agesic

Uruguay **Presidencia**

MARCO DE CIBERSEGURIDAD

Versión 4.1

SEGURIDAD DE LA INFORMACIÓN

Versión 4.1 – Noviembre 2019

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

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

1 Revisiones

Versión 1.0 (agosto 2016):

a. Versión inicial

Versión 2.0 (noviembre 2016):

a. Se realizan cambios menores de redacción.

Versión 3.0 (junio 2017):

a. Se realiza cambio de enfoque respecto al modelo de madurez propuesto en la versión 1.0

Versión 4.0 (enero 2018):

a. Se neutraliza los términos para que el Marco se adapte a cualquier organización, no solo a los organismos de la Administración central.

b. Se agrega referencias a la norma ISO/IEC 27799:2016.

c. En la subcategoría PR.PI-1 se elimina el requisito SO.8.

d. En la subcategoría ID.ER-4 se agrega el requisito CO.4.

e. En la subcategoría ID.GA-6 se agrega el requisito GA.1.

f. En la subcategoría DE.AE-4 se agrega el requisito SF.3 y se elimina el requisito GI.5.

g. En la subcategoría DE.MC-1 se agrega el requisito SF.3 y se elimina el requisito SO.7.

h. En la subcategoría RE.AN-1 se agrega el requisito GI.5.

i. En la subcategoría ID.GA-1 se agrega el requisito OR.5.

j. En la subcategoría DE.MC-5 se elimina el requisito OR.5.

k. El modelo de madurez se adecua para ajustarse a los requisitos. Las siguientes subcategorías han sufrido alguna modificación en la redacción sus niveles: ID.GA-1, ID.GA-2, ID.GA-5, ID.AN-3, ID.AN-5, ID.GO-3, ID.ER-1, PR.CA-1, PR.CA-2, PR.CA-5, PR.CF-1, PR.CF-4, PR.CF-5, PR.SD-2, PR.SD-3, PR.SD-4, PR.SD-6, PR.PI-9, PR.PI-11, PR.PI-12, PR.TP-1, PR.TP-2, DE.AE-4, RE.PR-1, RE.CO-1, RE.CO-4, RE.AN-2, RE.MI-1, RC.PR-1, RC.CO-1

   Las modificaciones realizadas no cambian las valoraciones preexistentes.

Versión 4.1 (noviembre 2019):

a. Se elimina la norma ISO 27799:2016, de que los controles en ella mencionada se mapean uno a uno con la norma ISO/IEC 27001:13

b. Se incluyen los controles referentes a todos los estándares mencionados en el CSF de NIST.

c. Se agregó la nueva categoría “Cadena de Suministro” en la función Identificar.

d. Se agregaron dos nuevas Sub categorías PR.CA-6 y PR.CA-7 a la categoría “Control de Acceso” en la función Proteger.

e. Se agregó una nueva Sub categorías PR.SD-8 a la categoría “Control de Acceso” en la función Proteger.

f. Se agregó una nueva Sub categorías PR.TP-5 a la categoría “Tecnología de Protección” en la función Proteger.

g. Se agregó una nueva Sub categorías RE.AN-5 a la categoría “Análisis” en la función Responder.

h. Se revisan y adecuan los requisitos asociados en cada una de las subcategorías.

i. Se revisan y adecuan las prioridades asignadas a los perfiles de organización.

j. Se incorporan los modelos de madurez referidos a las nuevas subcategorías y a las subcategorías que en la versión 4.0 tenían prioridad P4.

k. Se ajusta redacción del modelo de madurez para la subcategoría: ID.ER-3, PR.PI-10, PR.SD-2, PR.PI-9, RE.MI-1, RC.CO-1.

2 Introducción

El uso de las Tecnologías de la Información y la Comunicación 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 2009, en el marco de la estrategia relacionada a la seguridad de la información y protección de los activos críticos del Estado, se publicaron dos decretos que establecen el marco de seguridad de la información en la Administración Central, exhortando la adopción de las disposiciones establecidas también por parte de los Gobiernos Departamentales, los Entes Autónomos, los Servicios Descentralizados y, en general, a todos los órganos del Estado:

- Decreto 451/009: regula el funcionamiento y organización del CERTuy[1].
- Decreto 452/009: regula la adopción de una política de seguridad de la información para organismos de la Administración Pública.

En esta línea, y reforzando los esfuerzos ya realizados, es que en 2014 se aprobó el decreto 92/014 referente a ciberseguridad, con el objetivo de mejorar la seguridad de la información y las infraestructuras tecnológicas que le dan soporte.

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.

Continuando con los esfuerzos para mejorar las estrategias en ciberseguridad en Uruguay, en agosto de 2016 se lanza el Marco de Ciberseguridad, cuyo principal objetivo es dar lineamientos y buenas prácticas para un abordaje integral de la ciberseguridad.

[1] CERTuy - Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay (www.cert.uy)

3 Objetivo y alcance

El objetivo de este documento es presentar un Marco de Ciberseguridad organizado y con referencias a estándares internacionales que contemplan la normativa nacional. Está basado en el Marco de Ciberseguridad definido por el Instituto Nacional de Estándares y Tecnología (NIST[2] CSF) para la mejora de la ciberseguridad en infraestructuras críticas, y contextualizado a las organizaciones que requieren:

- Gestionar los riesgos inherentes a la seguridad de la información y al uso de la infraestructura tecnológica que le da soporte.
- Adoptar en forma urgente una política de gestión de seguridad de la información.
- Contar con una política de gestión de incidentes.
- Adoptar las medidas necesarias para lograr centros de datos seguros.
- Cumplir con la normativa vigente en materia de seguridad de la información: decretos 451/009, 452/009, 92/014 y leyes N°18331, N°18381, entre otras.

El Marco provee un enfoque homogéneo para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información. Se encuentra alineado con las mejores prácticas internacionales, como ISO/IEC 27001:2013[3], COBIT 5[4] para Seguridad de la Información, NIST SP 800-53 rev.4 entre otros. Ha sido contextualizado teniendo en cuenta la normativa vigente y las mejores prácticas sugeridas por Agesic.

Se toma como referencia el marco definido por NIST con el cometido de que las respuestas a las amenazas cibernéticas, la gestión de los riesgos y la gestión de la seguridad de la información estén alineadas al nivel de estándares internacionales. Esto permite a las organizaciones alinear sus procesos de gestión de seguridad informática a nivel internacional en forma práctica y estableciendo objetivos claros. Cabe aclarar que el marco es flexible y adaptable a diferentes realidades e industrias y no solamente es utilizable en entornos de infraestructuras críticas.

El Marco puede ayudar a una organización a planificar su estrategia de gestión de riesgos de ciberseguridad y desarrollarla a lo largo del tiempo en función de su actividad, tamaño y otras características distintivas y elementos específicos. No es un documento estático, sino que se irá modificando de acuerdo a los cambios tecnológicos, la evolución de las amenazas y los cambios en las técnicas de gestión de riesgos.

[2] NIST - National Institute of Standards and Technology (www.nist.gov)

[3] International Organization for Standarization / International Electrotechnical Commission (http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)

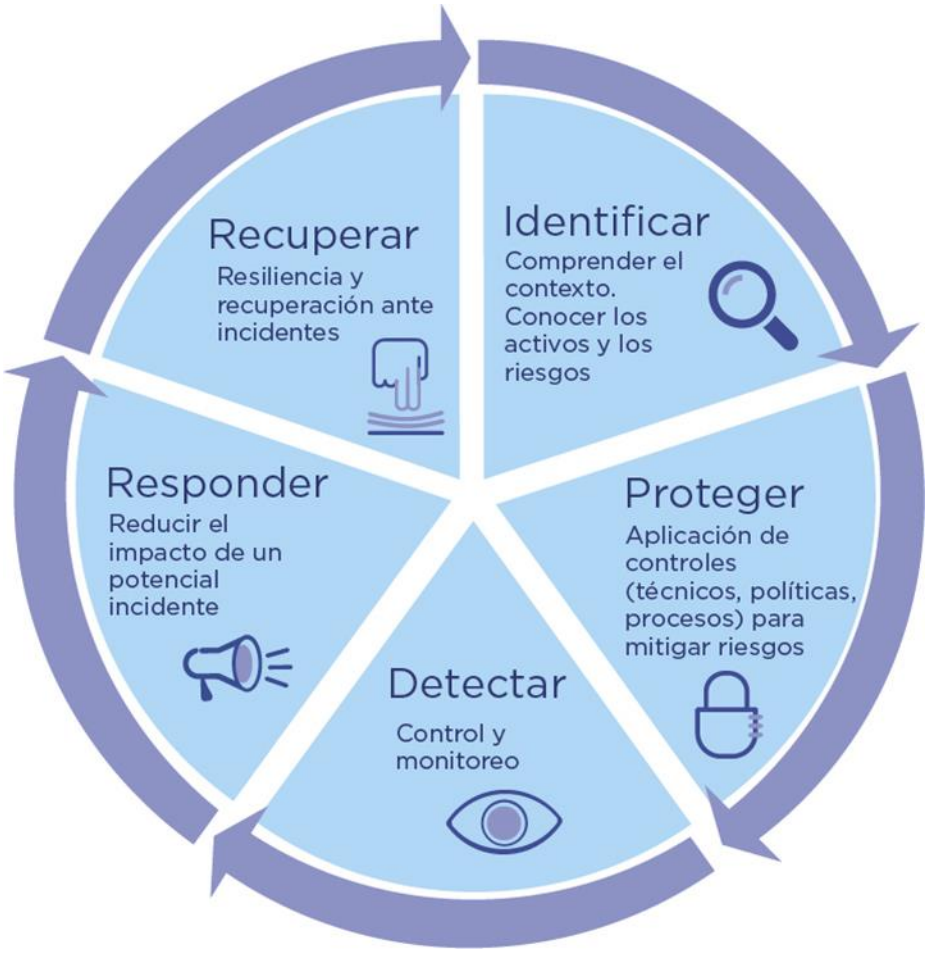
[4] Control Objectives for Information and related Technology (http://www.isaca.org/cobit/pages/default.aspx)

4 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 norma ISO/IEC 27001:2013, la normativa vigente y las mejores prácticas internacionales en materia de seguridad de la información.

4.1 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.

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; Ambiente del negocio; Gobernanza; Evaluación de riesgos y Estrategia para la gestión de riesgos.

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: Control de acceso; Concientización y formación; Seguridad de los datos; Procesos y procedimientos para la protección de la información; Mantenimiento y Tecnología de protección.

Detectar

Está vinculada a 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: Anomalías y eventos; Monitoreo continuo de la seguridad; Procesos de detección.

Responder

Está vinculada a 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: Planificación de la respuesta; Comunicaciones; Análisis; Mitigación; Mejoras.

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: Planificación de la recuperación; Mejoras y Comunicaciones.

4.2 Estructura del Marco de Ciberseguridad

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

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

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: “Gestión de activos”, “Evaluación de riesgos”, “Mantenimiento”.

Subcategoría

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

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:

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

Modelo de Madurez

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

El modelo de madurez está definido para las subcategorías que tengan prioridad P1 en alguno de los perfiles establecidos. En cada perfil se analiza el modelo de madurez para las subcategorías que tengan prioridad P1.

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

Los niveles de madurez en cada subcategoría serán descritos 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.

Referencias

En esta columna se transcriben todas las referencias mencionadas el Marco de Ciberseguridad de NIST para cada subcategoría.

Tal como se menciona en el CSF NIST, la información sobre las referencias informativas descritas aquí, se pueden encontrar en los siguientes enlaces:

- Control Objectives for Information and Related Technology, (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx.
- CIS Critical Security Controls for Effective Cyber Defense, (CIS Controls): https://www.cisecurity.org.
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731.
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785.
- ISO/IEC 27001, *Information technology -Security techniques -Information security management systems -Requirements*: https://www.iso.org/standard/54534.html.
- NIST SP 800-53 Rev. 4-NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, abril de 2013 (incluidas las actualizaciones al 22 de enero de 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Las referencias informativas solo se asignan al nivel de control, aunque cualquier mejora de control posiblemente puede resultar útil para lograr un resultado de subcategoría.

Las Referencias no son exhaustivas, es decir que no todos los elementos (por ejemplo, control, requisitos) de una Referencia dada se asignan a las Subcategorías del Marco de trabajo.

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.

5 Marco de Ciberseguridad

5.1 Función: IDENTIFICAR (ID)

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
	B	E	A		
ID.GA Gestión de activos Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.					
ID.GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	P 1	P 1	P 1	**COBIT 5** BAI09.01, BAI09.02 **CIS CSC** 1 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5	**GA.1** Identificar formalmente los activos de la organización junto con la definición de su responsable. **GA.3** Pautar el uso aceptable de los activos. **OR.5** Pautar el uso de dispositivos móviles.
ID.GA-2. Las plataformas de software y aplicaciones se encuentran inventariadas.	P 1	P 1	P 1	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5	**GA.1** Identificar formalmente los activos de la organización junto con la definición de su responsable. **GA.3** Pautar el uso aceptable de los activos. **CN.4** Gestionar las licencias de software.
ID.GA-3. Se utilizan medidas de seguridad y procedimientos de gestión para proteger y controlar el flujo de información interna y externa.	P 2	P 2	P 1	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8	**SC.14** Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización.
ID.GA-4. El equipamiento y los sistemas de información utilizados fuera de las instalaciones se encuentran identificados y se aplican medidas para mantener la seguridad de la información.	P 2	P 1	P 1	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9	**GA.3** Pautar el uso aceptable de los activos.

ID.GA-5. Los activos (por ejemplo: hardware, dispositivos, datos y software) se encuentran clasificados en función del tipo de información que contienen o procesan y en el valor que poseen para el negocio.	P 2	P 2	P 1	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6	**GA.2** Clasificar y proteger la información de acuerdo a la normativa y a los criterios de valoración definidos.
ID.GA-6. Los roles y responsabilidades de seguridad de la información y ciberseguridad se encuentran asignados.	P 1	P 1	P 1	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11	**OR.1** Designar un Responsable de la Seguridad de la Información. **OR.2** Conformar un Comité de Seguridad de la Información.
ID.AN. Ambiente del negocio La misión de la organización, sus objetivos, interesados y actividades son comprendidos y priorizados. Esta información es utilizada para informar a los recursos de ciberseguridad sobre responsabilidades y decisiones relacionadas a la gestión de riesgos.					
ID.AN-1. Se identifica y comunica el rol de la organización en la cadena de suministro.	N / A	N/ A	N / A	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12	-
ID.AN-2. El lugar que ocupa la organización en la infraestructura crítica y en su sector de industria se encuentra identificado y comunicado.	N / A	N/ A	N / A	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Cláusula 4.1 **NIST SP 800-53 Rev. 4** PM-8	-
ID.AN-3. Se establecen y se comunican las prioridades para la misión de la organización, sus objetivos y actividades.	P 1	P 1	P 1	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14	**PL.1** Establecer objetivos anuales con relación a la seguridad de la información.
ID.AN-4. Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	P 3	P 2	P 1	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14	**SF.2** Implementar controles ambientales en los centros de datos y áreas relacionadas. **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos. **SO.3** Gestionar la capacidad de los servicios y recursos que se encuentran operativos.
ID.AN-5. Se establecen requisitos de resiliencia para soportar la entrega de servicios críticos.	P 3	P 2	P 1	**COBIT 5** BAI03.02, SS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14	**CO.1** Contar con componentes redundantes que contribuyan al normal funcionamiento del centro 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. **CO.3** Establecer los medios necesarios para garantizar la continuidad de las operaciones. **CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres. **CO.5** Definir las ventanas de tiempo soportadas para la continuidad de las operaciones.
ID.GO. Gobernanza Las políticas, procedimientos y procesos para gestionar y monitorear los requisitos regulatorios, legales, ambientales y operativos de la organización, son comprendidos y se informa a las gerencias sobre los riesgos de ciberseguridad.					
ID.GO-1. La política de seguridad de la información se encuentra establecida.	P 1	P 1	P 1	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA 62443-2-1:2009** 4.3.2.6 **ISO/IEC 27001:2013** A.5.1.1 **NIST SP 800-53 Rev. 4**-1 controles de todas las familias de control de seguridad	**PS.1** Adoptar una Política de Seguridad de la Información.
ID.GO-2. Los roles y las responsabilidades de la seguridad de la información están coordinados y alineados con roles internos y socios externos.	P 1	P 1	P 1	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 **NIST SP 800-53 Rev. 4** PS-7, PM1, PM-2	**OR.1** Designar un Responsable de la Seguridad de la Información. **OR.2** Conformar un Comité de Seguridad de la Información.
ID.GO-3. Los requisitos legales y regulatorios sobre la ciberseguridad, incluyendo las obligaciones de privacidad, son comprendidos y se gestionan.	P 1	P 1	P 1	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NIST SP 800-53 Rev. 4**-1 controles de todas las familias de control de seguridad	**CN.1** Cumplir con los requisitos normativos. **SC.1** Los portales Web institucionales de los organismos de la Administración Central y sus dependencias deben identificarse con la extensión “gub.uy” y “mil.uy”, según corresponda. **SC.2** Los portales Web institucionales de Unidades Ejecutoras, aplicaciones, portales y sitios Web correspondientes a proyectos y programas, sitios promocionales y temáticos, incluyendo zonas restringidas de acceso mediante usuario y contraseña disponibles para ciudadanos y funcionarios del organismo (contenidos Web), deberán ser subdominios del dominio del inciso correspondiente. **SC.3** El portal del organismo jerarca deberá hacer referencia a todos los dominios y subdominios que se correspondan con todos los contenidos Web que le reporten. **SC.4** Los nombres de dominio del organismo o dependencias serán sus iniciales, su acrónimo, o el nombre con el cual se los conoce públicamente. Deberá justificarse que la denominación elegida sea la más representativa. **SC.5** La información de contacto de los responsables de los dominios y subdominios deberá ser comunicada a Agesic y actualizada en períodos de seis meses. **SC.7** Los servidores de correo electrónico (MTA) de dominios gubernamentales deben alojarse dentro del territorio nacional, y no se permite su

					implementación sobre tecnologías que no garanticen dicho requerimiento.
ID.GO-4. Construcción de procesos de gobernanza y administración de riesgos dirigidos a atender los problemas de ciberseguridad.	P 2	P 1	P 1	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC 27001:2013** Cláusula 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM9, PM10, PM-11	**GR.1** Adoptar una metodología de Evaluación de Riesgo alineada a las necesidades del SGSI. **PL.1** Establecer objetivos anuales con relación a la Seguridad de la Información.
ID.ER. Evaluación de riesgos La empresa comprende los riegos de ciberseguridad de sus operaciones, activos e individuos.					
ID.ER-1. Se identifican y documentan las vulnerabilidades de los activos.	P 2	P 2	P 1	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	**SO.1** Gestionar las vulnerabilidades técnicas. **CN.3** Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades.
ID.ER-2. Recepción de información sobre amenazas y vulnerabilidades por parte de grupos y fuentes especializadas.	P 2	P 2	P 1	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16	**OR.3** Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.
ID.ER-3. Identificación y documentación de las amenazas internas y externas.	P 1	P 1	P 1	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.
ID.ER-4. Identificación del impacto potencial en el negocio y la probabilidad de ocurrencia.	P 1	P 1	P 1	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI. **GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.
ID.ER-5. Las amenazas, vulnerabilidades, probabilidad de ocurrencia e impactos se utilizan para determinar el riesgo.	P 1	P 1	P 1	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.
ID.ER-6. Identificación y priorización de las respuestas a los riesgos.	P 2	P 1	P 1	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Cláusula 6.1.3	**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.

