Marco de ciberseguridad 5.0

Presidencia Uruguay

agesic

Marco de ciberseguridad
Version 5.0

SEGURIDAD DE LA INFORMACIÓN

Versión 5.0 – Agosto 2025

Este documento ha sido elaborado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (Agesic).

El Marco de ciberseguridad es un conjunto de requisitos normativos y buenas prácticas, que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Contenido

1. Introducción

El uso de las Tecnologías de la Información y la Comunicación (TIC) se ha incorporado de forma generalizada a la vida cotidiana. Este nuevo escenario facilita un desarrollo sin precedentes del intercambio de información y comunicaciones, pero, al mismo tiempo, conlleva nuevos riesgos y amenazas que pueden afectar a la seguridad de los sistemas de información.

Es por esto que en agosto de 2016 se lanzó el Marco de ciberseguridad, cuyo principal objetivo es dar lineamientos y buenas prácticas para un abordaje integral de la ciberseguridad.

La seguridad de la información es un trabajo permanente que exige un proceso de mejora continua y sistematizada para minimizar la exposición y determinar posibles puntos que puedan comprometer la integridad, disponibilidad o confidencialidad de los activos o la información que estos gestionan, y además establece los criterios de seguridad que permiten potenciar el servicio prestado de manera confiable y segura.

2. Objetivo y alcance

El presente documento establece un Marco de ciberseguridad estructurado y alineado con la normativa nacional. Su diseño se fundamenta en el Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF), reconocido por su eficacia en la mejora de la ciberseguridad para infraestructuras críticas.

Este marco ha sido contextualizado para las organizaciones que requieren gestionar sistemáticamente los riesgos inherentes a la seguridad de la información y al uso de la infraestructura tecnológica que le da soporte. Asimismo, está orientado a aquellas que precisan adoptar políticas formalizadas para la gestión tanto de la seguridad de la información como de los incidentes, e implementar las medidas necesarias para lograr centros de datos seguros, todo ello en cumplimiento con la regulación vigente.

De esta forma, el Marco provee un abordaje integral de la ciberseguridad para reducir el riesgo asociado a amenazas que puedan comprometer los activos de información y la continuidad operativa. Su desarrollo considera tanto la normativa vigente como las mejores prácticas sugeridas por Agesic.

La adopción del marco NIST como referencia tiene como cometido principal alinear la respuesta a amenazas, la gestión de riesgos y la gestión general de la seguridad de la información. Esto permite, además, que las organizaciones puedan homologar sus procesos de gestión de ciberseguridad con estándares internacionales de una forma práctica y estableciendo objetivos claros. Cabe destacar que el marco posee la flexibilidad para ser adaptado a diferentes realidades e industrias, trascendiendo su aplicación original en entornos de infraestructuras críticas.

En su aplicación, el Marco puede asistir a una organización en la planificación y desarrollo evolutivo de su estrategia de gestión de riesgos de ciberseguridad, ajustándola en función de su actividad, tamaño y otras características específicas. No se trata de un

documento estático, sino de un modelo dinámico que se modificará de acuerdo a los cambios tecnológicos, la evolución de las amenazas y las innovaciones en las técnicas de gestión de riesgos.

3. Características

El núcleo del Marco se basa en el ciclo de vida del proceso de gestión de la ciberseguridad desde el punto de vista técnico y organizacional. Proporciona un conjunto de actividades para lograr resultados específicos de ciberseguridad. Se divide en funciones, categorías y subcategorías. Cada subcategoría tiene asociada referencias a normas y estándares de seguridad internacionales.

En el proceso de contextualización se agregaron prioridades a las subcategorías, se les asignaron requisitos y se elaboraron perfiles. Los requisitos fueron elaborados siguiendo los lineamientos de la normativa vigente y las mejores prácticas internacionales en materia de seguridad de la información y ciberseguridad.

3.1 Ciclo de vida de la ciberseguridad

El ciclo de vida de la ciberseguridad se compone de funciones que permiten abstraer los principales conceptos de la seguridad de la información, en particular de la ciberseguridad.

A continuación, se describen las funciones del Marco de ciberseguridad.

Gobernar

La función Gobernar informa acerca de lo que una organización puede hacer para lograr resultados de las otras cinco funciones en el contexto de su misión y las expectativas de las partes interesadas.

Las categorías dentro de esta función son: Contexto organizativo, Estrategia de gestión de riesgos, Funciones, responsabilidades y autoridades, Política, Supervisión y Gestión de riesgos de la cadena de suministro en materia de ciberseguridad.

Identificar

La función Identificar está vinculada a la comprensión del contexto de la organización, de los activos que soportan los procesos críticos de las operaciones y los riesgos asociados pertinentes. Esta comprensión permite definir los recursos y las inversiones de acuerdo con la estrategia de gestión de riesgos y sus objetivos.

Las categorías dentro de esta función son: Gestión de activos, Evaluación de riesgos y Mejora.

Proteger

Es una función vinculada a la aplicación de medidas para proteger los procesos y los activos de la organización, independientemente de su naturaleza TI.

Las categorías dentro de esta función son: Gestión de identidades, autenticación y control de acceso, Concientización y capacitación, Seguridad de datos, Seguridad de plataformas y Resiliencia de la infraestructura tecnológica.

Detectar

Relacionada con la definición y ejecución de las actividades apropiadas dirigidas a la identificación temprana de los incidentes de seguridad.

Las categorías dentro de esta función son: Monitoreo continuo y Análisis de eventos adversos.

Responder

Se asocia con la definición y ejecución de las actividades apropiadas para tomar medidas en caso de detección de un evento de seguridad. El objetivo es reducir el impacto de un potencial incidente de seguridad informática.

Las categorías dentro de esta función son: Gestión de incidentes, Análisis de incidentes, Notificación y comunicación de la respuesta de incidentes.

Recuperar

Está vinculada a la definición y ejecución de las actividades dirigidas a la gestión de los planes y actividades para restaurar los procesos y servicios deficientes debido

a un incidente de seguridad. El objetivo es asegurar la resistencia de los sistemas e instalaciones y, en caso de incidentes, apoyar la recuperación oportuna de las operaciones.

Las categorías dentro de esta función son: Ejecución de un plan de recuperación de incidentes y Comunicación de la recuperación de incidentes.

3.2 Estructura del Marco de ciberseguridad

A continuación, se describe el Marco de ciberseguridad y su estructura.

Función

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

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: “Contexto organizativo”, “Concientización y capacitación”, “Análisis de incidentes”.

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: “Se mantienen inventarios de los servicios prestados por los proveedores.”, “Se mantienen inventarios de los servicios prestados por los proveedores”, “Se correlaciona la información procedente de diversas fuentes”, “Se estima y valida la magnitud de un incidente”.

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 48h 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 24h corridas de indisponibilidad.

Prioridad

Las subcategorías del Marco, dentro de un perfil (Básico - B, Estándar - E, Avanzado - A) tienen asociado un nivel de prioridad de abordaje.

Las prioridades definidas son:

- **Alta:** son críticas y deben ser abordadas de inmediato, ya que representan la primera línea de defensa. Su implementación es esencial para la seguridad y el funcionamiento óptimo. Retrasar su atención podría resultar en riesgos significativos, como vulnerabilidades críticas, interrupciones de servicio o incumplimiento de normativas clave. Se consideran la base indispensable sobre la cual se construyen las demás capas de seguridad y eficiencia.
- **Media:** son importantes para fortalecer la postura general y mejorar la resiliencia del sistema. Si bien no son tan críticas como los de alta prioridad para la operación inmediata, su abordaje es necesario para optimizar el rendimiento, reducir riesgos potenciales a mediano plazo y asegurar una mayor robustez. Una vez que las tareas de alta prioridad estén encauzadas, estas deberían ser el siguiente foco de atención para evitar que se conviertan en problemas mayores en el futuro.
- **Baja:** son valiosas para perfeccionar la configuración, mejorar la eficiencia y añadir capas adicionales de seguridad o funcionalidad. Aunque no son urgentes ni representan riesgos inmediatos, su implementación contribuye a un marco más completo y maduro. Abordar estas tareas demuestra un compromiso con la mejora continua y la búsqueda de la excelencia, incluso si su realización puede planificarse con mayor flexibilidad una vez que las prioridades más altas estén gestionadas. No deben ser ignoradas, sino programadas para ser ejecutadas cuando los recursos y el tiempo lo permitan, ya que su cumplimiento mejora el nivel general de madurez y protección.

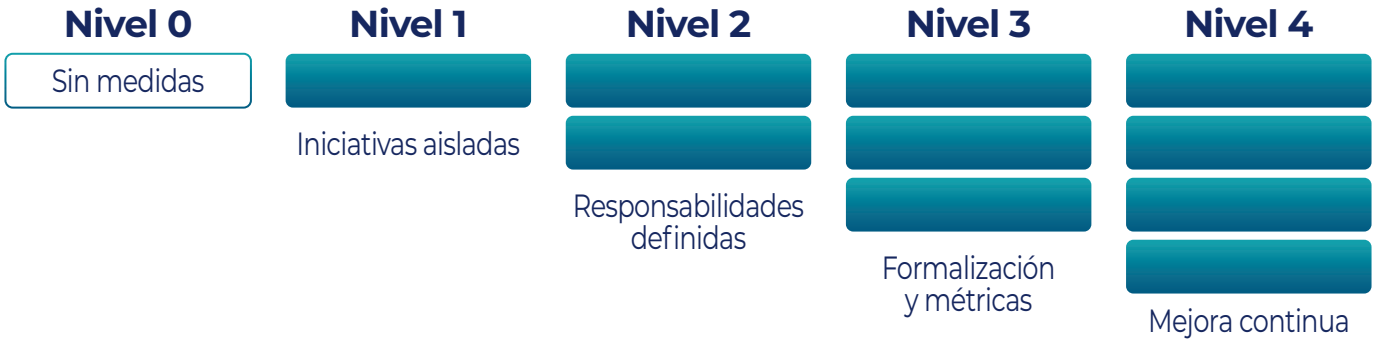
La asignación de prioridades a las subcategorías del Marco se adapta fundamentalmente al perfil de riesgo y dependencia tecnológica de cada organización. Para un perfil Básico, donde el riesgo percibido es bajo y la recuperación se basa en el mejor esfuerzo, las prioridades “altas” se enfocarán en la implementación de medidas fundamentales que prevengan interrupciones básicas, ya que la afectación al negocio es mínima. En contraste, un perfil Estándar, con una dependencia moderada de las TIC y una tolerancia a la indisponibilidad de 48 horas, requerirá que las prioridades “altas” aborden no solo la prevención, sino también la capacidad de respuesta y recuperación para mantener la continuidad del servicio dentro de ese plazo. Finalmente, para un perfil Avanzado, con alto riesgo y una tolerancia a la indisponibilidad de solo 24 horas, las prioridades “altas” serán las más estrictas y urgentes, centradas en la resiliencia proactiva, la protección

de servicios críticos y transversales, y la minimización del impacto, dado que cualquier interrupción puede tener consecuencias significativas para la organización y terceros. En esencia, la prioridad de una medida se magnifica a medida que la dependencia de la tecnología y el impacto de una falla se incrementan en cada perfil.

Asimismo, podrían definirse otros perfiles (por ejemplos sectoriales) que manifiesten otra priorización según los riesgos identificados.

Modelo de Madurez

El modelo de madurez propuesto para la evaluación consta de cinco niveles, que se describen a continuación según sus requisitos.



- **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.

Requisitos

Requisito o conjunto de requisitos mínimos incluidos en cada subcategoría. El detalle de cada requisito podrá consultarse en la "Guía de implementación".

Un requisito podrá mencionarse en más de una subcategoría, dependiendo de su enfoque.

4. Marco de ciberseguridad

4.1 Función: Gobernar (GV)

GV.OC Contexto organizativo

Se comprenden las circunstancias (misión, expectativas de las partes interesadas, dependencias y requisitos legales, normativos y contractuales) que afectan a las decisiones de gestión de riesgos de ciberseguridad de la organización.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.OC-01: Se comprende la misión de la organización y se informa sobre la gestión de riesgos de ciberseguridad.	Baja	Media	Media	**PL.1** Establecer objetivos anuales con relación a la Seguridad de la Información.
GV.OC-02: Las partes interesadas internas y externas son comprendidas, y sus necesidades y expectativas con respecto a la gestión de riesgos de ciberseguridad son comprendidas y consideradas.	Baja	Media	Media	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.OC-03: Se comprenden y gestionan los requisitos legales, normativos y contractuales relativos a la ciberseguridad, incluidas las obligaciones en materia de privacidad y libertades civiles.	Baja	Media	Media	**CN.1** Cumplir con los requisitos normativos. **PD.1** Principio de Legalidad. **PD.2** Principio de Veracidad. **PD.4** Principio de previo consentimiento informado. **PD.8** Derechos de los titulares de los datos.
GV.OC-04: Se comprenden y comunican los objetivos, las capacidades y los servicios críticos de los que dependen las partes interesadas externas o que esperan de la organización.	Baja	Media	Media	**CO.5** Definir las ventanas de tiempo soportadas para la continuidad de las operaciones. **SO.3** Gestionar la capacidad de los servicios y recursos que se encuentran operativos.
GV.OC-05: Se comprenden y comunican los resultados, capacidades y servicios de los que depende la organización.	Baja	Baja	Baja	**OR.7** Conocer el contexto de la organización.

GV.RM Estrategia de gestión de riesgos

Se establecen, comunican y utilizan las prioridades, las restricciones, las declaraciones de tolerancia y apetito por el riesgo y los supuestos de la organización para respaldar las decisiones sobre el riesgo operativo.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.RM-01: Los objetivos de la gestión de riesgos son establecidos y acordados por las partes interesadas de la organización.	Baja	Media	Media	**PL.1** Establecer objetivos anuales con relación a la Seguridad de la Información.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.RM-02: Se establecen, se comunican y se mantienen las declaraciones sobre el apetito de riesgo y la tolerancia al riesgo.	Baja	Media	Media	**CO.5** Definir las ventanas de tiempo soportadas para la continuidad de las operaciones. **GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos. **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.
GV.RM-03: Las actividades y los resultados de la gestión de riesgos de ciberseguridad se incluyen en los procesos de gestión de riesgos de la empresa.	Baja	Baja	Baja	**GR.1** Adoptar una metodología de Evaluación de Riesgo.
GV.RM-04: Se establece y comunica una dirección estratégica que describa las opciones adecuadas de respuesta al riesgo.	Baja	Baja	Media	**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.
GV.RM-05: Se establecen líneas de comunicación en toda la organización para los riesgos de ciberseguridad, lo que incluye a los riesgos de proveedores y otros terceros.	Baja	Baja	Baja	**GI.4** Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes. **GR.1** Adoptar una metodología de Evaluación de Riesgo. **OR.2.** Conformar un Comité de Seguridad de la Información.
GV.RM-06: Se establece y comunica un método estandarizado para calcular, documentar, categorizar y priorizar los riesgos de ciberseguridad.	Baja	Baja	Baja	**GR.1** Adoptar una metodología de Evaluación de Riesgo.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.RM-07: Se caracterizan las oportunidades estratégicas (es decir, los riesgos positivos) y se incluyen en las discusiones sobre riesgos de ciberseguridad de la organización.	Baja	Baja	Baja	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos.

GV.RR Funciones, responsabilidad y autoridades

Se establecen y comunican las funciones, las responsabilidades y las competencias en materia de ciberseguridad para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.RR-01: El liderazgo organizativo es responsable de los riesgos de ciberseguridad y fomenta una cultura consciente de los riesgos, ética y de mejora continua.	Baja	Baja	Baja	**OR.2** Conformar un Comité de Seguridad de la Información. **PS.1** Adoptar una Política de Seguridad de la Información.
GV.RR-02: Se establecen, comunican, comprenden y aplican las funciones, responsabilidades y autoridades relacionadas con la gestión de riesgos de ciberseguridad.	Media	Alta	Alta	**OR.1** Designar un Responsable de la Seguridad de la Información. **OR.2** Conformar un Comité de Seguridad de la Información. **OR.3** Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.
GV.RR-03: Se asignan recursos adecuados de acuerdo con la estrategia de riesgos de ciberseguridad, las funciones, las responsabilidades y las políticas.	Baja	Baja	Media	**GR.3** Tratamiento o un plan de acción correctivo sobre los riesgos encontrados y, de acuerdo con su resultado, implementar las acciones correctivas y preventivas correspondientes.
GV.RR-04: La ciberseguridad se incluye en las prácticas de recursos humanos.	Media	Media	Media	**GH.1** Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información. **PD.6** Principio de reserva.

GV.PO Política

La política de ciberseguridad de la organización es establecida, comunicada y aplicada.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.PO-01: La política de gestión de riesgos de ciberseguridad se establece en base al contexto organizativo, la estrategia de ciberseguridad y las prioridades, y es comunicada y aplicada.	Media	Alta	Alta	**PS.1** Adoptar una Política de Seguridad de la Información.
GV.PO-02: La política de gestión de riesgos de ciberseguridad se revisa, actualiza, comunica y aplica para reflejar los cambios en los requisitos, las amenazas, la tecnología y la misión de la organización.	Baja	Baja	Baja	**PS.1** Adoptar una Política de Seguridad de la Información.

GV.OV Supervisión

Los resultados de las actividades de gestión de riesgos de ciberseguridad en toda la organización y el rendimiento se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.OV-01: Los resultados de la estrategia de gestión de riesgos de ciberseguridad se revisan para informar y ajustar la estrategia y la dirección.	N/A	N/A	N/A	
GV.OV-02: La estrategia de gestión de riesgos de ciberseguridad se revisa y ajusta para garantizar la cobertura de los requisitos y riesgos de la organización.	N/A	N/A	N/A	
GV.OV-03: El rendimiento de la gestión de riesgos de ciberseguridad de la organización se evalúa y revisa para realizar los ajustes necesarios.	N/A	N/A	N/A	

GV.SC Gestión de riesgos de la cadena de suministro en materia de ciberseguridad

Las partes interesadas de la organización identifican, establecen, gestionan, supervisan y mejoran los procesos de gestión de riesgos de la cadena de suministro en materia de ciberseguridad.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.SC-01: Las partes interesadas de la organización establecen y acuerdan un programa, estrategia, objetivos, políticas y procesos de gestión de riesgos de ciberseguridad en la cadena de suministro.	Baja	Baja	Baja	**GR.1** Adoptar una metodología de Evaluación de Riesgo. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
GV.SC-02: Se establecen, comunican y coordinan interna y externamente las funciones y responsabilidades de ciberseguridad para proveedores, clientes y colaboradores.	Baja	Media	Media	**SC.6** Establecer acuerdos de no divulgación.
GV.SC-03: La gestión de riesgos de la cadena de suministro en materia de ciberseguridad está integrada en la ciberseguridad y la gestión de riesgos empresariales, la evaluación de riesgos y los procesos de mejora.	Baja	Media	Media	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos.
GV.SC-04: Los proveedores son conocidos y priorizados por criticidad.	Baja	Media	Alta	**RP.1** Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.
GV.SC-05: Los requisitos para abordar los riesgos de ciberseguridad en las cadenas de suministro se establecen, priorizan e integran en contratos y otros tipos de acuerdos con proveedores y otras terceras partes pertinentes.	Media	Media	Media	**AD.2** Incluir requisitos de seguridad de la información para la adquisición de productos y servicios de tecnología. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
GV.SC-06: Se llevan a cabo la planificación y la diligencia debida para reducir los riesgos antes de entablar relaciones formales con proveedores u otros terceros.	Baja	Baja	Baja	**AD.2** Incluir requisitos de seguridad de la información para la adquisición de productos y servicios de tecnología. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
GV.SC-07: Los riesgos planteados por un proveedor, sus productos y servicios y otros terceros se comprenden, registran, priorizan, evalúan, responden y monitorean a lo largo de la relación.	Baja	Baja	Baja	**RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
GV.SC-08: Los proveedores pertinentes y otros terceros se incluyen en las actividades de planificación, respuesta y recuperación de incidentes.	Baja	Baja	Media	**GI.1** Planificar la gestión de los incidentes de seguridad de la información.
GV.SC-09: Las prácticas de seguridad de la cadena de suministro se integran en los programas de ciberseguridad y de gestión de riesgos empresariales, y su rendimiento se monitorea a lo largo del ciclo de vida de los productos y servicios tecnológicos.	Baja	Baja	Baja	**AD.2** Incluir requisitos de seguridad de la información para la adquisición de productos y servicios de tecnología. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
GV.SC-10: Los planes de gestión de riesgos de la cadena de suministro de ciberseguridad incluyen disposiciones para las actividades que ocurren después de la conclusión de un acuerdo de colaboración o servicio.	Baja	Baja	Media	**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. **RP.1** Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.

4.2 Función: Identificar (ID)

ID.AM Gestión de activos

Los activos (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar sus objetivos empresariales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
ID.AM-01: Se mantienen inventarios del hardware gestionado por la organización.	Media	Media	Media	**GA.4** Gestionar los medios de almacenamiento externos. **OR.5** Pautar el uso de dispositivos móviles.
ID.AM-02: Se mantienen inventarios de software, servicios y sistemas gestionados por la organización.	Alta	Alta	Alta	**CN.4** Gestionar las licencias de software. **GA.1** Identificar formalmente los activos de la organización junto con la definición de su responsable. **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).
ID.AM-03: Se mantienen representaciones de la comunicación de red autorizada de la organización y de los flujos de datos de red internos y externos.	Baja	Baja	Baja	**SC.13** Debe existir segregación a nivel de servicios de información.
ID.AM-04: Se mantienen inventarios de los servicios prestados por los proveedores.	Baja	Media	Alta	**RP.1** Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.
ID.AM-05: Se priorizan los activos en función de su clasificación, criticidad, recursos e impacto en la misión.	Baja	Baja	Baja	**GA.2** Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos. **GA.3** Pautar el uso aceptable de los activos.
ID.AM-07: Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados.	Baja	Baja	Baja	**GA.2** Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.
ID.AM-08: Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de vida.	Baja	Media	Media	**GA.5** Establecer los mecanismos para destruir la información y medios de almacenamiento. **PD.3** Principio de Finalidad.

