Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

Curso Ciberseguridad para Auditores Internos

Taller del Marco de Ciberseguridad del NIST

Santiago, 18 de octubre de 2018

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia

Ciberseguridad

Carlos Silva

Certified Information Systems Auditor (CISA), Licenciado en Informática, Master en Gestión de Proyectos

Consultor Internacional

Sobre el conferencista

Carlos Silva

Certified Information Systems Auditor (CISA)

Consultor Internacional

<

- 2018 a la fecha Gerente de Infotecnología, Dirección Adjunta de Rentas Aduaneras
- 2016 -2017 Cowater-Sogema Internacional Inc. Latin America Audit ExpertOttawa, Canadá, Consultor Experto para Latinoamérica de Auditoría de Sistemas de Información y Comunicaciones, Implementación de Gobierno y Gestión de las Tecnologías de la información (TI), Análisis y Evaluación de Riesgos y elaboración de Planes de Contingencia.
- 2017, Banco Nacional de Desarrollo Agrícola, Gerente de Tecnología, • Implementación de mejoras en el Core Bancario BYTE e implementación de nuevos servicios financieros
- • Implementación de gobierno y gestión de TI empresarial, • Análisis y evaluación de riesgos y elaboración de Planes de Contingencia, • Soporte para la creación de políticas institucionales de TI, asesoramiento para la creación de comités tecnológicos de información, evaluación de procesos y controles de TI, elaboración de procesos de planificación de TI, implementación de medidas de seguridad informática, • Supervisión y monitoreo de la plataforma tecnológica del banco
- 2016-2017 Contraloría General de la República de Cuba, La Habana, Cuba, • Facilitador COBIT5, • Implementación del marco comercial para la gobernanza y la gestión de las TI empresariales
- - 2005 – 2017, TRIBUNAL SUPERIOR DE CUENTAS; Director de Tecnología, Experiencia en realización de auditorías informáticas integrales y evaluación de estructuras de gobierno de Tecnologías de la Información (TI) en varias entidades gubernamentales del Gobierno de Honduras

Marco de trabajo de ciberseguridad del NIST

Historia y antecedentes

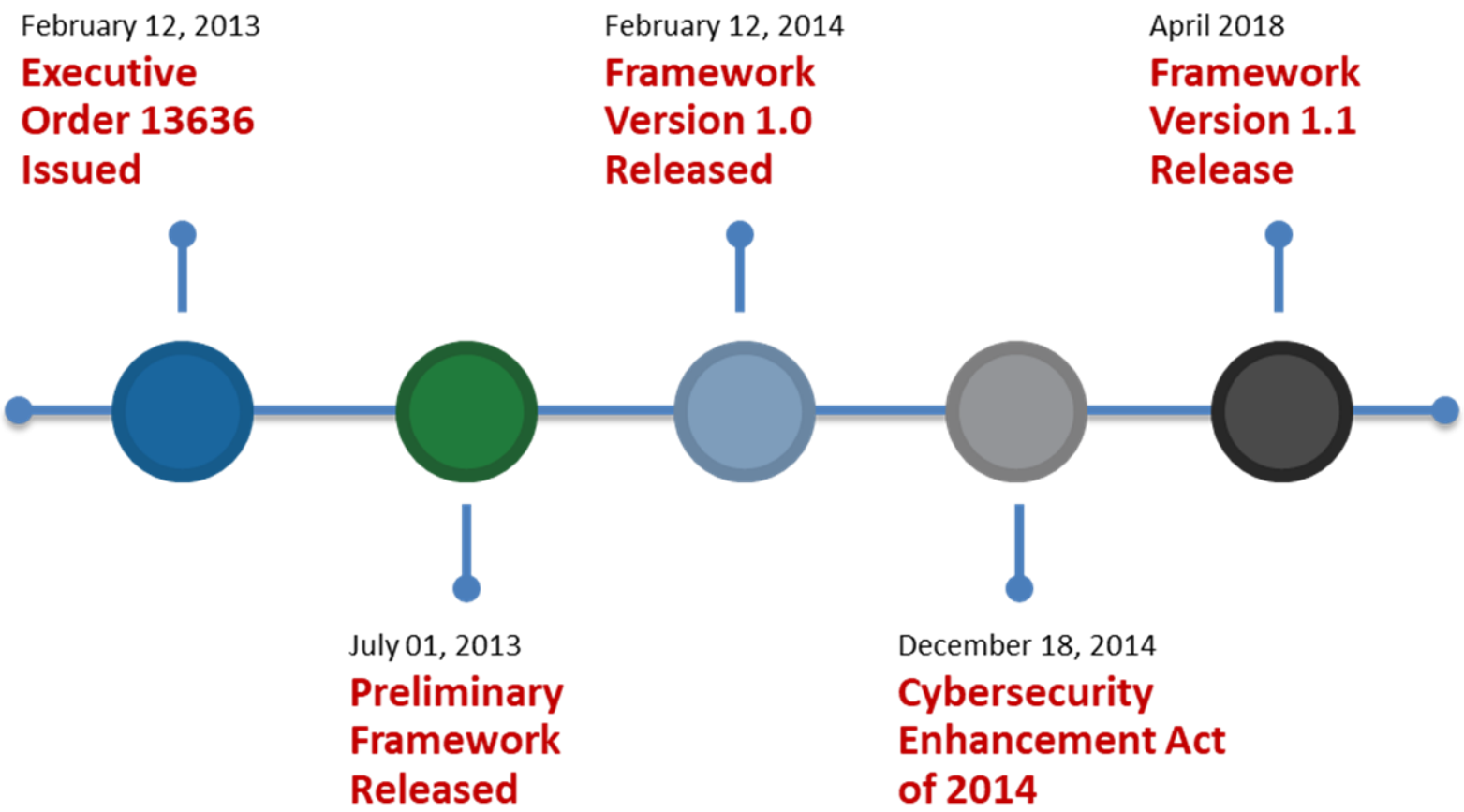
Como resultado de la creciente cantidad de ataques informáticos a sistemas de infraestructuras críticas y al impacto que dichos ataques pudieran tener en el contexto de la seguridad nacional de Estados Unidos, el 12 de febrero de 2013 el Presidente Barack Obama redactó la Orden Ejecutiva (EO) de Mejora de Ciberseguridad de Infraestructuras Críticas (Executive Order 13636 -- Improving Critical Infrastructure Cybersecurity) en donde se delegaba en el NIST (National Institute of Standards and Technology) el desarrollo de un marco de trabajo para la reducción de riesgos asociados con este tipo de entornos, con el soporte del Gobierno, la industria y los usuarios.