				NIST SP 800-53 Rev. 4 PM-4, PM-9	
ID.GR. Estrategia para la gestión de riesgos Se establecen las prioridades, restricciones, tolerancia al riesgo y supuestos de la organización y se utilizan para soportar las decisiones de los riesgos operacionales.					
ID.GR-1. Los procesos de gestión de riesgos se encuentran establecidos, gestionados y aprobados por todos los interesados de la organización.	P 3	P 1	P 1	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 4** PM-9	**GR.1** Adoptar una metodología de Evaluación de Riesgo alineada a las necesidades del SGSI.
ID.GR-2. Se determina y se expresa de forma clara la tolerancia al riesgo a nivel de toda la organización.	P 2	P 1	P 1	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** PM-9	**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.
ID.GR-3. La tolerancia al riesgo de la organización es determinada por su rol y pertenencia a la infraestructura crítica y por la evaluación de riesgos específicos del sector al que pertenece.	P 2	P 1	P 1	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11	**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.
ID.CS. Gestión de riesgos en la cadena de suministros Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.					
ID.CS-1. Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	P 1	P 1	P 1	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** SA-9, SA12, PM-9	**RP.1** Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos.
ID.CS-2. Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de	P 1	P 1	P 1	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2	**GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI.

evaluación de riesgos de la cadena de suministro cibernético.				**NIST SP 800-53 Rev. 4** RA2, RA-3, SA-12, SA-14, SA-15, PM-9	
ID.CS-3. Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	P 2	P 1	P 1	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9	**RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
ID.CS-4. Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	P 2	P 1	P 1	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12	**RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
ID.CS-5. Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	P 3	P 2	P 1	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR3, IR-4, IR6, IR8, IR-9	**CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres.

5.2 Función: Proteger (PR)

Subcategoría	Prioridad x Perfil	Referencias	Requisitos relacionados
PR.CA. Control de acceso El acceso a los activos e instalaciones se limita a usuarios, procesos o dispositivos, actividades y transacciones autorizadas.			

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
PR.CA-1. Las identidades y credenciales para usuarios y dispositivos autorizados son gestionadas.	P 1	P 1	P 1	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	**CA.1** Gestionar el acceso lógico. **CA.2** Revisar los privilegios de acceso lógico.
PR.CA-2. Se gestiona y protege el acceso físico a los activos.	P 1	P 1	P 1	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE8	**SF.1** Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas.
PR.CA-3. Gestión de acceso remoto.	P 2	P 1	P 1	**CIS CSC** 12 **COBIT 5** APO13.01, DSS01.04, DSS05.03 **ISA 62443-2-1:2009** 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15	**OR.6** Establecer controles para proteger la información a la que se accede de forma remota. **SC.6** Establecer acuerdos de no divulgación.
PR.CA-4. Gestión de permisos de acceso, incorporando los principios de menor privilegio y segregación de funciones.	P 1	P 1	P 1	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC14, AC16, AC24	**CA.1** Gestionar el acceso lógico.
PR.CA-5. Protección de la integridad de la red incorporando segregación cuando es apropiado.	P 2	P 2	P 1	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7	**SC.13** Debe existir segregación a nivel de servicios de información.

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
PR.CA-6. Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	P 1	P 1	P 1	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	**CA.1** Gestionar el acceso lógico.
PR.CA-7. Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	P 1	P 1	P 1	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC7, AC-8, AC9, AC-11, AC-12, AC-14, IA1, IA-2, IA-3, IA-4, IA5, IA-8, IA-9, IA-10, IA11	**CA.1** Gestionar el acceso lógico. **CN.1** Cumplir con los requisitos normativos.
PR.CF. Concientización y formación El personal de la organización y socios de negocios, reciben entrenamiento y concientización sobre seguridad de la información. Están adecuadamente entrenados para cumplir con sus obligaciones referentes a la seguridad de la información y alineados con las políticas, procedimientos y acuerdos existentes.					
PR.CF-1. Todos los usuarios se encuentran entrenados e informados.	P 1	P 2	P 1	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NIST SP 800-53 Rev. 4** AT-2, PM-13	**GH.2** Concientizar y formar en materia de seguridad de la información a todo el personal.
PR.CF-2. Los usuarios privilegiados comprenden sus roles y responsabilidades.	P 2	P 2	P 1	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, PM-13	**GH.2** Concientizar y formar en materia de seguridad de la información a todo el personal.
PR.CF-3. Interesados externos (proveedores, clientes, socios) comprenden sus roles y responsabilidades.	P 3	P 2	P 1	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16	**GH.2** Concientizar y formar en materia de seguridad de la información a todo el personal.
PR.CF-4. La gerencia ejecutiva comprende sus roles y responsabilidades.	P 1	P 1	P 1	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2	**GH.2** Concientizar y formar en materia de seguridad de la información a todo el personal.

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
				NIST SP 800-53 Rev. 4 AT-3, PM-13	
PR.CF-5. El personal de seguridad física y de seguridad de la información comprende sus roles y responsabilidades.	P 2	P 2	P 1	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM13	**GH.2** Concientizar y formar en materia de seguridad de la información a todo el personal.
PR.SD. Seguridad de los datos La información y registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.					
PR.SD-1. Los datos en reposo (inactivos) se encuentran protegidos.	P 2	P 2	P 1	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28	**SO.6** Respaldar la información y realizar pruebas de restauración periódicas. **CA.3** Establecer controles criptográficos. **CA.4** Establecer los controles para el uso de firma electrónica.
PR.SD-2. Los datos en tránsito se encuentran protegidos.	P 2	P 2	P 1	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12	**SC.14** Mantener la seguridad de la información durante su intercambio dentro o fuera de la organización. **CA.3** Establecer controles criptográficos. **CA.4** Establecer los controles para el uso de firma electrónica.
PR.SD-3. Los activos se gestionan formalmente a lo largo de la eliminación, las transferencias y disposición.	P 2	P 2	P 1	**CIS CSC 1** **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16	**GA.5** Establecer los mecanismos para destruir la información y medios de almacenamiento.
PR.SD-4. Se mantiene una adecuada capacidad para asegurar la disponibilidad.	P 3	P 3	P 1	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5	**SO.3** Gestionar la capacidad de los servicios que se encuentran operativos.
PR.SD-5. Se implementan medidas de protección contra fuga de datos.	P 2	P 1	P 1	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	**GH.1** Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las de la organización respecto a la seguridad de la información. **SC.6** Establecer acuerdos de no divulgación.

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
PR.SD-6. Se realizan chequeos de integridad para verificar software, firmware e integridad de la información.	P 1	P 1	P 1	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NIST SP 800-53 Rev. 4** SC-16, SI7	**SO.5** Controlar software malicioso. **SO.8** Gestionar la instalación de software.
PR.SD-7. Los entornos de desarrollo y pruebas están separados del entorno de producción.	P 2	P 2	P 1	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NIST SP 800-53 Rev. 4** CM-2	**SO.4** Definir entornos separados para desarrollo, pruebas y producción.
PR.SD-8. Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	P 3	P 2	P 1	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NIST SP 800-53 Rev. 4** SA-10, SI-7	**SF.2** Implementar controles ambientales en los centros de datos y áreas relacionadas. **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.
PR.PI. Procesos y procedimientos para la protección de la información Las políticas de seguridad, procesos y procedimientos se mantienen y son utilizados para gestionar la protección de los sistemas de información y los activos.					
PR.PI-1. Existe una línea base de la configuración de los sistemas de información que es mantenida.	P 3	P 3	P 1	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10	**SO.2** Gestionar formalmente los cambios.
PR.PI-2. Se implementa el ciclo de vida de desarrollo para gestionar los sistemas.	P 2	P 2	P 1	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA8, SA-10, SA-11, SA12, SA-15, SA-17, SI-12, SI-13, SI14, SI-16, SI17	**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.
PR.PI-3. Existen procesos de gestión del cambio en las configuraciones.	P 2	P 2	P 1	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10	**SO.2** Gestionar formalmente los cambios. **SO.8** Gestionar la instalación de software.

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
PR.PI-4. Se realizan y mantienen respaldos de la información y se testean periódicamente.	P 1	P 1	P 1	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9	**SO.6** Respaldar la información y realizar pruebas de restauración periódicas.
PR.PI-5. Las políticas y reglamentos relacionados con el medio ambiente físico operativo se cumplen.	P 2	P 2	P 1	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE13, PE-14, PE-15, PE-18	**SF.2** Implementar controles ambientales en los centros de datos y áreas relacionadas. **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.
PR.PI-6. Los datos son eliminados de acuerdo a las políticas de seguridad.	P 2	P 2	P 1	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NIST SP 800-53 Rev. 4** MP-6	**GA.5** Establecer los mecanismos para destruir la información y medios de almacenamiento.
PR.PI-7. Existe mejora continua de los procesos de protección.	P 3	P 2	P 1	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 9, Cláusula 10 **NIST SP 800-53 Rev. 4** CA2, CA-7, CP-2, IR8, PL-2, PM-6	**PL.2** Revisión periódica y mejora continua del SGSI.
PR.PI-8. La eficacia de las tecnologías de protección se comparten con las partes apropiadas.	P 3	P 2	P 1	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA7, SI4	**GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.
PR.PI-9. Existen y se gestionan planes de respuesta a incidentes (respuesta a incidentes y continuidad del negocio) y planes de recuperación (recuperación de incidentes y recuperación de desastres).	P 2	P 2	P 1	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	**GI.1** Planificar la gestión de los 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. **GI.5** Responder ante incidentes de seguridad de la información. **CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres.
PR.PI-10. Los planes de respuesta y recuperación se testean regularmente.	P 3	P 2	P 1	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NIST SP 800-53 Rev. 4** CP-4, IR3, PM-14	**CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres. **GI.5** Responder ante incidentes de seguridad de la información.
PR.PI-11. La ciberseguridad se encuentra incluida en las prácticas de RRHH.	P 2	P 2	P 1	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05	**SC.6** Establecer acuerdos de no divulgación. **GH.1** Establecer acuerdos contractuales con el personal donde figuren sus responsabilidades y las

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
				ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NIST SP 800-53 Rev. 4** PS-1, PS2, PS-3, PS-4, PS-5, PS6, PS7, PS-8, SA-21	de la organización respecto a la seguridad de la información.
PR.PI-12. Existe un plan de gestión de vulnerabilidades.	P 2	P 2	P 1	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NIST SP 800-53 Rev. 4** RA3, RA-5, SI-2	**SO.1** Gestionar las vulnerabilidades técnicas. **CN.2** Realizar auditorías independientes de seguridad de la información.
PR.MA. Mantenimiento El mantenimiento y las reparaciones de los componentes de los sistemas de información y de control industrial se lleva a cabo en consonancia con las políticas y procedimientos.					
PR.MA-1. El mantenimiento y la reparación de los activos de la organización se lleva a cabo y es registrado en forma oportuna con herramientas aprobadas y controladas.	P 3	P 2	P 1	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NIST SP 800-53 Rev. 4** MA-2, MA3, MA-5, MA-6	**SF.1** Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas. **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.
PR.MA-2. El mantenimiento a distancia de los activos de la organización se aprueba, registra y lleva a cabo de forma tal que se impide el acceso no autorizado.	P 3	P 2	P 1	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NIST SP 800-53 Rev. 4** MA-4	**SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
PR.TP. Tecnología de protección Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y resistencia de los sistemas y activos de la organización, en consonancia con las políticas, procedimientos y acuerdos.					
PR.TP-1. Los registros de auditoría (logs) se documentan, implementan y se revisan de conformidad con la política.	P 2	P 2	P 1	**CIS CSC** 1, 3, 5, 6, 14, 15, 16 **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 **NIST SP 800-53 Rev. 4** Familia AU	**SO.7** Registrar y monitorear los eventos de los sistemas.
PR.TP-2. Los medios extraíbles se encuentran protegidos y su uso se encuentra	P 3	P 3	P 1	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3	**GA.4** Gestionar los medios de almacenamiento.

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
restringido de acuerdo con las políticas.				**ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NIST SP 80053 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8	
PR.TP-3. El acceso a los sistemas y activos se controla incorporando el principio de menor privilegio.	P 1	P 1	P 1	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NIST SP 80053 Rev. 4** AC-3, CM-7	**CA.1** Gestionar el acceso lógico.
PR.TP-4. Las redes y comunicaciones se encuentran protegidas.	P 1	P 1	P 1	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NIST SP 800-53 Rev. 4** AC-4, AC17, AC18, CP8, SC7, SC-19, SC-20, SC-21, SC-22, SC-23, SC24, SC-25, SC29, SC-32, SC-36, SC-37, SC38, SC39, SC-40, SC-41, SC-43	**SC.8** Garantizar que los correos electrónicos en tránsito entre dos MTAs, o entre un MUA y un MTA, no comprometa la confidencialidad de la información cuando esto sea posible. **SC.9** La implementación de canales de comunicación cifrados entre MTA de dominios gubernamentales es obligatoria y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales deberán interrumpir el intento de entrega o recepción de mensajes si este canal cifrado no se puede negociar. **SC.10** La implementación de canales de comunicación cifrados con protocolos seguros entre MTA de dominios gubernamentales y un MTA de terceros deberá ser el método preferido de comunicación. Cuando el establecimiento de estos canales cifrados no sea posible, se podrá establecer un canal en texto claro. **SC.11** La implementación de canales de comunicación cifrados entre MUA y MTA de dominios gubernamentales es mandatoria, y deberá implementarse utilizando protocolos seguros. Los MTA de dominios gubernamentales no deberán aceptar la descarga o entrega de correos por parte de MUA si este canal cifrado no se puede negociar. Los MTA no deberán aceptar la descarga o consulta de correos electrónicos sobre canales en texto claro. **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.15** Todo sitio Web que contenga u oficie de enlace a un trámite en línea debe tener un firewall

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
					de aplicación Web (Web Application Firewall - WAF).
PR.TP-5. Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	P 3	P 2	P 1	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 **NIST SP 80053 Rev. 4** CP7, CP-8, CP-11, CP-13, PL-8, SA14, SC-6	**CO.2** Los sistemas críticos de la infraestructura de telecomunicaciones, como el cableado, routers y switches (LAN, SAN, etc.), deben contar con redundancia.

5.3 Función: DETECTAR (DE)

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
DE.AE. Anomalías y eventos La actividad anómala se detecta de forma oportuna y el potencial impacto de los eventos es comprendido.					
DE.AE-1. Se establece y gestiona una línea base de operaciones de red y flujos de datos esperados para usuarios y sistemas.	P 3	P 3	P 2	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4	**SO.7** Registrar y monitorear los eventos de los sistemas.

