso deben ser institucionales.
- Se deberá seguir las pautas y procedimientos definidos por la organización, para el traspaso de usuarios en casos de cambio o desvinculación de los administradores de los perfiles.
- Siempre que la red social lo permita, se debe verificar la cuenta, de manera de garantizar a los ciudadanos o clientes que es la cuenta oficial de la organización.
- La contraseña utilizada en cada cuenta de red social debe ser diferente; la misma deberá ser una contraseña segura conforme a las pautas establecidas en las políticas vigentes.
- Si se detecta un contenido potencialmente inseguro, se debe reportar a la División TIC, y eliminar si corresponde.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

OBJETIVO

Asegurar que los usuarios conozcan, entiendan sus responsabilidades y cumplan con las políticas de seguridad de la información.

Proteger los intereses del organismo como parte del proceso de cambio de función o dependencia o al finalizar la relación laboral.

ALCANCE

Todos los usuarios del organismo.

RESPONSABILIDADES

Comisión de Seguridad de la Información

Participar en la redacción y revisión del Compromiso de Confidencialidad a firmar por los usuarios del organismo que utilicen activos de información y en la definición de sus consecuencias en caso de incumplimiento del mismo.

División TIC

Realizar la gestión de los proyectos tecnológicos del organismo.

Informar a los usuarios, en conjunto con el área de Comunicación Institucional, de sus obligaciones respecto del cumplimiento de la presente Política de Seguridad de la Información.

Realizar actividades de capacitación y sensibilización respecto del cumplimiento de la Política de Seguridad de la Información, asegurándose de su entendimiento.

División Gestión y Desarrollo Humano

Incorporar en las descripciones de las funciones y perfiles de cargo, la obligatoriedad de la notificación y el cumplimiento de las Políticas de Seguridad de la Información vigente.

División Adquisiciones

Incorporar en todos los pliegos la obligación de firmar el compromiso de Confidencialidad a las empresas de bienes y servicios del organismo.

Direcciones y/o Jefes de Unidad

Controlar el cumplimiento de las Políticas de Seguridad de la Información por parte de su personal a cargo. Ante un incumplimiento se aplicará el procedimiento disciplinario vigente, previsto en el Reglamento de Procedimiento Administrativo del organismo.

Solicitar la eliminación o redefinición del acceso a los activos de información a todo funcionario que cambie de unidad o tarea.

Previo a finalizar la relación laboral con el organismo de un usuario bajo su dependencia:

- Comunicar las responsabilidades y las obligaciones de seguridad de la información que permanecen válidas una vez finalizado su vínculo laboral.
- Solicitar todos los elementos que fueron suministrados para desarrollar sus tareas.
- Solicitar la baja del usuario que se desvincula del organismo.

DESCRIPCIÓN

- **Gestión de Proyectos Tecnológicos:** El área de Tecnologías de la Información y Comunicaciones (TIC) será la responsable de gestionar y coordinar todos los proyectos tecnológicos en el organismo. Esto incluye la planificación, ejecución, seguimiento y cierre de los proyectos relacionados con sistemas de información y tecnología.

Los proyectos tecnológicos que involucren a otras dependencias del Estado deberán contar con la aprobación previa del área de TIC antes de su inicio. Esta medida tiene como fin asegurar que los proyectos cumplan con los estándares de seguridad de la información y se alineen con los objetivos institucionales.

- **Adquisición de Software y Desarrollos:** Únicamente el área de TIC estará autorizada a contactar y tratar con proveedores de software en nombre del organismo. La adquisición de software deberá seguir un proceso formal de evaluación, selección y aprobación, que garantice la seguridad y la compatibilidad con la infraestructura existente.
- **Términos y Condiciones del Empleo:** Establecer en los acuerdos contractuales con los usuarios y terceras partes sus responsabilidades y las del organismo en cuanto a la Seguridad de la información.
- **Promoción y Educación en la Seguridad de la Información:** Los usuarios participarán regularmente de las actividades de capacitación necesarias para proteger adecuadamente los recursos de información del organismo. Estas

actividades estarán incluidas en un plan de formación continua que abarque los diferentes aspectos de la presente Política.

- Finalización o Cambio de Responsabilidades Laborales: Los usuarios son responsables de cumplir con obligaciones después de la terminación de su vínculo laboral con el organismo o ante un cambio de tareas.