Marco de trabajo de ciberseguridad del NIST

El resultado de este trabajo - posterior a la publicación de múltiples versiones preliminares y recepción de contribuciones de voluntarios a través del modelo de Request for Information (RFI) – fue la primera versión del documento "Framework for Improving Critical Infrastructure Cybersecurity", conocido como "NIST Cybersecurity Framework" , que se publicó el 12 de febrero de 2014.

Es de anotar que esta iniciativa no es pionera en su campo. Desde mucho tiempo antes, la OTAN (a través del Centro de Excelencia de Ciberdefensa Cooperativa – CCDCOE) ya había desarrollado una serie de manuales orientados hacia la protección de infraestructuras críticas para la defensa nacional, como es el caso del "Manual del Marco de Trabajo de Ciberseguridad Nacional" (National Cyber Security Framework Manual) publicado en 2012 . Igualmente, ISO/IEC con su estándar ISO/IEC 27032:2012 "Information technology -- Security techniques -- Guidelines for cybersecurity" había sentado un precedente en la definición de guías para la mejora de ciberseguridad. Esto no quiere decir que el marco de trabajo de ciberseguridad del NIST excluya estos documentos, al contrario, los complementa y mejora.

Eras del Marco de Ciberseguridad



Versiones del Marco de Ciberseguridad

Componente	Version 1.0	Version 1.1	Comentarios
Funciones	5	5	
Categorias	22	23	• Adiciona una nueva categoría ID.SC – Riesgo de la cadena de suministro Gestión (ID.SC)
Subcategorias	98	108	• Adiciona 5 subcategorias in ID.SC • Adiciona 2 subcategorias in PR.AC • Adiciona 1 subcategoria para PR.DS, PR.PT, RS.AN • Lenguaje clarificado en 7 otras
Referencias Informátivas	5	5	

¿Cuáles son los objetivos del marco de trabajo de ciberseguridad del NIST?

- Las bases del CSF fueron establecidas directamente en la Orden Ejecutiva 13636:
- Identificar estándares de seguridad y guías aplicables de forma trasversal a todos los sectores de infraestructuras críticas
- Establecer un lenguaje común para gestionar riesgos de ciberseguridad
- Proveer un enfoque priorizado, flexible, repetible, neutral, basado en desempeño y efectivo en términos de coste-beneficio basado en las necesidades del negocio
- Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos

¿Cuáles son los objetivos del marco de trabajo de ciberseguridad del NIST?

- Establecer criterios para la definición de métricas para el control del desempeño en la implementación.
- Establecer controles para proteger la propiedad intelectual, la privacidad de los individuos y las libertades civiles cuando se ejecuten actividades de ciberseguridad.
- Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones orientadas al desarrollo de estándares.
- No introducir nuevos estándares cuando existan iniciativas ya desarrolladas que cubran los objetivos de la orden ejecutiva.

¿Cuáles son los objetivos del marco de trabajo de ciberseguridad del NIST?

- De acuerdo con el NIST:

- *"El marco de trabajo de Ciberseguridad: es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la seguridad cibernética entre los interesados internos y externos de la organización*".

¿Cuáles son los objetivos del marco de trabajo de ciberseguridad del NIST?

De acuerdo con lo anterior, los objetivos del marco de trabajo en su implementación en una organización se podrían catalogar en los siguientes puntos:

- Describir la postura actual de ciberseguridad
- Describir el estado objetivo de ciberseguridad
- Identificar y priorizar oportunidades de mejora en el contexto de un proceso continuo y repetible
- Evaluar el progreso hacia el estado objetivo
- Comunicación entre las partes interesadas internas y externas sobre el riesgo de ciberseguridad
- Todo esto enmarcado en un enfoque orientado a la gestión del riesgo.

¿Es obligatoria su implementación?

- En principio, no.

Se trata de una guía de implementación discrecional con base en las mejores prácticas y estándares de la industria. No obstante, es posible que socios de negocio, clientes o incluso organizaciones gubernamentales requieran el cumplimiento del marco de trabajo dentro de sus consideraciones contractuales.

¿A qué tipo de organizaciones aplica?

A pesar que el marco de trabajo fue desarrollado teniendo en mente la protección de la infraestructura crítica de Estados Unidos, su implementación es asumible de forma indistinta en cualquier organización independientemente de su tamaño, grado de riesgo o sofisticación de ciberseguridad.

Es importante tener presente que el marco de trabajo no es un documento estático, sino que cada organización puede determinar – con base en sus necesidades – las actividades que considera prioritarias, permitiendo de esa forma un despliegue personalizado y paulatino.

¿Se puede implementar en organizaciones fuera de Estados Unidos?

Debido a que la base del marco de trabajo está fundamentada en la integración de los criterios de diferentes estándares, directrices y mejores prácticas a nivel internacional, su implementación no está limitada únicamente a Estados Unidos. De hecho, su despliegue fuera de las fronteras de ese país agrega una nueva capa de cooperación e integración global en ciberseguridad, tema que no está restringido a un ámbito geográfico en particular.

¿En qué estándares, directrices y mejores prácticas está basado?

- El CSF está basado y/o hace referencia a los siguientes estándares, directrices y mejores prácticas:
  Control Objectives for Information and Related Technology (COBIT)
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC)
- 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
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels
- ISO/IEC 27001:2013, Information technology --Security techniques --Information security management systems --Requirements
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

¿Cómo está esquematizado el CSF?

- El marco de trabajo se encuentra compuesto de tres partes principales: **El marco básico** (Framework Core), **los niveles de implementación del marco** (Framework Implementation Tiers) **y los perfiles del marco** (Framework Profiles).

Componentes del Marco de Ciberseguridad

Marco básico (Framework Core)

Es un conjunto de actividades de ciberseguridad, resultados esperados y referencias aplicables que son comunes a los sectores de infraestructuras críticas, en términos de estándares de la industria, directrices y prácticas que permiten la comunicación de actividades de ciberseguridad y sus resultados a lo largo de la organización, desde el nivel ejecutivo hasta el nivel de implementación/operación.

Marco básico (Framework Core)

- **Para ello, emplea cinco funciones fundamentales:**

- Identificar (Identify): Permite determinar los sistemas, activos, datos y competencias de la organización, su contexto de negocio, los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan este entorno.

- Proteger (Protect): Permite desarrollar e implementar las contramedidas y salvaguardas necesarias para limitar o contener el impacto de un evento potencial de ciberseguridad.

- Detectar (Detect): Permite desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través de la monitorización continua.

- Responder (Respond): Permite la definición y despliegue de actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.