ID.RA. Evaluación de riesgos

La organización comprende el riesgo de ciberseguridad para la organización, los activos y los individuos.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
ID.RA-01: Se identifican, validan y registran las vulnerabilidades de los activos.	Media	Alta	Alta	**CN.3** Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades. **SO.1** Gestionar las vulnerabilidades técnicas.
ID.RA-02: Se recibe información sobre ciberamenazas de foros y fuentes de intercambio de información.	Baja	Baja	Media	**GR.4** Inteligencia de amenazas.
ID.RA-03: Se identifican y registran las amenazas internas y externas a la organización.	Baja	Media	Media	**GR.4** Inteligencia de amenazas.
ID.RA-04: Se identifican y registran los impactos potenciales y las probabilidades de que las amenazas exploten las vulnerabilidades.	Baja	Media	Media	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI. **GR.4** Inteligencia de amenazas.
ID.RA-05: Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para comprender el riesgo inherente e informar sobre la priorización de la respuesta al riesgo.	Baja	Media	Media	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI. **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. **GR.4** Inteligencia de amenazas.
ID.RA-06: Se eligen, priorizan, planifican, controlan y comunican las respuestas al riesgo.	Baja	Baja	Media	**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.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
ID.RA-07: Se gestionan los cambios y las excepciones, se evalúa su impacto en el riesgo, se registran y se realiza su seguimiento.	Baja	Media	Media	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI. **SO.2** Gestionar formalmente los cambios.
ID.RA-08: Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades.	Media	Alta	Alta	**SO.1** Gestionar las vulnerabilidades técnicas.
ID.RA-09: Se evalúa la autenticidad e integridad del hardware y software antes de su adquisición y uso.	Baja	Baja	Media	**SF.4** Seguridad del equipamiento.
ID.RA-10: Se evalúan los proveedores críticos antes de su adquisición.	Baja	Media	Media	**AD.2** Incluir requisitos de seguridad de la información para la adquisición de productos y servicios de tecnología. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.

ID.IM Mejora

Se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos de ciberseguridad de la organización en todas las funciones del Marco.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
ID.IM-01: Las mejoras se identifican a partir de evaluaciones.	Baja	Baja	Baja	**CN.2** Realizar auditorías independientes de seguridad de la información. **PD.7** Principio de responsabilidad proactiva.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
ID.IM-02: Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, lo que incluye a los realizados en coordinación con proveedores y terceros pertinentes.	Baja	Baja	Baja	**CN.3** Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades. **GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.
ID.IM-03: Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativos.	Baja	Baja	Baja	**CN.3** Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades. **GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.
ID.IM-04: Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de ciberseguridad que afectan a las operaciones.	Baja	Baja	Baja	**CN.3** Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades. **GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.

4.3 Función: Proteger (PR)

PR.AA Gestión de identidades, autenticación y control de acceso

El acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
PR.AA-01: La organización gestiona las identidades y credenciales de los usuarios, servicios y equipos autorizados.	Media	Alta	Alta	**CA.5** Segregación de funciones en el acceso lógico. **CA.6** Gestión de accesos y permisos.
PR.AA-02: Las identidades están comprobadas y vinculadas a credenciales basadas en el contexto de las interacciones.	Baja	Media	Media	**CA.1** Gestión de identidades y credenciales.
PR.AA-03: Los usuarios, servicios y hardware están autenticados.	Alta	Alta	Alta	**CA.1** Gestión de identidades y credenciales. **OR.6** Establecer controles para proteger la información a la que se accede de forma remota.
PR.AA-04: Las afirmaciones de identidad se protegen, transmiten y verifican.	Alta	Alta	Alta	**CA.1** Gestión de identidades y credenciales.
PR.AA-05: Los permisos de acceso, los derechos y las autorizaciones se definen en una política, se gestionan, se aplican y se revisan, e incorporan los principios de privilegio mínimo y separación de funciones.	Alta	Alta	Alta	**CA.2** Revisar los privilegios de acceso lógico. **CA.6** Gestión de accesos y permisos. **OR.6** Establecer controles para proteger la información a la que se accede de forma remota. **PD.5** Principio de seguridad de los datos. **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 de mensaje.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
PR.AA-06: El acceso físico a los activos se gestiona, supervisa y aplica de forma proporcional al riesgo.	Baja	Media	Alta	**SF.1** Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas **SF.4** Seguridad del equipamiento

PR.AT Concientización y capacitación

Se proporciona al personal de la organización concienciación y capacitación en ciberseguridad para que puedan realizar sus tareas relacionadas con la ciberseguridad.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
PR.AT-01: Se sensibiliza y capacita al personal para que disponga de los conocimientos y habilidades necesarios para realizar tareas generales teniendo en cuenta los riesgos de ciberseguridad.	Media	Alta	Alta	**GH.2** Concientizar y formar en materia de seguridad de la información a todo el personal.
PR.AT-02: Se sensibiliza y capacita a las personas que desempeñan funciones especializadas para que posean los conocimientos y aptitudes necesarios para realizarlas tareas pertinentes teniendo en cuenta los riesgos de ciberseguridad.	Baja	Media	Media	**GH.3** Concientizar y formar en materia de seguridad de la información al personal que desempeñan funciones especializadas.

PR.DS Seguridad de datos

Los datos se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
PR.DS-01: La confidencialidad, la integridad y la disponibilidad de los datos en reposo están protegidas.	Media	Media	Alta	**CA.3** Establecer controles criptográficos. **CA.4** Establecer los controles para el uso de firma electrónica. **GA.4** Gestionar los medios de almacenamiento externos. **PD.5** Principio de seguridad de los datos. **PD.6** Principio de reserva.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
PR.DS-02: La confidencialidad, la integridad y la disponibilidad de los datos en tránsito están protegidas.	Media	Media	Alta	**CA.3** Establecer controles criptográficos. **CA.4** Establecer los controles para el uso de firma electrónica. **OR.6** Establecer controles para proteger la información a la que se accede de forma remota. **PD.5** Principio de seguridad de los datos. **PD.6** Principio de reserva. **SC.6** Establecer acuerdos de no divulgación. **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 de mensaje. **SC.14** Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.
PR.DS-10: La confidencialidad, la integridad y la disponibilidad de los datos en uso están protegidas	Baja	Baja	Baja	**GA.3** Pautar el uso aceptable de los activos. **OR.5** Pautar el uso de dispositivos móviles. **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 de mensaje.
PR.DS-11: Se crean, protegen, mantienen y comprueban copias de seguridad de los datos.	Media	Media	Alta	**CA.3** Establecer controles criptográficos. **SO.6** Respaldar la información y realizar pruebas de restauración periódicas.

PR.PS Seguridad de plataformas

El hardware, el software (por ejemplo, firmware, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales se gestionan de acuerdo con la estrategia de riesgos de la organización para proteger su confidencialidad, integridad y disponibilidad.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
PR.PS-01: Se establecen y aplican prácticas de gestión de la configuración.	Baja	Media	Media	**GA.3** Pautar el uso aceptable de los activos. **OR.5** Pautar el uso de dispositivos móviles. **SO.2** Gestionar formalmente los cambios.
PR.PS-02: Se mantiene, sustituye y elimina el software en función del riesgo.	Baja	Media	Media	**GA.1** Identificar formalmente los activos de la organización junto con la definición de su responsable. **GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.
PR.PS-03: Se mantiene, sustituye y elimina el hardware en función del riesgo.	Baja	Media	Media	**GA.5** Establecer los mecanismos para destruir la información y medios de almacenamiento. **GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI. **SF.5** Establecer el mantenimiento de los componentes críticos.
PR.PS-04: Se generan registros y se pongan a disposición para una supervisión continua.	Media	Alta	Alta	**SO.7** Registrar y monitorear los eventos de los sistemas.
PR.PS-05: Se impide la instalación y la ejecución de software no autorizado.	Media	Media	Alta	**SO.8** Gestionar la instalación de software.
PR.PS-06: Se integran prácticas seguras de desarrollo de software y se supervisa su rendimiento durante todo el ciclo de vida de desarrollo del software.	Baja	Media	Media	**AD.1** Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software. **OR.4** Abordar la seguridad de la información en la gestión de los proyectos. **SO.4** Definir entornos separados para desarrollo, pruebas y producción.

PR.IR Resiliencia de la infraestructura tecnológica

Las arquitecturas de seguridad se gestionan con la estrategia de riesgos de la organización a fin de proteger la confidencialidad, la integridad y la disponibilidad de los activos, así como la resiliencia de la organización.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
PR.IR-01: Las redes y los entornos están protegidos contra el acceso lógico y el uso no autorizados.	Alta	Alta	Alta	**CA.6** Gestión de accesos y permisos. **OR.6** Establecer controles para proteger la información a la que se accede de forma remota. **SC.13** Debe existir segregación a nivel de servicios de información. **SO.4** Definir entornos separados para desarrollo, pruebas y producción.
PR.IR-02: Los activos tecnológicos de la organización están protegidos de las amenazas del entorno.	Baja	Baja	Media	**SF.2** Implementar controles ambientales en los centros de datos y áreas relacionadas.
PR.IR-03: Se implementan mecanismos para lograr los requisitos de resiliencia en situaciones normales y adversas.	Baja	Baja	Baja	**CO.1** Contar con componentes redundantes que contribuyan al normal funcionamiento del centro de procesamiento de datos. **CO.2** Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia.
PR.IR-04: Se mantiene una capacidad de recursos adecuada para garantizar la disponibilidad.	Media	Media	Media	**SO.3** Gestionar la capacidad de los servicios y recursos que se encuentran operativos.

4.4 Función: Detectar (DE)

DE.CM. Monitoreo continuo

Los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros eventos potencialmente adversos.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
DE.CM-01: Las redes y los servicios de red se monitorean para detectar eventos potencialmente adversos.	Media	Alta	Alta	**SO.7** Registrar y monitorear los eventos de los sistemas.
DE.CM-02: Se monitorea el entorno físico para detectar posibles eventos adversos.	Baja	Media	Alta	**SF.1** Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas.
DE.CM-03: Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos.	Baja	Baja	Baja	**GA.3** Pautar el uso aceptable de los activos. **GI.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.
DE.CM-06: Se monitorean las actividades y los servicios de los proveedores de servicios externos para detectar eventos potencialmente adversos.	Baja	Baja	Baja	**GI.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. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
DE.CM-09: Se monitorean el hardware y el software informáticos, los entornos de ejecución y sus datos para detectar posibles eventos adversos.	Media	Media	Alta	**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). **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos. **SO.5** Controlar software malicioso. **SO.7** Registrar y monitorear los eventos de los sistemas.

DE.AE. Análisis de eventos adversos

Se analizan anomalías, indicadores de compromiso y otros eventos potencialmente adversos para caracterizarlos y detectar incidentes de ciberseguridad.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
DE.AE-02: Los eventos potencialmente adversos se analizan para comprender mejor las actividades asociadas.	Baja	Media	Media	**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 de mensaje. **SO.7** Registrar y monitorear los eventos de los sistemas.
DE.AE-03: Se correlaciona la información procedente de diversas fuentes.	Baja	Baja	Baja	**GA.3** Pautar el uso aceptable de los activos. **GI.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. **GI.4** Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes. **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.
DE.AE-04: Se comprende el impacto estimado y el alcance de los eventos adversos.	Baja	Baja	Baja	**GI.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.
DE.AE-06: La información sobre eventos adversos se proporciona al personal y a las herramientas autorizadas.	Baja	Media	Media	**SO.7** Registrar y monitorear los eventos de los sistemas.
DE.AE-07: La inteligencia sobre ciberamenazas y otra información contextual se integran en el análisis.	Baja	Media	Media	**GR.4** Inteligencia de amenazas.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
DE.AE-08: Se declaran incidentes cuando los eventos adversos cumplen con los criterios de incidente definidos.	Alta	Alta	Alta	**GI.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. **SO.7** Registrar y monitorear los eventos de los sistemas.

4.5 Función: Responder (RS)

RS.MA Gestión de incidentes

Se gestionan las respuestas a los incidentes de ciberseguridad detectados.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
RS.MA-01: Se ejecuta el plan de respuesta a incidentes en coordinación con los terceros pertinentes una vez que se declara un incidente.	Baja	Baja	Media	**GI.1** Planificar la gestión de los incidentes de seguridad de la información. **GI.5** Responder ante incidentes de seguridad de la información.
RS.MA-02: Se clasifican y validan los informes de incidentes.	Baja	Baja	Baja	**GI.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. **GI.5** Responder ante incidentes de seguridad de la información.
RS.MA-03: Se clasifican y priorizan los incidentes.	Baja	Baja	Baja	**GI.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.
RS.MA-04: Se escalan o elevan los incidentes según sea necesario.	Media	Alta	Alta	**GI.3** Informar de forma completa e inmediata a las partes interesadas. **GI.5** Responder ante incidentes de seguridad de la información. **PD.5** Principio de seguridad de los datos.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
RS.MA-05: Se aplican los criterios para iniciar la recuperación de incidentes.	Media	Media	Media	**CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres.

RS.AN. Análisis de incidentes

Se llevan a cabo investigaciones con el fin de garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
RS.AN-03: Se realizan análisis para determinar lo que ocurrió durante un incidente y la causa raíz del mismo.	Baja	Baja	Baja	**GI.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. **GI.5** Responder ante incidentes de seguridad de la información.
RS.AN-06: Se registran las acciones realizadas durante una investigación y se preservan la integridad y la procedencia de los registros.	Baja	Baja	Baja	**GI.4** Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes.
RS.AN-07: Se recopilan los datos y metadatos del incidente y se preservan su integridad y su procedencia.	Baja	Baja	Media	**GI.1** Planificar la gestión de los incidentes de seguridad de la información.
RS.AN-08: Se estima y valida la magnitud de un incidente.	Baja	Baja	Baja	**GI.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.

RS.CO. Notificación y comunicación de la respuesta al incidente

Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según lo exijan las leyes, las normativas o las políticas.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
RS.CO-02: Se notifican los incidentes a las partes interesadas internas y externas.	Media	Alta	Alta	**GI.3** Informar de forma completa e inmediata a las partes interesadas. **GI.5** Responder ante incidentes de seguridad de la información. **PD.5** Principio de seguridad de los datos.
RS.CO-03: La información se comparte con las partes interesadas internas y externas designadas.	Media	Alta	Alta	**GI.3** Informar de forma completa e inmediata a las partes interesadas. **PD.5** Principio de seguridad de los datos.

RS.MI. Mitigación de incidentes

Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
RS.MI-01: Se contienen los incidentes.	Alta	Alta	Alta	**GI.5** Responder ante incidentes de seguridad de la información.
RS.MI-02: Se erradican los incidentes.	Alta	Alta	Alta	**GI.5** Responder ante incidentes de seguridad de la información.

4.6 Función: Recuperar (RC)

RC.RP Ejecución del plan de recuperación de incidentes

Se realizan actividades de restauración que garantizan la disponibilidad operativa de los sistemas y servicios afectados por incidentes de ciberseguridad.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
RC.RP-01: La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez que se inicia desde el proceso de respuesta a incidentes.	Alta	Alta	Alta	**CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres. **GI.5** Responder ante incidentes de seguridad de la información.
RC.RP-02: Se seleccionan, delimitan, priorizan y llevan a cabo las acciones de recuperación.	Media	Media	Media	**CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres.
RC.RP-03: Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para la restauración.	Alta	Alta	Alta	**SO.6** Respaldar la información y realizar pruebas de restauración periódicas.
RC.RP-04: Se tienen en cuenta las funciones críticas de la misión y la gestión de riesgos de ciberseguridad para establecer normas operativas posteriores al incidente.	Baja	Baja	Baja	**GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.
RC.RP-05: Se verifica la integridad de los activos restaurados, se restauran los sistemas y servicios y se confirma el estado operativo normal.	Baja	Media	Media	**CO.5** Definir las ventanas de tiempo soportadas para la continuidad de las operaciones.
RC.RP-06: Se declara el fin de la recuperación del incidente sobre la base de criterios y se completa la documentación relacionada con el incidente.	Baja	Baja	Baja	**GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.

RC.CO Comunicación de la recuperación del incidente

Se coordinan las actividades de restauración con las partes internas y externas.

Subcategoría	Prioridad Básico	Prioridad Estándar	Prioridad Avanzado	Requisitos relacionados
RC.CO-03: Las actividades de recuperación y los progresos en el restablecimiento de las capacidades operativas se comunican a las partes interesadas internas y externas designadas.	Baja	Baja	Media	**CO.6** Definir los mecanismos de comunicación e interlocutores válidos.
RC.CO-04: Las actualizaciones públicas sobre la recuperación del incidente se comparten mediante el uso de métodos y mensajes aprobados.	Baja	Baja	Media	**CO.6** Definir los mecanismos de comunicación e interlocutores válidos.

5. Modelo de madurez

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.

El nivel 0 de madurez (que no se incluye en el presente modelo de madurez) indica que las acciones vinculadas a seguridad de la información y ciberseguridad son casi o totalmente inexistentes.

Es importante resaltar que el nivel de madurez deseado en cada subcategoría dependerá del análisis de riesgos que cada organización realice, o en su defecto, el establecido por algún mandato de su sector o comunidad de pertenencia.