DE.AE-2. Los eventos detectados son analizados para entender los objetivos y métodos de ataque.	P 2	P 2	P 1	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4	**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. **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).
DE.AE-3. Los datos de los eventos se agrupan y correlacionan desde múltiples fuentes y sensores.	P 3	P 2	P 1	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4	**SO.7** Registrar y monitorear los eventos de los sistemas.
DE.AE-4. Se determina el impacto de los eventos.	P 3	P 2	P 1	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR4, RA-3, SI-4	**GI.1** Planificar la gestión de los incidentes de seguridad de la información. **GR.2** Realizar de manera sistemática el proceso de evaluación de riesgos del SGSI. **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.
DE.AE-5. Se establecen los umbrales de alerta de incidentes.	P 3	P 2	P 1	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** IR4, IR-5, IR-8	**GI.1** Planificar la gestión de los incidentes de seguridad de la información. **GI.5** Responder ante incidentes de seguridad de la información. **SO.7** Registrar y monitorear los eventos de los sistemas.
DE.MC. Monitoreo continuo de la seguridad Los sistemas de información y los activos son monitoreados a intervalos discretos para identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.					
DE.MC-1. Se monitorea la red para detectar potenciales eventos de ciberseguridad.	P 2	P 2	P 1	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM3, SC5, SC-7, SI-4	**SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.
DE.MC-2. Se monitorea el ambiente físico para detectar potenciales eventos de ciberseguridad.	P 2	P 2	P 1	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NIST SP 80053 Rev. 4** CA-7, PE-3, PE-6, PE-20	**SF.1** Implementar controles de acceso físico a las instalaciones y equipos ubicados en los centros de datos y áreas relacionadas. **SF.3** Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas en componentes críticos.
DE.MC-3. Se monitorea la actividad del personal para detectar potenciales eventos de ciberseguridad.	P 2	P 2	P 1	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NIST SP 80053 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM10, CM-11	**SO.7** Registrar y monitorear los eventos de los sistemas.
DE.MC-4. Se detecta el código malicioso.	P 1	P 1	P 1	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1	**SO.5** Controlar software malicioso.

				NIST SP 80053 Rev. 4 SI3, SI8	
DE.MC-5. Se detecta el código móvil no autorizado.	P 3	P 3	P 2	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NIST SP 80053 Rev. 4 SC**18, SI-4, SC-44	**SO.8** Gestionar la instalación de software.
DE.MC-6. Se controla la actividad de los proveedores de servicios externos para detectar posibles eventos de ciberseguridad.	P 2	P 1	P 1	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA- 9, SI-4	**RP.1** Definir acuerdos de niveles de servicio (SLA) con los proveedores de servicios críticos. **RP.2** Establecer pautas, realizar seguimiento y revisión de los servicios de los proveedores, y gestionar sus cambios.
DE.MC-7. Se realiza monitoreo para personas, conexiones, dispositivos y software.	P 2	P 2	P 1	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NIST SP 80053 Rev. 4** AU-12, CA-7, CM-3, CM8, PE-3, PE-6, PE-20, SI-4	**SO.7** Registrar y monitorear los eventos de los sistemas.
DE.MC-8. Se realizan escaneos de vulnerabilidades.	P 2	P 2	P 1	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 80053 Rev. 4** RA-5	**CN.3** Revisar regularmente los sistemas de información mediante pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades.
DE.PD. Procesos de detección Se mantienen procesos, procedimientos de detección y prueba para asegurar el conocimiento oportuno y adecuado de los eventos anómalos.					
DE.PD-1. Los roles y las responsabilidades de detección se encuentran definidos para asegurar responsabilidades.	P 2	P 2	P 1	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NIST SP 80053 Rev. 4** CA-2, CA7, PM-14	**SO.7** Registrar y monitorear los eventos de los sistemas.
DE.PD-2. Las actividades de detección cumplen con todos los requisitos aplicables.	P 3	P 2	P 1	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NIST SP 80053 Rev. 4** AC-25, CA-2, CA7, SA-18, SI4, PM-1	**CN.1** Cumplir con los requisitos normativos.
DE.PD-3 Los procesos de detección son probados.	P 3	P 2	P 1	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NIST SP 80053 Rev. 4** CA-2, CA7, PE3, SI3, SI-4, PM-14	**AD.1** Incluir requisitos de seguridad de la información durante todo el ciclo de vida de los proyectos de desarrollo o adquisiciones de software.
DE.PD-4. La información de la detección de eventos es comunicada a las partes pertinentes.	P 2	P 2	P 1	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NIST SP 80053 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4	**OR.3** Definir los para el contacto formal con autoridades y equipo de respuesta. **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.3** Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy o equipo de respuesta externo correspondiente.

					GI.4 Registrar y reportar las violaciones a la seguridad de la información, confirmadas o sospechadas de acuerdo a los procedimientos correspondientes. **SO.7** Registrar y monitorear los eventos de los sistemas.
DE.PD-5. Los procesos de detección son mejorados continuamente.	P 3	P 2	P 2	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 80053 Rev. 4**, CA-2, CA-7, PL-2, RA5, SI4, PM-14	**GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.

5.4 Función: RESPONDER (RE)

RE.PR. Planificación de la respuesta Los procesos y procedimientos de respuesta se ejecutan y se mantienen garantizando una respuesta oportuna para detectar eventos de ciberseguridad.					
RE.PR-1. El plan de respuesta se ejecuta durante o luego de un evento.	P 2	P 1	P 1	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8	**GI.5** Responder ante incidentes de seguridad de la información.
RE.CO. Comunicaciones Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según corresponda.					
RE.CO-1. El personal conoce sus roles y el orden de operaciones cuando es necesaria una respuesta.	P 2	P 1	P 1	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR3, IR-8	**GH.2** Concientizar y formar en materia de seguridad de la información a todo el personal. **GI.1** Planificar la gestión de los incidentes de seguridad de la información. **GI.3** Informar de forma completa e inmediata la existencia de un potencial incidente de seguridad informática al CERTuy o equipo de respuesta externo correspondiente. **GI.5** Responder ante incidentes de seguridad de la información.
RE.CO-2. Los eventos son reportados consistentemente con los criterios establecidos.	P 2	P 2	P 1	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR8	**OR.3** Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta. **GI.1** Planificar la gestión de los 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.
RE.CO-3. La información se comparte consistentemente	P 2	P 1	P 1	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Cláusula 7.4, Cláusula 16.1.2	**GI.5** Responder ante incidentes de seguridad de la información.

con los planes de respuesta.				**NIST SP 800-53 Rev. 4** CA2, CA-7, CP-2, IR4, IR-8, PE6, RA-5, SI-4	
RE.CO-4. La coordinación con las partes interesadas se realiza consistentemente con los planes de respuesta.	P 2	P 1	P 1	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR4, IR-8	**OR.3** Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta. **GI.1** Planificar la gestión de los incidentes de seguridad de la información. **GI.5** Responder ante incidentes de seguridad de la información.
RE.CO-5. Se realiza intercambio de información voluntaria con partes interesadas externas para alcanzar una conciencia de ciberseguridad más amplia.	P 3	P 1	P 1	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15	**OR.3** Definir los mecanismos para el contacto formal con autoridades y equipo de respuesta.
RE.AN. Análisis Se efectúa análisis para asegurar una respuesta adecuada y dar soporte a las actividades de recuperación.					
RE.AN-1. Se investigan las notificaciones de los sistemas de detección.	P 2	P 2	P 1	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	**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. **SO.7** Registrar y monitorear los eventos de los sistemas.
RE.AN-2. El impacto del incidente es comprendido.	P 2	P 1	P 1	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NIST SP 800-53 Rev. 4** CP-2, IR4	**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.
RE.AN-3. Se realiza análisis forense.	P 2	P 1	P 1	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NIST SP 800-53 Rev. 4** AU-7, IR-4	**GI.5** Responder ante incidentes de seguridad de la información.
RE.AN-4. Los incidentes son categorizados consistentemente con los planes de respuesta.	P 2	P 2	P 1	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NIST SP 800-53 Rev. 4** CP-2, IR4, IR-5, IR-8	**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.
RE-AN-5. Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o	P 2	P 1	P 1	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15	**GI.5** Responder ante incidentes de seguridad de la información.

investigadores de seguridad).					
RE.MI. Mitigación Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.					
RE.MI-1. Se logra contener los incidentes.	P 2	P 1	P 1	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR4	**GI.5** Responder ante incidentes de seguridad de la información.
RE.MI-2. Se logra mitigar los incidentes.	P 2	P 1	P 1	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NIST SP 800-53 Rev. 4** IR4	**GI.5** Responder ante incidentes de seguridad de la información.
RE.MI-3. Las nuevas vulnerabilidades identificadas se mitigan o documentan como riesgos aceptados.	P 2	P 2	P 1	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA7, RA-3, RA-5	**SO.1** Gestionar las vulnerabilidades técnicas.
RE.ME. Mejoras Las actividades de respuesta de la organización son mejoradas por la incorporación de lecciones aprendidas de las actividades de detección y respuesta actuales y anteriores.					
RE.ME-1. Los planes de respuesta incorporan lecciones aprendidas.	P 3	P 2	P 1	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR4, IR-8	**GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.
RE.ME-2. Las estrategias de respuesta se actualizan.	P 2	P 1	P 1	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR4, IR-8	**GI.5** Responder ante incidentes de seguridad de la información.

5.5 Función: RECUPERAR (RC)

Subcategoría	Prioridad x Perfil	Referencias	Requisitos relacionados
RC.PR. Planificación de la recuperación Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad.			

Subcategoría	Prioridad x Perfil			Referencias	Requisitos relacionados
RC.PR-1. El plan de recuperación se ejecuta durante o luego de un evento.	P 2	P 1	P 1	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8	**GI.5** Responder ante incidentes de seguridad de la información. **GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos. **CO.4** Planificar la continuidad de las operaciones y recuperación ante desastres.
RC.ME. Mejoras Se mejoran los planes y procesos de recuperación incorporando las lecciones aprendidas en actividades futuras.					
RC.ME-1. Los planes de recuperación incorporan lecciones aprendidas.	P 3	P 2	P 1	**COBIT 5** APO12.06, BAI05.07, DSS04.08 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR4, IR-8	**GI.6** Establecer los mecanismos que le permitan a la organización aprender de los incidentes ocurridos.
RC.ME-2 Las estrategias de recuperación se actualizan.	P 2	P 1	P 1	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR4, IR-8	**PL.2** Revisión periódica y mejora continua del SGSI.
RC.CO. Comunicaciones Las actividades de recuperación se coordinan con las partes interesadas internas y externas, como centros de coordinación, proveedores de servicios de Internet, propietarios de los sistemas afectados, las víctimas, otros CSIRT y vendedores.					
RC.CO-1. Se gestionan las relaciones públicas.	P 3	P 2	P 1	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4	**CO.6** Definir los mecanismos de comunicación e interlocutores válidos.
RC.CO-2. Se repara la reputación luego del evento.	P 3	P 2	P 1	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Cláusula 7.4	**CO.6** Definir los mecanismos de comunicación e interlocutores válidos.
RC.CO-3. Se comunican las actividades de recuperación a los interesados internos y a los equipos ejecutivos y de gestión.	P 3	P 2	P 1	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR4	**CO.6** Definir los mecanismos de comunicación e interlocutores válidos.

6 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.

6.1 Función: IDENTIFICAR (ID)

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
ID.GA. Gestión de activos Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.				
ID.GA-1. Los dispositivos físicos y sistemas se encuentran inventariados.	Se confeccionan y mantienen inventarios de los dispositivos físicos (servidores, racks, dispositivos de networking, UPS, etc.) del centro de datos.	Se incluyen en el inventario los dispositivos físicos (PC, almacenamiento extraíble, dispositivos de networking, impresoras, otro tipo de equipamiento utilizado, etc.) y sistemas de otras áreas de la organización.	Los procesos y procedimientos de actualización de inventario se encuentran documentados y están basados en software de inventario. Se automatiza el proceso cuando esto es posible.	Se realizan actividades periódicas de control interno para verificar el cumplimiento y alineación con los procedimientos establecidos.
ID.GA-2. Las plataformas de software y aplicaciones se encuentran inventariadas.	Se confeccionan y mantienen inventarios de software de base y software de aplicación del centro de datos.	Se incluyen en el inventario las plataformas de software y aplicaciones de otras áreas de la organización. Se lleva control del licenciamiento de software de equipos servidores.	Ver ID.GA-1 (nivel 3) Además, se lleva control del licenciamiento de software de equipos personales.	Ver ID.GA-1 (nivel 4)

ID.GA-3 Se utilizan medidas de seguridad y procedimientos de gestión para proteger y controlar el flujo de información interna y externa.	Ver PR.SD-2 (nivel 1)	Ver PR.SD-2 (nivel 2)	Ver PR.SD-2 (nivel 3)	Ver PR.SD-2 (nivel 4)
ID.GA-4. El equipamiento y los sistemas de información utilizados fuera de las instalaciones se encuentran identificados y se aplican medidas para mantener la seguridad de la información.	Los equipos portátiles y móviles de la organización que serán usados fuera de las instalaciones se encuentran inventariados, así como las aplicaciones y sistemas instalados en dichos dispositivos. Estos activos cuentan con al menos un factor de autenticación para acceder a la información. Los equipos móviles cuentan con un sistema de borrado del dispositivo en caso extravió o robo. Los equipos portátiles cuentan con medidas mínimas de protección física (como por ejemplo linga de seguridad).	Los activos informáticos de la organización a los que acceden los usuarios cuentan con un responsable identificado. Se limita el almacenamiento de información sensible en el activo, o la misma cuenta con controles adicionales (por ejemplo, cifrado de la información).	Se han definido una política para el uso adecuado de los activos informáticos y de los sistemas de información que son usados fuera de las instalaciones de la organización. Se cuenta con un programa de capacitación a los usuarios que hacen uso de los activos. Se realiza un control periódico de los activos que contienen información sensible y existe un plan de respuesta en caso de pérdida o robo de los mismos. Los activos de información identificados como críticos son accedidos con doble factor de autenticación.	Las medidas de protección implementadas en los activos informáticos se monitorean de forma proactiva 7x24. Los sistemas de cifrado de los activos manejan clave única a nivel de la organización, además utilizan una clave de cifrado personal.
ID.GA-5. Los activos (por ejemplo: hardware, dispositivos, datos y software) se encuentran clasificados en función del tipo de información que contienen o procesan y en el valor que poseen para el negocio.	Se identifican los activos (servidores, PC, dispositivos móviles o de almacenamiento) que contienen la información más crítica de la organización.	Se clasifican los activos de acuerdo a los criterios de clasificación de la información establecidos (alineados a la normativa vigente) y a la valoración de esta.	Ver ID.GA-1 (nivel 3) Además, el software de inventario gestiona la clasificación de la información contenida en los activos.	La clasificación de la información es parte integral de la gestión de los activos. Se realizan actividades periódicas de control interno, o cuando el negocio así lo requiere, para verificar que el inventario de activos se encuentra clasificado y actualizado.
ID.GA-6. Los roles y responsabilidades de seguridad de la	Se ha designado al RSI y al CSI. Se definen los propietarios de los activos, los cuales	El CSI sesiona periódicamente y se registran las reuniones.	Se definen formalmente y documentan las responsabilidades del RSI y del CSI.	Se realizan actividades de control interno para verificar la segregación de roles en conflicto y

información y ciberseguridad se encuentran asignados.	son responsables por su protección.		Se definen otros roles y responsabilidades de seguridad de la información que incluyen, por ejemplo, responsable por la gestión de riesgos de seguridad, responsable de la gestión de incidentes, responsable de la gestión de vulnerabilidades y parches, responsable de monitoreo, entre otros. Los roles y responsabilidades se encuentran documentados.	áreas de responsabilidad. El resultado de estas actividades es comunicado al RSI y demás interesados.
ID.AN. Ambiente del negocio La misión de la organización, sus objetivos, interesados y actividades son comprendidos y priorizados; esta información es utilizada para informar a los roles de ciberseguridad sobre responsabilidades y decisiones relacionadas a la gestión de riesgos.				
ID.AN-3. Se establecen y se comunican las prioridades para la misión de la organización, sus objetivos y actividades.	Se establecen objetivos anuales en relación con la seguridad de la información, documentados y discutidos a nivel del CSI. Se establecen acciones para lograr el cumplimiento de los objetivos.	Los objetivos de seguridad de la información se llevan a cabo mediante un plan de acción.	Se difunden los objetivos anuales de seguridad de la información al personal y/o partes interesadas. Se trabaja en el plan de acción de forma articulada con actores de la organización para cumplir con los objetivos.	Los objetivos de seguridad de la información se llevan a cabo mediante proyectos formales de seguridad de la información. Se define una estrategia de seguridad de la información y ciberseguridad alineada a la estrategia a mediano-largo plazo y ésta es difundida.
ID.AN-4. Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	Se identifican los servicios críticos de la organización y cuáles son los componentes prioritarios del centro de datos para la entrega de los mismos. Se define el tratamiento proactivo para atender eventos e incidentes de ciberseguridad.	Se identifican las dependencias de los componentes prioritarios y se establecen planes de mantenimiento para los mismos. Se determina los niveles de capacidad mínima para poder garantizar la entrega de los servicios críticos. Se realiza gestión de capacidad.	Se documentan, aprueban y gestionan los cambios en los componentes prioritarios y sus dependencias (actualización, mantenimiento y reemplazo) vinculados a los servicios críticos. Se realizan las notificaciones pertinentes a todas	Se documenta y prioriza el manejo de los servicios críticos de toda la infraestructura tecnológica, haciendo énfasis en los componentes prioritarios para el funcionamiento de la organización, los cuales son monitoreados de manera automatizada.

			las partes interesadas. Periódicamente se valida y formaliza la gestión de capacidad y forma parte de la gobernanza de ciberseguridad.	Se envían alertas del estado de los componentes ante los cambios de entorno. Se realiza una gestión de capacidad a largo plazo (más de 3 años).
ID.AN-5. Se establecen requisitos de resiliencia para soportar la entrega de servicios críticos.	El centro de datos cuenta con UPS y componentes redundantes en lo que refiere a conexión eléctrica, componentes de acondicionamiento térmico e infraestructura de comunicaciones.	Se han definido las ventanas de tiempo máximo soportadas por el negocio sin poder operar. El centro de datos cuenta con generador eléctrico capaz de alimentar a todos los componentes críticos. La Dirección apoya la planificación de la contingencia, por ejemplo, facilitando la participación de recursos humanos y proveyendo los recursos materiales necesarios.	Se cuenta con un plan de contingencia y recuperación aprobado por la Dirección. Su alcance está asociado al menos a los procesos críticos de la organización. Se comienzan las pruebas del plan para uno o varios de los procesos críticos.	Se definen y ejecutan pruebas al plan de contingencia y recuperación. Todos los involucrados están interiorizados en el plan y su ejecución. Las pruebas son tomadas como insumo para las lecciones aprendidas y retroalimentan la toma de decisiones.
ID.GO. Gobernanza Las políticas, procedimientos y procesos para gestionar y monitorear los requisitos regulatorios, legales, ambientales y operativos de la organización, son comprendidos y se informa a las gerencias sobre los riesgos de ciberseguridad.				
ID.GO-1. La política de seguridad de la información se encuentra establecida.	Se cuenta con una política de seguridad de la información aprobada por la Dirección. La política de seguridad de la información se difunde al personal.	Se definen formalmente políticas sobre temas específicos que dan soporte a la política de seguridad de la información.	La política de seguridad de la información y las políticas específicas son revisadas cuando ocurren cambios significativos (ambiente de negocio, ambiente técnico, normativa, etc.) para analizar su vigencia, idoneidad y pertinencia, siendo deseable que las mismas sean revisadas formalmente a intervalos regulares. El resultado de	Se ha desarrollado un conjunto razonable de políticas y procedimientos específicos alineados al Marco de Ciberseguridad y a la guía de implementación conformando un SGSI. Se definen indicadores para medir la efectividad del SGSI y se planifica y realiza la revisión formal de éste por parte del CSI.

			estas revisiones de documentan y comunican al CSI y demás partes interesadas.	
ID.GO-2. Los roles y las responsabilidades de la seguridad de la información están coordinados y alineados con roles internos y socios externos.	El RSI coordina las actividades de seguridad de la información de su organización.	El RSI es referente de la temática ante su organización y participa en la gestión de incidentes y la gestión de riesgos de seguridad. El RSI, o quien este determine, oficia como punto de contacto con el CERTuy o CSIRT según corresponda.	El RSI, o quien este determine, coordina las tareas de gestión de riesgos con los responsables de gestión de riesgos de seguridad y con los propietarios de los activos de información.	El RSI coordina las actividades del plan anual (las cuales se documentan) con los principales actores involucrados de su organización (directores de área, gerentes, otros RSI, etc.).
ID.GO-3. Los requisitos legales y regulatorios sobre la ciberseguridad, incluyendo las obligaciones de privacidad son comprendidos y se gestionan.	Se identifican los requisitos normativos relacionados a seguridad de la información y ciberseguridad, protección de datos personales, acceso a la información pública y propiedad intelectual.	Las pautas que ha definido la organización relacionadas con seguridad de la información están alineadas o hacen referencia a la normativa vigente en la materia.	Se realizan revisiones basadas en la normativa aplicable para detectar desvíos de cumplimiento. El resultado es comunicado a la RSI y/o al CSI.	Se realizan actividades de control interno para verificar el cumplimiento del SGSI. Los resultados de las revisiones se utilizan para la mejora continua del SGSI y apoyan a la toma de decisiones.
ID.GO-4. Construcción de procesos de gobernanza y administración de riesgos dirigidos a atender los problemas de ciberseguridad.	El área responsable de del centro de datos realiza las actividades de gestión de riesgo para apoyar sus procesos en base a su experiencia y apreciación de la ciberseguridad.	Se establece un responsable de la gestión de riesgo, el cual se encarga de desarrollar una metodología unificada para la evaluación de riesgos de ciberseguridad de la organización. Los riesgos de ciberseguridad son evaluados para toda la organización. Se incorporan los actores críticos de cada área, que serán los encargados de implementar los controles definidos.	Se establece la política de gestión de riesgo. El proceso de gestión de riesgos se encuentra centralizado, por lo que se analiza de forma integral los riesgos de ciberseguridad (operativos, de negocio, etc.) de todas las áreas de la organización.	La gestión de riesgos está en línea con los objetivos de negocio. Se elaboran informes y reportes que sirven que permiten elaborar métricas e indicadores de cumplimiento de la organización, ayudando a reducir los efectos no deseados de los riesgos evaluados. Se retroalimenta el proceso con auditorías internas o externas que ayudan a evitar desviación en el proceso.
ID.ER. Evaluación de riesgos La organización comprende los riegos de ciberseguridad de sus operaciones, activos e individuos.				

ID.ER-1. Se identifican y documentan las vulnerabilidades de los activos.	El software de base y aplicaciones críticas se encuentran actualizados y con los últimos parches que les correspondan. Se tienen identificados aquellos activos que por su tecnología no pueden ser actualizados, detallando los controles compensatorios implementados.	Se cuenta con un ambiente para pruebas de los parches previo a su puesta en producción. Se realizan pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades de los sistemas críticos de la organización. El resultado de las pruebas y el plan de acción se comunican a las partes interesadas.	Existe un procedimiento documentado y un responsable de la gestión de vulnerabilidades y parches. Las pruebas de intrusión (ethical hacking) y evaluación de vulnerabilidades de los sistemas críticos se realizan con una periodicidad establecida, alineada a las necesidades de la organización. Como mínimo se realiza un escaneo de vulnerabilidades semestral y una prueba de intrusión anual.	Se realizan auditorías independientes en forma periódica. Las mismas son tomadas como insumo para la toma de decisiones y la mejora continua del SGSI.
ID.ER-2. Recepción de información sobre amenazas y vulnerabilidades por parte de grupos y fuentes especializadas.	El personal de seguridad de la información y/o de TI se mantiene actualizado sobre las últimas amenazas y vulnerabilidades que surgen para sus sistemas y plataformas.	El personal de seguridad de la información y/o de TI recibe algún tipo de entrenamiento periódico sobre amenazas y vulnerabilidades.	Se ha definido un procedimiento documentado de contacto con autoridades internas y externas (contemplando especialmente los centros de respuesta a incidentes de seguridad que existan, por ejemplo, DCSIRT, CSIRT Antel, CERTuy, CSIRT Ceibal, etc.). El punto de contacto (RSI o quien este determine) y demás personal de seguridad de la información, forman parte de grupos especializados que participan al menos una vez por año en eventos y conferencias sobre seguridad.	Existe sinergia entre el personal de seguridad de la información de la organización y el personal que oficia como punto de contacto con autoridades, por medio de reuniones periódicas u otros mecanismos, donde se tratan temas de actualidad sobre amenazas y vulnerabilidades. La sinergia debe contemplar al equipo de respuesta a incidentes que corresponda.
ID.ER-3. Identificación y documentación de las amenazas	Se han identificado las amenazas y vulnerabilidades de los activos de información del centro de datos. La	Se cuenta con un inventario de riesgos de seguridad de la información que incluye riesgos	Se define una política de gestión de riesgos. Los riesgos se revisan periódicamente. La	El responsable de la gestión de los riesgos de seguridad de la información trabaja en forma coordinada con el RSI, los

internas y externas	revisión de los riesgos se realiza ad-hoc y sin periodicidad establecida.	asociados a otros activos de información que no se encuentran en el alcance del centro de datos. Se define un responsable de la gestión de riesgos de la ciberseguridad.	revisión se documenta formalmente y es comunicada al CSI y demás partes interesadas.	propietarios de los activos de información y el CSI. El resultado de la revisión de los riesgos se eleva formalmente al CSI, a la Dirección de la organización y demás partes interesadas. Se realizan actividades de control interno para verificar el cumplimiento con la política establecida.
ID.ER-4. Identificación del impacto potencial en el negocio y la probabilidad de ocurrencia.	La identificación de los principales riesgos incluye el impacto potencial en el negocio determinado de forma cualitativa (por ejemplo: alto, medio-alto, medio y bajo) y la probabilidad de ocurrencia (por ejemplo: alta, media, baja).	Se cuenta con un inventario de riesgos de seguridad de la información que incluye el impacto potencial en el negocio, determinado al menos en forma cualitativa.	Los riesgos se revisan con una frecuencia al menos semestral. La revisión se documenta formalmente. Se trabaja en la elaboración de un BIA. Este análisis incluye la identificación de los procesos críticos y sistemas de información que los soportan.	Se cuenta con el BIA definido, considerando al menos el impacto a nivel de imagen, económico y en los usuarios. Se ha definido un responsable de la gestión de los riesgos de seguridad de la información que trabaja en forma coordinada con el RSI, los responsables de los activos de información y el CSI. El responsable de gestión de riesgos de seguridad de la información identifica los riesgos de seguridad de la información de todos los activos de información de la organización. El resultado de la revisión de los riesgos se eleva formalmente al CSI, a la Dirección y demás partes interesadas. La revisión periódica de los riesgos y del BIA aporta información para la toma de decisiones.
ID.ER-5. Las amenazas, vulnerabilidades, probabilidad de ocurrencia e impactos se utilizan para determinar el riesgo.	Ver ID.ER-4 (nivel 1)	Ver ID.ER-4 (nivel 2)	Ver ID.ER-4 (nivel 3)	Ver ID.ER-4 (nivel 4)

ID.ER-6. Identificación y priorización de las respuestas a los riesgos.	Se han definido controles para la mitigación de riesgos y respuesta a las principales amenazas identificadas. Los controles podrán ser físicos, lógicos o administrativos.	Las respuestas a los riesgos se incluyen en el inventario de riesgos de seguridad de la información. Se agregan respuestas a riesgos de seguridad de la información que se encuentran fuera del alcance del centro de datos.	Las respuestas a los riesgos se revisan con una frecuencia al menos semestral y la revisión se documenta formalmente y es comunicada al CSI y a las otras partes interesadas.	La implementación de los controles se realiza de acuerdo a la prioridad explícita y formal establecida por la Dirección. Se ha definido un responsable de la gestión de los riesgos de seguridad de la información que trabaja en forma coordinada con el RSI, los propietarios de los activos de información y el CSI.
ID.GR. Estrategia para la gestión de riesgos Se establecen las prioridades, restricciones, tolerancia al riesgo y supuestos de la organización y se utilizan para soportar las decisiones de los riesgos operacionales.				
ID.GR-1. Los procesos de gestión de riesgos se encuentran establecidos, gestionados y aprobados por todos los interesados de la organización.	Se cuenta con un proceso para la gestión de riesgos de los componentes del centro de datos y servicios críticos de forma independiente.	Se cuenta con una metodología de gestión de riesgo que permite evaluar los riesgos de ciberseguridad de forma periódica. Se establece un plan de trabajo para el tratamiento del riesgo. Se ha definido un responsable de la gestión de riesgos de la ciberseguridad.	Ver ID.ER-3 (nivel 3).	Ver ID.ER-3 (nivel 4).
ID.GR-2. Se determina y se expresa de forma clara la tolerancia al riesgo a nivel de toda la organización.	Se define la tolerancia de los riesgos inherentes que pueden afectar los activos que se encuentran en el centro de datos y que soportan los servicios críticos para el funcionamiento de la organización.	Se establece claramente los umbrales de tolerancia al riesgo, basados en análisis de riesgo o análisis de impacto del negocio (BIA) para las áreas vinculadas a tecnología.	La metodología de gestión de riesgo permite delimitar las tolerancias que puede soportar la organización en base a sus objetivos, RTO, RPO y BIA entre otros. Los niveles de servicios de los proveedores se ajustan conforme la gestión de riesgo de la organización. Se define la tolerancia al riesgo para todos los procesos considerados	La tolerancia establecida se revisa periódicamente y se modifica ante cambios o las necesidades del negocio, la cual es apoyada por todas las partes interesadas, dirección y gerencias.

			críticos para la organización.	
ID.GR-3. La tolerancia al riesgo de la organización es determinada por su rol y pertenencia a la infraestructura crítica y por la evaluación de riesgos específicos del sector al que pertenece.	La tolerancia al riesgo es determinada por la posición de la organización con respecto a la entrega de los servicios que suministran y que puedan afectar el desempeño de otras organizaciones (en particular la que se hayan identificado como prioritarias o críticas para el sector) que estén interconectadas y dependan de sus servicios.	Ver ID.GR-2 (nivel 2)	Ver ID.GR-2 (nivel 3)	Ver ID.GR-2 (nivel 4)
ID.CS. Gestión de riesgos en la cadena de suministros Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.				
ID.CS-1. Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	Se identifica los participantes de la cadena de suministro de los activos y servicios críticos del centro de datos de la organización.	Se implementan modelos de identificación para abordar la gestión de riesgo asociado a los participantes de la cadena de suministro de los activos y servicios críticos de la organización. Se definen métricas e indicadores para el seguimiento y control.	Se cuenta con una política y procedimiento que define la gestión de riesgos, la cual debe contemplar toda la cadena de suministro (incluyendo proveedores y demás servicios subcontratados). Se define la periodicidad de las evaluaciones de los proveedores.	Los procesos de gestión de riesgo se utilizan en la adquisición de productos y servicios, y se mantiene en todo el ciclo de vida de los mismos. Esta gestión de riesgos es utilizada para la evaluación de los proveedores en base a servicio brindado en relación a las necesidades del negocio. Las evaluaciones son tomadas en cuenta para las actualizaciones de contratos y las futuras adquisiciones.
ID.CS-2. Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se	Los proveedores y demás partes externas que forman parte de la cadena de suministro de los servicios críticos de la organización, vinculados al centro	Se identifican y priorizan todos los proveedores de la cadena de suministro de servicios críticos de la organización.	Se cuenta con una política y metodología para la gestión de riesgo, las que contemplan en su evaluación de riegos a los proveedores de la cadena de	Los procesos de adquisición cuentan con todos los aspectos de evaluación de seguridad de la información y ciberseguridad durante todo el ciclo

evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	de datos, son identificados, priorizados y evaluados en el análisis de riesgos, considerando su impacto en el negocio.	Se definen aspectos de seguridad de la información y ciberseguridad para identificar las acciones permitidas y no permitidas por lo proveedores.	suministro de los servicios críticos.	de vida desde la contratación de un servicio o sistema, hasta su culminación ya sea por cambios de entorno u obsolescencia, permitiendo que el proceso de gestión de riesgo evalúe cada fase a fin de satisfacer las necesidades de seguridad de la organización.
ID.CS-3. Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	Se cuenta con un inventario de proveedores, identificando en cada caso su participación en la cadena de suministro de los servicios críticos. El proceso de adquisición de soluciones y servicios establece requisitos mínimos de seguridad de la información.	Informar a los proveedores de su participación en el alcance de los objetivos de negocio de la organización, determinando los roles y responsabilidades en cada caso. Los contratos y SLA con los proveedores contemplan la política de seguridad y demás medidas pertinentes que le exigen su la alineación a la estrategia de seguridad del negocio.	Se cuenta con una política de gestión de proveedores. Se realizan gestión de cambios de los proveedores conforme las necesidades de adecuación del negocio. Se revisan periódicamente los niveles de servicios de los proveedores en relación con el SLA acordado. Los desvíos son gestionados.	Se realizan auditorias periódicas para la evaluación de los proveedores. La misma es utilizada para ajustar los servicios de los proveedores en base a las necesidades del negocio.
ID.CS-4. Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	Las áreas tecnológicas que mantienen el centro de datos cuentan con un proceso, que se ajusta a parámetros determinados en los contratos establecidos entre las partes, para la evaluación de desempeño de proveedores y demás partes externas vinculadas a la cadena de suministro de los servicios críticos de la organización.	Se verifica que el trabajo realizado por los proveedores está ajustado a los parámetros esperados según los términos pautados en los contratos. Se establecen reuniones periódicas, o a solicitud de la organización, para contrastar los acuerdos establecidos contra los resultados de la evaluación del proveedor, permitiendo	La política de la seguridad de la información (o vinculada) establece la ejecución de auditorías externas e independientes sobre aquellos proveedores catalogados como críticos para las operaciones de la organización. Los desvíos identificados en la evaluación de proveedores cuentan con un plan de acciones correctivas para minimizar su afectación a los	Las auditorías externas a proveedores se realizan sistemáticamente conforme el apetito de riesgo de la organización. Se establece un monitoreo permanente de los servicios brindados por los proveedores. Se realiza seguimiento de los planes de acciones correctivas y se mide su efectividad. Lo antes mencionado está integrado a la evaluación de riesgos y es utilizado para ajustar los SLA

		apoyar los procesos de gestión de riesgo en la cadena de suministro. Se deja registro de las reuniones, de los desvíos y de las acciones correctivas.	objetivos del negocio. Cada acción está priorizada cuenta con un plazo de ejecución alineado a las necesidades del negocio.	conforme a las necesidades del negocio.
ID.CS-5. Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	Ver PR.PI-10 (nivel 1)	Ver PR.PI-10 (nivel 2)	Ver PR.PI-10 (nivel 3)	Ver PR.PI-10 (nivel 4)

6.2 Función PROTEGER (PR)

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.CA. Control de acceso El acceso a los activos e instalaciones se limita a usuarios, procesos o dispositivos, actividades y transacciones autorizadas.				
PR.CA-1. Las identidades y credenciales para usuarios y dispositivos autorizados son gestionadas.	Existen controles de acceso lógico a redes, recursos y sistemas de información basados en usuarios nominados.	Existen pautas definidas para la realización de altas, bajas y modificaciones de acceso lógico que además incluyen aprobaciones.	Se define una política y procedimiento de acceso lógico a redes, recursos y sistemas de información. La gestión de identidades y credenciales se realiza en forma centralizada, al menos en forma administrativa. La revisión de privilegios se realiza en forma reactiva frente a un cambio o baja, al menos para los sistemas críticos.	Se realizan revisiones proactivas periódicas de los privilegios de acceso de los usuarios, especialmente los privilegiados, según un procedimiento formal. Los resultados de las revisiones se documentan formalmente y se comunican al RSI, a las gerencias y demás partes interesadas. Existe sinergia entre las áreas de gestión humana, las gerencias y los responsables de la revisión de privilegios para obtener en tiempo y forma la información para las revisiones. Se realizan actividades de control interno para verificar la realización de revisiones de privilegios.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.CA-2. Se gestiona y protege el acceso físico a los activos.	Existen controles de acceso físico a las instalaciones de los centros de datos. Se gestionan las autorizaciones de acceso al centro de datos.	Existen controles de acceso físico para otras áreas definidas como seguras y se gestionan las autorizaciones de acceso.	Se cuenta con una política de control de acceso físico. Se establecen perímetros de seguridad al centro de datos y áreas seguras. Se realizan revisiones reactivas.	Se revisan periódicamente los registros de accesos realizados a los centros de datos y áreas seguras, según un procedimiento formal. La revisión periódica de accesos retroalimenta la gestión del acceso físico. Se realizan actividades de control interno para verificar el cumplimiento de los procedimientos establecidos.
PR.CA-3. Gestión de acceso remoto.	El acceso remoto se realiza mediante el uso de comunicaciones y mecanismos de autenticación seguros.	Existen acuerdos de no divulgación firmados por el personal de la organización con permisos de acceso remoto y para proveedores que lo requieran. Se otorga el acceso remoto con base en una lista blanca de todos los recursos disponibles.	Existe un procedimiento documentado de solicitud de acceso remoto. Existe un responsable para la asignación de permisos de acceso remoto. 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. Se implementa el doble factor de autenticación para el acceso remoto. Se centraliza el acceso remoto al menos en forma administrativa.	Se realizan revisiones periódicas de los usuarios con acceso remoto. Las revisiones periódicas de accesos remotos incluyen la revisión de los registros de acceso remoto. Esta información retroalimenta la gestión del acceso remoto y proporciona información para la toma de decisiones de mejora continua. Se realizan actividades de control interno para verificar el cumplimiento de los procedimientos establecidos.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.CA-4. Gestión de permisos de acceso, incorporando los principios de menor privilegio y segregación de funciones.	El acceso a la red y los sistemas cuentan con, al menos, usuario y contraseña con usuarios nominados. El uso de usuarios genéricos y/o privilegiados se encuentra controlado.	Se incorpora los principios de menor privilegio y segregación de funciones. Se identifican los casos que requieren una fuerte autenticación y verificación de identidad para determinar métodos alternativos (token, factor de doble autenticación, etc.). La gestión de usuarios y permisos de acceso se realiza en forma centralizada, al menos del punto de vista administrativo.	Se define una política de acceso lógico que incluye el uso de usuarios privilegiados. Se define una política de gestión de usuarios y contraseñas, y se instruye al personal para su uso correcto. Se cuenta con un procedimiento para el ABM de usuarios. Los derechos de acceso son autorizados y se cuenta con registro de tales acciones. Se realizan revisiones de los derechos de acceso de los usuarios y se cuenta con registro de tales acciones.	Se define un procedimiento documentado de revisión periódica de derechos de acceso de los usuarios incluyendo los privilegiados. El resultado de las revisiones se comunica formalmente a las gerencias y otras partes interesadas. Existe sinergia entre las áreas de gestión humana, las gerencias y las áreas de tecnología encargadas de habilitar técnicamente los derechos de acceso y se logra actuar proactivamente frente a cambios relacionados con el personal (altas, bajas, modificaciones).
PR.CA-5. Protección de la integridad de la red incorporando segregación cuando es apropiado.	La red se encuentra segmentada al menos en redes con contacto directo con redes externas (por ejemplo, Internet) y redes privadas de la organización. Existe un diagrama de red actualizado.	Se identifican los posibles dominios de red en función de las necesidades de la organización. Se establece la segmentación de las redes en función de los dominios definidos para proteger la infraestructura y los servicios de red. Se genera una postura de manejo de tráfico por defecto entre segmentos.	Se conoce y se analiza el tráfico en los diferentes dominios de la red. Se protegen las comunicaciones entrantes y salientes entre los diferentes segmentos. Se trabaja en la definición de controles de detección de amenazas. Se definen alertas cuando el tráfico no autorizado es bloqueado o detectado. Se define un procedimiento de contención de incidentes en el segmento cuando se detectan las amenazas.	Existe un procedimiento documentado de monitoreo de los diferentes segmentos apoyado, si es viable, por herramientas automatizadas. El procedimiento de contención de incidentes se encuentra alineado con la política de gestión de incidentes. Se registran los incidentes que se detectan en los diferentes segmentos para aprender de ellos y retroalimentar las lecciones aprendidas facilitando la toma de decisiones.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
PR.CA-6. Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	Existe segregación de los distintos roles o perfiles del personal que accede al centro de datos, y se generan y almacenan los registros de las actividades que desempeñan.	Todos los usuarios nominados que ingresan a los sistemas de la organización y en especial a los que contienen información catalogada como sensible conocen y entienden sus responsabilidades en base a la seguridad de la información y están notificados de las medidas de auditoria implementadas en los sistemas.	Existen y se aplican procedimientos formales de revisión de permisos que abarcan todo el ciclo de vida (alta, baja y modificación) de los usuarios nominados y genéricos de los sistemas de información.	Ver PR.CA-1 (nivel 4)
PR.CA-7. Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	Todos los sistemas requieren autenticación. Todos los usuarios son nominados conforme la política de control de acceso definida por la organización. La autenticación de dispositivos para conexión y uso está autorizada.	Se realiza control sobre los usuarios privilegiados de los sistemas y aplicaciones (por ejemplo: bases de datos, servidores, etc.). Los accesos remotos a aplicaciones críticas del negocio se realizar utilizando más de un control de autenticación. El uso de dispositivos externos requiere identificación (inventariado y responsable) y autentificación (permiso de acceso por el rol del usurario o algún otro método).	Se define un procedimiento de acceso lógico a las redes, sistemas, recursos y dispositivos. Se disponen de controles de autenticación diferenciados, así como también autenticación de dispositivos, conforme la clasificación de la información a ser accedida. Las medidas implementadas para el acceso están directamente asociadas al análisis de riesgos sobre el acceso a la información. Se aplica el criterio de menor privilegio para la asignación de permisos.	Se establecen procesos de revisiones y auditorias continua para verificar que las redes, sistemas, recursos y dispositivos están funcionando con la autenticación y configuración requerida y acordada por la organización a fin de mantener confidencialidad, integridad y disponibilidad de la información. Al realizar estos procedimientos de revisión continua, se consideran las políticas, normas, estándares y regulaciones aplicables a la organización en relación a la protección de datos y privacidad de la información.

PR.CF. Concientización y formación El personal de la organización y socios de negocios, reciben entrenamiento y concientización sobre seguridad de la información. Están adecuadamente entrenados para cumplir con sus obligaciones referentes a la seguridad de la información en alineación con las políticas, procedimientos y acuerdos existentes.				
PR.CF-1. Todos los usuarios se encuentran entrenados e informados.	Se comienza a trabajar en actividades propias de difusión de información relacionada con seguridad de la información, incluyendo la difusión de las políticas y mecanismos de protección.	Se trabaja en la elaboración de campañas de concientización para el personal. Se cuenta formalmente con los recursos para llevarla adelante.	Las campañas de concientización son aprobadas y se determina cómo se medirá su éxito. Se planifica un cronograma para la realización de las campañas. Se definen actores críticos, objetivos, estrategias, tácticas y audiencia. Se elabora el material educativo necesario.	Se realizan actividades de control interno para verificar el desarrollo de las campañas. Se evalúa el nivel de conocimiento adquirido por el personal mediante actividades de evaluación periódicas. Estas actividades son aprobadas por el CSI y apoyadas por la Dirección.
PR.CF-2. Los usuarios privilegiados comprenden sus roles y responsabilidades.	Los usuarios privilegiados demuestran conocimiento respecto a la importancia de sus roles y responsabilidades.	Se realizan actividades de concientización para usuarios privilegiados con cierta periodicidad.	Los usuarios privilegiados son capacitados a través de cursos o talleres relevantes.	Se define un plan de capacitación y entrenamiento en seguridad de la información teniendo en cuenta los perfiles e intereses de grupos considerados estratégicos. El plan está aprobado por la Dirección que se compromete con su aplicación. El plan es revisado y actualizado periódicamente y se realizan acciones de mejora incorporando lecciones aprendidas.
PR.CF-3. Interesados externos (proveedores, clientes, socios) comprenden sus roles y responsabilidades.	Se han pautado los roles y responsabilidades de los interesados externos.	Se realizan iniciativas de concientización para interesados externos.	Los interesados externos comprenden sus roles y responsabilidades.	Ver PR.CF-2 (nivel 4)
PR.CF-4. La gerencia ejecutiva comprende sus roles y responsabilidades.	La Gerencia conoce y comprende los riesgos de seguridad de la información.	La Dirección conoce y comprende los riesgos de seguridad de la información. La Gerencia tiene una participación activa en las iniciativas de concientización.	La Dirección tiene una participación activa en las instancias de concientización.	Ver PR.CF-2 (nivel 4)
PR.CF-5. El personal de	El personal de seguridad física y	Se realizan con cierta periodicidad	El personal de seguridad física y	Ver PR.CF-2 (nivel 4)

seguridad física y de seguridad de la información comprende sus roles y responsabilidades.	de seguridad de la información demuestra concientización respecto a la importancia de sus roles y responsabilidades.	actividades de concientización para el personal de seguridad física y seguridad de la información.	seguridad de la información es capacitado a través de cursos o talleres relevantes.	
PR.SD. Seguridad de los datos La información y registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.				
PR.SD-1. Los datos en reposo (inactivos) se encuentran protegidos.	Se identifican los datos históricos y respaldos que deben ser protegidos mediante mecanismos seguros. Se establecen al menos mecanismos de control de acceso lógico y físicos.	Los respaldos y/o datos históricos offline se almacenan en forma cifrada.	Se define una política de uso de controles criptográficos para respaldos y datos históricos. Se determinan los responsables de la generación de las claves que abarca todo su ciclo de vida.	Se realizan revisiones periódicas sobre los respaldos y datos históricos para garantizar que se encuentran protegidos según lo determinado en la política. Los resultados de estas revisiones son registrados e informados al RSI.
PR.SD-2. Los datos en tránsito se encuentran protegidos.	Se implementa algún control criptográfico para asegurar la protección de los datos en tránsito.	Los datos en tránsito de todas las aplicaciones y sistemas se encuentran protegidos mediante un mismo conjunto reducido de tecnologías y prácticas criptográficas.	Se define una política de uso de controles criptográficos que determina los lineamientos de protección necesaria de la información en tránsito. Se determinan los responsables de la generación de las claves que abarca todo su ciclo de vida.	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. Los resultados de estas revisiones son registrados e informados al RSI.
PR.SD-3. Los activos se gestionan formalmente a lo largo de la eliminación, las transferencias y disposición.	Se definen pautas para la disposición final y borrado seguro de medios de almacenamiento. El personal está informado de la importancia de la eliminación de medios de almacenamientos que no se utilizarán más, para preservar la confidencialidad de la información contenida en ellos.	Se definen puntos de disposición de los medios. La disposición y/o borrado seguro de medios de almacenamiento se lleva a cabo mediante actividades coordinadas.	Se define una política de destrucción de la información y existe un procedimiento documentado alineado con la política.	Se realizan actividades de control interno sobre los procedimientos de eliminación y de los lugares de disposición de medios. Se informan los resultados al RSI y demás partes interesadas. En caso de desvíos se toman las acciones correctivas correspondientes.

PR.SD-4. Se mantiene una adecuada capacidad para asegurar la disponibilidad.	La capacidad actual instalada para la prestación de los servicios críticos es suficiente.	Se toman en cuenta las necesidades de capacidad al momento de dimensionar los servicios críticos que se hayan identificado, de acuerdo a las necesidades actuales del negocio. Se realizan mediciones objetivas para detectar problemas de capacidad.	Se planifica y define el proceso de gestión de la capacidad actual. Se identifica al responsable del proceso de gestión de la capacidad, sus roles y responsabilidades.	Se cuenta con un plan de capacidad formal. Se define un proceso de estimación de la capacidad que acompaña al plan. La información se utiliza para generar pronósticos. El plan se revisa a intervalos regulares. Se proponen acciones para la mejora continua de la gestión de la capacidad.
PR.SD-5. Se implementan medidas de protección contra fuga de datos	Se firman acuerdos de no divulgación para los nuevos proveedores de servicios y para los nuevos ingresos de personal.	Se extiende la firma de acuerdos de no divulgación progresivamente a toda la organización.	Los acuerdos contractuales con el personal y proveedores reflejan las responsabilidades de seguridad de la información según el rol que ocupen en la organización. Existe un procedimiento documentado para la desvinculación del personal que incorpora la revocación de accesos físicos y lógicos. Se establecen las responsabilidades y acuerdos de no divulgación indicando el tiempo por el cual continuarán siendo válidos estos aspectos. Se implementan sistemas DLP para controlar los datos, según los objetivos del negocio y normativa actual.	Se revisan los contratos y procedimientos de desvinculación de forma periódica para verificar el cumplimiento. Se registra el resultado de las revisiones y se utilizan para la mejora de los procesos y procedimientos, así como para la mejora continua de acuerdos y contratos. Se registran y revisan los desvíos e incumplimientos con los acuerdos de no divulgación y otras obligaciones contractuales relacionadas a seguridad de la información. El resultado de las revisiones se comunica al RSI y demás partes interesadas.
PR.SD-6. Se realizan chequeos de integridad para verificar software, firmware e integridad de la información.	Se definen pautas para la instalación de software. Los equipos del personal cuentan con protección antivirus. Se realizan tareas de concientización	La posibilidad de instalar software en los equipos queda restringida a los usuarios que se encuentran autorizados para ese fin. Se define un procedimiento	Se trabaja en la elaboración de listas de software autorizado y prohibido. Se cuenta con una solución antivirus centralizada y existe un	Se cuenta con listas de software autorizado y/o prohibido, revisadas por el RSI. Todos los servidores cuentan con algún tipo de protección o detección de

	sobre prevención ante software malicioso.	y los responsables para la instalación de software en producción. Los servidores que ofician de distribuidores de archivos (por ejemplo, servidores de archivos o correo electrónico), cuentan con una solución antivirus.	responsable de ella. Se define una política de protección contra software malicioso. Se cuenta con algún mecanismo de control de acceso a sitios Web maliciosos y/o no autorizados.	malware. Se realizan actividades de control interno sobre la solución antivirus y sobre el software instalado con el fin de determinar el cumplimiento con las políticas y procedimientos. Los resultados de estas revisiones son enviados al RSI y demás partes interesadas. En caso de desvíos se determinan las acciones correctivas.
PR.SD-7. Los entornos de desarrollo y pruebas están separados del entorno de producción	El entorno de producción se encuentra separado del resto de los entornos y su uso es exclusivo para las aplicaciones que dan soporte a los servicios críticos que brinda la organización.	Se cuenta con plataformas adecuadas e independientes que soportan el ciclo de vida de desarrollo de los sistemas. Se implementan controles para el pasaje entre los ambientes.	Se define una política de separación de entornos y un procedimiento documentado para su gestión. Se definen responsables para la gestión de los ambientes existentes, y para los pasajes a producción. Durante la realización de las pruebas se registra la información del entorno (características, información de los datos de prueba, etc.) y esta información es conservada para asegurar la calidad de los resultados de las pruebas y lograr replicar a futuro las condiciones en las que se efectúan.	Los responsables de la gestión de entornos participan desde el inicio en los proyectos. Se toman los recaudos necesarios para el manejo de información según su clasificación durante las pruebas. Se realizan auditorías de cumplimiento y control interno de la política de separación de entornos y procedimientos relacionados. Se registran los resultados y se toman acciones correctivas en casos de desvíos.
PR.SD-8. Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	Ver DE.MC-1 (nivel 1)	Ver DE.MC-1 (nivel 2)	Ver DE.MC-1 (nivel 3)	Ver DE.MC-1 (nivel 4)
PR.PI. Procesos y procedimientos para la protección de la información Las políticas de seguridad, procesos y procedimientos se mantienen y son utilizados para gestionar la protección de los sistemas de información y los activos.				

PR.PI-1. Existe una línea base de la configuración de los sistemas de información que es mantenida.	Existen medidas para comunicar y autorizar los cambios en el ámbito tecnológico.	Se define versionado y líneas base de configuración de los productos de software que permiten la trazabilidad de los cambios.	Se define una política de gestión de cambios que contempla también los cambios de emergencia en el ámbito tecnológico. Se cuenta con un procedimiento documentado para la gestión de los cambios. Los cambios a las líneas base se registran.	Se cuenta con herramientas para dar soporte a la gestión de los cambios. Se realizan actividades de control interno para revisar el cumplimiento con los procedimientos actuales. El resultado de estas actividades es comunicado al RSI y demás partes interesadas. Se toman medidas correctivas ante desvíos.
PR.PI-2. Se implementa el ciclo de vida de desarrollo para gestionar los sistemas.	Se utilizan lineamientos generales para el desarrollo de los sistemas incluyendo principios básicos de la gestión de proyectos (ágiles, tradicionales o ambas). Los usuarios participan directamente o mediante algún rol que los represente en el ciclo de vida de los sistemas.	La seguridad de la información se toma en cuenta en la especificación de requisitos. Se incorporan principios de desarrollo seguro de sistemas. Se controlan las versiones de software. Se sistematizan las actividades de pruebas.	Se define un procedimiento documentado de pruebas, contemplando la participación de usuarios, directa o mediante algún rol que los represente. Se definen los criterios de aceptación de los productos.	Se realizan actividades de control interno para determinar el nivel de cumplimiento con la metodología y procedimientos definidos. El resultado de estas actividades se comunica al RSI y demás partes interesadas. Se toman acciones correctivas frente a desvíos.
PR.PI-3. Existen procesos de gestión del cambio en las configuraciones	Ver PR.PI-1 (nivel 1)	Ver PR.PI-1 (nivel 2)	Ver PR.PI-1 (nivel 3)	Ver PR.PI-1 (nivel 4)
PR.PI-4. Se realizan y mantienen respaldos de la información y se testean periódicamente.	Se realizan respaldos periódicos de al menos los activos de información del centro de datos (aplicaciones, bases de datos, máquinas virtuales, etc.).	Se cuenta con soluciones automatizadas para asistir en la realización de los respaldos. Los respaldos se almacenan en lugares seguros y con acceso restringido.	Los respaldos son probados regularmente. Se ha determinado el uso de almacenamiento externo para copias de respaldos. Existe una política y procedimiento documentado de respaldos y de pruebas de recuperación, que incluye las frecuencias. Se establece el grado (completo, diferencial, etc.) y los requisitos de retención de los respaldos.	La política y el procedimiento de respaldo se encuentran alineados al plan de contingencia y al plan de recuperación, los cuales aseguran que resuelven los requisitos de recuperación de la organización ante un evento anormal. La política y procedimiento de respaldos se revisan con regularmente.

			El procedimiento de respaldos se actualiza ante cambios de requerimientos del negocio o cambios de infraestructura o sistemas que requieran acciones de respaldo.	
PR.PI-5. Las políticas y reglamentos relacionados con el medio ambiente físico operativo se cumplen.	Existen medidas de control del medio ambiente físico en los centros de datos.	Se implementan herramientas automatizadas que apoyan el monitoreo de los controles relacionados al medio ambiente físico.	Se define una política de seguridad del equipamiento. Se cuenta con un procedimiento documentado de monitoreo que incluye el uso de herramientas automatizadas.	Se realizan actividades de control interno para verificar el cumplimiento de la política y procedimientos asociados. Los resultados del monitoreo son utilizados para mejorar los procedimientos y retroalimentación de las lecciones aprendidas.
PR.PI-6. Los datos son eliminados de acuerdo a las políticas de seguridad.	Ver PR.SD-3 (nivel 1)	Ver PR.SD-3 (nivel 2)	Ver PR.SD-3 (nivel 3)	Ver PR.SD-3 (nivel 4)
PR.PI-7 Existe mejora continua de los procesos de protección.	Los procesos de protección de los activos críticos del centro de datos se revisan periódicamente.	Los procesos de protección de los activos y servicios de la organización se revisan periódicamente y se comunican a todas las partes interesadas conforme a las necesidades del negocio para ajustar o mejorar los procesos usados para la protección.	Se deja registro de los cambios realizados a los procesos (por ejemplo, configuración de sistemas de protección). Se realiza la gestión de cambio en los mismos.	La revisión periódica aporta a la mejora continua del SGSI.
PR.PI-8. La eficacia de las tecnologías de protección se comparten con las partes apropiadas.	Se establece una sistemática que permite aprender de los incidentes de seguridad de la información ocurridos en el centro de datos. Las lecciones aprendidas son registradas.	Se establece una sistemática que permite aprender de los incidentes de seguridad de la información ocurridos en la organización. Las lecciones aprendidas son difundidas a las partes interesadas.	Las lecciones aprendidas se registran y contemplan para mejorar los planes de respuesta a incidentes. Además, son utilizadas para mejorar los canales de comunicación establecidos con las partes involucradas y los procesos de escalamiento.	Las lecciones aprendidas son analizadas para mejorar el SGSI de la organización y retroalimenta el análisis de riesgos. Se definen indicadores para poder medir la efectividad de los controles.

PR.PI-9. Existen y se gestionan planes de respuesta a incidentes (respuesta a incidentes y continuidad del negocio) y planes de recuperación (recuperación de incidentes y recuperación de desastres).	Los incidentes de seguridad se reportan internamente de acuerdo a lineamientos preestablecidos. Se instruye al personal sobre los mecanismos de reporte de incidentes. Los incidentes se registran. Se cuenta con ciertas medidas de contingencia y recuperación para los sistemas que dan soporte a los servicios críticos.	Se cuenta con ciertas medidas de contingencia y recuperación. Se conocen los procesos críticos del negocio. Se cuenta con herramientas que apoyan la gestión de los incidentes.	Se define una política de gestión de incidentes de seguridad de la información y se difunde. Se define un plan de respuesta para la gestión de incidentes. Se define un plan de contingencia y de recuperación. Se realizan pruebas puntuales de los planes.	Se ha definido el responsable de la respuesta a incidentes que opera coordinadamente con el RSI. El responsable de la respuesta a incidentes opera de forma coordinada con el CERTuy o CSIRT que corresponda. Se ha definido el o los responsables del mantenimiento del plan de contingencia y de recuperación. El plan de contingencia y de recuperación y el plan de respuesta a incidentes son probados anualmente. Se realizan actividades de control interno para verificar el cumplimiento con la política y procedimientos relacionados. El resultado de estas actividades se informa al RSI y se toman acciones correctivas frente a desvíos y para la mejora continua.
PR.PI-10. Los planes de respuesta y recuperación se testean regularmente.	El personal conoce las actividades básicas necesarias que deben realizar si se detecta o sospecha un incidente. Se han identificado los proveedores que dan soporte a los servicios críticos.	Se cuenta con un plan de respuesta a incidentes y con un plan de recuperación. Los involucrados están entrenados en su uso.	El plan de respuesta a incidentes y el plan de recuperación (DRP) se encuentran documentado. Existen evidencias de escenarios de falla o incidentes en los que se ejecutaron las actividades del procedimiento de acuerdo al caso o se diseñaron escenarios simulados para ello. Se registran los resultados en todos los casos.	El plan de respuesta a incidentes se encuentra alineado al plan de contingencia y recuperación, y se realizan pruebas al menos anuales de ambos. Se registran las pruebas. El resultado de las pruebas retroalimenta las lecciones aprendidas y sirven para la mejora continua de los planes y procedimientos.
PR.PI-11. La ciberseguridad se encuentra	Ver PR.SD-5 (nivel 1)	Ver PR.SD-5 (nivel 2)	Ver PR.SD-5 (nivel 3)	Ver PR.SD-5 (nivel 4)

incluida en las prácticas de RRHH.				
PR.PI-12. Existe un plan de gestión de vulnerabilidades .	Se gestionan las vulnerabilidades técnicas mediante, al menos, la gestión de parches.	Se define un plan documentado para la gestión de las vulnerabilidades y parches. Se reciben notificaciones de vulnerabilidades por parte del CERTuy u otras organizaciones y se analizan.	Las responsabilidades de gestión de vulnerabilidades están establecidas. Se incorporan como fuentes de notificación: escaneos de infraestructura y aplicaciones. Existe un ambiente para pruebas de parches previo a su puesta en producción.	Se realizan revisiones de control interno sobre el plan de gestión de vulnerabilidades. El resultado de las revisiones se comunica al RSI. Se documentan lecciones aprendidas que aportan a la mejora de futuras resoluciones frente a vulnerabilidades similares.
PR.MA. Mantenimiento El mantenimiento y las reparaciones de los componentes de los sistemas de información y de control industrial se lleva a cabo en consonancia con las políticas y procedimientos.				
PR.MA-1. El mantenimiento y la reparación de los activos de la organización se lleva a cabo y es registrado en forma oportuna con herramientas aprobadas y controladas.	El área de tecnología gestiona y/o realiza el mantenimiento sobre los activos del centro de datos, en función de los requerimientos técnicos.	Se establecen los planes anuales de mantenimiento, gestionando el acceso a los usuarios autorizados para realizar las tareas de mantenimiento programado. Se conservan los registros del mantenimiento, fallos y cambios realizados sobre los activos.	Se cuenta con un procedimiento, donde se estandariza la planificación preventiva y correctiva de la plataforma tecnológica de la organización.	Se implementa los procesos control de cambio, la documentación requerida y la aprobación por parte del CSI, con el fin de que todos estos requerimientos de mantenimiento estén acordados por las partes y que los mismos no impacten la entrega de servicios críticos. Se cuenta con un proceso de control interno para la verificación de cumplimiento de los procedimientos de mantenimiento del equipamiento.

PR.MA-2. El mantenimiento a distancia de los activos de la organización se aprueba, registra y lleva a cabo de forma tal que se impide el acceso no autorizado.	El área de tecnología aprueba la alta y baja de los usuarios (internos o externos) que realizan mantenimiento de forma remota a los activos informáticos del centro de datos.	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 aprobado por las partes. Se lleva a cabo el registro de los eventos de accesos de cada usuario, exigiendo el estricto cumplimiento de las cláusulas de confidencialidad, integridad y disponibilidad de la información.	Se cuenta con un procedimiento que contempla que todos los eventos de conexión remota a los activos informáticos generan alertas de forma automática; las mismas permiten identificar y trazar las actividades de los usuarios que se han conectado para validar que todas las acciones de mantenimiento corresponden con las acciones esperadas o alertar de una posible desviación.	Se realiza una revisión periódica de logs de acceso y actividades de los usuarios a la plataforma de la organización.
PR.TP. Tecnología de protección Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y resistencia de los sistemas y activos de la organización, en consonancia con las políticas, procedimientos y acuerdos.				
PR.TP-1. Los registros de auditoría (logs) se documentan, implementan y son revisados de conformidad con la política.	Se configuran los registros de auditoría para todos los sistemas definidos como críticos. Los registros son utilizados para tratar situaciones puntuales.	Los registros de auditoría se centralizan. La revisión de los registros se realiza en forma ad-hoc. Los registros están protegidos contra accesos no autorizados y posibles alteraciones. Se tiene en cuenta los requisitos de confidencialidad de la información y protección de la privacidad de los datos contenidos en los registros.	Se define una política y procedimientos de auditoría y registro de eventos. Los registros de auditoría se respaldan fuera de línea en forma periódica y se revisan periódicamente con herramientas de apoyo automatizadas. Los relojes de todos los sistemas deben estar sincronizados (servidores, aplicaciones, etc.).	Se establecen los requisitos de retención de los registros y se implementan. Se toman medidas para facilitar el análisis de grandes volúmenes de información. Se cuenta con mecanismos para revisar las actividades de los administradores. Se realizan actividades de control interno para verificar el cumplimiento con la política y los procedimientos. El resultado de las revisiones se comunica al RSI y demás partes interesadas.
PR.TP-2. Los medios extraíbles se encuentran protegidos y su uso se	Existe difusión sobre la importancia de la protección y uso de los medios extraíbles.	Se identifican los tipos de medios extraíbles autorizados. Se establecen pautas para el uso	Se realiza el reporte de hurto, pérdida o daño del medio y su eliminación al final de su vida útil.	Se realizan revisiones de control interno sobre el cumplimiento de las pautas de uso de medios extraíbles y del procedimiento.

encuentra restringido de acuerdo con las políticas.		de medios extraíbles y son comunicadas a todo el personal.		Los resultados de las revisiones son utilizados para la mejora del procedimiento y se comunican al RSI y demás partes interesadas.
PR.TP-3. El acceso a los sistemas y activos se controla, incorporando el principio de menor privilegio.	Ver PR.CA-4 (nivel 1)	Ver PR.CA-4 (nivel 2)	Ver PR.CA-4 (nivel 3)	Ver PR.CA-4 (nivel 4)
PR.TP-4. Las redes y comunicaciones se encuentran protegidas.	[AC]*Los servicios del organismo son prestados con infraestructura dentro del territorio nacional, o al menos se cuenta con una planificación para la migración de todos los servicios que están fuera de él.* La comunicación entre MTAs se encuentra cifrada como método preferido de comunicación. Los servicios de Webmail se encuentran implementados sobre el protocolo HTTPS utilizando un certificado válido.	[AC]*La mayoría de los servicios se encuentran en territorio nacional, y los restantes están en proceso de migración conforme a la planificación realizada.* Todas las aplicaciones Web disponibles en Internet se encuentran protegidas mediante el uso de WAF, al menos configurados en modo "detección".	[AC]*Todos los servicios se encuentran en territorio nacional.* El WAF de producción ha evolucionado de modo detección a modo bloqueo. Se cuenta con un WAF instalado en ambiente de prueba para la realización de pruebas funcionales y otro WAF en ambiente de producción donde se impactan las reglas actualizadas luego de ser probadas. Los registros de los WAF se encuentran centralizados.	[AC]*La comunicación entre MTAs de dominios gubernamentales se encuentra cifrada en forma mandatoria. El organismo envía un reporte mensual al CERTuy sobre estadísticas de la actividad detectada en el WAF. El organismo colabora con el CERTuy en la centralización de registros de WAF a nivel nacional.* El análisis de los registros del WAF incluye automatismos que favorecen las actividades de revisión. Se establece un procedimiento para la preservación y gestión de los registros del WAF.
PR.TP-5. Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	Los componentes críticos del centro de datos cuentan con redundancia para la entrega de servicios y para tolerar los fallos en situaciones adversas, según los requisitos de resiliencia establecidas por el negocio.	Se cuenta con un centro de datos alterno donde los componentes y activos que soportan los servicios críticos pueden alcanzar los requisitos de resiliencia del negocio para la prolongación operativa.	Se documenta la implementación y pruebas de los mecanismos para tolerar fallos en sistemas y activos de información críticos del centro de datos principal. También se cuenta con una estructura de pruebas periódicas sobre el centro de datos alterno para constatar que los sistemas se encuentran	Se cuenta con redundancia en todos los componentes que dan soporte a los servicios críticos. Se trabaja en la mejora continua de los procesos basado en las pruebas periódicas, lo que permite calibrar los activos en base a la necesidad del negocio.

			configurado de forma correcta.	

6.3 Función: DETECTAR (DE)

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
DE.AE. Anomalías y eventos La actividad anómala se detecta de forma oportuna y el potencial impacto de los eventos es comprendido.				
DE.AE-1. Se establece y gestiona una línea base de operaciones de red y flujos de datos esperados para usuarios y sistemas.	Se definen y gestionan los parámetros esperables para usuarios privilegiados y sistemas críticos del centro de datos.	Se definen y gestionan los parámetros esperables de todos los usuarios y sistemas asociados a servicios críticos de la organización, así como aquellos sistemas de soporte u otros que deban ser monitoreados. Los desvíos son reportados al RSI.	Se documenta la línea base. Se define el procedimiento de monitoreo y actuación antes desvíos. Se generan indicadores y métricas sobre los eventos monitoreados.	La configuración de la línea base es revisada periódicamente o ante cambios tecnológicos y/o de los objetivos de negocio. Los indicadores son utilizados para la mejora continua y apoyar a la gestión de la línea base.
DE.AE-2. Los eventos detectados son analizados para entender los objetivos y métodos de ataque.	Se registran los eventos de los sistemas y redes. Los eventos irregulares detectados puntualmente se analizan. Se contacta al CERTuy o CSIRT que corresponda en los casos que sea necesario contar con asistencia.	Se revisan los eventos de los sistemas y redes, y de configuración y uso de WAF. Se cuenta con herramientas de apoyo automatizadas para el monitoreo de los eventos, excepciones y fallas.	Se define una política de auditoría y registro de eventos. Existen procedimientos documentados para la revisión y gestión de los eventos de los sistemas y redes y de configuración y uso de WAF. Los procedimientos incluyen la gestión de anomalías en alineación a la política y procedimiento de gestión de incidentes.	La revisión de los eventos se realiza a intervalos regulares y cuando se detecta actividad anormal para detectar objetivos, métodos de ataque, patrones, etc., permitiendo orientar y optimizar las estrategias y/o esfuerzos en ciberseguridad. La periodicidad de las revisiones se establece en los procedimientos y se informa al RSI y demás partes interesadas sobre los resultados de la revisión.
DE.AE-3. Los datos de los eventos se agrupan y correlacionan	Se revisan los eventos locales generados por el equipamiento y	Los sistemas que soportan los servicios críticos emiten alertas de eventos de forma	Se cuenta con procesos, procedimientos y herramientas para	Se implementan procesos automatizados que permiten correlacionar

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
desde múltiples fuentes y sensores.	activos del centro de datos. Se deja registro de la revisión.	independiente, basados en las pautas establecidas por el apetito de riesgo de la organización. Se cuenta con un sistema de centralización de logs.	la centralización de logs. Se emiten alertas que permita tomar acciones para salvaguardar la confidencialidad, integridad y disponibilidad de los sistemas de información.	información, pudiendo tomar acciones de forma automatizada. Se realiza una revisión periódica de los procedimientos, y la misma se utiliza para la mejora continua.
DE.AE-4. Se determina el impacto de los eventos.	Se analiza el impacto de los eventos que afectan a los sistemas y servicios más críticos, dentro o fuera del centro de datos. La detección es reactiva.	Se identifican los activos afectados tomando como base el inventario de activos críticos del centro de datos. Se establecen los umbrales tolerables de los activos (por ejemplo, tiempo de espera tolerable para una aplicación Web). Se automatizan algunas alertas ante incidentes.	Las actividades de identificación de impacto y determinación de umbrales están contenidas en el procedimiento de detección y monitoreo. Se automatizan las alertas ante incidentes correspondientes con los umbrales de tolerancia para los activos críticos del centro de datos. Se clasifican las alertas ante incidentes tomando en cuenta el riesgo asociado.	Se realizan actividades de control interno para verificar el cumplimiento con el procedimiento de detección y monitoreo. Los resultados de estas actividades se utilizan para la mejora del procedimiento y se retroalimentan las lecciones aprendidas.
DE.AE-5. Se establecen los umbrales de alerta de incidentes.	Ver DE.AE-4 (nivel 1)	Ver DE.AE-4 (nivel 2)	Ver DE.AE-4 (nivel 3)	Ver DE.AE-4 (nivel 4)
DE.MC. Monitoreo continuo de la seguridad Los sistemas de información y los activos son monitoreados a intervalos discretos para identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.				
DE.MC-1. Se monitorea la red para detectar potenciales eventos de ciberseguridad.	Se monitorea de forma reactiva o esporádica los sistemas o servicios más críticos.	Se monitorea de forma automatizada los activos críticos del centro de datos, generando alertas ante la detección de problemas.	En el centro de datos se implementan alertas sobre anomalías que podrían transformarse en problemas para los activos críticos. Estas alertas notifican cuando se comienzan a dar las casuísticas que pueden derivar en un incidente aún no concretado.	Se monitorean todos los activos de información del centro de datos, con cruzamiento de información de diversas fuentes, contemplando, entre otros, alertas preventivas y reactivas. Se cuenta con un mecanismo alternativo de monitoreo, al menos

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
				manual, ante fallas del principal.
DE.MC-2. Se monitorea el ambiente físico para detectar potenciales eventos de ciberseguridad.	Existen controles de acceso físico a las instalaciones del centro de datos. Se definen alertas reactivas (ínsita) de control en los dispositivos físicos del centro de datos. Se monitorean esporádicamente los dispositivos para detectar amenazas sobre ellos (alimentación eléctrica, enfriamiento, etc.).	Existen funciones integradas en los dispositivos que permiten el monitoreo de las amenazas típicas (alimentación eléctrica, enfriamiento, etc.). Se definen notificaciones de alertas (correo, SMS, etc.) al personal designado.	Se cuenta con una política de control de acceso físico. Se cuenta con los sensores instalados y se recolecta la información. Se define dónde se almacena la información de los sensores. Se determina la estrategia de recolección que sea más adecuada, siempre evitando un punto único de falla. Se trabaja en la identificación de otro tipo de amenazas físicas (personas, sustancias suspendidas en el aire, humedad, filtración de líquidos, temperatura del aire, etc.) y en el establecimiento de sensores para capturar la información.	Se cuenta con un sistema de monitoreo inteligente que proporciona información histórica útil para la generación de informes. Los informes son utilizados para evaluar el centro de datos y tomar acciones correctivas o preventivas.
DE.MC-3. Se monitorea la actividad del personal para detectar potenciales eventos de ciberseguridad.	Se registran los eventos relevantes de los usuarios que suceden en los sistemas o aplicaciones críticas.	Se realizan revisiones de los eventos registrados en forma reactiva. Los resultados de las revisiones son utilizados para la evaluación de potenciales incidentes.	Se han definido las responsabilidades del monitoreo. Se ha definido un procedimiento de revisión periódica de registros que cubre al menos inicios de sesión fallidos y acceso y uso de Internet. La información generada se reporta a la gerencia que corresponda y/o demás partes interesadas para la toma de decisiones.	Se realizan actividades de control interno para verificar el cumplimiento con el procedimiento de monitoreo. Se genera información que se utiliza con fines estadísticos y de mejora de los servicios. Los resultados de estas revisiones se utilizan para la mejora del procedimiento y se retroalimentan las lecciones aprendidas.
DE.MC-4. Se detecta el código malicioso.	Los equipos del personal cuentan con protección antivirus. Las soluciones a los problemas	Los servidores que ofician de distribuidores de archivos (por ejemplo, servidores de	Se define una política y procedimientos para el manejo de software malicioso.	Se implementan controles para evitar el acceso a sitios Web maliciosos y/o no autorizados.

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
	detectados se realizan en forma ad-hoc.	archivos o correo electrónico), cuentan con una solución antivirus. Se configuran chequeos periódicos en los equipos del personal. Las actividades de concientización al personal contienen temas específicos sobre riesgos y problemas derivados del software malicioso.	Se cuenta con una solución centralizada de antivirus.	La protección ante software malicioso se extiende a otros dispositivos móviles y se refleja en la política de protección contra software malicioso. Existen procedimientos documentados para la detección de equipos que se encuentran desprotegidos y se realizan las acciones necesarias para subsanar la situación. 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.
DE.MC-5. Se detecta el código móvil no autorizado.	Ver DE.MC-4 (nivel 1)	Ver DE.MC-4 (nivel 2)	Ver DE.MC-4 (nivel 3)	Ver DE.MC-4 (nivel 4)
DE.MC-6. Se controla la actividad de los proveedores de servicios externos para detectar posibles eventos de ciberseguridad.	Se toman acciones ante desvíos detectados en el servicio de un proveedor de un servicio crítico del centro de datos.	Existen SLA con proveedores de servicios críticos del centro de datos. En los contratos con los proveedores de servicios críticos, se incluyen cláusulas de seguridad de la información.	Existen SLA con los proveedores de servicios críticos del centro de datos donde se establece el régimen de cobertura para los servicios críticos conforme las necesidades de la organización. En todos los contratos se incluyen cláusulas de seguridad de la información. Los contratos con los proveedores son revisados ante cambios del servicio.	Se realiza una revisión periódica de los contratos y SLA de los proveedores de servicios críticos para evaluar la adherencia a los acuerdos. La información que surge de la revisión apoya a la toma de decisiones.
DE.MC-7. Se realiza monitoreo para personas, conexiones,	Se establece el monitoreo de los logs generados por los sistemas del control de acceso, a nivel físico y lógico,	Se utilizan reglas para los sistemas de forma independiente, que permiten alertar cuando los	Se definen políticas y procedimientos que definen los términos y condiciones del monitoreo de	El sistema de recolección de log centralizado o sensores dispuestos en la red de la organización,

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
dispositivos y software.	dentro del centro de datos.	usuarios realizan conexiones fuera de la organización, y la conexión e instalación de dispositivos o software no autorizado en equipos de la organización.	personas, conexiones, dispositivos y software. Se amplía el monitoreo a todos los equipos de la organización.	recolectan y emiten alertas relacionadas a las acciones no permitidas por los usuarios sobre la infraestructura y sistemas de la organización.
DE.MC-8. Se realizan escaneos de vulnerabilidades .	Se realizan revisiones puntuales de los sistemas de información con recursos propios o con apoyo externo.	Se realizan revisiones de seguridad de los sistemas en forma periódica o como parte de un cambio significativo en ellos, con recursos propios o con apoyo externo.	Se define un responsable y un procedimiento documentado para la revisión periódica interna de vulnerabilidades con alcance a los sistemas base y de aplicación. Se cuenta con el apoyo de revisiones externas de vulnerabilidades y hackeo ético. Los resultados de las revisiones internas y externas se utilizan para la detección y corrección de vulnerabilidades.	Los resultados de las revisiones internas y externas se utilizan para la mejora continua de la seguridad de los sistemas. Se realizan actividades de control interno para verificar el cumplimiento con el procedimiento de revisión periódica de vulnerabilidades. El procedimiento de revisión de vulnerabilidades se encuentra incorporado en las actividades de seguridad de la información y se decide su realización con una frecuencia mayor, ante cualquier cambio de magnitud (previo análisis de riesgo) o cada vez que se considera necesario.
DE.PD. Procesos de detección Se mantienen procesos y procedimientos de detección y pruebas para asegurar el conocimiento oportuno y adecuado de los eventos anómalos.				
DE.PD-1. Los roles y las responsabilidades de detección se encuentran definidos para asegurar responsabilidades.	Existe personal con tareas asignadas para la detección de eventos a nivel de sistemas base y de protección perimetral.	Se define la participación de roles de TI para las actividades de monitoreo basado en herramientas automatizadas. Se revisan los registros de eventos.	Se ha definido un responsable para las tareas de monitoreo de eventos y existe un procedimiento documentado para la gestión de las actividades de monitoreo. Se realizan pruebas periódicas al	Se realizan actividades de control interno de cumplimiento con el procedimiento de monitoreo de eventos. El resultado de las actividades se comunica al RSI y demás partes interesadas, se utiliza para mejorar el

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
			procedimiento de monitoreo. Este procedimiento define las actividades de comunicación formales que deben realizarse. Se definen los escenarios a probar y los ambientes.	procedimiento y las pruebas y se retroalimentan las lecciones aprendidas.
DE.PD-2 Las actividades de detección cumplen con todos los requisitos aplicables.	La información contenida en los logs es utilizada conforme a los requisitos aplicables, en particular los requisitos legales.	Se utilizan los datos recolectados de acuerdo con la regulación y normativa del sector que corresponda, por ejemplo, protección de datos.	Los procedimientos y actividades de detección son revisados ante cambios en los requisitos aplicables.	De forma periódica se controla el cumplimiento de los requisitos aplicables sobre el monitoreo y las actividades relacionadas.
DE.PD-3 Los procesos de detección son probados.	Se realizan pruebas de los procesos de detección y monitoreo (físico y lógico) de los activos del centro de datos.	Se realizan pruebas de los procesos de detección y monitoreo (físico y lógico) de los activos y usuarios de la organización.	Existen procedimientos que establecen la periodicidad y los criterios para la realización de pruebas de detección. Las pruebas se apoyan en la automatización del proceso para la detección de desvíos. Las pruebas se documentan y se realiza la gestión de cambios. Se identifican las lecciones aprendidas.	Las lecciones aprendidas son utilizadas para la mejora del SGSI, particularmente para la gestión de riesgos.
DE.PD-4. La información de la detección de eventos es comunicada a las partes pertinentes.	Al detectar eventos anómalos o potencialmente anómalos, se comunica a algún referente o autoridad con capacidad de articular soluciones.	Existen mecanismos de comunicación definidos ante la detección de eventos anómalos, y estos son ejecutados cuando efectivamente se detectan.	Existe un procedimiento de monitoreo que contiene actividades de comunicación. Dentro de las pruebas realizadas al procedimiento de monitoreo, se incluyen pruebas a las actividades de comunicación.	El responsable del monitoreo de eventos trabaja en forma coordinada con el RSI. Se realizan revisiones de control interno de cumplimiento con el procedimiento de monitoreo y de las actividades de comunicación. El resultado de las revisiones se utiliza para mejorar el procedimiento y las

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
				pruebas. Se retroalimentan las lecciones aprendidas.
DE.PD-5. Los procesos de detección son mejorados continuamente.	Toda incorporación o modificación de los sistemas críticos e infraestructuras del centro de datos son reflejados en el monitoreo.	Toda incorporación o modificación de los sistemas del negocio son reflejados en el monitoreo.	Se define el procedimiento monitoreo de los activos de información de la organización. Se correlacionan los eventos de los distintos sistemas de monitoreo. Se automatizan las alertas ante desvíos.	Ver DE.PD-4 (nivel 4)

6.4 Función: RESPONDER (RE)

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RE.PR. Planificación de la respuesta Los procesos y procedimientos de respuesta se ejecutan y se mantienen garantizando una respuesta oportuna para detectar eventos de ciberseguridad.				
RE.PR-1. El plan de respuesta se ejecuta durante o luego de un evento.	Se establecen los mecanismos de respuesta a incidentes. Se informa al CERTuy o CSIRT que corresponda, sobre los incidentes detectados.	Los mecanismos de respuesta a incidentes se documentan en un plan y/o procedimiento que son difundidos a todos los interesados. Los incidentes y la respuesta realizada se registran. Se informa a las gerencias involucradas sobre los incidentes.	El plan y/o procedimiento de respuesta es ajustado según la política de gestión de incidentes. Se define un responsable de la respuesta a incidentes. Se trabaja en la mejora de los procesos operativos post incidentes de seguridad de la información lo cual se ve reflejado a nivel de política, plan y/o procedimientos. El responsable de la respuesta trabaja activamente con el CERTuy o CSIRT correspondiente.	Se realizan revisiones de control interno para verificar el cumplimiento del plan y/o procedimiento de respuesta. La Dirección, el RSI y el CSI reciben información periódica sobre incidentes de seguridad de la información. Dicha información apoya la toma de decisiones y se registran lecciones aprendidas que son utilizadas para la mejora continua de la respuesta a incidentes.

RE.CO. Comunicaciones Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según corresponda.				
RE.CO-1. El personal conoce sus roles y el orden de operaciones cuando es necesaria una respuesta	Ver RE.PR-1 (nivel 1)	Se determina el plan y/o procedimiento de respuesta a incidentes. Se han definido y realizado actividades de concientización en seguridad de la información.	Existe una política de gestión de incidentes que ha sido difundida al personal. En las actividades de concientización y capacitación se incluyen temas que abarcan las actividades del plan y/o procedimiento de respuesta y el procedimiento de reporte de incidentes en función de cada rol.	Se realizan pruebas del plan de respuesta, incluyendo a usuarios clave para reforzar sus conocimientos sobre sus roles. Se realizan actividades de control interno para verificar el cumplimiento del plan y/o procedimiento de respuesta.
RE.CO-2. Los eventos son reportados consistentemente con los criterios establecidos.	Ver PR.PI-9 (nivel 1)	Existe un único punto de contacto interno a la organización. El punto de contacto reporta los incidentes de seguridad informática al CERTuy o equipo de respuesta que corresponda de acuerdo a los criterios establecidos por éste.	Existe una política de gestión de incidentes y se ha definido un plan y/o procedimiento alineado a ella, que contiene actividades de comunicación con interesados. El reporte de eventos y la gestión de incidentes se apoyan en herramientas automatizadas.	Se realizan actividades de control interno de cumplimiento con el procedimiento de reporte y gestión de incidentes. El resultado de las actividades se utiliza para mejorar el procedimiento de reporte y gestión de incidentes y se retroalimentan las lecciones aprendidas.
RE.CO-3. La información se comparte consistentemente con los planes de respuesta.	Ver PR.PI-9 (nivel 1)	Ver PR.PI-9 (nivel 2)	Ver PR.PI-9 (nivel 3)	Ver PR.PI-9 (nivel 4)

RE.CO-4. La coordinación con las partes interesadas se realiza consistentemente con los planes de respuesta.	Se mantiene contacto con actores clave internos y externos durante la gestión de incidentes. Se escalan las necesidades puntuales, por ejemplo, al CERTuy o CSIRT del sector.	Se identifican los potenciales actores internos y externos ante un incidente y se registran sus datos de contacto. Se determina y documenta el mecanismo de escalamiento de incidentes.	Existe una política de gestión de incidentes y se ha definido un plan y/o procedimiento alineado a ella, que contiene actividades de comunicación con interesados.	Se ha definido un responsable que coordina la respuesta ante incidentes. Se realizan actividades de control interno de cumplimiento con el procedimiento de reporte y gestión de incidentes, y plan de respuesta. El resultado de las actividades se utiliza para mejorar el procedimiento y los planes. Se retroalimentan las lecciones aprendidas.
RE.CO-5. Se realiza intercambio de información voluntaria con partes interesadas externas para alcanzar una conciencia de ciberseguridad más amplia.	Ver RE.CO-4 (nivel 1)	Ver RE.CO-4 (nivel 2)	Ver RE.CO-4 (nivel 3)	Ver RE.CO-4 (nivel 4)
RE.AN. Análisis Se efectúa análisis para asegurar una respuesta adecuada y dar soporte a las actividades de recuperación.				
RE.AN-1. Se investigan las notificaciones de los sistemas de detección.	Los sistemas registran eventos y/o envían notificaciones de seguridad que se analizan reactivamente y se escalan cuando corresponde.	Se definen pautas generales para el registro de eventos y los nuevos sistemas se despliegan de acuerdo a ellas. Se determina cuando un evento o notificación conforma un incidente y se clasifica según su criticidad y severidad.	Se define una política de auditoría y registro de eventos. Existe un procedimiento documentado y alineado a la política. Se define si se escala un incidente considerando: activos afectados, criticidad y severidad.	El procedimiento incorpora mejores prácticas que incluyen actividades de análisis forense y custodia de la información. Se realizan actividades de control interno de cumplimiento del procedimiento. El resultado de las actividades se utiliza para el proceso de mejora continua.

RE.AN-2. El impacto del incidente es comprendido.	Se llevan a cabo actividades de análisis de impacto y actividades de respuesta en forma ad-hoc. Se informa al CERTuy o CSIRT que corresponda, sobre los incidentes detectados.	Existen pautas para la clasificación de incidentes, que son utilizadas en la gestión de todos los incidentes.	La respuesta a incidentes se realiza dentro del marco del plan y/o procedimiento de respuesta, alineado a la política de gestión de incidentes. Existe un procedimiento de gestión de incidentes que incluye las tareas de análisis de impacto. Se cuenta con herramientas automatizadas para el registro de incidentes alineadas con el plan y/o procedimiento de respuesta definido.	El procedimiento incorpora mejores prácticas que incluyen actividades de análisis forense y custodia de la información, así como también actividades a realizar post incidente. Se sistematizan las lecciones aprendidas, que son utilizadas para la mejora de los procedimientos, los procesos y las estrategias de mitigación y respuesta.
RE.AN-3. Se realiza análisis forense.	Ante un incidente de seguridad de la información en el centro de datos, la organización realiza un análisis forense o contacta a su CSIRT de referencia para llevarlo adelante.	Ante un incidente de seguridad de la información, la organización realiza un análisis forense o contacta a su CSIRT de referencia para llevarlo adelante. Se tienen pautas establecidas para garantizar la cadena de custodia. Se generan los informes pertinentes y se distribuyen a las partes interesadas.	Todos los procedimientos vinculados al análisis forense se encuentran documentados. La documentación es realizada por personal calificado.	El resultado del análisis forense es utilizado para la mejora continua del SGSI de la organización; en particular para la gestión de riesgos de seguridad de la información.
RE.AN-4. Los incidentes son categorizados consistentemente con los planes de respuesta.	Se han definido lineamientos para la categorización de los incidentes según su tipo y criticidad.	Se determinan las acciones y tiempos de respuesta asociados a cada categoría según severidad.	Se define una política de gestión de incidentes de seguridad de la información y se difunde. Se define un plan de respuesta para la gestión de incidentes. Las acciones asociadas a cada categoría están alineadas al plan de respuesta. Se cuenta con herramientas que apoyan la gestión de los incidentes.	La categorización de incidentes y los planes de respuesta se revisan periódicamente, considerando las necesidades del negocio y las tendencias de amenazas. Se realizan estadísticas utilizando las categorizaciones, los resultados son utilizados para mejorar o incrementar los controles existentes.

RE-AN-5. Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	Se establecen canales de comunicación y fuentes de información para alertar las posibles vulnerabilidades que puedan afectar los activos y servicios críticos del centro de datos.	Se establecen canales de comunicación y fuentes de información para alertar las posibles vulnerabilidades que puedan afectar los activos y servicios críticos de la organización. Se establece un mecanismo de acción en base a la criticidad de las vulnerabilidades.	Se define una metodología para la gestión de vulnerabilidades, así como los procedimientos necesarios para su implementación. Se cuenta con herramientas que apoyan la gestión de vulnerabilidades.	Las fuentes de datos son revisadas periódicamente. La metodología se adecua conforme las necesidades del negocio y su contexto. La gestión de vulnerabilidades es utilizada para la mejora continua del SGSI.
RE.MI. Mitigación Se ejecutan actividades para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.				
RE.MI-1. Se logra contener los incidentes.	Existen mecanismos de respuesta a incidentes, especialmente para contenerlos. Se atiende y se mitigan las consecuencias de los incidentes. Se mantiene un registro de los incidentes. Se informa al CERTuy o CSIRT que corresponda, así como a otras partes interesadas, sobre los incidentes detectados.	Se han definido pautas para contener el daño y minimizar el riesgo en el entorno operativo. Se informa a las gerencias sobre los incidentes. Se cuenta con planes de remediación de los incidentes.	Existe una política de gestión de incidentes que ha sido difundida al personal y se ha definido un plan y/o procedimiento alineado a ella. Se cuenta con herramientas automatizadas para el registro de incidentes, alineadas con el plan de respuesta definido.	Ver RE.AN-2 (nivel 4)
RE.MI-2. Se logra mitigar los incidentes.	Ver RE.MI-1 (nivel 1)	Ver RE.MI-1 (nivel 2)	Ver RE.MI-1 (nivel 3)	Ver RE.MI-1 (nivel 4)
RE.MI-3. Las nuevas vulnerabilidades identificadas se mitigan o documentan como riesgos aceptados.	Ver RE.MI-1 (nivel 1)	Ver RE.MI-1 (nivel 2)	Ver RE.MI-1 (nivel 3)	Ver RE.MI-1 (nivel 4)
RE.ME. Mejoras Las actividades de respuesta de la organización son mejoradas por la incorporación de lecciones aprendidas de las actividades de detección y respuesta actuales y anteriores.				

RE.ME-1. Los planes de respuesta incorporan lecciones aprendidas.	Se identifican las lecciones aprendidas de los incidentes de seguridad de la información vinculados al centro de datos.	Se identifican las lecciones aprendidas de los incidentes de seguridad de la información en toda la organización.	Las lecciones aprendidas son puestas a disposición y comunicadas a todas las partes interesadas. Se cuenta con herramientas que dan soporte a su registro y gestión.	Las lecciones aprendidas son utilizadas para la mejora del SGSI, en particular para la gestión de riesgos de seguridad de la información. Se generan indicadores para seguimiento y control.
RE.ME-2. Las estrategias de respuesta se actualizan.	Se revisan periódicamente las estrategias de respuesta del centro de datos, o ante cambios en las necesidades del negocio.	Se revisan periódicamente las estrategias de respuesta de los procesos de la organización que afecten los servicios críticos.	Se cuenta con pautas o políticas documentadas para llevar adelante las revisiones de las estrategias de respuesta.	Las mejoras identificadas en las revisiones de estrategia son utilizadas para su ajuste, así como para la mejora del SGSI, en particular para la gestión de riesgos de seguridad de la información. Se generan indicadores para seguimiento y control.

6.5 Función: RECUPERAR (RC)

Subcategoría	Nivel 1	Nivel 2	Nivel 3	Nivel 4
RC.PR. Planificación de la recuperación Los procesos y procedimientos de recuperación son ejecutados y mantenidos para asegurar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad.				
RC.PR-1. El plan de recuperación se ejecuta durante o luego de un evento.	Existen medidas de continuidad en el centro de datos (alimentación redundante de energía eléctrica, medidas de control ambiental y redundancia en las telecomunicaciones) que favorecen a la recuperación luego de un evento de ciberseguridad. Se informa al CERTuy o CSIRT que corresponda sobre los incidentes detectados.	Se trabaja en la elaboración de un plan y/o procedimiento de respuesta a incidentes. Existen lineamientos establecidos para la ejecución de actividades de recuperación ante incidentes.	Existe un plan de contingencia y recuperación. Se realizan algunas pruebas (que se registran) al plan de contingencia y recuperación.	Se define un responsable de respuesta a incidentes que lleva adelante las tareas de recuperación en coordinación con los actores involucrados. El plan y/o procedimiento de respuesta y el plan de contingencia y recuperación son probados anualmente. Los resultados de las pruebas son comunicados a la Dirección y otras partes interesadas. La información de las pruebas, retroalimentan las lecciones aprendidas que se utilizan para la mejora continua de los planes y procedimientos.

RC.ME. Mejoras Se mejoran los planes y procesos de recuperación incorporando las lecciones aprendidas en actividades futuras.				
RC.ME-1. Los planes de recuperación incorporan lecciones aprendidas.	Ver RE.ME-1 (nivel 1)	Ver RE.ME-1 (nivel 2)	Ver RE.ME-1 (nivel 3)	Ver RE.ME-1 (nivel 4)
RC.ME-2 Las estrategias de recuperación se actualizan.	Se revisan periódicamente las estrategias de recuperación del centro de datos, o ante cambios en las necesidades del negocio.	Se revisan periódicamente las estrategias de recuperación de los procesos de la organización, en particular de los servicios críticos. Las estrategias son comunicadas a toda la organización y se hace énfasis en aquellas que por su relación con el funcionamiento de los servicios críticos requieren apoyar la recuperación.	Se cuenta con pautas o políticas documentadas para llevar adelante las revisiones de las estrategias de recuperación en base a los cambios que son determinados por el BIA.	Ver RE.ME-2 (nivel 4)
RC.CO. Comunicaciones Las actividades de recuperación se coordinan con las partes interesadas internas y externas, como centros de coordinación, proveedores de servicios de Internet, propietarios de los sistemas afectados, las víctimas, otros CSIRT y vendedores.				

RC.CO-1. Se gestiona las relaciones públicas.	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. Las áreas técnicas no realizan comunicación externa salvo autorización expresa.	Se ha definido un único interlocutor (vocero) autorizado a comunicar una situación de crisis o situación que afecta la ciberseguridad o seguridad de la información de la organización. Se difunde al personal quién es el vocero y cuál es la vía de contacto.	Se ha definido un plan de comunicaciones ante crisis junto con un procedimiento que cubre la evaluación del evento, las notificaciones, nivel de comunicación requerido, mensajes, audiencia, interesados y monitoreo de las comunicaciones. El plan y el procedimiento son difundidos a los actores correspondientes.	Se realizan ensayos de crisis poniendo en práctica el plan y el procedimiento de comunicación. Se realizan revisiones de control interno para verificar el cumplimiento del plan y procedimiento de comunicaciones ante crisis. Los resultados de las revisiones se registran y se utilizan para la mejora continua. La Dirección participa activamente en las actualizaciones del plan, en especial, en la aprobación y modo de difusión de los mensajes.
RC.CO-2. Se repara la reputación luego del evento.	Ver RC.CO-1 (nivel 1)	Ver RC.CO-1 (nivel 2)	Ver RC.CO-1 (nivel 3)	Ver RC.CO-1 (nivel 4)
RC.CO-3. Se comunican las actividades de recuperación a los interesados internos y a los equipos ejecutivos y de gestión.	Ver RC.CO-1 (nivel 1)	Ver RC.CO-1 (nivel 2)	Ver RC.CO-1 (nivel 3)	Ver RC.CO-1 (nivel 4)

7 Glosario

7.1 Abreviaturas

ABM	Altas Bajas Modificaciones
BIA	Business Impacto Analysis
DLP	Data Loss Prevention
EMG	Estándar Mínimo de Gestión (Banco Central de Uruguay)
CPD	Centro de Procesamiento de Datos. Centro de datos. Data center.
CSI	Comité de Seguridad de la Información
CSIRT	Computer Security Incident Response Team (Equipo de Respuesta ante Incidentes de Seguridad Informática)
RSI	Responsable de la Seguridad de la Información
SGSI	Sistema de Gestión de Seguridad de la Información
SLA	Service Level Agreement (Acuerdo de Nivel de Servicio)
TI	Tecnología de la Información
WAF	Web Application Firewall

7.2 Definiciones

A

Amenaza

Causa potencial de un incidente no deseado, que puede dar lugar a daños en un sistema o en una organización. [ISO/IEC 27000:2009]

B

BIA (del inglés Business Impact Analysis)
Un análisis de impacto en el negocio está orientado a identificar qué procesos de negocio podrían verse afectados y de qué forma, ante la materialización de los riesgos identificados. Sus objetivos principales son identificar los procesos críticos del negocio y definir su prioridad en función del impacto relacionado a una interrupción (organizacional, financiero, de imagen, etc.) para la organización.

C

CERTuy
El CERTuy es el Centro Nacional de Respuesta a Incidentes de Seguridad Informática del Uruguay. Un CERT (del inglés Computer Emergency Response Team / Coordination Center) es un equipo de respuesta y un centro de coordinación de emergencias informáticas. [Sitio oficial del CERTuy: www.cert.uy]

Código móvil
Programas de software o partes de programas obtenidos de sistemas de información remoto, transmitidos a través de una red y ejecutados en un sistema de información local sin instalación o ejecución explícita por parte del destinatario (por ejemplo, un agente o una macro de un documento). [NIST SP 800-53 Rev. 4 - “Mobile code” p93]

Cadena de suministro
Sistema organizacional, personas, actividades, información y recursos, posiblemente de alcance internacional, que proporciona productos o servicios a los consumidores. [NIST SP 800-53 Rev. 4 - “Supply Chain” Page B-19]

E

Evento de seguridad informática
Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica que una posible violación de la política de seguridad de la información, la falla de medidas de seguridad o una situación previamente desconocida, que pueda ser relevante para la seguridad. [Decreto N° 451/009 de 28 de Setiembre 2009 – Art.3 Definiciones]

I

Incidente de seguridad informática
Es una violación o una amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que compromete la seguridad de un sistema (confidencialidad, integridad o disponibilidad). [Decreto N° 451/009 de 28 de Setiembre 2009- Art.3 Definiciones]

Incidente de seguridad de la información
Un incidente de seguridad de la información es indicado por un único o una serie de eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información. [ISO/IEC 27035:2011]

L

Línea base
Una especificación o producto que se ha revisado formalmente y sobre los que se ha llegado a un acuerdo, y que de ahí en adelante sirve como base para un desarrollo posterior y que puede cambiarse solamente a través de procedimientos formales de control de cambios. [IEEE 610.12/1990]

P

Propietario de activos
El término propietario identifica un individuo o entidad que ha probado habilidades de gestión para controlar la producción, desarrollo, mantenimiento, uso y seguridad de un activo. El término propietario no significa que la persona tiene efectivamente derechos de propiedad sobre el activo. [Agesic (políticas marco, políticas del SGSI, políticas de Presidencia – Manual de Políticas de Seguridad de la Información / Gestión de Activos / Responsabilidad sobre los activos]

Plan de respuesta a incidentes
Este documento contiene, además del procedimiento de respuesta a incidentes, la planificación de la respuesta, por ejemplo: introducción, roles y responsabilidades, metodología, fases de las respuestas a incidentes, plan de comunicación, documentación, etc.

R

Remediación de incidente
Consiste en las actividades necesarias de reparación o mitigación realizadas para subsanar la causa raíz que viabilizó un incidente o vulnerabilidad detectadas en sistemas o procesos.

S

SLA (del inglés Service Level Agreement)
Acuerdo negociado entre dos partes, una cliente y otra proveedora, donde se definen puntos comunes de entendimiento sobre servicios, prioridades, responsabilidades y garantías. Incluye elementos tales como definición de los servicios, garantías y finalización del acuerdo, medición del rendimiento, gestión de problemas, obligaciones de las partes, entre otros.

Software de aplicación
Programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos.

Software de base
Software que sirve para controlar e interactuar con el sistema operativo, proporcionando control sobre el hardware y dando soporte a otros programas, incluyendo el propio sistema operativo.

U

Usuario privilegiado
Es aquel que tiene autorización administrativa. Usuario con rol administrador.

V

Vulnerabilidad
Debilidad de un activo o control que puede ser explotada por una amenaza. [ISO/IEC 27000:2009]

W

WAF (del inglés Web Application Firewall)
Un Firewall de Aplicaciones Web es un dispositivo de hardware o software que permite proteger los servidores de aplicaciones Web de determinados ataques específicos en Internet.