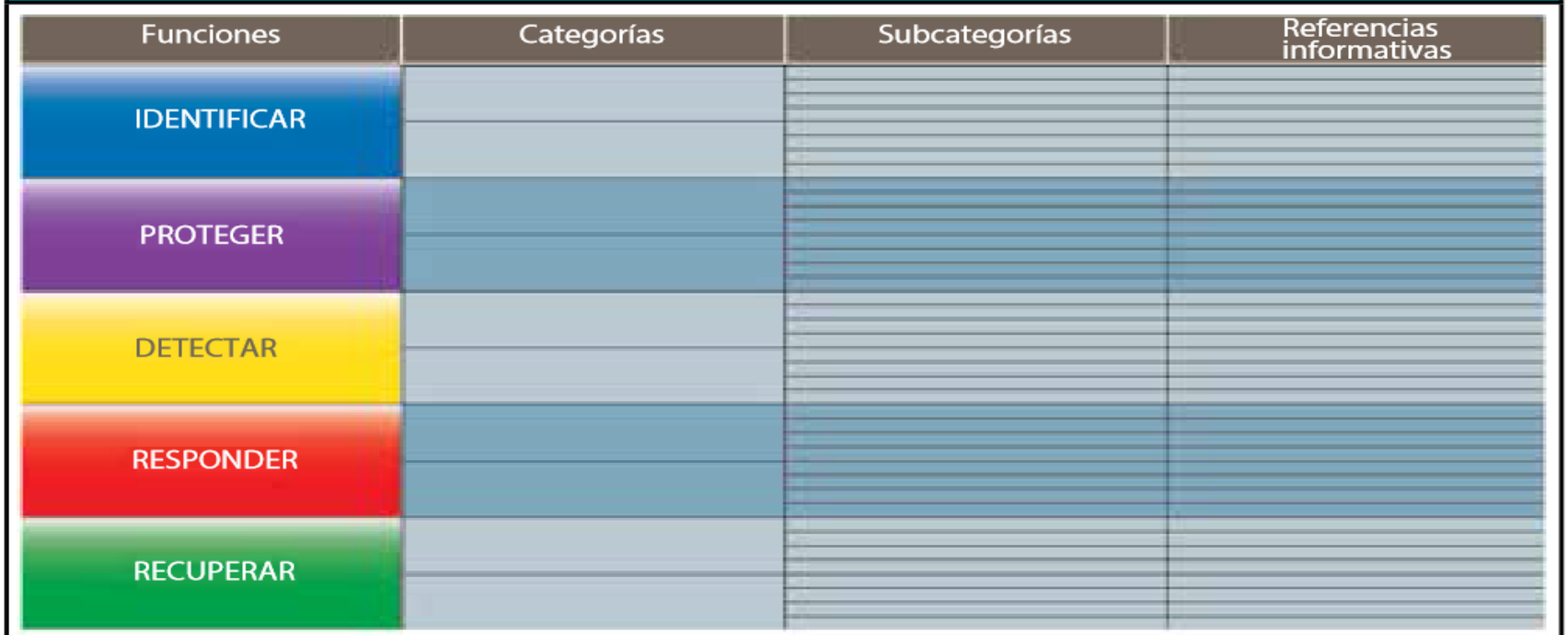
- Recuperar (Recover): Permite el despliegue de actividades para la gestión de resiliencia y el retorno a la operación normal después de un incidente.

Marco básico (Framework Core)

Marco básico (Framework Core)

A su vez, cada una de estas funciones cuenta con categorías y sub-categorías con sus referencias informativas relacionadas (estándares, directrices y prácticas).

Figura 11: Componentes del Marco Básico



Fuente: *Marco para Mejorar la Ciberseguridad de la Infraestructura Crítica*, NIST, EE. UU., 2014, figura 1

Marco básico (Framework Core)

Figura 12: Identificadores y Categorías del Marco Básico

Categoría Único Identificador	Funciones	Función Único Identificador	Categorías
ID	Identificar	AM	Gestión de Activos
		BE	Entorno de Negocio
		GV	Gobierno
		RA	Evaluación del riesgo
		RM	Estrategia de Gestión de Riesgos
PR	Proteger	AC	Control de Acceso
		AT	Concienciación y Capacitación
		DS	Seguridad de los Datos
		IP	Procesos e Información de Protección de Información
		PT	Tecnología de Protección
DE	Detectar	AE	Anomalías y Eventos
		CM	Monitoreo Continuo de Seguridad
		DP	Procesos de Detección
RS	Responder	CO	Comunicaciones
		AN	Análisis
		MI	Mitigación
		IM	Mejoras
RC	Recuperar	RP	Planificación de Recuperación
		IM	Mejoras
		CO	Comunicaciones

Fuente: *Marco para Mejorar la Ciberseguridad de la Infraestructura Crítica*, NIST, EE. UU., 2014, tabla 1

Niveles de implementación del marco (Framework Implementation Tiers)

Los niveles de implementación le permiten a la organización catalogarse en un umbral predefinido en función de las prácticas actuales de gestión de riesgo, el entorno de amenazas, los requerimientos legales y regulatorios, los objetivos y misión del negocio y las restricciones de la propia empresa

Función	Categoría	Subcategoría	Referencias Informativas
IDENTIFICAR (ID)	**Gestión de Activos (ID.AM):** Los datos, personal, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio están identificados y gestionados de manera consistente con su importancia relativa para los objetivos de negocio y la estrategia de riesgo de la organización.	**ID.AM-1:** Se mantiene un inventario de los dispositivos físicos y sistemas dentro de la organización.	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **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
		ID.AM-2: Se mantiene un inventario de las plataformas y aplicaciones de software dentro de la organización.	• **CCS 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 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Se mapea la comunicación organizacional con los flujos de datos.	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Se catalogan los sistemas de información externos .	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, y software) se priorizan en base a su clasificación, importancia y valor para el negocio.	• **COBIT 5** APO03.03, APO03.04, 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
		ID.AM-6: Se establecen los roles y responsabilidades de ciberseguridad para todo el personal y partes interesadas (por ejemplo: proveedores, clientes o socios).	• **COBIT 5** APO01.02, 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