5.1 Función: Gobernar (GV)

GV.OC Contexto organizativo

Se comprenden las circunstancias (misión, expectativas de las partes interesadas, dependencias y requisitos legales, normativos y contractuales) que afectan a las decisiones de gestión de riesgos de ciberseguridad de la organización.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.OC-01. Se comprende la misión de la organización y se informa sobre la gestión de riesgos de ciberseguridad.	**PL.1-1:** Están establecidos los objetivos anuales de seguridad de la información. **PL.1-2:** Están definidas las acciones para lograr el cumplimiento de los objetivos.	**PL.1-3:** Los objetivos forman parte de un plan de acción de seguridad de la información. **PL.1-4:** Los objetivos están documentados y aprobados por el CSI.	**PL.1-5:** Los objetivos anuales de seguridad de la información son difundidos al personal y partes interesadas. **PL.1-6:** El plan de acción para cumplir con los objetivos se desarrolla y ejecuta de manera coordinada con los distintos actores de la organización. **PL.1-7:** Se definen indicadores para el seguimiento del cumplimiento de los objetivos.	**PL.1-8:** Los objetivos se traducen en proyectos o iniciativas de seguridad de la información. **PL.1-9:** Se revisa periódicamente el cumplimiento de los objetivos y el avance del plan de acción.
GV.OC-02. Las partes interesadas internas y externas son comprendidas, y sus necesidades y expectativas con respecto a la gestión de riesgos de ciberseguridad son comprendidas y consideradas.	**GR.2-1:** Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia.	**GR.2-3:** Se cuenta con un inventario de riesgos de seguridad de la información que incluye riesgos asociados a todos los activos de información.	**GR.2-5:** Se incorporan riesgos vinculados a la cadena de suministro.	**GR.2-7:** Debe revisarse periódicamente la tolerancia al riesgo establecida, y modificarse ante cambios normativos, tecnológicos o necesidades del negocio.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.OC-03 Se comprenden y gestionan los requisitos legales, normativos y contractuales relativos a la ciberseguridad, incluidas las obligaciones en materia de privacidad y libertades civiles.	**CN.1-1:** Se identifican los requisitos normativos relacionados a seguridad de la información y ciberseguridad, protección de datos personales, acceso a la información pública, propiedad intelectual, y otras obligaciones legales, contractuales o políticas que resulten exigibles para la organización. **PD.1-1:** Se lleva un inventario actualizado de bases de datos personales, incluyendo responsables, categoría de datos y sistemas que las soportan.	**CN.1-2:** El delegado de protección de datos personales trabaja de manera coordinada con el RSI y/o CSI. **PD.1-3:** Se cuenta con un estudio de la normativa vigente que debe cumplir cada base de datos registrada. **PD.2-3:** Se lleva un registro documentado de todas las solicitudes recibidas por parte de los titulares de datos personales, relativas a la actualización, eliminación o rectificación de sus datos, incluyendo el plazo en que cada solicitud fue atendida.	**CN.1-3:** Se han definido procedimientos para incorporar nuevos requisitos legales o normativos cuando sean publicados. **CN.1-4:** El resultado es comunicado al RSI y/o al CSI. **PD.1-4:** Se realizan revisiones periódicas del cumplimiento legal del tratamiento de datos personales en los sistemas y procesos de la organización. **PD.1-5:** Se implementan medidas correctivas cuando se detectan incumplimientos en materia de legalidad del tratamiento de datos.	**CN.1-5:** Se realizan auditorías internas para verificar el cumplimiento. **CN.1-6:** Los resultados de las revisiones se utilizan para la mejora continua y apoyan a la toma de decisiones. **PD.1-6:** Se ha integrado la revisión del cumplimiento legal del tratamiento de datos personales dentro del proceso de auditoría interna. **PD.4-8:** Se ha incorporado la verificación del consentimiento informado como parte de las auditorías internas periódicas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	PD.1-2: Todas las bases de datos que contienen datos personales están registradas ante la URCDP. **PD.2-1:** Se cuenta con mecanismos para recibir solicitudes expresas de los titulares de corrección manual de datos personales. **PD.2-2:** La organización establece qué datos personales son necesarios para cada trámite o servicio, y limita su recolección únicamente a esa información.	**PD.2-4:** Cuando el titular de los datos personales se encuentra presente, se procede a validar la exactitud de los datos y, en caso de corresponder, se actualizan los datos en los sistemas correspondientes en ese mismo momento. **PD.4-3:** Se verifica, previo al tratamiento de datos personales, si el consentimiento del titular es requerido según lo establecido por la normativa vigente.	**PD.2-5:** Los sistemas implementan funcionalidades que requieren a los usuarios la revisión y validación periódica de sus datos personales, con el objetivo de identificar y corregir información inexacta o desactualizada. **PD.2-6:** Los sistemas que gestionan datos personales registran las modificaciones realizadas, incluyendo la fecha del cambio y la identidad del usuario que lo efectuó. **PD.4-6:** Existen procedimientos documentados que establecen cómo identificar los casos en los que se requiere consentimiento, y cómo obtener, registrar y conservarlo de manera adecuada.	**PD.4-9:** Se revisan y actualizan periódicamente los textos, formularios y canales utilizados para recabar el consentimiento informado. **PD.8-8:** Se definen indicadores sobre el procedimiento de gestión de solicitudes de derechos. **PD.8-9:** Se revisa periódicamente el procedimiento de gestión de solicitudes de derechos, se registran los desvíos o puntos de mejora.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	PD.4-1: Cuando corresponde, se incluye una cláusula de consentimiento libre, previa e informada en los medios utilizados para recabar los datos personales (formularios, grabaciones, sitios web, etc.). **PD.4-2:** Se conservan registros que evidencien el consentimiento otorgado por los titulares, siempre que sea exigido por la normativa. **PD.8-1:** Se reciben y atienden las solicitudes relacionadas con los derechos sobre datos personales de los usuarios. **PD.8-2:** Se han gestionado respuestas a solicitudes de titulares dentro del plazo legal.	**PD.4-4:** Los mecanismos que requieren consentimiento informado garantizan que la opción de aceptar o rechazar esté claramente visible y no preseleccionada. **PD.4-5:** Cuando el tratamiento se basa en el consentimiento, se han definido mecanismos que permiten a los titulares revocar el consentimiento otorgado en cualquier momento, sin afectar la licitud del tratamiento previo. **PD.8-3:** Se encuentra asignado personal encargado de recibir, procesar y responder las solicitudes vinculadas a los derechos de los titulares. **PD.8-4:** Las solicitudes y su tratamiento son registrados.	**PD.4-7:** Los mecanismos para ejercer la revocación del consentimiento están disponibles públicamente y son fácilmente accesibles. **PD.8-5:** Existe un procedimiento formal de gestión de las solicitudes de derechos de los titulares que contempla todos los derechos mencionados en la normativa (Información, Acceso, Actualización y Rectificación, Inclusión, Supresión, Impugnación de Valoraciones Personales). **PD.8-6:** Se encuentra definido un procedimiento para verificar la identidad del solicitante del derecho. **PD.8-7:** Los procedimientos para ejercer los derechos son difundidos a los titulares de los datos, el personal y terceras partes interesadas.	**PD.8-10:** Se implementan las mejoras al procedimiento de gestión de solicitudes de derechos en base a las revisiones periódicas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.OC-04. Se comprenden y comunican los objetivos, las capacidades y los servicios críticos de los que dependen las partes interesadas externas o que esperan de la organización.	**CO.5-1:** Está designado un responsable o equipo para la identificación de métricas de recuperación para procesos críticos. **SO.3-1:** La capacidad actual instalada es suficiente para garantizar la prestación de los servicios críticos.	**CO.5-2:** Se han definido formalmente las ventanas de tiempo máximo soportadas por el negocio sin poder operar (MTD), para cada sistema que soporte un proceso crítico. **CO.5-3:** Se ha determinado el RTO (Recovery Time Objective) para cada sistema que soporte un proceso crítico. **CO.5-4:** Se ha definido el RPO (Recovery Point Objective) para cada sistema que soporte un proceso crítico.	**CO.5-5:** Las métricas MTD, RTO y RPO han sido utilizadas para identificar brechas entre los tiempos actualmente alcanzables y los requerimientos definidos. **CO.5-6:** Las métricas definidas han sido incorporadas como insumo obligatorio en el diseño, pruebas y evaluación de los planes de continuidad. **CO.5-7:** Las métricas son revisadas periódicamente y actualizadas ante cambios en procesos o tecnologías. **SO.3-5:** Está establecido el proceso de gestión de la capacidad. **SO.3-6:** Los roles y responsabilidades asociados al proceso de gestión de la capacidad están definidos y documentados.	**CO.5-8:** Los resultados de las pruebas de continuidad son comparados contra las métricas definidas y se documentan desviaciones con planes de mejora asociados. **CO.5-9:** Las métricas son utilizadas como insumo en análisis costo-beneficio para priorizar inversiones en infraestructura, redundancia o automatización de recuperación.
GV.OC-05. Se comprenden y comunican los resultados, capacidades y servicios de los que depende la organización.	**OR.7-1:** Se han identificado los servicios críticos para la organización. **OR.7-2:** Se han identificado los proveedores y/o otras partes interesadas críticas para la organización.	**OR.7-3:** Se cuenta con un mapeo de procesos. **OR.7-4:** Se cuenta con un análisis FODA.	**OR.7-5:** Se cuenta con un mapeo de dependencias de servicios.	**OR.7-6:** Se realizan revisiones periódicas del contexto de la organización.

GV.RM Estrategia de gestión de riesgos

Se establecen, comunican y utilizan las prioridades, las restricciones, las declaraciones

de tolerancia y apetito por el riesgo y los supuestos de la organización para respaldar las decisiones sobre el riesgo operativo.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RM-01. Los objetivos de la gestión de riesgos son establecidos y acordados por las partes interesadas de la organización.	**PL.1-1:** Están establecidos los objetivos anuales de seguridad de la información.	**PL.1-3:** Los objetivos forman parte de un plan de acción de seguridad de la información.	**PL.1-5:** Los objetivos anuales de seguridad de la información son difundidos al personal y partes interesadas. **PL.1-6:** El plan de acción para cumplir con los objetivos se desarrolla y ejecuta de manera coordinada con los distintos actores de la organización. **PL.1-7:** Se definen indicadores para el seguimiento del cumplimiento de los objetivos.	**PL.1-9:** Se revisa periódicamente el cumplimiento de los objetivos y el avance del plan de acción.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RM-02. Se establecen, se comunican y se mantienen las declaraciones sobre el apetito de riesgo y la tolerancia al riesgo.	**GR.3-1:** Se toman acciones ad-hoc con el objetivo de llevar los principales riesgos de seguridad de la información a niveles aceptables para la organización.	**CO.5-2:** Se han definido formalmente las ventanas de tiempo máximo soportadas por el negocio sin poder operar (MTD), para cada sistema que soporte un proceso crítico. **CO.5-3:** Se ha determinado el RTO (Recovery Time Objective) para cada sistema que soporte un proceso crítico. **CO.5-4:** Se ha definido el RPO (Recovery Point Objective) para cada sistema que soporte un proceso crítico.	**GR.2-4:** El apetito de riesgo y la tolerancia al riesgo se ha definido formalmente por el negocio.	**GR.2-7:** Debe revisarse periódicamente la tolerancia al riesgo establecida, y modificarse ante cambios normativos, tecnológicos o necesidades del negocio.
GV.RM-03. Las actividades y los resultados de la gestión de riesgos de ciberseguridad se incluyen en los procesos de gestión de riesgos de la empresa.	**GR.1-1:** Existe un proceso para la gestión de riesgos de seguridad de la información.	**GR.1-2:** Se cuenta con una metodología de evaluación de riesgos de seguridad de la información definida y documentada.	**GR.1-3:** Existe una política aprobada de gestión de riesgos de seguridad de la información. **GR.1-4:** La política de gestión de riesgos de seguridad de la información ha sido difundida a todas las partes interesadas.	**GR.1-5:** La metodología de evaluación de riesgos es revisada periódicamente y ajustada en función de los resultados obtenidos, los cambios en el contexto organizacional o normativo, y las oportunidades de mejora identificadas en su aplicación.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RM-04. Se establece y comunica una dirección estratégica que describa las opciones adecuadas de respuesta al riesgo.	**GR.3-1:** Se toman acciones ad-hoc con el objetivo de llevar los principales riesgos de seguridad de la información a niveles aceptables para la organización.	**GR.3-2:** Se elaboran planes de tratamiento para los riesgos de seguridad de la información que excedan los niveles de tolerancia definidos por la organización. **GR.3-3:** Cada plan de tratamiento identifica las acciones necesarias, el responsable de su ejecución y el plazo previsto.	**GR.3-4:** Los planes de tratamiento son revisados y validados por los responsables de ejecutarlos antes de su ejecución. **GR.3-5:** Los planes de tratamiento de riesgos incluyen métricas e indicadores que permiten evaluar su avance. **GR.3-6:** La implementación de los controles debe realizarse conforme a la prioridad explícita y formalmente establecida por la Dirección. **GR.3-7:** La efectividad de los controles implementados es evaluada, y el riesgo residual resultante es documentado y validado por las partes interesadas.	**GR.3-9:** La revisión se documenta formalmente y es comunicada al CSI y a las otras partes interesadas. **GR.3-10:** Se ajustan los planes de tratamiento de riesgos en función de los resultados obtenidos y las oportunidades de mejora identificadas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RM-05. Se establecen líneas de comunicación en toda la organización para los riesgos de ciberseguridad, lo que incluye a los riesgos de proveedores y otros terceros.	**GR.1-1:** Existe un proceso para la gestión de riesgos de seguridad de la información que abarca los componentes del centro de datos y servicios críticos de forma independiente. **GI.4-1:** Los incidentes de seguridad se reportan internamente de acuerdo con lineamientos preestablecidos. **GI.4-2:** El personal ha sido instruido sobre los mecanismos y canales habilitados para reportar incidentes.	**GI.4-4:** Los registros de incidentes permiten trazabilidad completa de su evolución, desde la detección hasta el cierre.	**GR.1-3:** Existe una política aprobada de gestión de riesgos de seguridad de la información. **GR.1-4:** La política de gestión de riesgos de seguridad de la información ha sido difundida a todas las partes interesadas. **OR.2-5:** El CSI participa en la definición de niveles aceptables de riesgo y en la aprobación del plan de tratamiento de riesgos.	**GR.1-5:** La metodología de evaluación de riesgos es revisada periódicamente y ajustada en función de los resultados obtenidos, los cambios en el contexto organizacional o normativo, y las oportunidades de mejora identificadas en su aplicación.
GV.RM-06. Se establece y comunica un método estandarizado para calcular, documentar, categorizar y priorizar los riesgos de ciberseguridad.	**GR.1-1:** Existe un proceso para la gestión de riesgos de seguridad de la información que abarca los componentes del centro de datos y servicios críticos de forma independiente.	**GR.1-2:** Se cuenta con una metodología de evaluación de riesgos de seguridad de la información definida y documentada.	**GR.1-3:** Existe una política aprobada de gestión de riesgos de seguridad de la información. **GR.1-4:** La política de gestión de riesgos de seguridad de la información ha sido difundida a todas las partes interesadas.	**GR.1-5:** La metodología de evaluación de riesgos es revisada periódicamente y ajustada en función de los resultados obtenidos, los cambios en el contexto organizacional o normativo, y las oportunidades de mejora identificadas en su aplicación.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RM-07. Se caracterizan las oportunidades estratégicas (es decir, los riesgos positivos) y se incluyen en las discusiones sobre riesgos de ciberseguridad de la organización.	**GR.1-1:** Existe un proceso para la gestión de riesgos de seguridad de la información que abarca los componentes del centro de datos y servicios críticos de forma independiente.	**GR.1-2:** Se cuenta con una metodología de evaluación de riesgos de seguridad de la información definida y documentada.	**GR.1-3:** Existe una política aprobada de gestión de riesgos de seguridad de la información. **GR.1-4:** La política de gestión de riesgos de seguridad de la información ha sido difundida a todas las partes interesadas.	**GR.1-5:** La metodología de evaluación de riesgos es revisada periódicamente y ajustada en función de los resultados obtenidos, los cambios en el contexto organizacional o normativo, y las oportunidades de mejora identificadas en su aplicación.

GV.RR Funciones, responsabilidad y autoridades

Se establecen y comunican las funciones, las responsabilidades y las competencias en materia de ciberseguridad para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RR-01. El liderazgo organizativo es responsable de los riesgos de ciberseguridad y fomenta una cultura consciente de los riesgos, ética y de mejora continua.	**PS.1-2:** La política es difundida a todo el personal y partes interesadas relevantes.	**PS.1-4:** La política se encuentra disponible en un sitio accesible.	**PS.1-6:** Los resultados de las revisiones de la política son documentados y comunicado al CSI. **PS.1-7:** Ante modificaciones la política es difundida nuevamente. **OR.2-5:** El CSI participa en la definición de niveles aceptables de riesgo y en la aprobación del plan de tratamiento de riesgos.	**PS.1-8:** La política es revisada periódicamente. **OR.2-8:** El CSI revisa los indicadores asociados a los planes anuales de mejora de seguridad de la información.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RR-02. Se establecen, comunican, comprenden y aplican las funciones, responsabilidades y autoridades relacionadas con la gestión de riesgos de ciberseguridad.	**OR.1-1:** Existe una persona que cumple el rol de RSI. **OR.1-2:** El RSI coordina actividades de seguridad de la información. **OR.2-1:** Se encuentra designado formalmente el CSI de la organización. **OR.3-1:** Está designado un punto de contacto oficial para incidentes de ciberseguridad. **OR.3-2:** Se han identificado los contactos de autoridades ante aspectos de ciberseguridad.	**OR.1-3:** Está designado formalmente el RSI. **OR.1-4:** Las responsabilidades del RSI están documentadas e incluyen: la gestión de seguridad de la información, gestión de incidentes, gestión de riesgos de seguridad, entre otras. **OR.2-2:** El CSI se reúne periódicamente y documenta dichas reuniones. **OR.3-3:** El punto de contacto oficial es conocido por todo el personal.	**OR.1-5:** El RSI coordina la evaluación de riesgos junto con los responsables de los activos o designa referentes delegados. **OR.1-6:** El RSI participa en el CSI de la organización. **OR.2-3:** Las responsabilidades y atribuciones del CSI están documentadas y aprobadas por la Dirección. **OR.2-4:** El CSI tiene establecidas pautas para su funcionamiento. **OR.3-4:** Los contactos con las autoridades, CSIRT y otros actores externos relevantes están documentados.	**OR.1-7:** El RSI elabora y presenta planes anuales de mejora de seguridad, incluyendo indicadores. **OR.1-8:** El RSI forma parte de los procesos de planificación estratégica. **OR.2-6:** El CSI revisa los planes y políticas de seguridad y aprueba sus actualizaciones. **OR.2-7:** El CSI aprueba la planificación estratégica de seguridad. **OR.3-5:** Se revisan y actualizan periódicamente los contactos.
GV.RR-03. Se asignan recursos adecuados de acuerdo con la estrategia de riesgos de ciberseguridad, las funciones, las responsabilidades y las políticas.	**GR.3-1:** Se toman acciones ad-hoc con el objetivo de llevar los principales riesgos de seguridad de la información a niveles aceptables para la organización.	**GR.3-2:** Se elaboran planes de tratamiento para los riesgos de seguridad de la información que excedan los niveles de tolerancia definidos por la organización. **GR.3-3:** Cada plan de tratamiento identifica las acciones necesarias, el responsable de su ejecución y el plazo previsto.	**GR.3-4:** Los planes de tratamiento son revisados y validados por los responsables de ejecutarlos antes de su ejecución. **GR.3-8:** Existe una línea presupuestal que permite implementar el plan de tratamiento de riesgos.	**GR.3-9:** Los planes de tratamiento de los riesgos se revisan periódicamente y se actualizan si es necesario.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.RR-04. La ciberseguridad se incluye en las prácticas de recursos humanos.	**GH.1-1:** Las condiciones laborales del personal, ya sea mediante contrato, estatuto o normativa interna, incluyen cláusulas o disposiciones que establecen sus responsabilidades en materia de seguridad de la información.	**GH.1-2:** Las responsabilidades del personal respecto a la seguridad de la información están documentadas. **GH.1-3:** Las responsabilidades en seguridad de la información son comunicadas al personal al momento de su incorporación. **PD.6-2:** Están definidos y documentados los roles autorizados a acceder a datos personales y las finalidades permitidas para su uso. **PD.6-3:** Los contratos, reglamentos o políticas internas contemplan sanciones explícitas ante el uso o divulgación indebida de datos personales. **PD.6-4:** El personal autorizado a tratar datos personales está sujeto a compromisos de confidencialidad, los cuales pueden formalizarse mediante cláusulas en contratos, reglamentos internos, políticas institucionales o documentos específicos firmados, según corresponda al vínculo con la organización.	**GH.1-4:** Existe un procedimiento documentado para la desvinculación del personal que contempla la revocación de accesos físicos y lógicos, y la devolución de activos. **GH.1-5:** La organización cuenta con un proceso disciplinario formalizado que aplica ante incumplimientos de las políticas de seguridad, de acuerdo con la normativa laboral o administrativa vigente. **PD.6-5:** Están definidas y documentadas qué conductas constituyen violaciones al principio de reserva. **PD.6-6:** Existe un procedimiento formalizado para investigar violaciones al principio de reserva.	**GH.1-6:** Los documentos contractuales o reglamentarios relacionados con la incorporación y desvinculación del personal se revisan periódicamente para asegurar su vigencia y adecuación. **GH.1-7:** Se registran y revisan los desvíos e incumplimientos de las obligaciones contractuales relacionadas a seguridad de la información.

GV.PO Política

La política de ciberseguridad de la organización es establecida, comunicada y aplicada.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.PO-01. La política de gestión de riesgos de ciberseguridad se establece en base al contexto organizativo, la estrategia de ciberseguridad y las prioridades, y es comunicada y aplicada.	**PS.1-1:** Existe una política de seguridad aprobada por la Dirección.	**PS.1-3:** La política define los responsables de su cumplimiento.	**PS.1-5:** La política es revisada ante cambios significativos de índole normativo o del contexto de la organización.	**PS.1-9:** La política cuenta con indicadores definidos para su evaluación.
GV.PO-02. La política de gestión de riesgos de ciberseguridad se revisa, actualiza, comunica y aplica para reflejar los cambios en los requisitos, las amenazas, la tecnología y la misión de la organización.	**PS.1-2:** La política es difundida a todo el personal y partes interesadas relevantes.	**PS.1-4:** La política se encuentra disponible en un sitio accesible.	**PS.1-6:** Los resultados de las revisiones de la política son documentados y comunicado al CSI. **PS.1-7:** Ante modificaciones la política es difundida nuevamente.	**PS.1-8:** La política es revisada periódicamente.