Función	Categoría	Subcategoría	Referencias Informativas
IDENTIFICAR (ID)	**Entorno de Negocio (ID.BE):** Se comprende y prioriza la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar sobre los roles, las responsabilidades y la toma de decisiones de ciberseguridad.	**ID.BE-1:** Se identifica y comunica el rol de la organización en la cadena de suministro.	• **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 • **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 • **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: Se identifica y comunica la ubicación de la organización en la infraestructura crítica y en su sector industrial.	• **COBIT 5** APO02.06, APO03.01 • **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Se establecen y comunican las prioridades para la misión, objetivos y actividades de la organización.	• **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
		ID.BE-4: Se establecen las dependencias y las funciones críticas para la entrega de servicios críticos.	• **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
		ID.BE-5: Se establecen requisitos de resiliencia para dar soporte a la prestación de servicios críticos.	• **COBIT 5** DSS04.02 • **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-14
	Gobierno (ID.GV): Se comprenden las políticas, procedimientos y procesos para gestionar y monitorear los requisitos regulatorios, legales, de riesgos, ambientales y operacionales de la organización, y se informa a la gerencia sobre los riesgos de ciberseguridad.	**ID.GV-1:** Se ha establecido una política organizacional de seguridad de la información.	• **COBIT 5** APO01.03, 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
		ID.GV-2: Las responsabilidades y los roles de seguridad de la información se coordinan y alinean con los roles internos y los socios externos.	• **COBIT 5** APO13.12 • **ISA 62443-2-1:2009** 4.3.2.3.3 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1 • **NIST SP 800-53 Rev. 4** PM-1, PS-7

Función	Categoría	Subcategoría	Referencias Informativas
IDENTIFICAR (ID)	**Gobierno (ID.GV):** Se comprenden las políticas, procedimientos y procesos para gestionar y monitorear los requisitos regulatorios, legales, de riesgos, ambientales y operacionales de la organización, y se informa a la gerencia sobre los riesgos de ciberseguridad.	**ID.GV-3:** Se comprenden y gestionan los requerimientos regulatorios relacionados con la ciberseguridad, incluyendo las obligaciones de privacidad y libertades civiles.	• **COBIT 5** MEA03.01, MEA03.04 • **ISA 62443-2-1:2009** 4.4.3.7 • **ISO/IEC 27001:2013** A.18.1 • **NIST SP 800-53 Rev. 4** -1 controles de todas las familias (excepto PM-1)
		ID.GV-4: El gobierno y los procesos de gestión de riesgo abordan los riesgos de ciberseguridad.	• **COBIT 5** 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 • **NIST SP 800-53 Rev. 4** PM-9, PM-11
	Evaluación del riesgo (ID.RA): La organización entiende el riesgo de la ciberseguridad para las operaciones de la organización (incluyendo la misión, funciones, imagen o reputación), los activos de la organización y los individuos.	**ID.RA-1:** Se identifican y documentan las vulnerabilidades de los activos.	• **CCS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **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** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Se recibe información sobre amenazas y vulnerabilidades de los foros y recursos de intercambio de información.	• **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** PM-15, PM-16, SI-5
		ID.RA-3: Las amenazas, tanto externas como internas, son identificadas y documentadas.	• **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 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Se identifican los potenciales impactos en el negocio y sus probabilidades.	• **COBIT 5** DSS04.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14

Función	Categoría	Subcategoría	Referencias Informativas
IDENTIFICAR (ID)	**Evaluación de Riesgo (ID.RA):** La organización entiende el riesgo de ciberseguridad en las operaciones de la organización (incluyendo la misión, funciones, imagen o reputación), los activos de la organización y los individuos.	**ID.RA-5:** Las amenazas, vulnerabilidades, probabilidades e impactos se utilizan para determinar el riesgo.	• **COBIT 5** APO12.02 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	• **COBIT 5** APO12.05, APO13.02 • **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Estrategia de Gestión de Riesgos (ID. RM): Se establecen las prioridades de la organización, las restricciones, tolerancias al riesgo y supuestos que se utilizan para apoyar las decisiones de riesgo operacional.	**ID.RM-1:** Las partes interesadas de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	• **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 • **ISA 62443-2-1:2009** 4.3.4.2 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Se define y expresa claramente la tolerancia al riesgo organizacional.	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.3.2.6.5 • **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: La determinación de tolerancia al riesgo de la organización es informada por su rol en la infraestructura crítica y el análisis de riesgos específicos del sector.	• **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14
PROTEGER (PR)	**Control de Acceso (PR.AC):** El acceso a bienes y servicios asociados está limitado a usuarios, procesos o dispositivos autorizados y a las transacciones y actividades autorizadas.	**PR.AC-1:** Las identidades y credenciales son gestionadas por usuarios y dispositivos autorizados.	• **CCS CSC** 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.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • **NIST SP 800-53 Rev. 4** AC-2, Familia IA
		PR.AC-2: El acceso físico a los activos es gestionado y protegido.	• **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.11.1.4, A.11.1.6, A.11.2.3 • **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Control de Acceso (PR.AC):** El acceso a bienes y servicios asociados está limitado a usuarios, procesos o dispositivos autorizados y a las transacciones y actividades autorizadas.	**PR.AC-3:** El acceso remoto es gestionado.	• **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.6.2.2, A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC 17, AC-19, AC-20
		PR.AC-4: Se gestionan los permisos de acceso incorporando los principios de privilegio mínimo y la separación de funciones.	• **CCS CSC** 12, 15 • **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 • **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: La integridad de la red está protegida, incorporando la segregación de la misma cuando sea apropiado.	• **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 • **NIST SP 800-53 Rev. 4** AC-4, SC-7
	Concienciación y Capacitación (PR.AT): El personal y los socios de la organización reciben educación en concienciación de ciberseguridad y están capacitados adecuadamente para realizar sus funciones relacionadas con la seguridad de información y sus responsabilidades consistentes con los acuerdos, procedimientos y políticas relacionadas.	**PR.AT-1:** Todos los usuarios están informados y capacitados.	• **CCS CSC** 9 • **COBIT 5** APO07.03, BAI05.07 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.7.2.2 • **NIST SP 800-53 Rev. 4** AT-2, PM-13

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Concienciación y Capacitación (PR.AT):** El personal y los socios de la organización reciben educación en concienciación de ciberseguridad y están capacitados adecuadamente para realizar sus funciones relacionadas con la seguridad de información y sus responsabilidades consistentes con los acuerdos, procedimientos y políticas relacionadas.	**PR.AT-2:** Los usuarios privilegiados comprenden los roles y responsabilidades.	• **CCS CSC** 9 • **COBIT 5** APO07.02, 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
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden los roles y responsabilidades.	• **CCS CSC** 9 • **COBIT 5** APO07.03, APO10.04, APO10.05 • **ISA 62443-2-1:2009** 4.3.2.4.2 • **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 • **NIST SP 800-53 Rev. 4** PS-7, SA-9
		PR.AT-4: Los altos ejecutivos comprenden los roles y responsabilidades.	• **CCS CSC** 9 • **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, PM-13
		PR.AT-5: El personal de seguridad física y de la información comprende los roles y responsabilidades.	• **CCS CSC** 9 • **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, PM-13
	Seguridad de los Datos (PR.DS): La información y los registros (datos) se gestionan de manera consistente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos almacenados están protegidos.	• **CCS CSC** 17 • **COBIT 5** APO01.06, BAI02.01, BAI06.01, 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** SC-28

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Seguridad de los Datos (PR.DS):** La información y los registros (datos) se gestionan de manera consistente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-2:** Los datos en tránsito están protegidos.	• **CCS CSC** 17 • **COBIT 5** APO01.06, 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
		PR.DS-3: Los activos son gestionados formalmente a través de su eliminación, transferencia y disposición.	• **COBIT 5** BAI09.03 • **ISA 62443-2-1:2009** 4. 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.11.2.7 • **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	• **COBIT 5** APO13.01 • **ISA 62443-3-3:2013** SR 7.1, SR 7.2 • **ISO/IEC 27001:2013** A.12.3.1 • **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Se implementan medidas de protección contra las fugas de datos.	• **CCS CSC** 17 • **COBIT 5** APO01.06 • **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.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

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Seguridad de los Datos (PR.DS):** La información y los registros (datos) se gestionan de manera consistente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-6:** Los mecanismos de comprobación de la integridad se usan para verificar la integridad de la información, del software y del firmware.	• **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 • **NIST SP 800-53 Rev. 4** SI-7
		PR.DS-7: Los entornos de desarrollo y de prueba están separados del entorno de producción.	• **COBIT 5** BAI07.04 • **ISO/IEC 27001:2013** A.12.1.4 • **NIST SP 800-53 Rev. 4** CM-2
	Procesos y Procedimientos de Protección de la Información (PR.IP): Se mantienen las políticas de seguridad (que abordan el propósito, alcance, roles, responsabilidades, compromiso de la gerencia y coordinación entre las entidades de la organización), los procesos y procedimientos y se utiliza para gestionar la protección de activos y sistemas de información.	**PR.IP-1:** Se crea y se mantiene una configuración inicial de los sistemas de control de la tecnología de información/industrial.	• **CCS CSC** 3, 10 • **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, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Se implementa un Ciclo de Vida de Desarrollo de Sistemas para gestionar los sistemas.	• **COBIT 5** APO13.01 • **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** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Se han establecido procesos de control de cambio en la configuración.	• **COBIT 5** BAI06.01, BAI01.06 • **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

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Procesos y Procedimientos de Protección de la Información (PR.IP):** Se mantienen las políticas de seguridad (que abordan el propósito, alcance, roles, responsabilidades, compromiso de la gerencia y coordinación entre las entidades de la organización), los procesos y procedimientos y se utiliza para gestionar la protección de activos y sistemas de información.	**PR.IP-4:** Las copias de seguridad de la información se llevan a cabo, se mantienen y se prueban periódicamente.	• **COBIT 5** APO13.01 • **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.17.1.2A.17.1.3, A.18.1.3 • **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Se cumple con la política y las regulaciones relacionadas con el ambiente operacional físico para los activos de la organización.	• **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, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Los datos se destruyen de acuerdo con la política.	• **COBIT 5** BAI09.03 • **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
		PR.IP-7: Los procesos de protección se mejoran continuamente.	• **COBIT 5** APO11.06, 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 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: La eficacia de las tecnologías de protección es compartida con las partes adecuadas.	• **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Procesos y Procedimientos de Protección de la Información (PR.IP):** Se mantienen las políticas de seguridad (que abordan el propósito, alcance, roles, responsabilidades, compromiso de la gerencia y coordinación entre las entidades de la organización), los procesos y procedimientos y se utiliza para gestionar la protección de activos y sistemas de información.	**PR.IP-9:** Se establecen y gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación antes Incidentes y Recuperación ante Desastres).	• **COBIT 5** 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 • **NIST SP 800-53 Rev. 4** CP-2, IR-8
		PR.IP-10: Los planes de respuesta y recuperación se prueban.	• **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, IR-3, PM-14
		PR.IP-11: La ciberseguridad se incluye en las prácticas de recursos humanos (por ejemplo, sustituciones, selección de personal).	• **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • **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.7.3.1, A.8.1.4 • **NIST SP 800-53 Rev. 4** Familia PS
		PR.IP-12: Se desarrolla e implementa un plan de gestión vulnerabilidades.	• **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2 • **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes de los sistemas de información y de los de control industrial se lleva a cabo de manera consistente con las políticas y los procedimientos.	**PR.MA-1:** El mantenimiento y reparación de los activos de la organización se realiza y registra de manera oportuna, con herramientas aprobadas y controladas.	• **COBIT 5** BAI09.03 • **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 • **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
		PR.MA-2: El mantenimiento remoto de los activos de la organización es aprobado, registrado y realizado de una manera que previene el acceso no autorizado.	• **COBIT 5** DSS05.04 • **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 • **NIST SP 800-53 Rev. 4** MA-4

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Tecnología de Protección (PR.PT):** Se gestionan las soluciones técnicas de seguridad para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, de manera consistente con los acuerdos, procedimientos y políticas relacionadas.	**PR.PT-1:** Los registros de auditoría se determinan, documentan, implementan y revisan de acuerdo con la política.	• **CCS CSC** 14 • **COBIT 5** APO11.04 • **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
		PR.PT-2: Los medios extraíbles están protegidos y su uso está restringido según la política.	• **COBIT 5** DSS05.02, APO13.01 • **ISA 62443-3-3:2013** SR 2.3 • **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 • **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
		PR.PT-3: El acceso a los sistemas y activos está controlado, incorporando el principio de menor funcionalidad.	• **COBIT 5** DSS05.02 • **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 800-53 Rev. 4** AC-3, CM-7

Función	Categoría	Subcategoría	Referencias Informativas
PROTEGER (PR)	**Tecnología de Protección (PR.PT):** Se gestionan las soluciones técnicas de seguridad para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, de manera consistente con los acuerdos, procedimientos y políticas relacionadas.	**PR.PT-4:** Las redes de comunicaciones y control están protegidas.	• **CCS CSC** 7 • **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 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECTAR (DE)	**Anomalías y Eventos (DE. AE):** Se detecta la actividad anómala de manera oportuna y se entiende el impacto potencial de los eventos.	**DE.AE-1:** Se establece y gestiona una base de operaciones de red y flujos de datos esperados para los usuarios y sistemas.	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Los eventos detectados son analizados para comprender los métodos y objetivos del ataque.	• **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 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Los datos de un evento son agregados y correlacionados a partir de múltiples fuentes y sensores.	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Se determina el impacto de los eventos.	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
		DE.AE-5: Se establecen los umbrales de alerta para incidentes.	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Monitoreo Continuo de Seguridad (DE. CM): El sistema de información y los activos son monitoreados a intervalos discretos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	**DE.CM-1:** La red es monitoreada para detectar posibles eventos de ciberseguridad.	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4