GV.OV Supervisión

Los resultados de las actividades de gestión de riesgos de ciberseguridad en toda la organización y el rendimiento se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.OV -01. Los resultados de la estrategia de gestión de riesgos de ciberseguridad se revisan para informar y ajustar la estrategia y la dirección.	N/A	N/A	N/A	N/A
GV.OV -02. La estrategia de gestión de riesgos de ciberseguridad se revisa y ajusta para garantizar la cobertura de los requisitos y riesgos de la organización	N/A	N/A	N/A	N/A
GV.OV -03. El rendimiento de la gestión de riesgos de ciberseguridad de la organización se evalúa y revisa para realizar los ajustes necesarios.	N/A	N/A	N/A	N/A

GV.SC Gestión de riesgos de la cadena de suministro en materia de ciberseguridad

Las partes interesadas de la organización identifican, establecen, gestionan, supervisan y mejoran los procesos de gestión de riesgos de la cadena de suministro en materia de ciberseguridad.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.SC-01. Las partes interesadas de la organización establecen y acuerdan un programa, estrategia, objetivos, políticas y procesos de gestión de riesgos de ciberseguridad en la cadena de suministro.	**GR.1-1:** Existe un proceso para la gestión de riesgos de seguridad de la información que abarca los componentes del centro de datos y servicios críticos de forma independiente. **RP.2-1:** Se definen métricas e indicadores para el seguimiento y control de los proveedores, mínimamente para los proveedores críticos.	**GR.1-2:** Se cuenta con una metodología de evaluación de riesgos de seguridad de la información definida y documentada.	**GR.1-3:** Existe una política aprobada de gestión de riesgos de seguridad de la información. **RP.2-5:** Se registra y mantiene evidencia de los incumplimientos contractuales o desviaciones detectadas en los servicios provistos, incluyendo las acciones tomadas ante los mismos.	**GR.1-5:** La metodología de evaluación de riesgos es revisada periódicamente y ajustada en función de los resultados obtenidos, los cambios en el contexto organizacional o normativo, y las oportunidades de mejora identificadas en su aplicación. **RP.2-7:** La gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio.
GV.SC-02. Se establecen, comunican y coordinan interna y externamente las funciones y responsabilidades de ciberseguridad para proveedores, clientes y colaboradores.	**SC.6-1:** Los nuevos proveedores de servicios deben firmar acuerdos de confidencialidad o no divulgación (NDA) antes del inicio de la relación contractual. **SC.6-2:** Todo nuevo personal incorporado debe estar cubierto por cláusulas confidencialidad y no divulgación, ya sea en acuerdos, estatuto o normativa interna.	**SC.6-3:** La obligación de confidencialidad y no divulgación se extiende a todo el personal de la organización, independientemente de su rol o tipo de contratación. **SC.6-4:** Todos los proveedores que deban acceder a información confidencial de la organización deben tener firmado un acuerdo de no divulgación.	**SC.6-5:** Se detallan en los acuerdos de no divulgación las responsabilidades y sanciones por incumplimiento.	**SC.6-6:** Se revisan los acuerdos de no divulgación de forma periódica para verificar pertinencia en relación a los objetivos de negocio. **SC.6-7:** El resultado de las revisiones se comunica al RSI y demás partes interesadas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.SC-03. La gestión de riesgos de la cadena de suministro en materia de ciberseguridad está integrada en la ciberseguridad y la gestión de riesgos empresariales, la evaluación de riesgos y los procesos de mejora.	**GR.2-1:** Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia.	**GR.2-3:** Se cuenta con un inventario de riesgos de seguridad de la información que incluye riesgos asociados a todos los activos de información.	**GR.2-4:** El apetito de riesgo y la tolerancia al riesgo se ha definido formalmente por el negocio. **GR.2-5:** Se incorporan riesgos vinculados a la cadena de suministro.	**GR.2-7:** Debe revisarse periódicamente la tolerancia al riesgo establecida, y modificarse ante cambios normativos, tecnológicos o necesidades del negocio. **GR.2-8:** Los riesgos se revisan periódicamente, la revisión se documenta formalmente.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.SC-04. Los proveedores son conocidos y priorizados por criticidad.	**RP.1-1:** Se identifican todos los participantes de la cadena de suministro relacionados con los activos y servicios críticos, incluyendo un punto de contacto operativo designado por cada proveedor. **RP.1-2:** Se cuenta con acuerdos de nivel de servicio (SLA) firmados con proveedores que prestan servicios críticos.	**RP.1-3:** Se implementan mecanismos para identificar y gestionar los riesgos asociados a los participantes de la cadena de suministro que intervienen en los activos y servicios críticos de la organización. **RP.1-4:** Está definido un procedimiento documentado de gestión de proveedores que abarca la selección, contratación, seguimiento, y finalización del vínculo. **RP.1-5:** Los contratos con proveedores críticos deben incluir cláusulas que obliguen a notificar de forma oportuna cualquier incidente de seguridad, confirmado o sospechado, que pueda afectar a la organización.	**RP.1-6:** Se cuenta con una política formal de relacionamiento con proveedores.	**RP.1-8:** Se aplica la gestión de riesgos en la adquisición de productos y servicios, y se mantiene en todo el ciclo de vida de los mismos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.SC-05. Los requisitos para abordar los riesgos de ciberseguridad en las cadenas de suministro se establecen, priorizan e integran en contratos y otros tipos de acuerdos con proveedores y otras terceras partes pertinentes.	**AD.2-2:** Los requisitos de seguridad de la información se incluyen en las solicitudes y evaluaciones de compra.	**AD.2-3:** Se evalúa la capacidad de los proveedores para cumplir con los requisitos de seguridad antes de la contratación. **RP.2-2:** Los contratos y acuerdos con proveedores críticos incluyen cláusulas que permiten su revisión o ajuste en caso de cambios en los servicios prestados, en las tecnologías utilizadas o en las normativas aplicables.	**AD.2-5:** Los contratos con proveedores incluyen compromisos de mantenimiento de la seguridad a lo largo del ciclo de vida del producto o servicio. **RP.2-5:** Se registra y mantiene evidencia de los incumplimientos contractuales o desviaciones detectadas en los servicios provistos, incluyendo las acciones tomadas ante los mismos.	**AD.2-6:** Los procesos de adquisición consideran las lecciones aprendidas y resultados de auditorías para mejorar continuamente los requisitos de seguridad. **RP.2-6:** Se revisan periódicamente los acuerdos con proveedores críticos para asegurar su adecuación a los requerimientos actuales del negocio y a cambios regulatorios. **RP.2-8:** Las evaluaciones son tomadas en cuenta para las actualizaciones de contratos y las futuras adquisiciones.
GV.SC-06. Se llevan a cabo la planificación y la diligencia debida para reducir los riesgos antes de entablar relaciones formales con proveedores u otros terceros.	**AD.2-1:** Se cuenta con lineamientos generales para la adquisición de sistemas o servicios de tecnología.	**RP.2-2:** Los contratos y acuerdos con proveedores críticos incluyen cláusulas que permiten su revisión o ajuste en caso de cambios en los servicios prestados, en las tecnologías utilizadas o en las normativas aplicables.	**RP.2-4:** Se documentan los resultados de las evaluaciones de desempeño y cumplimiento de requisitos de seguridad de los proveedores.	**RP.2-7:** La gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.SC-07. Los riesgos planteados por un proveedor, sus productos y servicios y otros terceros se comprenden, registran, priorizan, evalúan, responden y monitorean a lo largo de la relación.	**RP.2-1:** Se definen métricas e indicadores para el seguimiento y control de los proveedores, mínimamente para los proveedores críticos.	**RP.2-2:** Los contratos y acuerdos con proveedores críticos incluyen cláusulas que permiten su revisión o ajuste en caso de cambios en los servicios prestados, en las tecnologías utilizadas o en las normativas aplicables.	**RP.2-3:** Se define la periodicidad de las evaluaciones de los proveedores. **RP.2-4:** Se documentan los resultados de las evaluaciones de desempeño y cumplimiento de requisitos de seguridad de los proveedores.	**RP.2-7:** La gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio.
GV.SC-08. Los proveedores pertinentes y otros terceros se incluyen en las actividades de planificación, respuesta y recuperación de incidentes.	**GI.1-1:** Se encuentran identificados los puntos de contacto inicial para la recepción de eventos de seguridad.	**GI.1-2:** Se identifican los potenciales actores internos y externos ante un incidente y se registran sus datos de contacto.	**GI.1-6:** La política de gestión de incidentes es difundida a todas las partes interesadas.	**GI.1-7:** Se realizan auditorías internas para verificar el cumplimiento con la política y procedimientos relacionados.
GV.SC-09. Las prácticas de seguridad de la cadena de suministro se integran en los programas de ciberseguridad y de gestión de riesgos empresariales, y su rendimiento se monitorea a lo largo del ciclo de vida de los productos y servicios tecnológicos.	**RP.2-1:** Se definen métricas e indicadores para el seguimiento y control de los proveedores, mínimamente para los proveedores críticos.	**RP.2-2:** Los contratos y acuerdos con proveedores críticos incluyen cláusulas que permiten su revisión o ajuste en caso de cambios en los servicios prestados, en las tecnologías utilizadas o en las normativas aplicables.	**AD.2-4:** Se revisan y aprueban los entregables para verificar que cumplen con los requisitos de seguridad definidos. **RP.2-3:** Se define la periodicidad de las evaluaciones de los proveedores. **RP.2-4:** Se documentan los resultados de las evaluaciones de desempeño y cumplimiento de requisitos de seguridad de los proveedores.	**RP.2-7:** La gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
GV.SC-10. Los planes de gestión de riesgos de la cadena de suministro de ciberseguridad incluyen disposiciones para las actividades que ocurren después de la conclusión de un acuerdo de colaboración o servicio.	**GR.3-1:** Se toman acciones ad-hoc con el objetivo de llevar los principales riesgos de seguridad de la información a niveles aceptables para la organización.	**GR.3-3:** Cada plan de tratamiento identifica las acciones necesarias, el responsable de su ejecución y el plazo previsto.	**GR.3-4:** Los planes de tratamiento son revisados y validados por los responsables de ejecutarlos antes de su ejecución. **RP.1-7:** Está definido un procedimiento documentado de gestión de proveedores que abarca la selección, contratación, seguimiento, y finalización del vínculo.	**GR.3-9:** Los planes de tratamiento de los riesgos se revisan periódicamente y se actualizan si es necesario.

5.2 Función: Identificar (ID)

ID.AM. Gestión de activos

Los activos (por ejemplo, datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar sus objetivos empresariales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.AM-01. Se mantienen inventarios del hardware gestionado por la organización	**GA.1-1:** Se confecciona y mantiene un inventario de activos físicos del centro de datos, incluyendo servidores, dispositivos de red, racks, UPS y otros componentes relevantes. **OR.5-1:** Se mantiene un inventario actualizado de los dispositivos móviles de la organización.	**GA.1-4:** El inventario de activos físicos debe incluir todos los dispositivos utilizados dentro y fuera del centro de datos, tales como estaciones de trabajo (PCs), dispositivos de almacenamiento extraíble, impresoras, dispositivos de red, entre otros. **GA.4-2:** Están identificados y documentados los tipos de medios de almacenamiento externos permitidos para su uso dentro de la organización. **GA.4-4:** Los medios de almacenamiento externo se encuentran inventariados y clasificados según la clasificación de su información y sus características.	**OR.5-6:** Los equipos móviles cuentan con un sistema de borrado del dispositivo en caso de extravío o robo. **OR.5-7:** Los dispositivos personales que se conectan a los servicios de la organización deben estar autorizados, registrados y sujetos a requisitos de seguridad.	**GA.1-13:** Se elimina el software y/o hardware que esté fuera de soporte o que represente un riesgo no aceptable.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.AM-02. Se mantienen inventarios de software, servicios y sistemas gestionados por la organización	**CN.4-1:** Se lleva control del licenciamiento de software de equipos servidores. **GA.1-2:** Se elabora y mantiene un inventario detallado del software base (ej.: sistemas operativos, servidores de aplicación, servidores de base de datos, hipervisores) y del software de aplicación instalado en los activos del centro de datos. **GA.1-3:** Cada activo registrado en el inventario debe tener un responsable asignado, cuya información debe estar documentada en el sistema de gestión de activos o inventario utilizado. **SC.15-1:** Existe un inventario de sitios Web institucionales.	**CN.4-3:** Se lleva control del licenciamiento de software de equipos personales. **GA.1-5:** El inventario debe incluir las plataformas de software y aplicaciones implementadas, independientemente de su ubicación física o modalidad (on premise o en la nube). **GA.1-7:** El inventario debe estar debidamente documentado y accesible para las personas autorizadas por la organización.	**CN.4-4:** El inventario centralizado de software instalado en la organización debe permitir asociar licencias activas con las instalaciones detectadas. **GA.1-8:** Las políticas, procesos y procedimientos para la actualización del inventario de activos deben estar formalmente documentados. **GA.1-9:** La organización debe utilizar una herramienta de software especializada para registrar, seguir y controlar sus activos de información y tecnológicos. **GA.1-10:** Los procesos y procedimientos de actualización del inventario deben incorporar, total o parcialmente, mecanismos de automatización. **GA.1-11:** Se debe establecer y mantener un proceso de control y monitoreo continuo del licenciamiento del software, con alertas ante vencimientos o irregularidades.	**GA.1-12:** Se realizan auditorías internas periódicas para verificar el cumplimiento y alineación de la política y los procedimientos establecidos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.AM-03 Se mantienen representaciones de la comunicación de red autorizada de la organización y de los flujos de datos de red internos y externos.	**SC.13-2:** Están identificados y documentados los principales servicios de red utilizados por la organización.	**SC.13-6:** Las conexiones con otras entidades están formalmente autorizadas mediante acuerdos de seguridad de interconexión que describen interfaz, requisitos de seguridad y datos intercambiados. **SC.13-7:** Los proveedores de servicios de red cuentan con acuerdos de nivel de servicio (SLA) y cláusulas de seguridad.	**SC.13-8:** Esta definida una política formal de seguridad de las comunicaciones. **SC.13-9:** Se cuenta con un diagrama de red actualizado que refleja la segregación vigente y las interconexiones externas.	**SC.13-12:** Se cuenta con un proceso de control interno que verifica el cumplimiento de la segregación definida y de los acuerdos de interconexión. **SC.13-13:** Se revisan periódicamente los SLA, contratos y condiciones técnicas de los proveedores de red y conectividad.
ID.AM-04. Se mantienen inventarios de los servicios prestados por los proveedores.	**RP.1-1:** Se identifican todos los participantes de la cadena de suministro relacionados con los activos y servicios críticos, incluyendo un punto de contacto operativo designado por cada proveedor. **RP.1-2:** Se cuenta con acuerdos de nivel de servicio (SLA) firmados con proveedores que prestan servicios críticos.	**RP.1-3:** Se implementan mecanismos para identificar y gestionar los riesgos asociados a los participantes de la cadena de suministro que intervienen en los activos y servicios críticos de la organización.	**RP.1-6:** Se cuenta con una política formal de relacionamiento con proveedores.	**RP.1-8:** Se aplica la gestión de riesgos en la adquisición de productos y servicios, y se mantiene en todo el ciclo de vida de los mismos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.AM-05. Se priorizan los activos en función de su clasificación, criticidad, recursos e impacto en la misión.	**GA.2-1:** Están identificados los activos que contienen información crítica para la organización, en base a criterio institucionalmente definido que establezca qué se considera información crítica o sensible. **GA.2-2:** Cada activo registrado en el inventario debe contar con una etiqueta o atributo que refleje su clasificación según los criterios previamente definidos.	**GA.2-3:** Los activos que almacenan o procesan información deben estar clasificados de acuerdo con los criterios establecidos en el procedimiento de clasificación. **GA.2-4:** La herramienta de inventario de activos debe permitir registrar, consultar y mantener la clasificación de la información asociada a cada activo.	**GA.2-5:** Se cuenta con una política y/o procedimiento de clasificación de la información, alineado a la normativa nacional vigente. **GA.2-6:** Se ha definido un procedimiento para el etiquetado de activos clasificados, que contemple tanto los activos digitales como los físicos. **GA.2-7:** La clasificación de la información debe estar integrada en todas las etapas del ciclo de vida del activo: alta, modificación, uso y baja. **GA.2-8:** Las restricciones de acceso deben definirse y aplicarse en función de la clasificación de los activos y el perfil de los usuarios autorizados. **GA.3-7:** Se realiza un control periódico de los activos que contienen o procesan información sensible.	**GA.2-9:** Se realizan controles internos periódicos para verificar que la clasificación de la información asociada a cada activo sea correcta y vigente.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.AM-07. Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados.	**GA.2-1:** Están identificados los activos que contienen información crítica para la organización, en base a criterio institucionalmente definido que establezca qué se considera información crítica o sensible. **GA.2-2:** Cada activo registrado en el inventario debe contar con una etiqueta o atributo que refleje su clasificación según los criterios previamente definidos.	**GA.2-3:** Los activos que almacenan o procesan información deben estar clasificados de acuerdo con los criterios establecidos en el procedimiento de clasificación.	**GA.2-5:** Se cuenta con una política y/o procedimiento de clasificación de la información, alineado a la normativa nacional vigente. **GA.2-7:** La clasificación de la información debe estar integrada en todas las etapas del ciclo de vida del activo: alta, modificación, uso y baja.	**GA.2-9:** Se realizan controles internos periódicos para verificar que la clasificación de la información asociada a cada activo sea correcta y vigente.
ID.AM-08. Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de vida.	**GA.5-1:** Están definidas las pautas para la disposición final y borrado seguro de medios de almacenamiento. **PD.3-1:** Se han eliminado de forma ad-hoc datos personales que ya no eran necesarios para el fin con el que fueron recolectados. **PD.3-2:** Se documenta la finalidad del tratamiento de datos personales en todos los procesos que los recolectan.	**GA.5-3:** Están definidos responsables o ubicaciones específicas para la eliminación segura de medios de almacenamiento. **PD.3-3:** Se han establecido criterios sobre cuánto tiempo se conservarán los datos personales en función de su finalidad. **PD.3-4:** Se han implementado procedimientos para eliminar o anonimizar los datos personales una vez cumplida su finalidad.	**GA.5-5:** Está definida formalmente una política de destrucción de la información. **GA.5-6:** Está definido formalmente un procedimiento de destrucción de la información. **PD.3-5:** Se mantienen registros de las eliminaciones o anonimizaciónes de datos personales, acorde al procedimiento. **PD.3-6:** Se revisan periódicamente las bases de datos con el objetivo de identificar datos cuya finalidad ya se ha cumplido.	**GA.5-9:** Se realizan actividades de control interno para evaluar la correcta aplicación del procedimiento de destrucción. **PD.3-7:** La revisión del cumplimiento de la finalidad del tratamiento de los datos personales ha sido incorporada como parte del alcance del proceso de auditoría interna.

ID.RA. Evaluación de riesgos

La organización comprende el riesgo de seguridad cibernética para la organización, los activos y los individuos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.RA-01. Se identifican, validan y registran las vulnerabilidades de los activos.	**SO.1-1:** El software de base y aplicaciones críticas se encuentran actualizados a versiones sin vulnerabilidades críticas. **SO.1-2:** Se tienen identificados aquellos activos que por su tecnología no pueden ser actualizados, detallando los controles compensatorios implementados.	**CN.3-2:** Se realizan pruebas de intrusión (ethical hacking) de los sistemas críticos de la organización en forma periódica o como parte de un cambio significativo en ellos, con recursos propios o con apoyo externo. **CN.3-3:** El resultado de las pruebas se comunica a las partes interesadas. **SO.1-3:** Está definido un plan documentado para la gestión de las vulnerabilidades y parches. **SO.1-5:** Las vulnerabilidades son evaluadas, clasificadas, y priorizadas según la criticidad identificada.	**CN.3-4:** Está establecido un procedimiento documentado para la revisión periódica interna de vulnerabilidades con alcance a los sistemas base y de aplicación. **CN.3-5:** En los sistemas críticos se realizan los escaneos de vulnerabilidades con un periodo entre ellos de máximo 6 meses y pruebas de intrusión con un periodo entre ellas de máximo un año. **SO.1-6:** Existe un procedimiento documentado de gestión de vulnerabilidades y parches. **SO.1-7:** Están establecidas las responsabilidades de gestión de vulnerabilidades. **SO.1-8:** Los escaneos de vulnerabilidades se realizan como mínimo semestralmente.	**CN.3-9:** El procedimiento de revisión de vulnerabilidades se encuentra incorporado en las actividades de seguridad de la información. **SO.1-9:** Se realizan revisiones de control interno sobre el plan de gestión de vulnerabilidades. **SO.1-10:** El resultado de las revisiones se comunica al RSI. **SO.1-11:** Se documentan las lecciones aprendidas, que aportan a la mejora de futuras resoluciones frente a vulnerabilidades similares.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.RA-02. Se recibe información sobre ciberamenazas de foros y fuentes de intercambio de información.	**GR.4-1:** La organización ha identificado y documentado sus fuentes confiables de inteligencia de amenazas, incluyendo al menos CERTuy y fuentes oficiales, comunitarias o sectoriales.	**GR.4-6:** La inteligencia de amenazas se utiliza como insumo para el análisis de riesgos de seguridad de la información.	**GR.4-8:** La información de inteligencia de amenazas se utiliza para ajustar o redefinir los controles existentes y apoyar el diseño de nuevos controles para los planes de tratamiento de riesgos.	**GR.4-10:** La organización actualiza sus análisis de riesgos en función de la nueva información derivada del análisis de la inteligencia de amenazas.
ID.RA-03. Se identifican y registran las amenazas internas y externas a la organización.	**GR.4-1:** La organización ha identificado y documentado sus fuentes confiables de inteligencia de amenazas, incluyendo al menos CERTuy y fuentes oficiales, comunitarias o sectoriales. **GR.4-2:** El personal de seguridad recibe capacitación sobre el uso de inteligencia de amenazas. **GR.4-3:** La organización recibe periódicamente información de amenazas a través de sus fuentes confiables, la misma se registra para su posterior análisis.	**GR.4-4:** Están asignados los responsables de recibir, filtrar y analizar la inteligencia de amenazas.	**GR.4-7:** Se cuenta con un procedimiento documentado sobre el uso de inteligencia de amenazas, abarcando como se recibe, filtra, analiza, clasifica y utiliza la información.	**GR.4-9:** Se revisa periódicamente las fuentes confiables de inteligencia identificadas para validar su vigencia.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.RA-04. Se identifican y registran los impactos potenciales y las probabilidades de que las amenazas exploten las vulnerabilidades	**GR.2-1:** Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia.	**GR.2-2:** Las amenazas, vulnerabilidades y controles existentes en la organización están documentados. **GR.2-3:** Se cuenta con un inventario de riesgos de seguridad de la información que incluye riesgos asociados a todos los activos de información (se incluyen riesgos positivos). **GR.4-5:** Se realiza un análisis del impacto potencial de las amenazas emergentes sobre la organización.	**GR.2-6:** Los incidentes de seguridad de la información y ciberseguridad son tenidos en cuenta para la evaluación de riesgos.	**GR.2-8:** Los riesgos se revisan periódicamente, la revisión se documenta formalmente.
ID.RA-05. Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para comprender el riesgo inherente e informar sobre la priorización de la respuesta al riesgo.	**GR.2-1:** Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia.	**GR.2-2:** Las amenazas, vulnerabilidades y controles existentes en la organización están documentados. **GR.4-5:** Se realiza un análisis del impacto potencial de las amenazas emergentes sobre la organización.	**GR.3-7:** La efectividad de los controles implementados es evaluada, y el riesgo residual resultante es documentado y validado por las partes interesadas.	**GR.3-9:** Los planes de tratamiento de los riesgos se revisan periódicamente y se actualizan si es necesario.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.RA-06. Se eligen, priorizan, planifican, controlan y comunican las respuestas al riesgo.	**GR.3-1:** Se toman acciones ad-hoc con el objetivo de llevar los principales riesgos de seguridad de la información a niveles aceptables para la organización.	**GR.3-2:** Se elaboran planes de tratamiento para los riesgos de seguridad de la información que excedan los niveles de tolerancia definidos por la organización. **GR.3-3:** Cada plan de tratamiento identifica las acciones necesarias, el responsable de su ejecución y el plazo previsto.	**GR.3-4:** Los planes de tratamiento son revisados y validados por los responsables de ejecutarlos antes de su ejecución. **GR.3-5:** Los planes de tratamiento de riesgos incluyen métricas e indicadores que permiten evaluar su avance. **GR.3-6:** La implementación de los controles debe realizarse conforme a la prioridad explícita y formalmente establecida por la Dirección. **GR.3-7:** La efectividad de los controles implementados es evaluada, y el riesgo residual resultante es documentado y validado por las partes interesadas.	**GR.3-9:** Los planes de tratamiento de los riesgos se revisan periódicamente y se actualizan si es necesario. **GR.3-10:** La revisión se documenta formalmente y es comunicada al CSI y a las otras partes interesadas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.RA-07. Se gestionan los cambios y las excepciones, se evalúa su impacto en el riesgo, se registran y se realiza su seguimiento.	**GR.2-1:** Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia. **SO.2-1:** Se han establecido mecanismos para comunicar los cambios en el ámbito tecnológico a las partes interesadas. **SO.2-2:** Los cambios tecnológicos son previamente autorizados por los responsables de los activos.	**GR.2-2:** Las amenazas, vulnerabilidades y controles existentes en la organización están documentados. **GR.2-3:** Se cuenta con un inventario de riesgos de seguridad de la información que incluye riesgos asociados a todos los activos de información (se incluyen riesgos positivos). **SO.2-4:** Los cambios de configuración sobre infraestructura crítica requieren validación previa mediante pruebas en ambientes controlados.	**SO.2-5:** Está definida una política de gestión de cambios, la misma contempla los cambios de emergencia en el ámbito tecnológico. **SO.2-6:** Está establecido y documentado un procedimiento para la gestión de los cambios. **SO.2-7:** Los cambios se registran y se les asocia una justificación y responsable.	**GR.2-8:** Los riesgos se revisan periódicamente, la revisión se documenta formalmente. **SO.2-8:** Se cuenta con herramientas para dar soporte a la gestión de los cambios. **SO.2-9:** Se realizan actividades de control interno para revisar el cumplimiento de los procedimientos relacionados a gestión de cambios. **SO.2-10:** El resultado de estas actividades es comunicado al RSI y demás partes interesadas. **SO.2-11:** Se toman medidas correctivas ante desvíos.
ID.RA-08. Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades,	**SO.1-1:** El software de base y aplicaciones críticas se encuentran actualizados a versiones sin vulnerabilidades críticas. **SO.1-2:** Se tienen identificados aquellos activos que por su tecnología no pueden ser actualizados, detallando los controles compensatorios implementados.	**SO.1-3:** Está definido un plan documentado para la gestión de las vulnerabilidades y parches. **SO.1-4:** Se reciben notificaciones de vulnerabilidades por parte del CERTuy u otras organizaciones y se analizan. **SO.1-5:** Las vulnerabilidades son evaluadas, clasificadas, y priorizadas según la criticidad identificada.	**SO.1-6:** Existe un procedimiento documentado de gestión de vulnerabilidades y parches. **SO.1-7:** Están establecidas las responsabilidades de gestión de vulnerabilidades. **SO.1-8:** Los escaneos de vulnerabilidades se realizan como mínimo semestralmente.	**SO.1-9:** Se realizan revisiones de control interno sobre el plan de gestión de vulnerabilidades.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.RA-09. Se evalúa la autenticidad e integridad del hardware y software antes de su adquisición y uso.	**SF.4-2:** Al recibir equipos nuevos se inspeccionan, y documenta el estado de los sellos o empaques de fábrica, registrando cualquier indicio de apertura o daño.	**SF.4-4:** Se instalan sellos o cintas de seguridad con código único en los puntos de acceso al interior de los chasis, de manera que cualquier manipulación quede registrada.	**SF.4-7:** Esta formalmente definida una política de seguridad del equipamiento que establece lineamientos para la protección física, manejo cuando esté los equipos estén sin supervisión, entre otros puntos. **SF.4-8:** Existe un procedimiento documentado de respuesta a eventos de manipulación detectada, que incluye la investigación inicial y evaluación de posibles compromisos de integridad.	**SF.4-10:** Se cuenta con un proceso de control interno para verificar el cumplimiento de los procedimientos de seguridad del equipamiento y documentar hallazgos. **SF.4-11:** Se realiza una revisión periódica de los procedimientos y de las medidas de seguridad implementadas en el equipamiento, incorporando ajustes derivados de incidentes, no conformidades y oportunidades de mejora.
ID.RA-10. Se evalúan los proveedores críticos antes de su adquisición.	**AD.2-2:** Los requisitos de seguridad de la información se incluyen en las solicitudes y evaluaciones de compra.	**AD.2-3:** Se evalúa la capacidad de los proveedores para cumplir con los requisitos de seguridad antes de la contratación.	**RP.2-4:** Se documentan los resultados de las evaluaciones de desempeño y cumplimiento de requisitos de seguridad de los proveedores.	**RP.2-7:** La gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio. **RP.2-8:** Las evaluaciones son tomadas en cuenta para las actualizaciones de contratos y las futuras adquisiciones.