Función	Categoría	Subcategoría	Referencias Informativas
DETECTAR (DE)	**Monitoreo Continuo de Seguridad (DE.CM):** El sistema de información y los activos son monitoreados a intervalos discretos para identificar eventos de ciberseguridad y verificar la efectividad de las medidas de protección.	**DE.CM-2:** El entorno físico es monitoreado para detectar posibles eventos de ciberseguridad.	• **ISA 62443-2-1:2009** 4.3.3.3.8 • **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: La actividad personal es monitoreada para detectar posibles eventos de ciberseguridad.	• **ISA 62443-3-3:2013** SR 6.2 • **ISO/IEC 27001:2013** A.12.4.1 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: El código malicioso es detectado.	• **CCS CSC** 5 • **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 • **NIST SP 800-53 Rev. 4** SI-3
		DE.CM-5: Se detecta el código móvil no autorizado.	• **ISA 62443-3-3:2013** SR 2.4 • **ISO/IEC 27001:2013** A.12.5.1 • **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
		DE.CM-6: La actividad de proveedores de servicios externos es monitoreada para detectar posibles eventos de ciberseguridad.	• **COBIT 5** APO07.06 • **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
		DE.CM-7: Se lleva a cabo el monitoreo del personal, las conexiones, los dispositivos y el software no autorizado.	• **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Se llevan a cabo análisis de vulnerabilidades.	• **COBIT 5** BAI03.10 • **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 • **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** RA-5

Función	Categoría	Subcategoría	Referencias Informativas
DETECTAR (DE)	**Procesos de Detección (DE.DP):** Se mantienen y prueban los procedimientos y procesos de detección para asegurar la oportuna y adecuada concienciación de eventos anómalos.	**DE.DP-1:** Las funciones y responsabilidades para la detección están bien definidas para asegurar la rendición de cuentas.	• **CCS CSC** 5 • **COBIT 5** DSS05.01 • **ISA 62443-2-1:2009** 4.4.3.1 • **ISO/IEC 27001:2013** A.6.1.1 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Las actividades de detección cumplen con todos los requerimientos aplicables.	• **ISA 62443-2-1:2009** 4.4.3.2 • **ISO/IEC 27001:2013** A.18.1.4 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4
		DE.DP-3: Los procesos de detección se prueban.	• **COBIT 5** APO13.02 • **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 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
		DE.DP-4: La información de detección de los eventos es comunicada a las partes adecuadas.	• **COBIT 5** APO12.06 • **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 • **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Los procesos de detección se mejoran continuamente.	• **COBIT 5** APO11.06, DSS04.05 • **ISA 62443-2-1:2009** 4.4.3.4 • **ISO/IEC 27001:2013** A.16.1.6 • **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14

Función	Categoría	Subcategoría	Referencias Informativas
RESPONDER (RS)	**Planificación de la Respuesta (RS.RP):** Los procedimientos y procesos de respuesta son ejecutados y mantenidos para garantizar una respuesta oportuna a los eventos de ciberseguridad detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un evento.	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **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
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según corresponda, para incluir el apoyo externo de las fuerzas del orden público.	**RS.CO-1:** El personal conoce sus funciones y el orden de las operaciones cuando es necesaria una respuesta.	• **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.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Los eventos son reportados de manera consistente con los criterios establecidos.	• **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, IR-8
		RS.CO-3: La información se comparte de manera consistente con los planes de respuesta.	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: La coordinación con las partes interesadas se lleva a cabo de manera consistente con los planes de respuesta.	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Se lleva a cabo el intercambio de información voluntaria con las partes interesadas externas para lograr la más amplia concienciación en materia de ciberseguridad.	• **NIST SP 800-53 Rev. 4** PM-15, SI-5

Función	Categoría	Subcategoría	Referencias Informativas
RESPONDER (RS)	**Análisis (RS.AN):** Se lleva a cabo un análisis para asegurar una respuesta adecuada y soportar las actividades de recuperación.	**RS.AN-1:** Las notificaciones del sistemas de detección son investigadas.	• **COBIT 5** 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
		RS.AN-2: El impacto del incidente es entendido.	• **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.16.1.6 • **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Se realizan análisis forenses	• **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
		RS.AN-4: Los incidentes se categorizan de manera consistente con los planes de respuesta.	• **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, IR-4, IR-5, IR-8
	Mitigación (RS.MI): Las actividades se realizan para prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente.	**RS.MI-1:** Los incidentes son contenidos.	• **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.16.1.5 • **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Los incidentes son mitigados.	• **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** IR-4
		RS.MI-3: Las vulnerabilidades identificadas recientemente son mitigadas o documentadas como riesgos aceptados.	• **ISO/IEC 27001:2013** A.12.6.1 • **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5

Función	Categoría	Subcategoría	Referencias Informativas
RESPONDER (RS)	**Mejoras (RS.IM):** Se mejoran las actividades de respuesta organizacional incorporando las lecciones aprendidas de las actividades de detección/respuesta actuales y anteriores.	**RS.IM-1:** Los planes de respuesta incorporan las lecciones aprendidas.	• **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 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Las estrategias de respuesta se actualizan.	• **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECUPERAR (RC)	**Planificación de Recuperación (RC. RP):** Los procedimientos y procesos de recuperación son ejecutados y mantenidos para asegurar la restauración oportuna de los sistemas o activos afectados por eventos de ciberseguridad.	**RC.RP-1:** El plan de recuperación es ejecutado durante o después de un evento.	• **CCS CSC** 8 • **COBIT 5** DSS02.05, DSS03.04 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Mejoras (RC.IM): Se mejora la planificación y los procesos de recuperación mediante la incorporación de las lecciones aprendidas en las actividades futuras.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas.	• **COBIT 5** BAI05.07 • **ISA 62443-2-1:2009** 4.4.3.4 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Las estrategias de recuperación se actualizan.	• **COBIT 5** BAI07.08 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con las partes interesadas internas y externas, tales como centros de coordinación, proveedores de servicios de Internet, dueños de sistemas de ataques, víctimas, otros CSIRT y proveedores.	**RC.CO-1:** Se gestionan las relaciones públicas.	• **COBIT 5** EDM03.02
		RC.CO-2: Se repara la reputación después de un evento.	• **COBIT 5** MEA03.02
		RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y a los equipos ejecutivo y de gestión.	• **NIST SP 800-53 Rev. 4** CP-2, IR-4

Fuente: NIST, *Marco para Mejorar la Ciberseguridad de la Infraestructura Crítica*, EE. UU., 2014, Apéndice A

Niveles de implementación del marco (Framework Implementation Tiers)

Los rangos de los niveles de implementación son los siguientes:

- Nivel 1 – Parcial (Partial): En este nivel las prácticas de gestión de riesgos de ciberseguridad no están formalizadas (ad-hoc) y actúan por lo general de forma reactiva. La priorización de actividades no se encuentra alineada con los objetivos de riesgo organizacionales, el entorno de amenazas ni con los requerimientos de negocio. Se cuenta con una mínima participación externa en términos de colaboración y compartición de información.

- Nivel 2 – Riesgos informados (Risk Informed): En este nivel las prácticas de gestión de riesgo están aprobadas por la Dirección, pero pueden no estar establecidas como una política global. Se cuenta con procedimientos y procesos definidos e implementados y con personal cualificado. La participación externa se realiza de manera informal.

Niveles de implementación del marco (Framework Implementation Tiers)

- **Nivel 3 – Repetible (Repeatable):** En este nivel las prácticas formales de gestión de riesgo son actualizadas regularmente como parte de la aplicación de análisis en cambios en requerimientos de negocio, amenazas o tecnologías. Se ha establecido un marco de colaboración formal con terceros.

- **Nivel 4 - Adaptativo (Adaptive):** Las prácticas de ciberseguridad están basadas en lecciones aprendidas e indicadores predictivos derivados de actividades previas y actuales de ciberseguridad, a través de un proceso de mejora continua de adaptación a los cambios. Estas tareas hacen parte de la cultura organizacional. Se colabora de forma activa con terceros, compartiendo información de eventos de ciberseguridad.

Niveles de implementación del marco (Framework Implementation Tiers)

Figura 13: Niveles de Implementación del Marco

Nivel	Proceso de Gestión de Riesgos	Programa Integrado de Gestión de Riesgos	Participación Externa
Nivel 1: Parcial	Las prácticas de la organización relativas a la gestión de riesgos de ciberseguridad no están formalizadas y el riesgo es gestionado *ad hoc* y a veces de forma reactiva. La priorización de las actividades de ciberseguridad puede no ser directamente derivada de los objetivos de riesgo de la organización, el entorno de amenaza o los requerimientos del negocio/misión.	Hay un conocimiento limitado del riesgo de ciberseguridad a nivel organizacional y no ha sido establecido el enfoque en toda la organización para gestionar el riesgo de ciberseguridad. La organización implementa la gestión de riesgo de ciberseguridad de una manera irregular atendiendo a cada caso de forma particular, debido a una experiencia diversa o una información obtenida de fuentes externas. Es posible que la organización no disponga de procesos que permitan compartir la información de ciberseguridad en su seno.	Es posible que la organización no disponga de procesos establecidos para participar en coordinación o colaboración con otras entidades.
Nivel 2: Riesgo Informado	Las prácticas de gestión de riesgo son aprobadas por la dirección, pero pueden no estar establecidas como política en toda la organización. La priorización de las actividades de ciberseguridad está directamente derivada de los objetivos de riesgo organizacional, el ambiente de amenaza o los requerimientos del negocio/misión.	Hay un conocimiento del riesgo de ciberseguridad en el nivel organizacional, pero no ha sido establecido el enfoque en toda la organización que permita gestionar el riesgo de ciberseguridad. Se han implementado procesos y procedimientos informados del riesgo y aprobados por la administración, y el personal tiene los recursos adecuados para llevar a cabo sus funciones de ciberseguridad. La información de ciberseguridad se comparte dentro de la organización de manera informal.	La organización conoce su rol dentro del ecosistema más amplio, pero no ha formalizado sus capacidades para interactuar y compartir información externamente.

Niveles de implementación del marco (Framework Implementation Tiers)

Figura 13: Niveles de Implementación del Marco *(cont.)*

Nivel	Proceso de Gestión de Riesgos	Programa Integrado de Gestión de Riesgos	Participación Externa
Nivel 3: Repetible	Las prácticas de gestión de riesgos de la organización están aprobadas formalmente y expresadas como política. Las prácticas organizacionales de ciberseguridad se actualizan regularmente basándose en la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos del negocio/ misión, y a un escenario cambiante de amenazas y tecnologías.	Hay un enfoque común en toda la organización para gestionar los riesgos de ciberseguridad. Las políticas, procesos y procedimientos informados del riesgo se definen y se aplican según lo previsto, y se revisan. Hay establecidos métodos consistentes para responder efectivamente a los cambios en el riesgo. El personal cuenta con el conocimiento y las habilidades para desempeñar los roles y las responsabilidades que tiene asignadas.	La organización comprende sus dependencias y socios, y recibe información de estos socios que permite la colaboración y las decisiones de gestión basadas en el riesgo dentro de la organización en respuesta a eventos.
Nivel 4: Adaptativo	La organización adapta sus prácticas de ciberseguridad basándose en lecciones aprendidas e indicadores predictivos que se derivan de actividades de ciberseguridad previas y actuales. Mediante un proceso de mejora continua, que incorpora prácticas y tecnologías avanzadas de ciberseguridad, la organización se adapta activamente a un panorama cambiante de ciberseguridad, y responde a amenazas sofisticadas y cambiantes de manera oportuna.	Hay un enfoque común en toda la organización para gestionar los riesgos de ciberseguridad que utiliza políticas, procesos y procedimientos informados del riesgo para abordar eventos potenciales de ciberseguridad. La gestión del riesgo de ciberseguridad es parte de la cultura organizacional y evoluciona desde una concienciación de las actividades previas, la información compartida por otras fuentes y la concienciación continua de las actividades en sus sistemas y redes.	La organización gestiona el riesgo y comparte activamente información con sus socios para asegurar que se está distribuyendo y consumiendo información exacta y actualizada para mejorar la ciberseguridad antes de que suceda un evento de ciberseguridad.