ID.IM Mejora

Se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos de ciberseguridad de la organización en todas las funciones del Marco.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.IM-01. Las mejoras se identifican a partir de evaluaciones.	**CN.2-1:** Se han realizado análisis de brechas para detectar el nivel de cumplimiento del presente marco. **CN.2-2:** En función de las brechas detectadas se elabora un portafolio de proyectos a incluir en el plan de seguridad de la información. **PD.7-1:** La organización ha definido criterios para incorporar medidas de privacidad por diseño y por defecto en la construcción o mejora de procesos, servicios o sistemas.	**CN.2-3:** Se realiza anualmente una auditoría interna sobre el cumplimiento del presente marco. **PD.7-2:** El delegado de protección de datos personales asesora en el diseño e implementación de medidas técnicas y organizativas destinadas a incorporar los principios de privacidad por diseño y por defecto en la organización.	**CN.2-4:** Se realiza con una periodicidad predefinida una auditoría externa sobre el cumplimiento del presente marco. **CN.2-5:** Los hallazgos de auditorías generan planes de acción documentados y se realiza su seguimiento. **PD.7-3:** Ante cambios en procesos, sistemas o incidentes de seguridad, se revisa de forma reactiva la efectividad de las medidas implementadas para garantizar la incorporación de los principios de privacidad por diseño y por defecto en la organización.	**CN.2-6:** Se evalúa periódicamente la calidad y alcance de las auditorías realizadas, incorporando lecciones aprendidas para futuras ejecuciones. **CN.2-7:** Las auditorías incluyen en su alcance la revisión completa del sistema de gestión de seguridad de la información y sus objetivos, políticas y controles definidos. **PD.7-4:** Se revisa periódicamente la efectividad de las medidas destinadas a incorporar los principios de privacidad por diseño y por defecto en la organización. **PD.7-5:** Las revisiones dan lugar a ajustes de las medidas técnicas implementadas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.IM-02. Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, lo que incluye a los realizados en coordinación con proveedores y terceros pertinentes.	**CN.3-1:** Se realizan revisiones puntuales de los sistemas de información con recursos propios o con apoyo externo. **GI.6-1:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en el centro de procesamiento de datos.	**GI.6-2:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en toda la organización.	**CN.3-6:** Se cuenta con el apoyo de revisiones externas de vulnerabilidades y hackeo ético. **GI.6-5:** Las lecciones aprendidas se contemplan para mejorar los planes de respuesta a incidentes. **GI.6-6:** Las lecciones aprendidas son utilizadas para mejorar los canales de comunicación establecidos con las partes involucradas y los procesos de escalamiento.	**CN.3-7:** Los resultados de las revisiones internas y externas se utilizan para la mejora continua de la seguridad de los sistemas. **CN.3-8:** Se realizan actividades de control interno para verificar el cumplimiento con el procedimiento de revisión periódica de vulnerabilidades.
ID.IM-03. Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativos.	**CN.3-1:** Se realizan revisiones puntuales de los sistemas de información con recursos propios o con apoyo externo. **GI.6-1:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en el centro de procesamiento de datos.	**GI.6-2:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en toda la organización.	**CN.3-6:** Se cuenta con el apoyo de revisiones externas de vulnerabilidades y hackeo ético. **GI.6-5:** Las lecciones aprendidas se contemplan para mejorar los planes de respuesta a incidentes. **GI.6-6:** Las lecciones aprendidas son utilizadas para mejorar los canales de comunicación establecidos con las partes involucradas y los procesos de escalamiento.	**CN.3-7:** Los resultados de las revisiones internas y externas se utilizan para la mejora continua de la seguridad de los sistemas. **CN.3-8:** Se realizan actividades de control interno para verificar el cumplimiento con el procedimiento de revisión periódica de vulnerabilidades.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.IM-04. Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de ciberseguridad que afectan a las operaciones.	**CN.3-1:** Se realizan revisiones puntuales de los sistemas de información con recursos propios o con apoyo externo. **GI.6-1:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en el centro de procesamiento de datos.	**GI.6-2:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en toda la organización.	**CN.3-6:** Se cuenta con el apoyo de revisiones externas de vulnerabilidades y hackeo ético. **GI.6-5:** Las lecciones aprendidas se contemplan para mejorar los planes de respuesta a incidentes. **GI.6-6:** Las lecciones aprendidas son utilizadas para mejorar los canales de comunicación establecidos con las partes involucradas y los procesos de escalamiento.	**CN.3-7:** Los resultados de las revisiones internas y externas se utilizan para la mejora continua de la seguridad de los sistemas. **CN.3-8:** Se realizan actividades de control interno para verificar el cumplimiento con el procedimiento de revisión periódica de vulnerabilidades.

5.3 Función: Proteger (PR)

PR.AA Gestión de identidades, autenticación y control de acceso

El acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.AA-01. La organización gestiona las identidades y credenciales de los usuarios, servicios y equipos autorizados.	**CA.5-1:** Están implementados controles que impiden que un mismo usuario solicite, apruebe y asigne accesos en los sistemas críticos. **CA.5-2:** La asignación de privilegios es ejecutada por un responsable distinto al que la aprueba. **CA.6-1:** Los derechos de acceso son autorizados.	**CA.5-3:** Se aplican mecanismos preventivos para evitar su asignación conjunta, salvo justificación formal y aprobación excepcional de roles en conflicto. **CA.5-4:** Está limitada la cantidad de usuarios con privilegios administrativos, siguiendo criterios establecidos. **CA.5-5:** La segregación de funciones abarca también los diferentes entornos de la organización, evitando que una persona realice actividades en más de un entorno al menos de que esté debidamente justificado y documentado. **CA.5-6:** El personal de administración de accesos no es el mismo que el que realiza la auditoría sobre dichos accesos.	**CA.5-7:** Están identificados, documentados y gestionados los posibles conflictos entre roles o combinaciones de privilegios. **CA.5-8:** Están definidos y documentados los criterios para autorizar privilegios administrativos. **CA.5-9:** Están definidos y documentados los criterios para determinar cuántos usuarios con privilegios de administrador deben existir por sistema o entorno. **CA.5-10:** La segregación de funciones está incluida en el procedimiento formal de control de acceso lógico. **CA.6-5:** Se define un procedimiento de acceso lógico a redes, recursos y sistemas de información.	**CA.5-11:** Se audita periódicamente el cumplimiento del procedimiento de segregación de funciones. **CA.5-12:** En caso de identificarse desviaciones se documentan, y se realizan acciones correctivas con responsables asignados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
		CA.6-2: El uso de dispositivos externos requiere identificación (inventariado y responsable) y autentificación (permiso de acceso por el rol del usuario o algún otro método). **CA.6-3:** Se aplica el principio de menor privilegio para la asignación de permisos.	**CA.6-6:** Se define una política de acceso lógico a redes, recursos y sistemas de información.	
PR.AA-02. Las identidades están comprobadas y vinculadas a credenciales basadas en el contexto de las interacciones.	**CA.1-2:** El acceso a la red y los sistemas debe realizarse con usuarios nominados. **CA.1-3:** El uso de usuarios privilegiados se encuentra controlado. **CA.1-5:** El uso de usuarios genéricos debe estar fundamentado y autorizado por excepción.	**CA.1-6:** Existen pautas definidas para la realización de altas, bajas y modificaciones de acceso lógico que además incluyen aprobaciones.	**CA.1-10:** Se cuenta con un procedimiento para el ABM de usuarios. **CA.1-11:** La gestión de identidades y credenciales se realiza en forma centralizada, al menos en forma administrativa. **SF.1-10:** Las aplicaciones que manejan información sensible requieren reautenticación periódica, especialmente cuando se accede desde ubicaciones de alto riesgo.	**CA.1-14:** La política y procedimientos son revisados periódicamente.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.AA-03. Los usuarios, servicios y hardware están autenticados.	**CA.1-1:** Todos los sistemas requieren autenticación. **CA.1-4:** Los accesos remotos a aplicaciones se realizan utilizando mecanismos de autenticación seguros.	**CA.1-7:** Se identifican los casos que requieren autenticación fuerte y se determinan los controles requeridos. **CA.1-8:** Las credenciales de autenticación (contraseñas, certificados, tokens) están protegidas en reposo y en tránsito mediante mecanismos criptográficos robustos. **OR.6-4:** Se implementa el múltiple factor de autenticación para el acceso remoto.	**CA.1-9:** Se define una política de gestión de usuarios y contraseñas, y se instruye al personal para su uso correcto. **CA.1-12:** Los tokens o credenciales utilizadas para el acceso (por ejemplo, SAML assertions, JWTs) se validan en cada acceso y su integridad es verificada.	**CA.1-13:** Se establecen procesos de revisiones y auditorías continuas para verificar que las redes, sistemas, recursos y dispositivos están funcionando con la autenticación y configuración requerida y acordada por la organización.
PR.AA-04. Las afirmaciones de identidad se protegen, transmiten y verifican.	**CA.1-4:** Los accesos a aplicaciones se realizan utilizando mecanismos de autenticación seguros.	**CA.1-7:** Se identifican los casos que requieren autenticación fuerte y se determinan los controles requeridos. **CA.1-8:** Las credenciales de autenticación (contraseñas, certificados, tokens) están protegidas en reposo y en tránsito mediante mecanismos criptográficos robustos.	**CA.1-12:** Los tokens o credenciales utilizadas para el acceso (por ejemplo, SAML assertions, JWTs) se validan en cada acceso y su integridad es verificada.	**CA.1-13:** Se establecen procesos de revisiones y auditorías continuas para verificar que las redes, sistemas, recursos y dispositivos están funcionando con la autenticación y configuración requerida y acordada por la organización.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.AA-05. Los permisos de acceso, los derechos y las autorizaciones se definen en una política, se gestionan, se aplican y se revisan, e incorporan los principios de privilegio mínimo y separación de funciones.	**CA.2-1:** La revisión de privilegios se realiza en forma reactiva frente a un cambio o baja, al menos para los sistemas críticos. **CA.6-1:** Los derechos de acceso son autorizados. **PD.5-1:** Se han restringido los accesos a los datos personales mediante usuarios nominados y aplicando el principio de mínimo privilegio.	**CA.2-2:** Está establecida la periodicidad con la que se realizan las revisiones de los privilegios y la validez de las cuentas asociadas. **CA.2-3:** Están definidos los responsables de la revisión de privilegios y de la validez de las cuentas en cada sistema. **CA.2-4:** Se mantiene un inventario de usuarios con permisos y privilegios elevados, validando también la vigencia de las cuentas. **CA.6-3:** Se aplica el principio de menor privilegio para la asignación de permisos. **CA.6-4:** Las autorizaciones de derechos de acceso son registradas. **SC.12-5:** Se revisan periódicamente los registros de acceso para verificar que no existan conexiones desde servicios de Webmail externos no autorizados.	**CA.2-5:** Existe una política de control de acceso lógico donde se estipula la revisión de privilegios periódicamente a todos los usuarios y en todos los sistemas. **CA.2-6:** Existen y se aplican procedimientos formales de revisión de permisos que abarcan todo el ciclo de vida (alta, baja y modificación) de los usuarios, incluyendo los privilegiados. **CA.2-7:** Se realizan revisiones de los derechos de acceso de los usuarios y se cuenta con registro de tales acciones. **CA.2-8:** Se documentan los resultados de cada revisión y se comunican al RSI, a las gerencias y demás partes interesadas. **CA.6-8:** La política de acceso lógico incluye el uso de usuarios privilegiados.	**CA.2-9:** El resultado de las revisiones se comunica formalmente a las gerencias y otras partes interesadas. **CA.2-10:** Se realizan auditorías internas sobre el cumplimiento del procedimiento de revisión de privilegios y la política de control de acceso lógico, en específico de su apartado de revisiones periódicas. **OR.6-11:** Se realizan revisiones periódicas de los usuarios con acceso remoto. **OR.6-12:** El resultado de las revisiones retroalimenta la gestión del acceso remoto y proporciona información para la toma de decisiones de mejora continua.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
			CA.6-9: El acceso a los activos de información identificados como críticos debe requerir autenticación con múltiple factor (MFA). **OR.6-9:** Los proveedores tienen permisos de acceso remoto que caducan luego de realizada la actividad (o de una fecha establecida) para la cual se les otorgó el acceso.	
PR.AA-06. El acceso físico a los activos se gestiona, supervisa y aplica de forma proporcional al riesgo.	**SF.1-1:** Están identificadas las áreas que requieren control de acceso físico. **SF.1-2:** Están implementados los controles de acceso físico a las instalaciones de los centros de procesamiento de datos.	**SF.1-4:** Están establecidos perímetros de seguridad en el centro de procesamiento de datos y las áreas seguras. **SF.1-5:** Están implementados controles de acceso físico para otras áreas definidas como seguras.	**SF.1-8:** Existe una política de control de acceso físico formalmente aprobada. **SF.1-9:** Se revisan de forma reactiva los registros de acceso a las diferentes áreas.	**SF.1-11:** Está establecido un procedimiento de revisión periódica de los accesos al centro de procesamiento de datos y a las áreas seguras.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	SF.1-3: Se gestionan (evalúan, autorizan y registran) las autorizaciones de acceso al centro de procesamiento de datos. **SF.4-1:** Todos los dispositivos con información sensible disponen de barreras físicas que impiden su extracción o manipulación no autorizada (cerraduras, tapas de seguridad, sensores de apertura, etc.).	**SF.1-6:** Se gestionan (evalúan, autorizan y registran) las autorizaciones de acceso a las áreas definidas como seguras. **SF.1-7:** Se lleva un registro de accesos físicos al centro de procesamiento de datos y áreas seguras. **SF.4-3:** Se deshabilitan los puertos no utilizados (USB, serie, módulos de expansión, etc.) en los dispositivos del centro de procesamiento de datos.	**SF.4-9:** Existe un procedimiento documentado para la seguridad del equipamiento, que describa las configuraciones preventivas y las acciones de respuesta ante incidentes o situaciones de riesgo, incluyendo escenarios como la detección de equipos sin supervisión.	**SF.1-12:** Se realizan actividades de control interno para verificar el cumplimiento de los procedimientos establecidos. **SF.1-13:** Se aplican controles de tiempo de conexión y condiciones de acceso desde ubicaciones públicas o externas a la organización.

PR.AT. Concientización y capacitación

Se proporciona al personal de la organización concienciación y capacitación en ciberseguridad para que puedan realizar sus tareas relacionadas con la ciberseguridad.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.AT-01. Se sensibiliza y capacita al personal para que disponga de los conocimientos y habilidades necesarios para realizar tareas generales teniendo en cuenta los riesgos de ciberseguridad.	**GH.2-1:** Se realizan actividades propias de difusión de información relacionada con seguridad de la información, como la difusión de las políticas y mecanismos de protección.	**GH.2-2:** Se elaboran campañas de concientización y/o formación para el personal.	**GH.2-3:** Las campañas de concientización son aprobadas y se les definen los indicadores de cumplimiento. **GH.2-4:** Se planifica un cronograma para la realización de las campañas. **GH.2-5:** Se define un plan de capacitación y entrenamiento en seguridad de la información para todo el personal. **GH.2-6:** Se elabora y/o obtiene el material educativo necesario para la realización de las campañas de concientización.	**GH.2-7:** Se realizan revisiones periódicas de los indicadores de las campañas para verificar su efectividad. **GH.2-8:** Se evalúa el nivel de conocimiento adquirido por el personal mediante actividades de evaluación periódicas. **GH.2-9:** Las actividades son aprobadas por el CSI y apoyadas por la Dirección. **GH.2-10:** El plan es revisado y actualizado periódicamente y se realizan acciones de mejora incorporando lecciones aprendidas. **GH.2-11:** Se realizan acciones de mejora a los planes incorporando lecciones aprendidas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.AT-02. Se sensibiliza y capacita a las personas que desempeñan funciones especializadas para que posean los conocimientos y aptitudes necesarios para realizarlas tareas pertinentes teniendo en cuenta los riesgos de ciberseguridad.	**GH.3-1:** Los usuarios privilegiados demuestran conocimiento respecto a la importancia de sus roles y responsabilidades. **GH.3-2:** El personal de seguridad física y de seguridad de la información demuestra concientización respecto a la importancia de sus roles y responsabilidades. **GH.3-3:** Están definidos los roles y responsabilidades de los interesados externos.	**GH.3-4:** Se realizan actividades de concientización específicas para usuarios privilegiados con cierta periodicidad. **GH.3-5:** Se realizan con cierta periodicidad actividades de concientización para el personal de seguridad física y seguridad de la información. **GH.3-6:** Se realizan actividades de concientización para interesados externos. **GH.3-7:** La alta gerencia participa de las actividades de concientización.	**GH.3-8:** Los usuarios privilegiados son capacitados a través de cursos o talleres relevantes adicionales. **GH.3-9:** El personal de seguridad física y seguridad de la información es capacitado a través de cursos o talleres relevantes adicionales. **GH.3-10:** Se realizan acciones para asegurar que los interesados externos comprendan sus roles y responsabilidades en materia de seguridad de la información. **SC.12-8:** Los titulares de cuentas institucionales reciben instrucciones y capacitación sobre el uso seguro del Webmail y la prohibición de acceso desde servicios externos.	**GH.3-11:** El plan de capacitación y entrenamiento en seguridad de la información tiene en cuenta los perfiles e intereses de grupos considerados estratégicos.

PR.DS. Seguridad de los datos

Los datos se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.DS-01. La confidencialidad, la integridad y la disponibilidad de los datos en reposo están protegidas.	**CA.3-1:** Se identifican los datos históricos y respaldos que deben ser protegidos mediante mecanismos seguros. **CA.4-1:** La organización identifica los sistemas y procesos que requieren firma electrónica avanzada. **CA.4-2:** Los sistemas con firma electrónica utilizados por la organización soportan el uso de certificados electrónicos X.509v3 emitidos por prestadores acreditados ante la UCE.	**CA.3-2:** Los respaldos y/o datos históricos fuera de línea se almacenan en forma cifrada. **CA.4-6:** La solución incorpora medidas de detección de firmas alteradas o invalidadas, incluyendo trazabilidad del error. **GA.4-3:** Se encuentran elaboradas y difundidas las pautas para el uso seguro de los medios de almacenamiento externos.	**CA.3-3:** Se documentan los mecanismos criptográficos implementados. **CA.3-4:** Está definida una política de uso de controles criptográficos. **CA.3-5:** Se determinan los responsables de la generación de las claves que abarca todo su ciclo de vida. **CA.4-7:** La organización documenta un procedimiento técnico y funcional para la implementación de firma electrónica avanzada.	**CA.3-6:** Se realizan revisiones periódicas sobre los controles criptográficos utilizados para asegurar la protección de los datos. **CA.3-7:** Los resultados de estas revisiones son registrados e informados al RSI. **GA.4-7:** Se realizan revisiones de control interno sobre el cumplimiento de las pautas de uso de medios extraíbles, de la política y el procedimiento.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	CA.4-3: Se utilizan protocolos seguros y actualizados, evitando tecnologías criptográficas obsoletas o vulnerables. **GA.4-1:** Se realiza difusión sobre la importancia de la protección y uso seguro de los medios extraíbles. **PD.5-2:** Se han implementado medidas para restringir el acceso no autorizado a documentos físicos que contienen datos personales. **PD.6-1:** El acceso a datos personales está limitado únicamente a las personas que realizan tareas directamente asociadas con la finalidad específica para la cual dichos datos fueron recabados.	**PD.5-3:** Se implementan medidas técnicas y organizativas necesarias para preservar la integridad, confidencialidad y disponibilidad de la información, garantizando así la seguridad de los datos personales.	**GA.4-5:** Están definidas acciones específicas en caso de hurto, pérdida o daño del medio, y se difunde el procedimiento a todos los interesados. **GA.4-6:** Se encuentra establecida formalmente la política y el procedimiento de gestión de medios de almacenamiento externos. **PD.5-5:** Se mantienen registros que permiten auditar el acceso a datos personales sensibles. Dichos registros permiten identificar quién accedió, en qué momento y a qué tipo de información.	**GA.4-8:** Los resultados de las revisiones son utilizados para la mejora de la política y el procedimiento, se comunican al RSI y demás partes interesadas. **PD.5-8:** Se realizan simulaciones para verificar la eficacia de las medidas de seguridad aplicadas a los datos personales, incluyendo escenarios de incidentes o accesos indebidos. **PD.5-9:** La Dirección revisa periódicamente el tratamiento de los riesgos sobre datos personales y aprueba medidas estratégicas para reforzar su protección. **PD.6-7:** Toda solicitud interna de acceso a datos personales debe indicar la finalidad específica de uso y ser aprobada por los responsables designados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.DS-02. La confidencialidad, la integridad y la disponibilidad de los datos en tránsito están protegidas.	**CA.4-1:** La organización identifica los sistemas y procesos que requieren firma electrónica avanzada. **CA.4-2:** Los sistemas con firma electrónica utilizados por la organización soportan el uso de certificados electrónicos X.509v3 emitidos por prestadores acreditados ante la UCE. **CA.4-4:** Deben utilizarse los estándares de codificación de firmas propios de los tipos de documentos firmados (XADES, PDFSignature, etc.). **CA.4-5:** Se debe hacer la validación de certificados a través de OCSP (Online Certificate Status Protocol), CRL (Certificate Revocation List) o equivalente.	**CA.4-6:** La solución incorpora medidas de detección de firmas alteradas o invalidadas, incluyendo trazabilidad del error. **OR.6-4:** Se implementa el múltiple factor de autenticación para el acceso remoto. **PD.5-3:** Se implementan medidas técnicas y organizativas necesarias para preservar la integridad, confidencialidad y disponibilidad de la información, garantizando así la seguridad de los datos personales. **SC.6-4:** Todos los proveedores que deban acceder a información confidencial de la organización deben tener firmado un acuerdo de no divulgación.	**CA.3-3:** Se documentan los mecanismos criptográficos implementados. **CA.3-4:** Está definida una política de uso de controles criptográficos. **CA.3-5:** Se determinan los responsables de la generación de las claves que abarca todo su ciclo de vida. **CA.4-7:** La organización documenta un procedimiento técnico y funcional para la implementación de firma electrónica avanzada. **CA.4-8:** Los sistemas deben soportar el uso de dispositivos criptográficos dedicados en todos los casos de uso de todos los prestadores de Firma Electrónica Avanzada acreditados por la UCE.	**CA.4-10:** Los sistemas deben permitir el uso de sellos de tiempo compatibles con RFC 3161. **CA.4-11:** Se realizan auditorías de los módulos de firma electrónica, incluyendo pruebas de cumplimiento de formatos, protocolos, protección de claves y servicios de sellado de tiempo. **CA.4-12:** Los resultados de las auditorías o revisiones son analizados e incorporados a la mejora de la solución y comunicados al RSI. **PD.5-8:** Se realizan simulaciones para verificar la eficacia de las medidas de seguridad aplicadas a los datos personales, incluyendo escenarios de incidentes o accesos indebidos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	PD.6-1: El acceso a datos personales está limitado únicamente a las personas que realizan tareas directamente asociadas con la finalidad específica para la cual dichos datos fueron recabados. **SC.12-1:** El servicio de Webmail de la organización se implementa exclusivamente sobre el protocolo HTTPS. **SC.12-3:** Los certificados digitales utilizados para el servicio de Webmail son válidos, vigentes y emitidos por una Autoridad Certificadora de confianza. **SC.14-1:** Se implementan controles criptográficos para proteger los datos en tránsito.	**SC.12-4:** Las configuraciones del servicio de Webmail bloquean el uso de protocolos inseguros o versiones obsoletas de TLS/SSL. **SC.14-2:** Los datos en tránsito de todas las aplicaciones y sistemas se encuentran protegidos mediante un mismo conjunto reducido de tecnologías y prácticas criptográficas.	**CA.4-9:** La firma digital está embebida en todos los procesos de la organización que la requieren, de modo que los usuarios pueden firmar o validar firmas en el contexto de cada sistema. **OR.6-7:** Existe un responsable para la asignación de permisos de acceso remoto. **OR.6-8:** Esta definida una política de control de acceso remoto. **SC.12-7:** Cuando corresponda según la clasificación de la información transmitida vía email, se utiliza cifrado a nivel de mensaje (por ejemplo, S/MIME o PGP, etc). **SC.14-3:** La organización cuenta con procedimientos documentados para la transferencia segura de información física y electrónica.	**PD.5-9:** La Dirección revisa periódicamente el tratamiento de los riesgos sobre datos personales y aprueba medidas estratégicas para reforzar su protección. **SC.12-10:** Se realizan pruebas técnicas para validar el cifrado de las comunicaciones y la correcta configuración de seguridad del servicio de Webmail. **SC.14-6:** Se realizan revisiones periódicas sobre los controles criptográficos utilizados para asegurar la protección de los datos que son enviados y recibidos por los diferentes sistemas y aplicaciones.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
			SC.14-4: Los procedimientos para la transferencia de información establecen medidas de seguridad diferenciadas según el nivel de sensibilidad de los datos involucrados. **SC.14-5:** Se realizan acuerdos formales con terceras partes que establecen responsabilidades y medidas de seguridad para la transferencia de información.	
PR.DS-10. L La confidencialidad, la integridad y la disponibilidad de los datos en uso están protegidas.	**GA.3-1:** Existen pautas del uso aceptable de los activos de la información. **GA.3-2:** Toda persona que acceda a activos de información debe aceptar formalmente, previo al acceso, las condiciones de uso establecidas por la organización.	**GA.3-3:** Se debe restringir el almacenamiento de información sensible en activos que no cuenten con controles adecuados; en caso de ser necesario, se deben aplicar mecanismos de protección como cifrado o control de acceso con MFA.	**GA.3-5:** Está definida formalmente la política sobre el uso adecuado de los activos de la información de la organización. **GA.3-7:** Se realiza un control periódico de los activos que contienen o procesan información sensible.	**GA.3-9:** Las medidas de protección implementadas en los activos informáticos se monitorean de forma proactiva 7x24. **GA.3-10:** Se realizan evaluaciones periódicas para verificar que el uso de los activos se ajusta a las condiciones establecidas en la política.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	SC.12-2: El acceso al Webmail institucional está restringido únicamente al servicio provisto por la organización, prohibiendo el acceso a cuentas institucionales desde Webmail externos.	**OR.5-5:** Los dispositivos de la organización cumplen con requisitos de seguridad como: antivirus, cifrado de disco, bloqueo, versión mínima de sistema operativo. **SF.4-5:** Los dispositivos de usuario final están configurados para bloquear automáticamente la sesión tras un máximo de 15 minutos, o menos, de inactividad. **SF.4-6:** Se implementa el cierre automático de sesión después de 30 minutos sin actividad, o menos, en los dispositivos de usuario final.		**SC.12-9:** Se realizan auditorías periódicas para verificar el cumplimiento de las restricciones de acceso y la vigencia de los certificados digitales.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.DS-11. Se crean, protegen, mantienen y comprueban copias de seguridad de los datos.	**CA.3-1:** Se identifican los datos históricos y respaldos que deben ser protegidos mediante mecanismos seguros. **SO.6-1:** Se realizan respaldos periódicos de al menos los activos de información del centro de datos (aplicaciones, bases de datos, máquinas virtuales, etc.).	**CA.3-2:** Los respaldos y/o datos históricos fuera de línea se almacenan en forma cifrada. **SO.6-2:** Los respaldos se almacenan en lugares seguros y con acceso restringido. **SO.6-3:** Se establece el grado (completo, diferencial, etc.) y los requisitos de retención de los respaldos. **SO.6-4:** Los respaldos son probados regularmente. **SO.6-5:** Los respaldos se almacenan en medios inmutables o fuera de línea, para evitar posibles compromisos de ransomware.	**CA.3-3:** Se documentan los mecanismos criptográficos implementados. **SO.6-6:** Se cuenta con soluciones automatizadas para asistir en la realización de los respaldos. **SO.6-7:** Existe una política de respaldos. **SO.6-8:** Existen procedimientos documentados de realización y prueba de recuperación de respaldos.	**SO.6-9:** El procedimiento de respaldos se actualiza ante cambios de requerimientos del negocio o cambios de infraestructura o sistemas que requieran acciones de respaldo. **SO.6-10:** La política y el procedimiento de respaldo se encuentran alineados al plan de contingencia y al plan de recuperación. **SO.6-11:** La política y procedimiento de respaldos se revisan regularmente.

PR.PS Seguridad de plataformas

El hardware, el software (por ejemplo, firmware, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales se gestionan de acuerdo con la estrategia de riesgos de la organización para proteger su confidencialidad, integridad y disponibilidad.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.PS-01. Se establecen y aplican prácticas de gestión de la configuración.	**OR.5-2:** Estos activos cuentan con al menos un factor de autenticación para acceder a la información. **OR.5-3:** Existen pautas que regulan el uso de los dispositivos móviles. **SO.2-1:** Se han establecido mecanismos para comunicar los cambios en el ámbito tecnológico a las partes interesadas. **SO.2-2:** Los cambios tecnológicos son previamente autorizados por los responsables de los activos.	**GA.3-4:** Se aplican restricciones técnicas o administrativas que limitan acciones no autorizadas sobre los activos, como la instalación de software no autorizado o el cambio de configuraciones críticas. **OR.5-4:** Las pautas de uso son comunicadas al personal y partes interesadas. **SO.2-3:** Se definen el versionado, las líneas base de configuración y los lineamientos de hardenizado de los productos de software. **SO.2-4:** Los cambios de configuración sobre infraestructura crítica requieren validación previa mediante pruebas en ambientes controlados.	**OR.5-8:** Existe una política formalmente aprobada de uso aceptable de dispositivos móviles. **SO.2-5:** Está definida una política de gestión de cambios, la misma contempla los cambios de emergencia en el ámbito tecnológico. **SO.2-6:** Está establecido y documentado un procedimiento para la gestión de los cambios. **SO.2-7:** Los cambios se registran y se les asocia una justificación y responsable.	**OR.5-9:** Se revisa y actualiza la política de uso de los dispositivos móviles periódicamente o ante cambios tecnológicos o normativos. **SO.2-8:** Se cuenta con herramientas para dar soporte a la gestión de los cambios. **SO.2-9:** Se realizan actividades de control interno para revisar el cumplimiento de los procedimientos relacionados a gestión de cambios.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.PS-02. Se mantiene, sustituye y elimina el software en función del riesgo.	**GR.2-1:** Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia.	**CN.4-2:** Se han definido responsables para la gestión del ciclo de vida del licenciamiento, incluyendo adquisición, asignación, renovación y baja. **GA.1-6:** Se debe llevar un control actualizado del licenciamiento del software instalado, incluyendo información sobre tipo de licencia, vigencia y uso asignado.	**GR.2-6:** Los incidentes de seguridad de la información y ciberseguridad son tenidos en cuenta para la evaluación de riesgos.	**CN.4-5:** Se realiza una revisión periódica del uso real de licencias adquiridas para detectar sobrelicenciamiento o subutilización. **CN.4-6:** Se realizan análisis periódicos del cumplimiento de los términos y condiciones de uso de las licencias adquiridas. **GA.1-13:** Se elimina el software y/o hardware que esté fuera de soporte o que represente un riesgo no aceptable.
PR.PS-03. Se mantiene, sustituye y elimina el hardware en función del riesgo.	**GA.5-1:** Están definidas las pautas para la disposición final y borrado seguro de medios de almacenamiento. **GA.5-2:** Está difundida la importancia de la eliminación de medios de almacenamientos que ya no serán utilizados. **GR.2-1:** Se identifican los principales riesgos de seguridad de la información, valorando su potencial impacto y su probabilidad de ocurrencia.	**GA.5-3:** Están definidos responsables o ubicaciones específicas para la eliminación segura de medios de almacenamiento. **GA.5-4:** Están establecidos los criterios para determinar cuándo corresponde la destrucción lógica y/o física de la información.	**GA.5-5:** Está definida formalmente una política de destrucción de la información. **GA.5-6:** Está definido formalmente un procedimiento de destrucción de la información. **GA.5-7:** Se registran las actividades de destrucción de la información, incluyendo fecha, tipo de medio, método aplicado y personal.	**GA.5-9:** Se realizan actividades de control interno para evaluar la correcta aplicación del procedimiento de destrucción. **SF.5-8:** Existe un proceso de control interno para verificar el cumplimiento del procedimiento de mantenimiento y la calidad de la documentación asociada.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	SF.5-1: Se gestiona y/o realiza el mantenimiento sobre los activos del centro de procesamiento de datos. **SF.5-2:** Se aprueba el alta y baja de los usuarios que realizan mantenimiento de forma remota a los activos informáticos del centro de procesamiento de datos.	**SF.5-3:** Se establecen planes de mantenimiento para las dependencias de los componentes críticos. **SF.5-4:** Se establecen los planes anuales de mantenimiento. **SF.5-5:** Se gestiona el acceso a los usuarios autorizados para realizar las tareas de mantenimiento programado.	**GA.5-8:** Se verifica la efectividad de los métodos de destrucción utilizados. **SF.5-6:** El RSI realiza la gestión de aprobación de los usuarios para conexión remota a los sistemas y activos de la organización, cumpliendo con el plan anual de mantenimiento. **SF.5-7:** Existe una política y/o procedimiento documentado de mantenimiento (criterios de prioridad, coordinación con operación, pruebas de validación y comunicación de resultados).	**SF.5-9:** Tras cualquier mantenimiento en el que se detecten desviaciones o incidentes, se elabora un registro formal de lecciones aprendidas que incluya la descripción de lo ocurrido, el análisis de causas, las acciones correctivas adoptadas y la actualización de los procedimientos afectados.
PR.PS-04. Se generan registros y se pongan a disposición para una supervisión continua.	**SO.7-1:** Están configurados los registros de auditoría y eventos para todos los sistemas definidos como críticos.	**SO.7-4:** Se cuenta con herramientas para la centralización de logs. **SO.7-5:** Los registros están protegidos contra accesos no autorizados y posibles alteraciones.	**SO.7-12:** Se tiene en cuenta los requisitos de confidencialidad de la información y protección de la privacidad de los datos contenidos en los registros.	**SO.7-21:** Se realizan actividades de control interno para verificar el cumplimiento con la política y los procedimientos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
		SO.7-10: Se establecen los requisitos de retención de los registros de auditoría. **SO.7-11:** Los relojes de todos los sistemas deben estar sincronizados (servidores, aplicaciones, etc.)	**SO.7-13:** Se define una política de auditoría y registro de eventos, como por ej. de los sistemas y redes y de configuración y uso de WAF. **SO.7-14:** Están establecidos procedimientos de auditoría y registro de eventos.	**SO.7-22:** El resultado de las revisiones se comunica al RSI y demás partes interesadas.
PR.PS-05. Se impide la instalación y la ejecución de software no autorizado.	**SO.8-1:** Están definidas las pautas para la instalación de software. **SO.8-2:** Las pautas de instalación de software fueron difundidas al personal.	**SO.8-3:** La posibilidad de instalar software en los equipos queda restringida a los usuarios que se encuentran autorizados para ese fin. **SO.8-4:** Se asegura una estricta segregación entre las utilidades del sistema y el software de aplicaciones, limitando el acceso a las utilidades del sistema.	**SO.8-5:** Existen listas de software autorizados, las que son revisadas y aprobadas por el RSI.	**SO.8-6:** Se realizan actividades de control interno sobre el software instalado con el fin de determinar el cumplimiento de la lista de software autorizado. **SO.8-7:** Los resultados de estas revisiones son enviados al RSI y demás partes interesadas.
PR.PS-06. Se integran prácticas seguras de desarrollo de software y se supervisa su rendimiento durante todo el ciclo de vida de desarrollo del software.	**AD.1-1:** Se utilizan lineamientos generales para el desarrollo de los sistemas incluyendo principios básicos de la gestión de proyectos.	**AD.1-2:** Se incorporan principios de desarrollo seguro en los proyectos de desarrollo de sistemas.	**AD.1-5:** Se define un procedimiento documentado de pruebas de seguridad. **AD.1-6:** Se definen los criterios de aceptación de los productos desde la perspectiva de seguridad de la información.	**AD.1-8:** Se realizan actividades de control interno para determinar el nivel de cumplimiento con la metodología y procedimientos definidos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	OR.4-1: Se tiene una lista actualizada de proyectos (finalizados, en curso o planificados) de la organización.	**AD.1-3:** Se cuenta con mecanismos para el control de versiones y revisión de código. **AD.1-4:** Se sistematizan las actividades de prueba, incluyendo casos de prueba orientados a las validaciones de seguridad. **OR.4-2:** Se incluye al RSI o a quien éste designe en la etapa de planificación o inicio de los proyectos. **OR.4-3:** Los contratos y pliegos vinculados a los proyectos contemplan cláusulas de seguridad. **SO.4-4:** Se evita el uso de datos reales de producción en ambientes de prueba; en caso de ser necesarios, se aplican controles de acceso adecuados al nivel de confidencialidad de la información.	**AD.1-7:** Los desarrollos subcontratados deben cumplir con requisitos mínimos de seguridad establecidos por la organización, independientemente del ciclo de desarrollo utilizado por el proveedor. **OR.4-4:** La documentación de los proyectos incluye requisitos de seguridad de la información. **OR.4-5:** La evaluación de riesgos del proyecto incluye riesgos de seguridad de la información. **OR.4-6:** Los informes de avance del proyecto deben incluir el seguimiento del tratamiento de los riesgos de seguridad. **SO.4-8:** Durante la realización de las pruebas se registra y conserva la información del entorno (características, información de los datos de prueba, etc.).	**AD.1-9:** El resultado de estas actividades se comunica al RSI y demás partes interesadas. **AD.1-10:** Se toman acciones correctivas frente a desvíos detectados en los proyectos de desarrollo o adquisición. **OR.4-7:** Se evalúa el cumplimiento de los requisitos de seguridad al finalizar un proyecto. **OR.4-8:** Se documentan las lecciones aprendidas sobre seguridad para la gestión de proyectos futuros.

PR.IR Resiliencia de la infraestructura tecnológica

Las arquitecturas de seguridad se gestionan con la estrategia de riesgos de la organización a fin de proteger la confidencialidad, la integridad y la disponibilidad de los activos, así como la resiliencia de la organización.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.IR-01. Las redes y los entornos están protegidos contra el acceso lógico y el uso no autorizados.	**CA.6-1:** Los derechos de acceso son autorizados. **OR.6-1:** Están definidos requisitos de seguridad mínimos para los dispositivos que se utilicen para acceder remotamente a los activos de la organización. **SC.13-1:** La red se encuentra segmentada al menos en redes con contacto directo con redes externas (por ejemplo, Internet) y redes privadas de la organización. **SC.13-2:** Están identificados y documentados los principales servicios de red utilizados por la organización.	**OR.6-2:** Se registra cada conexión remota como mínimo: hora, fecha, usuario, activo, etc. **OR.6-3:** Se otorga el acceso remoto con base en una lista blanca de todos los recursos disponibles. **OR.6-5:** Se requiere la aprobación explícita del responsable del activo antes de habilitar el acceso remoto. **SC.13-4:** Se segmenta la red en función de las necesidades de la organización. **SC.13-5:** Se genera una postura de manejo de tráfico por defecto entre segmentos.	**CA.6-5:** Se define un procedimiento de acceso lógico a redes, recursos y sistemas de información. **CA.6-6:** Se define una política de acceso lógico a redes, recursos y sistemas de información. **CA.6-7:** Las medidas implementadas para el acceso están directamente asociadas al análisis de riesgos sobre el acceso a la información. **OR.6-6:** Existe un procedimiento documentado de solicitud de acceso remoto. **OR.6-10:** Al menos en forma administrativa se centraliza el acceso remoto. **SC.13-10:** Se conoce y se analiza el tráfico en los diferentes segmentos de la red.	**CA.6-10:** Al realizar los procedimientos de revisión continua, se consideran las políticas, normas, estándares y regulaciones aplicables a la organización con relación a la protección de datos y privacidad de la información. **OR.6-13:** Se realizan actividades de control interno para verificar el cumplimiento de los procedimientos establecidos. **SO.4-9:** Se realizan auditorías de cumplimiento y control interno de la política de separación de entornos y procedimientos relacionados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	SC.13-3: Se mantiene un inventario actualizado de las interconexiones con otras entidades. **SO.4-1:** El entorno de producción se encuentra separado del resto de los entornos.	**SO.4-2:** Se cuenta con plataformas adecuadas e independientes que soportan el ciclo de vida de desarrollo de los sistemas. **SO.4-3:** Se implementan controles para el pasaje entre los ambientes.	**SC.13-11:** Las comunicaciones entrantes y salientes entre los diferentes segmentos son protegidas. **SO.4-5:** Se encuentra definida una política de separación de entornos. **SO.4-6:** Está establecido y documentado un procedimiento de gestión de ambientes. **SO.4-7:** Están definidos los responsables para la gestión de los ambientes existentes y de los pasajes a producción.	**SO.4-10:** Se registran los resultados y se toman acciones correctivas en casos de desvíos.
PR.IR-02. Los activos tecnológicos de la organización están protegidos de las amenazas del entorno.	**SF.2-1:** Están identificados los riesgos ambientales que pueden afectar al centro de datos. **SF.2-2:** Existen medidas de control del medio ambiente físico en los centros de datos.	**SF.2-3:** Están instalados sistemas de detección y extinción de incendios con mantenimiento periódico. **SF.2-4:** Se implementan herramientas automatizadas que apoyan el monitoreo de los controles relacionados al medio ambiente físico. **SF.2-5:** Está implementado un sistema de climatización que regula la temperatura y humedad.	**SF.2-6:** Existe una política de seguridad del equipamiento que incluye medidas ambientales. **SF.2-7:** Se cuenta con un procedimiento documentado de monitoreo de los controles ambientales. Incluye el uso de herramientas automatizadas.	**SF.2-8:** Los controles ambientales se revisan periódicamente y se ajustan según las nuevas condiciones climáticas y tecnológicas. **SF.2-9:** Se realizan actividades de control interno para verificar el cumplimiento de la política y procedimientos asociados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
				SF.2-10: Los resultados del monitoreo son utilizados para la realización de las lecciones aprendidas, las mismas son utilizadas para mejorar los procedimientos relacionados.
PR.IR-03. Se implementan mecanismos para lograr los requisitos de resiliencia en situaciones normales y adversas.	**CO.1-1:** El centro de datos cuenta con UPS y componentes redundantes en lo que refiere a conexión eléctrica. **CO.1-2:** El centro de datos cuenta con componentes redundantes de acondicionamiento térmico. **CO.2-1:** El centro de datos cuenta con componentes redundantes en lo que refiere a infraestructura de comunicaciones.	**CO.1-3:** El centro de datos cuenta con generador eléctrico capaz de alimentar a todos los componentes críticos. **CO.1-4:** Los sistemas de climatización del centro de datos están alimentados por líneas de energía respaldadas por el generador eléctrico. **CO.2-2:** La organización dispone de conectividad a internet a través de múltiples enlaces o proveedores. **CO.2-3:** Los equipos de red críticos del centro de datos están configurados con mecanismos de detección automática de fallos.	**CO.1-5:** El sistema de climatización está configurado para operar de forma continua 24/7 y contempla mecanismos automáticos de failover ante fallas. **CO.1-6:** Se realizan pruebas periódicas de funcionamiento de los mecanismos automáticos de failover en los sistemas de climatización. **CO.2-4:** La arquitectura de red del centro de datos, incluyendo su esquema de redundancia, está documentada y actualizada.	**CO.1-7:** Se realizan pruebas periódicas de funcionamiento del generador y UPS para validar su operatividad ante fallas reales. **CO.1-8:** Se realizan revisiones periódicas del diseño de redundancia del centro de datos considerando cambios tecnológicos, de carga o de riesgos identificados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
			CO.2-5: Se realizan pruebas periódicas de conmutación automática de enlaces o equipos de red redundantes, y se registran sus resultados.	**CO.1-9:** La organización cuenta con un sitio de contingencia capaz de asegurar la continuidad operativa en caso de indisponibilidad del centro de procesamiento de datos principal, incluyendo pruebas periódicas de su capacidad y tiempo de conmutación. **CO.2-6:** La organización realiza revisiones técnicas periódicas del diseño de la red para identificar nuevos puntos únicos de falla y definir mejoras. **CO.2-7:** Se analizan eventos o fallos reales en la infraestructura de red para ajustar la estrategia de redundancia y disponibilidad.
PR.IR-04. Se mantiene una capacidad de recursos adecuada para garantizar la disponibilidad.	**SO.3-1:** La capacidad actual instalada es suficiente para garantizar la prestación de los servicios críticos. **SO.3-2:** Ante eventos de saturación o cuellos de botella se toman medidas ad-hoc para restaurar la capacidad operativa.	**SO.3-3:** Se toman en cuenta las necesidades del negocio al momento de dimensionar los servicios críticos. **SO.3-4:** Se realizan mediciones objetivas para detectar problemas de capacidad.	**SO.3-5:** Está establecido el proceso de gestión de la capacidad. **SO.3-6:** Los roles y responsabilidades asociados al proceso de gestión de la capacidad están definidos y documentados. **SO.3-7:** La gestión de capacidad se integra en los acuerdos de nivel de servicio vigentes.	**SO.3-8:** Existe un plan de capacidad formalizado y documentado. **SO.3-9:** Está definido un proceso de estimación de la capacidad que acompaña al plan. **SO.3-10:** Se revisa periódicamente el plan de capacidad. **SO.3-11:** Se proponen acciones para la mejora continua de la gestión de la capacidad.

5.4 Función: Detectar (DE)

DE.CM. Monitoreo continuo

Los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros eventos potencialmente adversos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.CM-01. Las redes y los servicios de red se monitorean para detectar eventos potencialmente adversos.	**SO.7-1:** Están configurados los registros de auditoría y eventos para todos los sistemas definidos como críticos. **SO.7-2:** Se analiza el impacto de los eventos que afectan a los sistemas y servicios más críticos, dentro o fuera del centro de datos. **SO.7-3:** Existe personal con tareas asignadas para la detección de eventos a nivel de sistemas base y de protección perimetral.	**SO.7-5:** Los registros están protegidos contra accesos no autorizados y posibles alteraciones. **SO.7-8:** Se automatizan alertas ante eventos de seguridad de la información. Por ejemplo, permiten alertar cuando los usuarios realizan conexiones fuera de la organización, y la conexión e instalación de dispositivos o software no autorizado en equipos de la organización. **SO.7-9:** Se han definido las responsabilidades y la participación de los roles de TI en las actividades de monitoreo, incluyendo aquellas basadas en herramientas automatizadas.	**SO.7-13:** Se define una política de auditoría y registro de eventos, como por ej. de los sistemas y redes y de configuración y uso de WAF. **SO.7-14:** Están establecidos procedimientos de auditoría y registro de eventos. **SO.7-16:** Están establecidos procedimientos de detección y monitoreo. **SO.7-18:** Se realizan pruebas periódicas al procedimiento de monitoreo.	**SO.7-20:** Se cuenta con herramientas que permitan respuesta automatizada ante incidentes de seguridad de la información.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.CM-02. Se monitorea el entorno físico para detectar posibles eventos adversos.	**SF.1-1:** Están identificadas las áreas que requieren control de acceso físico. **SF.1-2:** Están implementados los controles de acceso físico a las instalaciones de los centros de procesamiento de datos. **SF.1-3:** Se gestionan (evalúan, autorizan y registran) las autorizaciones de acceso al centro de procesamiento de datos.	**SF.1-4:** Están establecidos perímetros de seguridad en el centro de procesamiento de datos y las áreas seguras. **SF.1-5:** Están implementados controles de acceso físico para otras áreas definidas como seguras. **SF.1-6:** Se gestionan (evalúan, autorizan y registran) las autorizaciones de acceso a las áreas definidas como seguras. **SF.1-7:** Se lleva un registro de accesos físicos al centro de procesamiento de datos y áreas seguras.	**SF.1-8:** Existe una política de control de acceso físico formalmente aprobada. **SF.1-9:** Se revisan de forma reactiva los registros de acceso a las diferentes áreas. **SF.1-10:** Las aplicaciones que manejan información sensible requieren reautenticación periódica, especialmente cuando se accede desde ubicaciones de alto riesgo.	**SF.1-11:** Está establecido un procedimiento de revisión periódica de los accesos al centro de procesamiento de datos y a las áreas seguras. **SF.1-12:** Se realizan actividades de control interno para verificar el cumplimiento de los procedimientos establecidos. **SF.1-13:** Se aplican controles de tiempo de conexión y condiciones de acceso desde ubicaciones públicas o externas a la organización.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.CM-03. Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos	**GA.3-1:** Existen pautas del uso aceptable de los activos de la información. **GA.3-2:** Toda persona que acceda a activos de información debe aceptar formalmente, previo al acceso, las condiciones de uso establecidas por la organización. **GI.2-1:** Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas.	**GI.2-3:** Está definido cuando una serie de eventos o una notificación conforman un incidente. **GI.2-4:** Está definido cuando una serie de eventos o una notificación conforman un delito conforme la normativa vigente.	**GA.3-5:** Está definida formalmente la política sobre el uso adecuado de los activos de la información de la organización. **GA.3-6:** La política de uso adecuado de los activos es difundida a todo el personal, proveedores y terceros que utilicen activos de información. **GA.3-8:** Existe un plan de respuesta en caso de pérdida o robo de los activos de información.	**GA.3-9:** Las medidas de protección implementadas en los activos informáticos se monitorean de forma proactiva 7x24. **GA.3-10:** Se realizan evaluaciones periódicas para verificar que el uso de los activos se ajusta a las condiciones establecidas en la política.
DE.CM-06. Se monitorean las actividades y los servicios de los proveedores de servicios externos para detectar eventos potencialmente adversos.	**GI.2-1:** Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas. **RP.2-1:** Se definen métricas e indicadores para el seguimiento y control de los proveedores, mínimamente para los proveedores críticos.	**GI.2-3:** Está definido cuando una serie de eventos o una notificación conforman un incidente. **GI.2-4:** Está definido cuando una serie de eventos o una notificación conforman un delito conforme la normativa vigente.	**RP.2-4:** Se documentan los resultados de las evaluaciones de desempeño y cumplimiento de requisitos de seguridad de los proveedores.	**RP.2-7:** La gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.CM-09. Se monitorean el hardware y el software informáticos, los entornos de ejecución y sus datos para detectar posibles eventos adversos.	**SC.15-2:** Todas las aplicaciones Web disponibles en Internet se encuentran protegidas mediante el uso de WAF, al menos configurados en modo “detección”. **SF.3-1:** Se monitorea de forma reactiva o esporádica los sistemas o servicios más críticos. **SF.3-2:** Se registran los logs de las fallas y alertas críticas, y se conserva su historial para revisión. **SO.5-1:** Todos los equipos del personal cuentan con una solución antimalware **SO.5-2:** Las soluciones a los problemas detectados se realizan en forma ad-hoc.	**SC.15-3:** El WAF de producción ha evolucionado de modo detección a modo bloqueo. **SF.3-3:** Se monitorea de forma automatizada los activos críticos del centro de procesamiento de datos, generando alertas ante la detección de problemas. **SF.3-4:** Existen funciones integradas en los dispositivos que permiten el monitoreo de las amenazas típicas (alimentación eléctrica, enfriamiento, etc.). **SF.3-5:** Se definen notificaciones de alertas (correo, SMS, etc.) al personal designado. **SO.5-3:** Todos los servidores cuentan con una solución antimalware.	**SC.15-4:** Se cuenta con un WAF instalado en ambiente de prueba para la realización de pruebas funcionales. **SC.15-5:** En el ambiente de producción se impactan las reglas actualizadas luego de ser probadas. **SC.15-6:** Los registros de los WAF se encuentran centralizados. **SF.3-6:** En el centro de procesamiento de datos se implementan alertas sobre anomalías que podrían transformarse en problemas para los activos críticos. **SF.3-8:** Establecer un procedimiento documentado de monitoreo que incluye el uso de herramientas automatizadas. **SO.5-5:** Está definida una política del manejo de software malicioso.	**SC.15-7:** El análisis de los registros del WAF incluye automatismos que favorecen las actividades de revisión. **SF.3-9:** Se envían alertas del estado de los componentes prioritarios para el funcionamiento de la organización ante los cambios de entorno. **SF.3-10:** Se monitorean todos los activos de información del centro de procesamiento de datos, con cruzamiento de información de diversas fuentes, contemplando, entre otros, alertas preventivas y reactivas. **SF.3-11:** Se cuenta con un proceso de control interno para la verificación de cumplimiento de los procedimientos de monitoreo del centro de procesamiento de datos. **SO.5-8:** Están implementados controles para evitar el acceso a sitios Web maliciosos y/o no autorizados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
		SO.5-4: Se encuentran configurados chequeos periódicos en los equipos del personal. **SO.7-7:** Los sistemas que soportan los servicios críticos emiten alertas de eventos de forma independiente, basados en las pautas establecidas por el apetito de riesgo de la organización.	**SO.5-6:** Está establecido un procedimiento del manejo de software malicioso. **SO.5-7:** Se cuenta con una solución centralizada de antimalware. **SO.7-16:** Están establecidos procedimientos de detección y monitoreo. **SO.7-18:** Se realizan pruebas periódicas al procedimiento de monitoreo.	**SO.5-9:** La protección ante software malicioso se extiende a otros dispositivos móviles y se refleja en la política de protección contra software malicioso. **SO.5-10:** Existen procedimientos documentados para la detección de equipos que se encuentran desprotegidos y se realizan las acciones necesarias para subsanar la situación. **SO.5-11:** Se cuenta con un registro estadístico de infecciones por software malicioso que aporta a la toma de decisiones y alimenta las lecciones aprendidas que se usan para la mejora continua. **SO.7-21:** Se realizan actividades de control interno para verificar el cumplimiento con la política y los procedimientos. **SO.7-22:** El resultado de las revisiones se comunica al RSI y demás partes interesadas.

DE.AE. Análisis de eventos adversos

Se analizan anomalías, indicadores de compromiso y otros eventos potencialmente adversos para caracterizarlos y detectar incidentes de ciberseguridad.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.AE-02. Los eventos potencialmente adversos se analizan para comprender mejor las actividades asociadas.	**SO.7-1:** Están configurados los registros de auditoría y eventos para todos los sistemas definidos como críticos.	**SC.12-6:** Se generan alertas ante intentos de acceso no autorizados al Webmail. **SO.7-6:** Se establecen los umbrales tolerables de los activos (por ejemplo, tiempo de espera tolerable para una aplicación Web).	**SO.7-15:** Se cuenta con herramientas que permitan la correlación de eventos de seguridad de la información.	**SO.7-19:** Se cuenta con mecanismos para revisar las actividades de los administradores.
DE.AE-03. Se correlaciona la información procedente de diversas fuentes.	**GI.2-1:** Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas.	**GI.4-4:** Los registros de incidentes permiten trazabilidad completa de su evolución, desde la detección hasta el cierre.	**SF.3-7:** Las alertas notifican cuando se comienzan a dar las casuísticas que pueden derivar en un incidente aún no concretado.	**GA.3-9:** Las medidas de protección implementadas en los activos informáticos se monitorean de forma proactiva 7x24.
DE.AE-04. Se comprende el impacto estimado y el alcance de los eventos adversos.	**GI.2-2:** Se han definido lineamientos para la categorización de los incidentes según su tipo y criticidad.	**GI.2-5:** Los incidentes identificados se clasifican utilizando una escala formal de severidad y criticidad. **GI.2-6:** Están definidas las acciones y tiempos de respuesta asociados a cada categoría según severidad.	**GI.2-7:** Existe un procedimiento de gestión de incidentes que incluye las tareas de análisis de impacto.	**GI.2-11:** La categorización de incidentes se revisa periódicamente, considerando las necesidades del negocio y las tendencias de amenazas. **GI.2-13:** Los resultados son utilizados para mejorar o incrementar los controles existentes.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.AE-06. La información sobre eventos adversos se proporciona al personal y a las herramientas autorizadas.	**SO.7-1:** Están configurados los registros de auditoría y eventos para todos los sistemas definidos como críticos.	**SO.7-6:** Se establecen los umbrales tolerables de los activos (por ejemplo, tiempo de espera tolerable para una aplicación Web).	**SO.7-15:** Se cuenta con herramientas que permitan la correlación de eventos de seguridad de la información.	**SO.7-19:** Se cuenta con mecanismos para revisar las actividades de los administradores.
DE.AE-07. La inteligencia sobre ciberamenazas y otra información contextual se integran en el análisis.	**GR.4-1:** La organización ha identificado y documentado sus fuentes confiables de inteligencia de amenazas, incluyendo al menos CERTuy y fuentes oficiales, comunitarias o sectoriales. **GR.4-2:** El personal de seguridad recibe capacitación sobre el uso de inteligencia de amenazas. **GR.4-3:** La organización recibe periódicamente información de amenazas a través de sus fuentes confiables, la misma se registra para su posterior análisis.	**GR.4-4:** Están asignados los responsables de recibir, filtrar y analizar la inteligencia de amenazas. **GR.4-5:** Se realiza un análisis del impacto potencial de las amenazas emergentes sobre la organización. **GR.4-6:** La inteligencia de amenazas se utiliza como insumo para el análisis de riesgos de seguridad de la información.	**GR.4-7:** Se cuenta con un procedimiento documentado sobre el uso de inteligencia de amenazas, abarcando como se recibe, filtra, analiza, clasifica y utiliza la información. **GR.4-8:** La información de inteligencia de amenazas se utiliza para ajustar o redefinir los controles existentes y apoyar el diseño de nuevos controles para los planes de tratamiento de riesgos.	**GR.4-9:** Se revisa periódicamente las fuentes confiables de inteligencia identificadas para validar su vigencia. **GR.4-10:** La organización actualiza sus análisis de riesgos en función de la nueva información derivada del análisis de la inteligencia de amenazas. **GR.4-11:** Las tendencias identificadas del análisis de la inteligencia de amenazas son utilizadas como insumo para la toma de decisiones estratégicas relacionadas a seguridad.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.AE-08. Se declaran incidentes cuando los eventos adversos cumplen con los criterios de incidente definidos.	**GI.2-1:** Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas.	**GI.2-3:** Está definido cuando una serie de eventos o una notificación conforman un incidente. **GI.2-4:** Está definido cuando una serie de eventos o una notificación conforman un delito conforme la normativa vigente. **SO.7-7:** Los sistemas que soportan los servicios críticos emiten alertas de eventos de forma independiente, basados en las pautas establecidas por el apetito de riesgo de la organización.	**SO.7-17:** Las actividades de identificación de impacto y determinación de umbrales están contenidas en el procedimiento de detección y monitoreo.	**GI.2-12:** La categorización de incidentes se revisa periódicamente, considerando las necesidades del negocio y las tendencias de amenazas.

5.5 Función: Responder (RS)

RS.MA Gestión de incidentes

Se gestionan las respuestas a los incidentes de ciberseguridad detectados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.MA-01. Se ejecuta el plan de respuesta a incidentes en coordinación con los terceros pertinentes una vez que se declara un incidente.	**GI.1-1:** Se encuentran identificados los puntos de contacto inicial para la recepción de eventos de seguridad.	**GI.1-2:** Se identifican los potenciales actores internos y externos ante un incidente y se registran sus datos de contacto. **GI.1-3:** Se cuenta con herramientas que apoyan la gestión de los incidentes. **GI.5-4:** Se han definido pautas establecidas para garantizar la cadena de custodia.	**GI.1-4:** Se ha definido un procedimiento general que cubre las distintas fases de gestión de incidentes (detección, registro, análisis, contención, erradicación y cierre). **GI.1-5:** Se encuentra definida formalmente la política de gestión de incidentes de seguridad de la información. **GI.1-6:** La política de gestión de incidentes es difundida a todas las partes interesadas. **GI.5-10:** Se cuenta con pautas o políticas documentadas para llevar adelante las revisiones de las estrategias de respuesta. **GI.5-11:** Se revisan periódicamente las estrategias de respuesta de los procesos de la organización que afecten los servicios críticos.	**GI.1-7:** Se realizan auditorías internas para verificar el cumplimiento con la política y procedimientos relacionados. **GI.1-8:** El resultado de estas actividades se informa al RSI y se toman acciones correctivas frente a desvíos y para la mejora continua. **GI.5-15:** Se realizan auditorías internas para verificar el cumplimiento del plan y/o procedimiento de respuesta. **GI.5-16:** Las mejoras identificadas en las revisiones de estrategia son utilizadas para su ajuste. **GI.5-17:** Se generan indicadores para seguimiento y control.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.MA-02. Se clasifican y validan los informes de incidentes.	**GI.2-1:** Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas. **GI.2-2:** Se han definido lineamientos para la categorización de los incidentes según su tipo y criticidad.	**GI.2-3:** Está definido cuando una serie de eventos o una notificación conforman un incidente. **GI.2-4:** Está definido cuando una serie de eventos o una notificación conforman un delito conforme la normativa vigente. **GI.2-5:** Los incidentes identificados se clasifican utilizando una escala formal de severidad y criticidad.	**GI.2-9:** Se cuenta con herramientas automatizadas para el registro de incidentes alineadas con el plan y/o procedimiento de respuesta definido. **GI.5-12:** Los incidentes de severidad alta son reportados mediante informe a la Dirección u otras partes interesadas.	**GI.2-11:** La categorización de incidentes se revisa periódicamente, considerando las necesidades del negocio y las tendencias de amenazas.
RS.MA-03. Se clasifican y priorizan los incidentes.	**GI.2-1:** Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas. **GI.2-2:** Se han definido lineamientos para la categorización de los incidentes según su tipo y criticidad.	**GI.2-3:** Está definido cuando una serie de eventos o una notificación conforman un incidente. **GI.2-4:** Está definido cuando una serie de eventos o una notificación conforman un delito conforme la normativa vigente. **GI.2-5:** Los incidentes identificados se clasifican utilizando una escala formal de severidad y criticidad. **GI.2-6:** Están definidas las acciones y tiempos de respuesta asociados a cada categoría según severidad.	**GI.2-7:** Existe un procedimiento de gestión de incidentes que incluye las tareas de análisis de impacto. **GI.2-8:** El procedimiento de gestión de incidentes define el criterio para escalar un incidente considerando: activos afectados, criticidad y severidad. **GI.2-9:** Se cuenta con herramientas automatizadas para el registro de incidentes alineadas con el plan y/o procedimiento de respuesta definido. **GI.2:10:** Las acciones asociadas a cada categoría están alineadas al plan de respuesta.	**GI.2-11:** La categorización de incidentes se revisa periódicamente, considerando las necesidades del negocio y las tendencias de amenazas. **GI.2-12:** Se realizan estadísticas utilizando las categorizaciones. **GI.2-13:** Los resultados son utilizados para mejorar o incrementar los controles existentes.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.MA-04. Se escalan o elevan los incidentes según sea necesario.	**GI.3-1:** Los incidentes de seguridad informática se reportan al CERTuy y/o al equipo de respuesta que corresponda de acuerdo a los criterios establecidos por éste. **GI.3-2:** Los incidentes de seguridad que involucre datos personales son reportados a la Unidad Reguladora y de Control de Datos Personales (URCDP), conforme a los plazos y requisitos establecidos por la normativa vigente. **GI.3-3:** Los incidentes de seguridad que pueda corresponder a un delito son denunciados ante la Unidad de cibercrimen.	**GI.3-4:** Se lleva un registro de las comunicaciones realizadas ante incidentes, incluyendo hora, contenido y destinatarios.	**GI.3-5:** Se ha documentado un procedimiento formal de comunicación de incidentes. **GI.5-12:** Los incidentes de severidad alta son reportados mediante informe a la Dirección u otras partes interesadas. **PD.5-6:** Existen procedimientos para notificar incidentes de seguridad a la URCDP dentro del plazo legal establecido, incluyendo la evaluación del impacto y acciones tomadas. **PD.5-7:** Está definido un procedimiento formal para comunicar a los titulares de datos las vulneraciones de seguridad.	**GI.3-6:** El procedimiento de comunicación de incidentes se revisa regularmente y se ajusta ante cambios regulatorios, lecciones aprendidas o recomendaciones del CERTuy. **GI.3-7:** Se realizan simulacros de reporte de incidentes para validar la efectividad del canal de comunicación y los tiempos de reacción. **GI.3-8:** Se auditan periódicamente los canales, mecanismos y procedimientos de notificación establecidos para incidentes de seguridad. **GI.5-14:** La Dirección, el RSI y el CSI reciben información periódica sobre incidentes de seguridad de la información.
RS.MA-05. Se aplican los criterios para iniciar la recuperación de incidentes.	**CO.4-3:** Existen respaldos de información de los sistemas que dan soporte a los servicios críticos.	**CO.4-5:** Se ha identificado el orden de prelación para la recuperación en base a la dependencia de los servicios.	**CO.4-6:** Se cuenta con un Análisis de Impacto al Negocio (BIA) que identifica los procesos críticos. **CO.4-7:** Se ejecutan pruebas puntuales o parciales de los planes.	**CO.4-10:** Se registran los resultados de las pruebas. **CO.4-11:** El resultado de las pruebas retroalimenta las lecciones aprendidas y sirven para la mejora continua de los planes y procedimientos.

RS.AN. Análisis de incidentes

Se llevan a cabo investigaciones con el fin de garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.AN-03. Se realizan análisis para determinar lo que ocurrió durante un incidente y la causa raíz del mismo.	**GI.2-1:** Los eventos anómalos o potencialmente anómalos se comunican a referentes con capacidad de decisión y articulación de respuestas. **GI.2-2:** Se han definido lineamientos para la categorización de los incidentes según su tipo y criticidad.	**GI.2-3:** Está definido cuando una serie de eventos o una notificación conforman un incidente. **GI.2-4:** Está definido cuando una serie de eventos o una notificación conforman un delito conforme la normativa vigente. **GI.2-5:** Los incidentes identificados se clasifican utilizando una escala formal de severidad y criticidad. **GI.2-6:** Están definidas las acciones y tiempos de respuesta asociados a cada categoría según severidad. **GI.5-3:** Ante un incidente de seguridad de la información en la organización, se realiza un análisis forense.	**GI.2-7:** Existe un procedimiento de gestión de incidentes que incluye las tareas de análisis de impacto. **GI.2-8:** El procedimiento de gestión de incidentes define el criterio para escalar un incidente considerando: activos afectados, criticidad y severidad. **GI.2-9:** Se cuenta con herramientas automatizadas para el registro de incidentes alineadas con el plan y/o procedimiento de respuesta definido. **GI.2-10:** Las acciones asociadas a cada categoría están alineadas al plan de respuesta. **GI.5-8:** Todos los procedimientos vinculados al análisis forense se encuentran documentados.	**GI.2-11:** La categorización de incidentes se revisa periódicamente, considerando las necesidades del negocio y las tendencias de amenazas. **GI.2-12:** Se realizan estadísticas utilizando las categorizaciones. **GI.2-13:** Los resultados son utilizados para mejorar o incrementar los controles existentes.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.AN-06. Se registran las acciones realizadas durante una investigación y se preservan la integridad y la procedencia de los registros.	**GI.4-1:** Los incidentes de seguridad se reportan internamente de acuerdo a lineamientos preestablecidos. **GI.4-2:** El personal ha sido instruido sobre los mecanismos y canales habilitados para reportar incidentes. **GI.4-3:** Los incidentes son registrados.	**GI.4-4:** Los registros de incidentes permiten trazabilidad completa de su evolución, desde la detección hasta el cierre.	**GI.4-5:** Existe un procedimiento de registro que incluye campos como: fecha/hora, tipo de incidente, activos afectados, estado, entre otros campos relevantes. **GI.4-6:** El reporte de incidentes se apoya en herramientas automatizadas.	**GI.4-7:** Se realizan actividades de control interno de cumplimiento con el procedimiento de reporte de incidentes. **GI.4-8:** El resultado de las actividades se utiliza para mejorar el procedimiento de reporte.
RS.AN-07. Se recopilan los datos y metadatos del incidente y se preservan su integridad y su procedencia.	**GI.1-1:** Se encuentran identificados los puntos de contacto inicial para la recepción de eventos de seguridad.	**GI.1-2:** Se identifican los potenciales actores internos y externos ante un incidente y se registran sus datos de contacto. **GI.1-3:** Se cuenta con herramientas que apoyan la gestión de los incidentes. **GI.5-4:** Se han definido pautas establecidas para garantizar la cadena de custodia.	**GI.1-4:** Se ha definido un procedimiento general que cubre las distintas fases de gestión de incidentes (detección, registro, análisis, contención, erradicación y cierre). **GI.1-5:** Se encuentra definida formalmente la política de gestión de incidentes de seguridad de la información. **GI.1-6:** La política de gestión de incidentes es difundida a todas las partes interesadas.	**GI.1-7:** Se realizan auditorías internas para verificar el cumplimiento con la política y procedimientos relacionados. **GI.1-8:** El resultado de estas actividades se informa al RSI y se toman acciones correctivas frente a desvíos y para la mejora continua.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.AN-08. Se estima y valida la magnitud de un incidente.	**GI.2-2:** Se han definido lineamientos para la categorización de los incidentes según su tipo y criticidad.	**GI.2-5:** Los incidentes identificados se clasifican utilizando una escala formal de severidad y criticidad. **GI.2-6:** Están definidas las acciones y tiempos de respuesta asociados a cada categoría según severidad.	**GI.2-8:** Existe un procedimiento de gestión de incidentes que incluye las tareas de análisis de impacto. **GI.2-9:** El procedimiento de gestión de incidentes define el criterio para escalar un incidente considerando: activos afectados, criticidad y severidad.	**GI.2-13:** Los resultados son utilizados para mejorar o incrementar los controles existentes.

RS.CO. Notificación y comunicación de la respuesta al incidente

Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según lo exijan las leyes, las normativas o las políticas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.CO-02. Se notifican los incidentes a las partes interesadas internas y externas.	**GI.3-1:** Los incidentes de seguridad informática se reportan al CERTuy y/o al equipo de respuesta que corresponda de acuerdo a los criterios establecidos por éste. **GI.3-2:** Los incidentes de seguridad que involucre datos personales son reportados a la Unidad Reguladora y de Control de Datos Personales (URCDP), conforme a los plazos y requisitos establecidos por la normativa vigente. **GI.3-3:** Los incidentes de seguridad que pueda corresponder a un delito son denunciados ante la Unidad de cibercrimen.	**GI.3-4:** Se lleva un registro de las comunicaciones realizadas ante incidentes, incluyendo hora, contenido y destinatarios. **PD.5-4:** Se mantiene un registro de incidentes de seguridad que involucren datos personales, incluyendo la fecha y tipo de evento.	**GI.3-5:** Se ha documentado un procedimiento formal de comunicación de incidentes. **GI.5-12:** Los incidentes de severidad alta son reportados mediante informe a la Dirección u otras partes interesadas. **PD.5-6:** Existen procedimientos para notificar incidentes de seguridad a la URCDP dentro del plazo legal establecido, incluyendo la evaluación del impacto y acciones tomadas. **PD.5-7:** Está definido un procedimiento formal para comunicar a los titulares de datos las vulneraciones de seguridad.	**GI.3-6:** El procedimiento de comunicación de incidentes se revisa regularmente y se ajusta ante cambios regulatorios, lecciones aprendidas o recomendaciones del CERTuy. **GI.3-7:** Se realizan simulacros de reporte de incidentes para validar la efectividad del canal de comunicación y los tiempos de reacción. **GI.3-8:** Se auditan periódicamente los canales, mecanismos y procedimientos de notificación establecidos para incidentes de seguridad.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.CO-03. La información se comparte con las partes interesadas internas y externas designadas.	**GI.3-1:** Los incidentes de seguridad informática se reportan al CERTuy y/o al equipo de respuesta que corresponda de acuerdo a los criterios establecidos por éste. **GI.3-2:** Los incidentes de seguridad que involucre datos personales son reportados a la Unidad Reguladora y de Control de Datos Personales (URCDP), conforme a los plazos y requisitos establecidos por la normativa vigente. **GI.3-3:** Los incidentes de seguridad que pueda corresponder a un delito son denunciados ante la Unidad de cibercrimen.	**GI.3-4:** Se lleva un registro de las comunicaciones realizadas ante incidentes, incluyendo hora, contenido y destinatarios.	**GI.3-5:** Se ha documentado un procedimiento formal de comunicación de incidentes. **PD.5-6:** Existen procedimientos para notificar incidentes de seguridad a la URCDP dentro del plazo legal establecido, incluyendo la evaluación del impacto y acciones tomadas. **PD.5-7:** Está definido un procedimiento formal para comunicar a los titulares de datos las vulneraciones de seguridad.	**GI.3-6:** El procedimiento de comunicación de incidentes se revisa regularmente y se ajusta ante cambios regulatorios, lecciones aprendidas o recomendaciones del CERTuy. **GI.3-7:** Se realizan simulacros de reporte de incidentes para validar la efectividad del canal de comunicación y los tiempos de reacción. **GI.3-8:** Se auditan periódicamente los canales, mecanismos y procedimientos de notificación establecidos para incidentes de seguridad.

RS.MI. Mitigación de incidentes

Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.MI-01. Se contienen los incidentes.	**GI.5-1:** Se han definido los mecanismos de respuesta a incidentes. **GI.5-2:** Los incidentes son atendidos y se aplican medidas para mitigar sus consecuencias.	**GI.5-5:** Se han definido pautas para contener el daño y minimizar el riesgo en el entorno operativo.	**GI.5-7:** Está definido un plan y/o procedimiento de respuesta ante incidentes. **GI.5-9:** Se define el responsable de la respuesta a incidentes.	**GI.5-13:** El plan de respuesta a incidentes es probado anualmente.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RS.MI-02. Se erradican los incidentes.	**GI.5-1:** Se han definido los mecanismos de respuesta a incidentes. **GI.5-2:** Los incidentes son atendidos y se aplican medidas para mitigar sus consecuencias.	**GI.5-6:** Se cuenta con planes de remediación de los incidentes.	**GI.5-7:** Está definido un plan y/o procedimiento de respuesta ante incidentes. **GI.5-9:** Se define el responsable de la respuesta a incidentes.	**GI.5-13:** El plan de respuesta a incidentes es probado anualmente.

5.6 Función: Recuperar (RC)

RC.RP Ejecución del plan de recuperación de incidentes

Se realizan actividades de restauración que garantizan la disponibilidad operativa de los sistemas y servicios afectados por incidentes de ciberseguridad.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RC.RP-01. La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez que se inicia desde el proceso de respuesta a incidentes.	**CO.4-1:** Se cuenta con ciertas medidas de contingencia y recuperación para los sistemas que dan soporte a los servicios críticos. **CO.4-2:** Están identificados un conjunto de amenazas que podrían afectar la continuidad operativa. **GI.5-1:** Se han definido los mecanismos de respuesta a incidentes.	**CO.4-4:** Existen planes formales de contingencia operativa y de recuperación ante desastres, validados por la alta dirección.	**GI.5-7:** Está definido un plan y/o procedimiento de respuesta ante incidentes.	**CO.4-8:** Se ha definido el o los responsables del mantenimiento de los planes de contingencia y de recuperación. **CO.4-9:** Los planes de contingencia y de recuperación contemplan la participación de proveedores de servicios críticos, acorde a los acuerdos de nivel de servicio (SLA) y su involucramiento en las pruebas de contingencia. **GI.5-13:** El plan de respuesta a incidentes es probado anualmente.
RC.RP-02. Se seleccionan, delimitan, priorizan y llevan a cabo las acciones de recuperación.	**CO.4-3:** Existen respaldos de información de los sistemas que dan soporte a los servicios críticos.	**CO.4-5:** Se ha identificado el orden de prelación para la recuperación en base a la dependencia de los servicios.	**CO.4-6:** Se cuenta con un Análisis de Impacto al Negocio (BIA) que identifica los procesos críticos. **CO.4-7:** Se ejecutan pruebas puntuales o parciales de los planes.	**CO.4-10:** Se registran los resultados de las pruebas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RC.RP-03. Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para la restauración.	**SO.6-1:** Se realizan respaldos periódicos de al menos los activos de información del centro de datos (aplicaciones, bases de datos, máquinas virtuales, etc.).	**SO.6-4:** Los respaldos son probados regularmente.	**SO.6-6:** Se cuenta con soluciones automatizadas para asistir en la realización de los respaldos. **SO.6-7:** Existe una política de respaldos. **SO.6-8:** Existen procedimientos documentados de realización y prueba de recuperación de respaldos.	**SO.6-10:** La política y el procedimiento de respaldo se encuentran alineados al plan de contingencia y al plan de recuperación. **SO.6-11:** La política y procedimiento de respaldos se revisan regularmente.
RC.RP-04. Se tienen en cuenta las funciones críticas de la misión y la gestión de riesgos de ciberseguridad para establecer normas operativas posteriores al incidente.	**GI.6-1:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en el centro de procesamiento de datos.	**GI.6-2:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en toda la organización.	**GI.6-3:** Las lecciones aprendidas son puestas a disposición y comunicadas a todas las partes interesadas. **GI.6-4:** Se cuenta con herramientas que dan soporte al registro y gestión de las lecciones aprendidas. **GI.6-5:** Las lecciones aprendidas se contemplan para mejorar los planes de respuesta a incidentes. **GI.6-6:** Las lecciones aprendidas son utilizadas para mejorar los canales de comunicación establecidos con las partes involucradas y los procesos de escalamiento.	**GI.6-7:** Las lecciones aprendidas son utilizadas para la mejora de los procesos de la organización. **GI.6-8:** Se generan indicadores para seguimiento y control. **GI.6-9:** Se definen indicadores para poder medir la efectividad de los controles.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RC.RP-05. Se verifica la integridad de los activos restaurados, se restauran los sistemas y servicios y se confirma el estado operativo normal.	**CO.5-1:** Está designado un responsable o equipo para la identificación de métricas de recuperación para procesos críticos.	**CO.5-3:** Se ha determinado el RTO (Recovery Time Objective) para cada sistema que soporte un proceso crítico. **CO.5-4:** Se ha definido el RPO (Recovery Point Objective) para cada sistema que soporte un proceso crítico.	**CO.5-5:** Las métricas MTD, RTO y RPO han sido utilizadas para identificar brechas entre los tiempos actualmente alcanzables y los requerimientos definidos. **CO.5-6:** Las métricas definidas han sido incorporadas como insumo obligatorio en el diseño, pruebas y evaluación de los planes de continuidad.	**CO.5-8:** Los resultados de las pruebas de continuidad son comparados contra las métricas definidas y se documentan desviaciones con planes de mejora asociados. **CO.5-9:** Las métricas son utilizadas como insumo en análisis costo-beneficio para priorizar inversiones en infraestructura, redundancia o automatización de recuperación.
RC.RP-06. Se declara el fin de la recuperación del incidente sobre la base de criterios y se completa la documentación relacionada con el incidente.	**GI.6-1:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en el centro de procesamiento de datos.	**GI.6-2:** Se cuenta con un mecanismo para identificar, registrar y analizar lecciones aprendidas de los incidentes de seguridad de la información en toda la organización.	**GI.6-3:** Las lecciones aprendidas son puestas a disposición y comunicadas a todas las partes interesadas. **GI.6-5:** Las lecciones aprendidas se contemplan para mejorar los planes de respuesta a incidentes. **GI.6-6:** Las lecciones aprendidas son utilizadas para mejorar los canales de comunicación establecidos con las partes involucradas y los procesos de escalamiento.	**GI.6-7:** Las lecciones aprendidas son utilizadas para la mejora de los procesos de la organización.

RC.CO Comunicación de la recuperación del incidente

Se coordinan las actividades de restauración con las partes internas y externas.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RC.CO-03. Las actividades de recuperación y los progresos en el restablecimiento de las capacidades operativas se comunican a las partes interesadas internas y externas designadas.	**CO.6-1:** La comunicación externa de las situaciones de crisis o incidentes mayores es llevada a cabo exclusivamente por la Dirección o por quien ésta haya determinado. **CO.6-2:** Las áreas técnicas pueden realizar comunicaciones externas sólo si cuentan con autorización expresa de la Dirección o por quien ésta haya determinado.	**CO.6-3:** Se ha comunicado quién es el vocero designado y a través de qué canales debe ser contactado.	**CO.6-4:** Se ha definido y documentado un plan y/o procedimiento de comunicaciones ante crisis que cubre la evaluación del evento, las notificaciones, nivel de comunicación requerido, mensajes, audiencia, interesados y monitoreo de las comunicaciones. **CO.6-5:** El plan y/o el procedimiento han sido difundidos entre todos los actores involucrados en la gestión de crisis y continuidad operativa.	**CO.6-6:** Se realizan ensayos periódicos que incluyen la ejecución del plan y procedimiento de comunicación ante crisis, de forma coordinada con los ejercicios de continuidad y recuperación. **CO.6-7:** Se realizan auditorías internas para verificar el cumplimiento del plan y procedimiento de comunicaciones ante crisis. **CO.6-8:** Los resultados de las revisiones y ensayos son documentados y utilizados para ajustar, actualizar y mejorar continuamente el plan y procedimiento de comunicaciones. **CO.6-9:** La Dirección participa activamente en las actualizaciones del plan, en especial, en la aprobación y modo de difusión de los mensajes.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RC.CO-04 Las actualizaciones públicas sobre la recuperación del incidente se comparten mediante el uso de métodos y mensajes aprobados.	**CO.6-1:** La comunicación externa de las situaciones de crisis o incidentes mayores es llevada a cabo exclusivamente por la Dirección o por quien ésta haya determinado. **CO.6-2:** Las áreas técnicas pueden realizar comunicaciones externas sólo si cuentan con autorización expresa de la Dirección o por quien ésta haya determinado.	**CO.6-3:** Se ha comunicado quién es el vocero designado y a través de qué canales debe ser contactado.	**CO.6-4:** Se ha definido y documentado un plan y/o procedimiento de comunicaciones ante crisis que cubre la evaluación del evento, las notificaciones, nivel de comunicación requerido, mensajes, audiencia, interesados y monitoreo de las comunicaciones. **CO.6-5:** El plan y/o el procedimiento han sido difundidos entre todos los actores involucrados en la gestión de crisis y continuidad operativa.	**CO.6-7:** Se realizan auditorías internas para verificar el cumplimiento del plan y procedimiento de comunicaciones ante crisis.

Presidencia
Uruguay

agesic