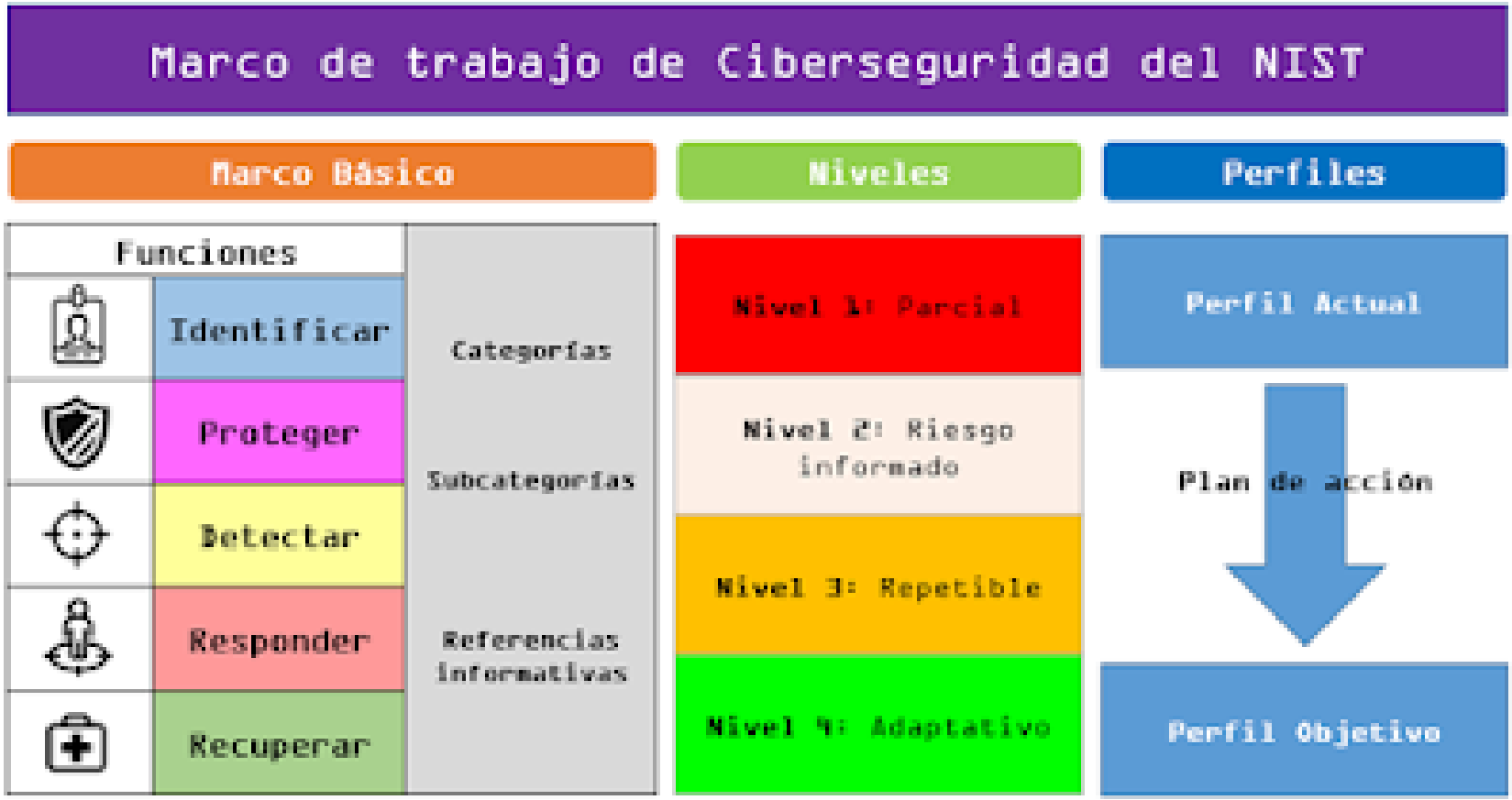
Perfiles del marco (Framework Profiles)

Los perfiles se emplean para describir el estado actual (Current profile) y el estado objetivo (Target profile) de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la identificación de brechas que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

Para ello, se requiere la definición de un plan de acción que incluya una priorización de actividades dependiendo de las necesidades de negocio y procesos de gestión de riesgos de la organización. Este enfoque basado en el riesgo le permite a la organización estimar los recursos necesarios (por ejemplo, personal y financiación) para lograr las metas de ciberseguridad establecidas de una manera rentable y priorizada.

Perfiles del marco (Framework Profiles)

De acuerdo con las descripciones anteriores, la arquitectura global del marco de trabajo de ciberseguridad quedaría de la siguiente manera:



¿Cómo se implementa el CSF?

- La implementación de un programa de ciberseguridad basado en CSF consta de los siguientes pasos iterativos:
- **Paso 1 – Priorización y definición de alcance:** Mediante la identificación de los objetivos y misión del negocio y las prioridades de alto nivel en términos organizacionales, se decide de forma estratégica el entorno de aplicabilidad de los controles. Este entorno puede ser toda la organización, una línea de negocio en particular o un proceso, teniendo presente que cada uno de estos elementos puede tener diferentes niveles de tolerancia al riesgo.
- **Paso 2 – Orientación:** Se identifican los sistemas, activos, requerimientos regulatorios, amenazas y vulnerabilidades vinculadas al entorno de aplicabilidad definido.
- **Paso 3 – Crear un perfil actual:** A través de las funciones del marco básico y empleando las categorías y subcategorías, se obtienen los resultados de implementación de controles en el entorno.
- **Paso 4 – Ejecutar un análisis de riesgos:** Se ejecuta un análisis de riesgos que permita determinar la probabilidad y el impacto de eventos de ciberseguridad en el entorno analizado

¿Cómo se implementa el CSF?

- **Paso 5 – Crear un perfil objetivo:** Se establecen los objetivos que en términos de ciberseguridad la organización pretende cubrir.

- **Paso 6 – Determinar, analizar y priorizar las brechas detectadas:** Mediante el análisis diferencial entre el perfil actual y el perfil objetivo, se define un plan de acción priorizado en términos de coste/beneficio, que permita la determinación de recursos y acciones de mejora.

- **Paso 7 – Implementar el plan de acción:** Se procede con la alineación de controles y despliegue de mejoras de forma paulatina y monitorizada.

¿Cómo se implementa el CSF?

Todas estas acciones deben ser implementadas dentro de un entorno de mejora continua, permitiendo que de forma continua la organización optimice sus controles de seguridad y escale a niveles superiores dentro del marco de trabajo.

¿¿Qué herramientas de software existen para soportar la implementación del CSF?

- Para facilitar el uso del contenido del CSF, el NIST ha desarrollado una hoja de cálculo en Microsoft Excel, que contiene las funciones, categorías, subcategorías y referencias informativas organizadas de tal forma que se pueden adaptar para convertirla en una hoja de trabajo.

  Adicionalmente, también se ha publicado la herramienta "NIST Cybersecurity Framework (CSF) Reference Tool" , una herramienta interactiva que permite la navegación a través del contenido del documento del CSF y facilitar su exportación a diferentes formatos (CSV, XML, etc.).

INFORMACIÓN DE CONTACTO

silvas_cr@hotmail.com

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

¡Gracias por su Atención!

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia