Marco para la mejora de la seguridad cibernética en infraestructuras críticas

Versión 1.1

Instituto Nacional de Estándares y Tecnología

16 de abril de 2018

https://doi.org/10.6028/NIST.CSWP.04162018es

Traducido Bajo Contrato Gubernamental.

The Spanish language Cybersecurity Framework Version 1.1 was translated under government contract. Official U.S. Government translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.04162018.

Nota para los lectores sobre la actualización

La Versión 1.1 de este Marco de seguridad cibernética refina, aclara y mejora la Versión 1.0 que se emitió en febrero de 2014. Incorpora los comentarios recibidos en los dos borradores de la Versión 1.1.

La intención es que la Versión 1.1 sea implementada por los usuarios nuevos y actuales del Marco de Ciberseguridad. Los usuarios actuales deberían poder implementar la Versión 1.1 con interrupción mínima o sin interrupción alguna; la compatibilidad con la Versión 1.0 ha sido un objetivo explícito.

La siguiente tabla resume los cambios realizados entre la Versión 1.0 y 1.1.

Tabla NTR-1: Resumen de cambios entre la Versión 1.0 y Versión 1.1 del Marco

Actualización	Descripción de la actualización
Se aclaró que los términos como "cumplimiento" pueden ser confusos y que pueden significar algo muy distinto para las diversas partes interesadas del Marco.	Añadimos claridad que el Marco tiene utilidad como estructura y lenguaje para organizar y expresar el cumplimiento de los requisitos de seguridad cibernética de una organización. Sin embargo, la variedad de formas en que una organización puede utilizar el Marco significa que frases como "cumplimiento del Marco" pueden ser confusas.
Una nueva sección sobre autoevaluación	Se agregó la Sección 4.0 *Autoevaluación del riesgo de seguridad cibernética con el Marco* para explicar cómo las organizaciones pueden utilizar el Marco para comprender y evaluar su riesgo de seguridad cibernética, incluido el uso de mediciones.
Se expandió la explicación sobre el uso del Marco para fines de gestión de riesgo de la cadena de suministro cibernético	Se expandió la Sección 3.3 *Comunicación de requisitos de seguridad cibernética a las partes interesadas* ayuda a los usuarios a comprender mejor la Gestión de riesgo de la cadena de suministro cibernética (SCRM), mientras que una nueva sección 3.4 *Decisiones de compra* destaca el uso del Marco para comprender el riesgo asociado con productos y servicios empresariales. Se agregó criterios adicionales SCRM cibernético a los Niveles de Implementación. Finalmente, se agregó una categoría de gestión de riesgo de la cadena de suministro, que incluye varias subcategorías, al Núcleo del Marco.
Refinamientos para una mejor explicación de autenticación, autorización y prueba de identidad	El lenguaje de la categoría de control de acceso se ha perfeccionado para considerar mejor la autenticación, la autorización y la prueba de identidad. Esto incluyó agregar unas subcategorías para la autenticación y la prueba de identidad. Además, la categoría ha cambiado de nombre a Gestión de Identidad y Control de Acceso (PR.AC) para representar mejor el alcance de la categoría y subcategorías correspondientes.
Mejor explicación de la relación entre Niveles de Implementación y Perfiles	Se agregó lenguaje a la Sección 3.2. *Establecimiento o mejora de un programa de seguridad cibernética* sobre el uso de los Niveles del Marco para la implementación del Marco. Se agregó lenguaje a los Niveles del Marco para reflejar la integración de las consideraciones del Marco dentro de los programas de gestión de riesgos organizacionales. Los conceptos del Nivel del Marco también se perfeccionaron. Se actualizó la Figura 2.0 para incluir las acciones de los Niveles del Marco.

Consideración de divulgación de vulnerabilidad coordinada	Se agregó una subcategoría relacionada con el ciclo de vida de divulgación de vulnerabilidades.

Al igual que con la Versión 1.0, se recomienda que los usuarios de la Versión 1.1 personalicen el Marco para maximizar el valor individual de la organización.

Agradecimientos

Esta publicación es el resultado de un esfuerzo continuo de colaboración que involucra a la industria, la academia y el gobierno. El Instituto Nacional de Estándares y Tecnología (NIST) lanzó el proyecto al convocar organizaciones y personas naturales del sector público y privado en el año 2013. Publicado en 2014 y revisado durante 2017 y 2018, este *Marco para la mejora de la seguridad cibernética en infraestructuras críticas* se ha basado en ocho talleres públicos, múltiples solicitudes de comentarios o información y miles de interacciones directas con las partes interesadas de todos los sectores de los Estados Unidos junto con muchos sectores de todo el mundo.

El ímpetu para cambiar la Versión 1.0 y los cambios que aparecen en esta Versión 1.1 se basaron en lo siguiente:

- Comentarios y preguntas frecuentes al NIST desde la publicación del Marco Versión 1.0.
- 105 respuestas a la solicitud de información (RFI) de diciembre de 2015: *Opiniones sobre el Marco para la mejora de la seguridad cibernética en infraestructuras críticas*.
- Más de 85 comentarios en el segundo borrador de la Versión 1.1 propuesto del 5 de diciembre de 2017.
- Más de 120 comentarios en el primer borrador de la Versión 1.1 propuesto el 10 de enero de 2017.
- Aporte de más de 1,200 asistentes a los talleres del Marco de 2016 y 2017.

Además, el NIST publicó previamente la Versión 1.0 del Marco de seguridad cibernética con un documento complementario, *Hoja de ruta del NIST para la mejora de la seguridad cibernética en infraestructuras críticas*. Esta hoja de ruta destacó las "áreas de mejora" clave para un mayor desarrollo, alineación y colaboración. Mediante los esfuerzos del sector público y privado, algunas áreas de mejora han avanzado lo suficiente como para ser incluidas en esta Versión 1.1 del Marco.

NIST reconoce y agradece a todos aquellos que han contribuido a este Marco.

Resumen ejecutivo

Los Estados Unidos depende del funcionamiento confiable de la infraestructura crítica. Las amenazas de seguridad cibernética explotan la mayor complejidad y conectividad de los sistemas de infraestructura crítica, lo que pone en riesgo la seguridad de la nación, su economía, y la salud y seguridad pública.. Similar a los riesgos financieros y de reputación, el riesgo de seguridad cibernética afecta el resultado final de una empresa. Puede aumentar los costos y afectar los ingresos. Así mismo, puede afectar la capacidad de una organización para innovar, y aumentar o mantener sus clientes. La seguridad cibernética puede ser un componente importante y amplificador de la gestión general de riesgos de una organización.

Para abordar mejor estos riesgos, la Ley de Mejora de la Seguridad Cibernética de 2014[1] (CEA) actualizó la función del Instituto Nacional de Estándares y Tecnología (NIST) para incluir identificación y desarrollo de marcos de riesgos de seguridad cibernética para uso voluntario por parte de propietarios y operadores de infraestructuras críticas. Mediante la CEA, el NIST debe identificar un "enfoque priorizado, flexible, repetible, basado en el desempeño y costo efectivo, que incluya medidas de seguridad de la información y controles que los propietarios y operadores de infraestructura crítica puedan adoptar voluntariamente para ayudarlos a identificar, evaluar y gestionar los riesgos cibernéticos". Esto formalizó el trabajo previo del NIST de desarrollo de la Versión 1.0 del Marco bajo la Orden Ejecutiva (EO) 13636, "Mejora de la seguridad cibernética en infraestructuras críticas" (febrero de 2013), y proporcionó una guía para la futura evolución del Marco. El Marco que fue desarrollado bajo la EO 13636, y que continúa evolucionando según la CEA, utiliza un lenguaje común para abordar y administrar el riesgo de seguridad cibernética de una manera rentable con base en las necesidades empresariales y organizativas sin imponer requisitos reglamentarios adicionales a las empresas.

El Marco se enfoca en el uso de impulsores de negocios para guiar las actividades de seguridad cibernética y en la consideración de los riesgos de seguridad cibernética como parte de los procesos de gestión de riesgos de la organización. El Marco consta de tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco. El Núcleo del Marco es un conjunto de actividades de seguridad cibernética, resultados y referencias informativas que son comunes en todos los sectores y en la infraestructura crítica. Los elementos del Núcleo proporcionan una guía detallada para desarrollar Perfiles individuales en las organizaciones. Mediante el uso de Perfiles, el Marco ayudará a una organización a alinear y priorizar sus actividades de seguridad cibernética con sus requisitos empresariales / de misión, tolerancias de riesgos y recursos. Los Niveles de Implementación proporcionan un mecanismo para que las organizaciones puedan ver y comprender las características de su enfoque para gestionar el riesgo de seguridad cibernética, lo que ayudará a priorizar y alcanzar los objetivos de la seguridad cibernética.

Si bien este documento se desarrolló para mejorar la gestión del riesgo de seguridad cibernética en la infraestructura crítica, el Marco puede ser utilizado por organizaciones en cualquier sector o comunidad. Este permite que las organizaciones, independientemente de su tamaño, grado de seguridad cibernética o sofisticación de seguridad cibernética, apliquen los principios y mejores prácticas de gestión de riesgos para mejorar la seguridad cibernética y la capacidad de recuperación.

El Marco proporciona una estructura de organización común para múltiples enfoques de seguridad cibernética mediante la conformación de estándares, directrices y prácticas que funcionan de manera efectiva en la actualidad. Además, debido a que hace referencia a normas reconocidas al nivel mundial para la seguridad cibernética, el Marco puede servir como modelo para la cooperación internacional en el

---

1 *Consulte* 15 USC § 272(e)(1)(A)(i). La Ley de Mejora de la Seguridad Cibernética de 2014 (S.1353) se convirtió en ley pública 113-274 el 18 de diciembre de 2014 y se puede encontrar en: https://www.congress.gov/bill/113th-congress/senate-.bill/1353/text.

fortalecimiento de la seguridad cibernética en infraestructura crítica, así como en otros sectores y comunidades.

El Marco ofrece una forma flexible de abordar la seguridad cibernética, lo que incluye el efecto de la seguridad cibernética en las dimensiones físicas, cibernéticas y de personas. Este es aplicable a organizaciones que dependen en la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en tecnología de la información (TI), sistemas de control industrial (ICS), sistemas ciber físicos (CPS) o dispositivos conectados en general, incluido el Internet de las Cosas (IoT), El Marco puede ayudar a las organizaciones a abordar la seguridad cibernética ya que afecta la privacidad de los clientes, empleados y otras partes.
Además, los resultados del Marco sirven como objetivos para el desarrollo de la fuerza laboral y las actividades de evolución.

El Marco no es un enfoque único para administrar el riesgo de seguridad cibernética para la infraestructura crítica. Las organizaciones seguirán teniendo sus riesgos únicos: diferentes amenazas, diferentes vulnerabilidades, y diferentes tolerancias de riesgo. También variarán en cómo personalizan las prácticas descritas en el Marco. Las organizaciones pueden determinar las actividades que son importantes para la prestación de servicios críticos y pueden priorizar las inversiones para maximizar el impacto de cada dólar gastado. En última instancia, el Marco tiene como objetivo reducir y gestionar mejor los riesgos de seguridad cibernética.

Para tener en cuenta las necesidades únicas de seguridad cibernética de las organizaciones, existe una gran variedad de formas de utilizar el Marco. La decisión sobre cómo aplicarlo queda en las manos de la organización implementadora. Por ejemplo, una organización puede decidir utilizar los Niveles de implementación del Marco para articular las prácticas de gestión de riesgos previstas. Otra organización puede utilizar las cinco funciones del Marco para analizar toda su cartera de gestión de riesgos; dicho análisis puede o no basarse en una guía complementaria más detallada, como los catálogos de controles. A veces se debate sobre el "cumplimiento" del Marco, y el Marco tiene utilidad como estructura y lenguaje para organizar y expresar el cumplimiento de los requisitos de seguridad cibernética de una organización. Sin embargo, la variedad de formas en que una organización puede utilizar el Marco significa que frases como "cumplimiento del Marco" pueden ser confusas y significar algo muy diferente para las distintas partes interesadas.

El Marco es un documento dinámico y se continuará actualizando y mejorando a medida que la industria proporcione comentarios sobre la implementación. El NIST continuará coordinando con el sector privado y las agencias gubernamentales a todos los niveles. A medida que el Marco se ponga en práctica, las lecciones aprendidas se integrarán a futuras versiones. Esto asegurará que el Marco satisfaga las necesidades de los propietarios y operadores de infraestructuras críticas en un entorno dinámico y desafiante de nuevas amenazas, riesgos y soluciones.

El siguiente paso para mejorar la seguridad cibernética de la infraestructura crítica de nuestra nación consiste en expandir y utilizar más efectivamente el uso voluntario de este Marco combinado con el intercambio de mejores prácticas; las cuales proporcionan dirección evolutiva para organizaciones individuales y al mismo tiempo aumentan la postura de seguridad cibernética en la infraestructura crítica de la nación, la economía y la sociedad en general.

Índice de contenidos

Lista de figuras

Lista de tablas

1.0 Introducción al Marco

Los Estados Unidos dependen del funcionamiento confiable de su infraestructura crítica. Las amenazas de seguridad cibernética explotan la mayor complejidad y conectividad de los sistemas de infraestructura crítica, lo que pone en riesgo la seguridad de la nación, su economía y la salud y seguridad pública. Similar a los riesgos financieros y de reputación, el riesgo de la seguridad cibernética afecta el resultado final de una empresa. Puede aumentar los costos y afectar los ingresos de la misma. Puede afectar la capacidad de una organización para innovar, añadir y mantener clientes. La seguridad cibernética puede ser un componente importante y amplificador de la gestión general de riesgos de una organización.

Para fortalecer la capacidad de recuperación de esta infraestructura, la Ley de Mejora de la Seguridad Cibernética de 2014[2] (CEA) actualizó el papel del Instituto Nacional de Estándares y Tecnología (NIST) para "facilitar y apoyar el desarrollo de" marcos de riesgo de seguridad cibernética. Mediante el CEA, el NIST debe identificar un "enfoque priorizado, flexible, repetible, basado en el desempeño y costo efectivo, que incluya medidas de seguridad de la información y controles que los propietarios y operadores de infraestructura crítica puedan adoptar voluntariamente para ayudarlos a identificar, evaluar y gestionar los riesgos cibernéticos". Esto formalizó el trabajo previo del NIST de desarrollo de la Versión 1.0 del Marco bajo la Orden Ejecutiva 13636, "Mejora de la seguridad cibernética de infraestructura crítica", emitida en febrero de 2013[3], y proporcionó una guía para la futura evolución del Marco.

La infraestructura crítica[4] se define en la Ley Patriótica de los EE. UU. de 2001[5] como "sistemas y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitador en la seguridad de la nación, la seguridad económica nacional, la salud y seguridad pública , o cualquier combinación de estos mismos". Debido al aumento de las amenazas externas e internas, las organizaciones responsables de la infraestructura crítica deben tener un enfoque constante e iterativo para identificar, evaluar y administrar el riesgo de seguridad cibernética. Este enfoque es necesario independientemente del tamaño de una organización, exposición a amenazas o actual sofisticación de seguridad cibernética.

La comunidad de infraestructura crítica incluye propietarios y operadores públicos y privados, y otras entidades con un rol para asegurar la infraestructura de la Nación. Los miembros de cada sector de infraestructura crítica realizan funciones que están respaldadas por la amplia categoría de tecnología, que incluye tecnología de la información (TI), sistemas de control industrial (ICS), sistemas ciber físicos (CPS) y dispositivos conectados en general, incluyendo el Internet de las Cosas (IoT). Esta dependencia de la tecnología, la comunicación y la interconexión ha cambiado y ampliado las posibles vulnerabilidades y a aumentado el riesgo potencial para las operaciones. Por ejemplo, a medida que la tecnología y los datos que produce y los procesos se utilizan cada vez más para brindar servicios críticos y para respaldar las decisiones empresariales o de misión, se debe considerar los impactos potenciales de un incidente de seguridad cibernética en una organización, en la salud

---

2 *Consulte* 15 USC § 272(e)(1)(A)(i). La Ley de Mejora de la Seguridad Cibernética de 2014 (S.1353) se convirtió en ley pública 113-274 el 18 de diciembre de 2014 y se puede encontrar en: https://www.congress.gov/bill/113th-congress/senate-.bill/1353/text.

3 Orden Ejecutiva nro. 13636, *Mejora de la seguridad cibernética de infraestructura crítica*, DCPD-201300091, 12 de febrero de 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf.

4 El programa de Infraestructura Crítica del Departamento de Seguridad Nacional (DHS) proporciona una lista de los sectores y sus funciones críticas y cadenas de valor asociadas. http://www.dhs.gov/critical-infrastructure-sectors.

5 Consulte 42 USC § 5195c(e). La Ley Patriótica de los Estados Unidos de 2001 (HR3162) se convirtió en ley pública 107-56 el 26 de octubre de 2001 y se puede encontrar en: https://www.congress.gov/bill/107th-congress/house-bill/3162.

y la seguridad de las personas, en el medioambiente, en las comunidades, y la economía y sociedad en general.

Para manejar los riesgos de seguridad cibernética, se requiere una comprensión clara de los impulsores empresariales de la organización y consideraciones de seguridad específicas para su uso de la tecnología. Debido a que los riesgos, las prioridades y los sistemas de cada organización son únicos, las herramientas y métodos utilizados para lograr los resultados descritos en el Marco van a variar.

Reconociendo la función que cumplen la protección para la privacidad y las libertades civiles en la creación de mayor confianza pública, el Marco incluye una metodología para proteger la privacidad individual y las libertades civiles cuando las organizaciones de infraestructuras críticas realicen actividades de seguridad cibernética. Muchas organizaciones ya tienen procesos para abordar la privacidad y las libertades civiles. La metodología está diseñada para complementar dichos procesos y proporcionar dirección para facilitar la gestión del riesgo de privacidad consistente con el enfoque de una organización para la gestión del riesgo de seguridad cibernética. La integración de la privacidad y la seguridad cibernética pueden beneficiar a las organizaciones al aumentar la confianza de los clientes, permitir un intercambio de información más estandarizado y simplificar las operaciones en todos los regímenes legales.

El Marco sigue siendo efectivo y respalda la innovación técnica ya que es neutral desde el punto de vista tecnológico, pero a la misma vez hace referencia a una variedad de normas, directrices y prácticas existentes que evolucionan con la tecnología. Al basarse en los estándares, directrices y prácticas globales desarrollados, administrados y actualizados por la industria, las herramientas y los métodos disponibles para alcanzar los resultados del Marco escalarán fronteras, reconocerán la naturaleza global de los riesgos de seguridad cibernética y evolucionarán con los avances tecnológicos y los requisitos empresariales. El uso de estándares existentes y emergentes permitirá economías de escala e impulsará el desarrollo de productos, servicios y prácticas efectivas que cumplan las necesidades identificadas del mercado. La competencia en el mercado también promueve una difusión más rápida de estas tecnologías y prácticas, y la realización de muchos beneficios por las partes interesadas en estos sectores.

A partir de esos estándares, directrices y prácticas, el Marco proporciona una taxonomía común y un mecanismo para que las organizaciones realicen lo siguiente:

1) Describir su postura actual de seguridad cibernética.
2) Describir su objetivo deseado para seguridad cibernética.
3) Identificar y priorizar oportunidades de mejora dentro del contexto de un proceso continuo y repetible.
4) Evaluar el progreso hacia el objetivo deseado.
5) Comunicarse entre las partes interesadas internas y externas sobre el riesgo de seguridad cibernética.

El Marco no es un enfoque único para administrar el riesgo de seguridad cibernética para la infraestructura crítica. Las organizaciones seguirán teniendo riesgos únicos: diferentes amenazas, diferentes vulnerabilidades, diferentes tolerancias de riesgo. También variarán en cómo personalizan las prácticas descritas en el Marco. Las organizaciones pueden determinar las actividades que son importantes para la prestación de servicios críticos y pueden priorizar las inversiones para maximizar el impacto de cada dólar gastado. En última instancia, el Marco tiene como objetivo reducir y gestionar mejor los riesgos de seguridad cibernética.

Tomando en cuenta las necesidades únicas de seguridad cibernética de las organizaciones, existe una gran variedad de formas de cómo utilizar el Marco. La decisión sobre cómo aplicarlo se deja a la organización implementadora. Por ejemplo, una organización puede decidir utilizar los Niveles de Implementación del Marco para articular las prácticas de gestión de riesgos previstas. Otra organización puede utilizar las cinco funciones del Marco para analizar toda su cartera de gestión de riesgos; dicho análisis puede o no basarse en una guía complementaria más detallada, dado como los catálogos de controles. A veces se debate el tema sobre el "cumplimiento" del Marco, y el Marco tiene utilidad como estructura y lenguaje para organizar y expresar el cumplimiento de los requisitos de seguridad cibernética de una organización. Sin embargo, la variedad de formas en que una organización puede utilizar el Marco significa que frases como "cumplimiento del Marco" pueden ser confusas y significar algo muy diferente para las distintas partes interesadas.

El Marco complementa, y no reemplaza, el proceso de gestión de riesgos y el programa de seguridad cibernética de una organización. La organización puede utilizar sus procesos actuales y aprovechar el Marco para identificar oportunidades para fortalecer y comunicar la gestión del riesgo de seguridad cibernética, y al mismo tiempo se alinea con las prácticas de la industria. Como alternativa, una organización sin un programa vigente de seguridad cibernética puede utilizar el Marco como referencia para establecer uno.

Si bien el Marco ha sido desarrollado para mejorar la gestión del riesgo de seguridad cibernética en lo que respecta a infraestructura crítica, este puede ser utilizado por organizaciones en cualquier sector de la economía o la sociedad. La intención es que sea útil para empresas, agencias gubernamentales y organizaciones sin fines de lucro, independientemente de su enfoque o tamaño. La taxonomía común de estándares, directrices y prácticas que proporciona tampoco es específica para un país. Las organizaciones fuera de los Estados Unidos también pueden utilizar el Marco para fortalecer sus propios esfuerzos de seguridad cibernética, y el Marco puede contribuir a desarrollar un lenguaje común para la cooperación internacional en la seguridad cibernética de la infraestructura crítica.

1.1 Descripción del Marco

El Marco es una metodología con un enfoque para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información, y está compuesto por tres partes: el Núcleo del Marco, los Niveles de Implementación y los Perfiles del Marco. Cada componente del Marco refuerza la conexión entre los impulsores empresariales o de misión y las actividades de seguridad cibernética. Estos componentes se explican a continuación.

- El *Núcleo del Marco* es un conjunto de actividades de seguridad cibernética, resultados deseados y referencias aplicables que son comunes en todos los sectores de infraestructura crítica. El Núcleo presenta estándares, directrices y prácticas de la industria de una manera que permite la comunicación de las actividades y los resultados de seguridad cibernética en toda la organización, desde el nivel ejecutivo hasta el nivel de implementación u operaciones. El Núcleo del Marco consta de cinco Funciones simultáneas y continuas: Identificar, Proteger, Detectar, Responder y Recuperar. Cuando se consideran juntas, estas Funciones proporcionan una visión estratégica de alto nivel del ciclo de vida del proceso de gestión de riesgos de la seguridad cibernética de una organización. El Núcleo del Marco identifica Categorías y Subcategorías claves y subyacentes (que son resultados discretos) para cada Función, y las compara con ejemplos de Referencias Informativas como estándares, directrices y prácticas existentes para cada Subcategoría.
- *Los Niveles de Implementación del Marco* ("Niveles") proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo. Los Niveles describen el grado en que las prácticas de gestión de riesgos de seguridad cibernética de una organización exhiben las características definidas en el Marco

(por ejemplo, consciente de los riesgos y amenazas, repetibles y adaptables). Los Niveles caracterizan las prácticas de una organización en un rango, desde Parcial (Nivel 1) hasta Adaptable (Nivel 4). Estos Niveles reflejan una progresión desde respuestas informales y reactivas a enfoques que son ágiles e informados sobre los riesgos. Durante el proceso de selección de Niveles, una organización debe considerar sus prácticas actuales de administración de riesgos, el entorno de amenazas, requisitos legales y reglamentarios, objetivos empresariales o de misión y las limitaciones organizacionales.

- Un *Perfil del Marco* ("Perfil") representa los resultados que se basan en las necesidades empresariales que una organización ha seleccionado de las categorías y subcategorías del Marco. El Perfil se puede caracterizar como la alineación de estándares, directrices y prácticas con el Núcleo del Marco en un escenario de implementación particular. Los Perfiles se pueden utilizar para identificar oportunidades para mejorar la postura de seguridad cibernética comparando un Perfil "actual" (el estado "tal como está") con un Perfil "objetivo" (el estado "por ser"). Para desarrollar un Perfil, una organización puede revisar todas las Categorías y Subcategorías y, en función de los impulsores empresariales / de misión y una evaluación de riesgos, determinar cuáles son los más importantes; puede agregar Categorías y Subcategorías según sea necesario para abordar los riesgos de la organización. El Perfil Actual se puede usar para apoyar la priorización y la medición del progreso hacia el Perfil Objetivo, mientras se tienen en cuenta otras necesidades empresariales, incluidas la rentabilidad y la innovación. Los Perfiles se pueden utilizar para realizar autoevaluaciones y comunicarse dentro de una organización o entre organizaciones.

1.2 Marco de gestión de riesgos y seguridad cibernética

La gestión de riesgos es el proceso continuo de identificación, evaluación y respuesta al riesgo. Para gestionar el riesgo, las organizaciones deben comprender la probabilidad de que ocurra un evento y los posibles impactos resultantes. Con esta información, las organizaciones pueden determinar el nivel aceptable de riesgo para lograr sus objetivos organizacionales y pueden expresar esto como su tolerancia al riesgo.

Con una comprensión de la tolerancia al riesgo, las organizaciones pueden priorizar las actividades de seguridad cibernética, para permitir a las organizaciones a tomar decisiones informadas sobre los gastos de seguridad cibernética. La implementación de programas de gestión de riesgos ofrece a las organizaciones la capacidad de cuantificar y comunicar los ajustes a sus programas de seguridad cibernética. Las organizaciones pueden optar por manejar el riesgo de diferentes maneras, incluida la mitigación de riesgos, la transferencia del riesgo, la evasión del riesgo o la aceptación del riesgo, dependiendo del impacto potencial en la prestación de los servicios críticos. El Marco utiliza procesos de gestión de riesgos para permitir que las organizaciones informen y prioricen las decisiones relacionadas con la seguridad cibernética. El mismo respalda las evaluaciones de riesgos recurrentes y la validación de los impulsores del negocio para ayudar a las organizaciones a seleccionar estados objetivo para actividades de seguridad cibernética que reflejen los resultados deseados. Por lo tanto, el Marco les brinda a las organizaciones la capacidad de seleccionar y dirigir dinámicamente las mejoras en la gestión de riesgos de seguridad cibernética para los entornos de TI e ICS.

El Marco es adaptable para proporcionar una implementación flexible y basada en el riesgo que se puede utilizar con una amplia gama de procesos de gestión de riesgos de ciberseguridad. Algunos ejemplos de procesos de gestión de riesgos de ciberseguridad incluyen la Organización Internacional de Normalización (ISO)

31000:2009[6], ISO/Comisión Electrotécnica Internacional (IEC) 27005:2011[7], Publicación Especial (SP) 800-39[8] del NIST y la directriz del *Proceso de gestión de riesgos de seguridad cibernética* (RMP) del *sector eléctrico*[9].

1.3 Descripción general del documento

El resto de este documento contiene las siguientes secciones y apéndices:

- La Sección 2 describe los componentes del Marco: el Núcleo del Marco, los Niveles y los Perfiles.
- La Sección 3 presenta ejemplos de cómo se puede utilizar el Marco.
- La Sección 4 describe cómo utilizar el Marco para autoevaluar y demostrar la seguridad cibernética mediante mediciones.
- El Apéndice A presenta el Núcleo del Marco en un formato tabular: las Funciones, Categorías, Subcategorías y Referencias Informativas.
- El Apéndice B contiene un glosario de términos seleccionados.
- El Apéndice C enumera los acrónimos utilizados en este documento.

6 Organización Internacional de Normalización, *Gestión de riesgos. Principios y directrices*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm.

7 Organización Internacional de Normalización/Comisión Electrotécnica Internacional, *Tecnología Informática - Técnicas de seguridad - Gestión del riesgo de seguridad de la información*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html.

8 Iniciativa de transformación de la Fuerza de Tarea Conjunta, *Gestión del riesgo de seguridad de la información: Vista de sistema de organización, misión e información*, Publicación Especial del NIST 800-39, marzo de 2011. https://doi.org/10.6028/NIST.SP.800-39.

9 Departamento de Energía de EE. UU., *Proceso de gestión de riesgos de seguridad cibernética del sector de eléctrico,* DOE/OE-0003, mayo de 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf.

2.0 Conceptos básicos sobre el Marco

El Marco proporciona un lenguaje común para comprender, gestionar y expresar el riesgo de seguridad cibernética para las partes interesadas internas y externas. Se puede utilizar para ayudar a identificar y priorizar acciones para reducir el riesgo de seguridad cibernética, y es una herramienta para alinear los enfoques de políticas, negocios y tecnología para manejar dicho riesgo. También se puede utilizar para administrar el riesgo de seguridad cibernética en todas las partes de una organización o se puede enfocar en la entrega de servicios críticos dentro de una parte de la organización. Los distintos tipos de entidades, incluyendo las estructuras de coordinación del sector, las asociaciones y las organizaciones, pueden utilizar el Marco para diferentes propósitos, incluyendo la creación de Perfiles comunes.

2.1 Núcleo del Marco

El *Núcleo del Marco* proporciona un conjunto de actividades para lograr *resultados* específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. El Núcleo no es una lista de verificación de las acciones a realizar. Este presenta los resultados clave de seguridad cibernética identificados por las partes interesadas como útiles para gestionar el riesgo de seguridad cibernética. El Núcleo consta de cuatro elementos: Funciones, Categorías, Subcategorías y Referencias Informativas, representadas en la **Figura 1**:

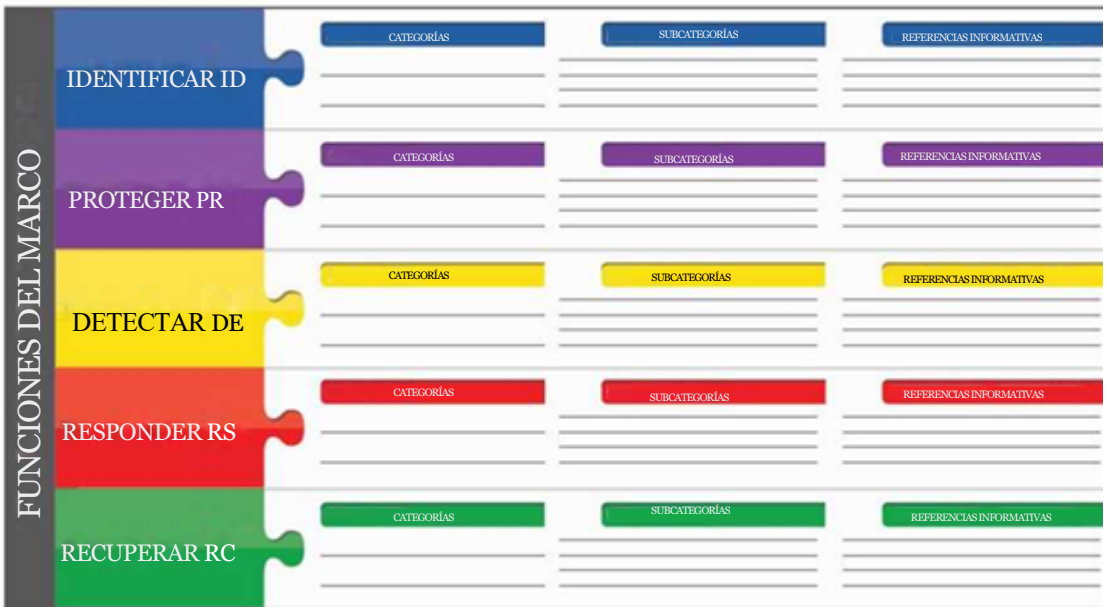

Figura 1: Estructura del Núcleo del Marco

Los elementos del Núcleo del Marco trabajan juntos en la siguiente manera:

- Las **Funciones** organizan actividades básicas de seguridad cibernética en su nivel más alto. Estas funciones son Identificar, Proteger, Detectar, Responder y Recuperar. Estas ayudan a una organización a expresar su gestión del riesgo de seguridad cibernética organizando información, habilitando decisiones de gestión de riesgos, abordando amenazas y mejorando el aprender de actividades previas. Las Funciones también se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en seguridad cibernética. Por ejemplo, las inversiones en planificación y ejercicios apoyan la respuesta oportuna y las acciones de recuperación, lo que resulta en un impacto reducido en la prestación de servicios.

- Las **Categorías** son las subdivisiones de una Función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas y actividades particulares. Los ejemplos de categorías incluyen "Gestión de activos", "Gestión de identidad y control de acceso" y "Procesos de detección".
- Las **Subcategorías** dividen aún más una Categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, ayudan a respaldar el logro de los resultados en cada Categoría. Algunos ejemplos de subcategorías incluyen "Los sistemas de información externos se catalogan", "Los datos en reposo se protegen" y "Las notificaciones de los sistemas de detección se investigan".
- Las **Referencias Informativas** son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada Subcategoría. Las referencias informativas presentadas en el Núcleo del Marco son ilustrativas y no exhaustivas. Se basan en la orientación intersectorial a la que se hace referencia con más frecuencia durante el proceso de desarrollo del Marco.

Las cinco funciones básicas del Marco se definen a continuación. Estas funciones no están destinadas a formar una ruta serial o conducir a un estado final estático deseado. Por el contrario, las funciones deben realizarse concurrente y continuamente para formar una cultura operativa que aborde el riesgo dinámico de seguridad cibernética. Consulte el Apéndice A para obtener la lista completa del Núcleo del Marco.

- **Identificar** – Desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades.

  Las actividades en la Función Identificar son fundamentales para el uso efectivo del Marco. Comprender el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de seguridad cibernética relacionados permite que una organización se enfoque y priorice sus esfuerzos de manera consistente con su estrategia de gestión de riesgos y sus necesidades empresariales. Los ejemplos de Categorías de resultados dentro de esta Función incluyen: Gestión de ctivos, Entorno de negocios, Gobernanza, Evaluación de riesgos y Estrategia de gestión de riesgos.

- **Proteger** – Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos.

  La función Proteger admite la capacidad de limitar o contener el impacto de un posible evento de seguridad cibernética. Los ejemplos de categorías de resultados dentro de esta función incluyen: Gestión de identidad y control de acceso, Conciencia y entrenamiento, Seguridad de datos, Procesos y procedimientos de protección de la información, Mantenimiento y Tecnología de protección.

- **Detectar** – Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.

  La Función Detectar permite el descubrimiento oportuno de eventos de seguridad cibernética. Los ejemplos de categorías de resultados dentro de esta función incluyen: Anomalías y eventos, Monitoreo continuo de seguridad y Procesos de detección.

- **Responder** – Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad cibernética.

  La función Responder respalda la capacidad de contener el impacto de un posible incidente de seguridad cibernética. Los ejemplos de categorías de resultados dentro de esta función incluyen: Planificación de respuesta, Comunicaciones, Análisis, Mitigación y Mejoras.

- **Recuperar** – Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.

  La función Recuperar admite la recuperación oportuna a las operaciones normales para reducir el impacto de un incidente de seguridad cibernética. Los ejemplos de categorías de resultados dentro de esta función incluyen: Planificación de recuperación, Mejoras y Comunicaciones.

2.2 Niveles de implementación del Marco

Los Niveles de Implementación del Marco ("Niveles") proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo. Los Niveles Parcial (Nivel 1) a Adaptable (Nivel 4) describen un grado cada vez mayor de rigor y sofisticación en las prácticas de gestión de riesgos de seguridad cibernética. Ayudan a determinar en qué medida la gestión del riesgo de seguridad cibernética se basa en las necesidades empresariales y se integra a las prácticas generales de gestión del riesgo de una organización. Las consideraciones de gestión de riesgos incluyen muchos aspectos de seguridad cibernética, entre ellos, el grado en que las consideraciones de privacidad y libertades civiles se integran a la gestión de riesgos de seguridad cibernética de una organización y posibles respuestas del riesgo.

El proceso de selección de Niveles considera las prácticas actuales de gestión de riesgos, el entorno de amenazas, los requisitos legales y reglamentarios, las prácticas de intercambio de información, los objetivos empresariales o de misión, los requisitos de seguridad cibernética de la cadena de suministro y las limitaciones organizativas. Las organizaciones deben determinar el Nivel deseado, asegurando que el nivel seleccionado cumpla con los objetivos de la organización, sea factible de implementar y reduzca el riesgo de seguridad cibernética para los activos y recursos críticos a niveles aceptables para la organización. Las organizaciones deben considerar aprovechar el consejo externo obtenido de los departamentos y agencias del gobierno federal, los Centros de Análisis e Intercambio de Información (ISAC), las Organizaciones de Análisis e Intercambio de Información (ISAO), modelos de madurez existentes u otras fuentes para ayudar a determinar su Nivel deseado.

Si bien se alienta a las organizaciones identificadas como Nivel 1 (Parcial) a considerar avanzar hacia el Nivel 2 o más, los Niveles no representan niveles de madurez. Los Niveles están destinados a respaldar la toma de decisiones organizacionales sobre cómo gestionar el riesgo de seguridad cibernética, así como qué dimensiones de la organización son de mayor prioridad y podrían recibir recursos adicionales. Se fomenta la progresión a Niveles más altos cuando un análisis de 'costo-beneficio' indica una reducción factible y rentable del riesgo de seguridad cibernética.

La implementación exitosa del Marco se basa en el logro de los resultados descritos en el Perfil(s) Objetivo(s) de la organización y no en la determinación del Nivel. Sin embargo, la selección y la designación de Nivel afecta naturalmente los Perfiles del Marco. La recomendación de Nivel por parte de los gerentes de niveles empresariales o de proceso, según aprobado por el Nivel Ejecutivo Senior, ayudará a establecer el tono general de cómo se gestionará el riesgo de seguridad cibernética dentro de la organización, y deberá influir la priorización dentro de un Perfil Objetivo y en las evaluaciones del progreso para abordar las brechas.

Las definiciones de Nivel son las siguientes:

Nivel 1: Parcial

- *Proceso de gestión de riesgos* – Las prácticas de gestión de riesgos de seguridad cibernética de la organización no están formalizadas, y el riesgo se gestiona de forma *ad hoc* y, en ocasiones, de forma reactiva. La priorización de las actividades de seguridad cibernética puede no estar directamente informada por los objetivos de riesgo de la organización, el entorno de amenaza o los requisitos empresariales o de misión.
- *Programa integrado de gestión de riesgos* – Existe una conciencia limitada sobre el riesgo de seguridad cibernética a nivel organizacional. La organización implementa la gestión del riesgo de seguridad cibernética de forma irregular, caso por caso, debido a la variación en experiencia o información que se obtiene de fuentes externas. La organización puede no tener procesos que permitan compartir información de seguridad cibernética dentro de la organización.
- *Participación externa* – La organización no comprende su función en el ecosistema más amplio con respecto a sus dependencias o dependientes. La organización no colabora ni recibe información (por ejemplo, inteligencia sobre amenazas, mejores prácticas, tecnologías) de otras entidades (por ejemplo, compradores, proveedores, dependencias, dependientes, ISAOs, investigadores, gobiernos), ni tampoco comparte información. La organización en general desconoce los riesgos cibernéticos de la cadena de suministro de los productos y servicios que proporciona y que utiliza.

Nivel 2: Riesgo informado

- *Proceso de gestión de riesgos* – Las prácticas de gestión de riesgos son aprobadas por la administración, pero posiblemente no son establecidas como políticas de toda la organización. La priorización de las actividades de seguridad cibernética y las necesidades de protección están directamente relacionadas con los objetivos de riesgo organizacional, el entorno de las amenazas, o los requisitos empresariales o de misión.
- *Programa integrado de gestión de riesgos* – Existe una conciencia del riesgo de seguridad cibernética a nivel organizacional, pero no se ha establecido un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética. La información de seguridad cibernética se comparte dentro de la organización de manera informal. La consideración de la seguridad cibernética en los objetivos y programas organizacionales puede ocurrir en algunos, pero no en todos los niveles de la organización. La evaluación del riesgo cibernético de los activos organizacionales y externos ocurre, pero no es típicamente repetible o recurrente.
- *Participación externa* – Generalmente, la organización entiende su función en el ecosistema más amplio con respecto a sus propias dependencias o dependientes, pero no ambos. La organización colabora y recibe alguna información de otras entidades y genera parte de su propia información, pero posiblemente no comparta información con otros. Además, la organización es consciente de los riesgos de la cadena de suministro cibernético asociados con los productos y servicios que ofrece y utiliza, pero no actúa de forma consistente o formal sobre dichos riesgos.

Nivel 3: Repetible

- *Proceso de gestión de riesgos* – Las prácticas para la gestión de riesgos de la organización se aprueban formalmente y se expresan como políticas. Las prácticas de seguridad cibernética organizacional se actualizan periódicamente basado en la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos empresariales / de misión, y un panorama cambiante de amenazas y tecnología.
- *Programa integrado de gestión de riesgos* – Existe un enfoque de toda la organización para gestionar el riesgo de seguridad cibernética. Las políticas, procesos y procedimientos informados sobre riesgos se definen e implementan según lo previsto, y se revisan. Se han implementado métodos consistentes para responder de manera efectiva a los cambios en el riesgo. El personal posee el conocimiento y las habilidades para realizar sus funciones y responsabilidades asignadas. La organización supervisa de manera consistente y precisa el riesgo de seguridad cibernética de los activos de la organización. Los altos ejecutivos de seguridad cibernética y seguridad no cibernética comunican regularmente sobre el riesgo de ciberseguridad. Los altos ejecutivos aseguran la consideración de la seguridad cibernética a través de todas las líneas de operación en la organización.
- *Participación externa* – La organización entiende su función, dependencias y dependientes en un ecosistema más amplio y posiblemente contribuya a una más amplia comprensión de los riesgos por parte de la comunidad. Colabora y recibe regularmente información de otras entidades que complementan la información generada internamente, y comparte información con otras entidades. La organización conoce los riesgos de la cadena de suministro cibernético asociados con los productos y servicios que proporciona y utiliza. Además, generalmente actúa formalmente sobre esos riesgos, lo que incluye mecanismos como los acuerdos escritos para comunicar los requisitos de referencia, las estructuras de gobierno (por ejemplo, los consejos de riesgo), y la implementación y supervisión de políticas.

Nivel 4: Adaptable

- *Proceso de gestión de riesgos* – La organización adapta sus prácticas de seguridad cibernética basándose en actividades previas y actuales de ciberseguridad, el cual incluye las lecciones aprendidas y los indicadores predictivos. A través de un proceso de mejora continua que incorpora prácticas y tecnologías avanzadas de seguridad cibernética, la organización continuamente se adapta a un panorama cambiante de amenazas y tecnologías, y responde de manera eficaz y oportuna a las nuevas y sofisticadas amenazas.
- *Programa integrado de gestión de riesgos* – Existe un enfoque en toda la organización para gestionar el riesgo de seguridad cibernética que utiliza las políticas, los procesos y los procedimientos informados sobre riesgos para abordar posibles eventos de seguridad cibernética. Se entiende claramente la relación entre el riesgo de seguridad cibernética y los objetivos de la organización, y se tienen en cuenta al tomar decisiones. Los altos ejecutivos vigilan el riesgo de seguridad cibernética en el mismo contexto que el riesgo financiero y otros riesgos organizacionales. El presupuesto de la organización se basa en la comprensión del entorno al riesgo actual y previsto, y su tolerancia al riesgo. Las unidades de negocios implementan la visión ejecutiva y analizan los riesgos a nivel del sistema en el contexto de las tolerancias del riesgo organizacional. La gestión del riesgo de seguridad cibernética es parte de la cultura organizacional y evoluciona a partir de la conciencia de las actividades previas y la conciencia continua de las actividades en sus sistemas y redes. La organización puede adaptar de forma rápida y eficiente a los cambios en los objetivos empresariales /de misión en la forma en que se aborda y comunica el riesgo.

- *Participación externa* – La organización entiende su rol, sus dependencias y sus dependientes en el ecosistema más amplio y contribuye a una mayor comprensión de los riesgos por parte de la comunidad. Recibe, genera y revisa información priorizada que informa el análisis continuo de sus riesgos a medida que evolucionan los paisajes de amenazas y tecnología. La organización comparte esa información con otros colaboradores de forma interna y externa. La organización utiliza información en tiempo real o casi en tiempo real para comprender y actuar de forma coherente sobre los riesgos de la cadena de suministro cibernético asociados con los productos y servicios que proporciona y que utiliza. Además, se comunica de manera proactiva, utilizando mecanismos formales (por ejemplo, acuerdos) e informales para desarrollar y mantener relaciones sólidas de la cadena de suministro.

2.3 Perfil del Marco

El Perfil del Marco ("Perfil") es la alineación de las Funciones, Categorías y Subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización. Un Perfil permite a las organizaciones establecer una hoja de ruta para reducir el riesgo de seguridad cibernética que está bien alineada con los objetivos organizacionales y sectoriales, considera los requisitos legales o reglamentarios y las mejores prácticas de la industria, y refleja las prioridades de gestión de riesgos. Dada la complejidad de muchas organizaciones, pueden elegir tener múltiples Perfiles, alineados con componentes particulares y reconociendo sus necesidades individuales.

Los Perfiles del Marco se pueden utilizar para describir el estado actual o el estado objetivo deseado de actividades específicas de seguridad cibernética. El Perfil Actual indica los resultados de seguridad cibernética que se están logrando actualmente. El Perfil Objetivo indica los resultados necesarios para alcanzar los objetivos de gestión de riesgos de seguridad cibernética deseados. Los Perfiles son compatibles con los requisitos empresariales o de misión y ayudan a comunicar los riesgos dentro y entre las organizaciones. Este Marco no prescribe plantillas de Perfil, lo que permite flexibilidad en la implementación.

La comparación de Perfiles (por ejemplo, el Perfil Actual y el Perfil Objetivo) puede revelar brechas que deben abordarse para cumplir con los objetivos de gestión del riesgo de seguridad cibernética. Un plan de acción para abordar estas brechas para cumplir con una Categoría o Subcategoría determinada puede contribuir a la hoja de ruta descrita anteriormente. La priorización de la mitigación de las brechas está impulsada por las necesidades empresariales de la organización y los procesos de gestión de riesgos. Este enfoque basado en el riesgo permite que una organización calcule los recursos necesarios (por ejemplo, dotación de personal, financiación) para alcanzar los objetivos de seguridad cibernética de manera rentable y priorizada. Además, el Marco es un enfoque que se basa en el riesgo donde la aplicabilidad y el cumplimiento de una Subcategoría determinada está sujeto al alcance del Perfil.

2.4 Coordinación de la implementación del Marco

La **Figura 2** describe un flujo común de información y decisiones en los siguientes niveles dentro de una organización:

- Ejecutivo.
- Empresarial / Proceso.
- Implementación / Operaciones.

El nivel ejecutivo comunica las prioridades de la misión, los recursos disponibles y la tolerancia al riesgo general a nivel empresarial / de proceso. El nivel empresarial o de proceso utiliza la información como entradas en el proceso de gestión de riesgos, y luego colabora con el nivel de implementación u operaciones para comunicar las necesidades del negocio y crear un Perfil. El nivel de implementación u operaciones comunica el progreso de la implementación del Perfil al nivel empresarial o de proceso. El nivel empresarial o de proceso utiliza esta información para realizar una evaluación de impacto. La administración de nivel empresarial o de proceso informa los resultados de esa evaluación de impacto al nivel ejecutivo para informar el proceso general de gestión de riesgos de la organización y el nivel de implementación u operaciones para la conciencia del impacto comercial.

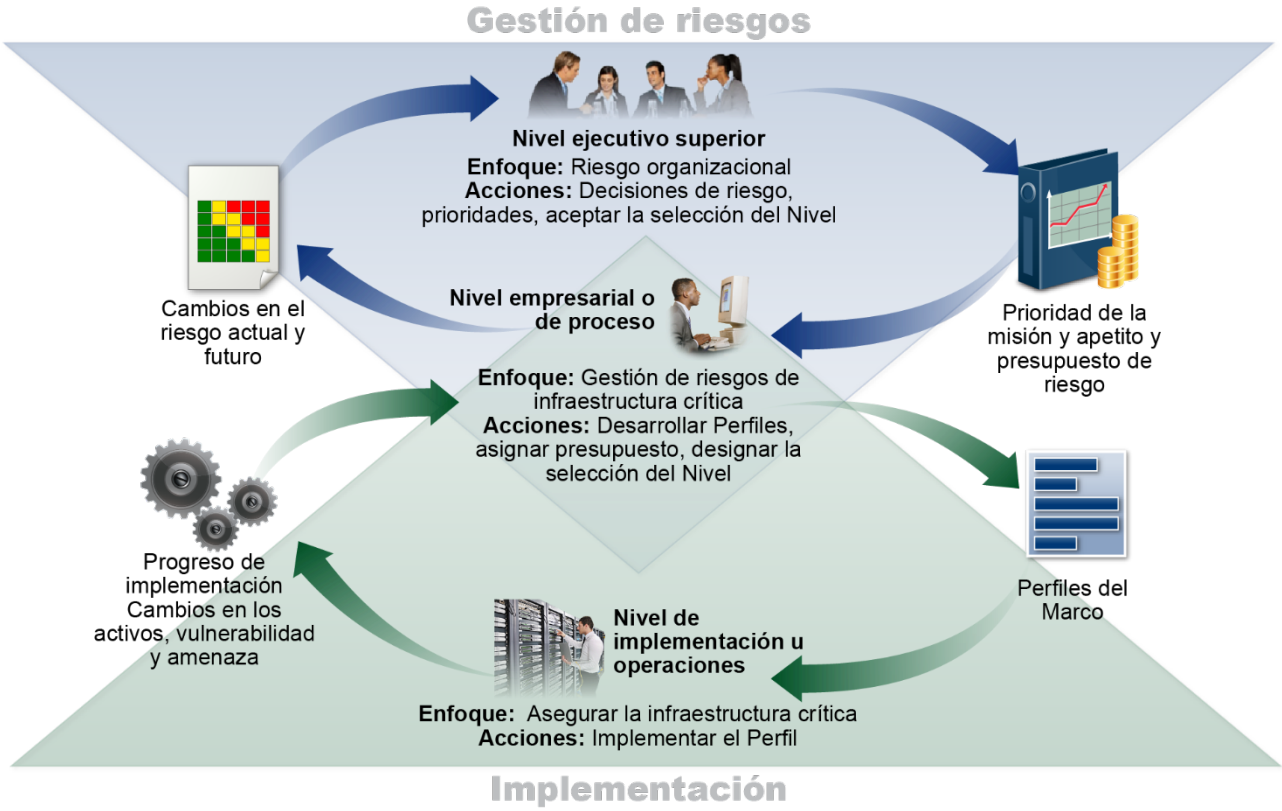

Figura 2: Información nocional y flujos de decisión dentro de una organización

3.0 Cómo utilizar el Marco

Una organización puede utilizar el Marco como una parte clave de su proceso sistemático para identificar, evaluar y administrar el riesgo de seguridad cibernética. El Marco no está diseñado para reemplazar los procesos existentes; una organización puede utilizar su proceso actual y superponerlo en el Marco para determinar las brechas en su enfoque actual de riesgo de seguridad cibernética y desarrollar una hoja de ruta hacia la mejora. Al utilizar el Marco como una herramienta de gestión de riesgos de seguridad cibernética, una organización puede determinar actividades que son los más importantes para la prestación de servicios críticos y priorizar los gastos para maximizar el impacto de la inversión.

El Marco está diseñado para complementar las operaciones empresariales y de seguridad cibernética existentes. Puede servir como base para un nuevo programa de seguridad cibernética o un mecanismo para mejorar un programa existente. El Marco proporciona un medio para expresar los requisitos de seguridad cibernética a los socios empresariales y clientes, y puede ayudar a identificar las brechas en las prácticas de seguridad cibernética de una organización. También proporciona un conjunto general de consideraciones y procesos para considerar las implicaciones de privacidad y libertades civiles en el contexto de un programa de seguridad cibernética.

El Marco se puede aplicar a lo largo de las fases del ciclo de vida de plan, diseño, construcción o compra, implementación, operación y desmantelamiento. La fase plan inicia el ciclo de cualquier sistema y establece la fundación para todo lo que sigue. Las consideraciones generales de seguridad cibernética deben ser declarado y descrito con la mayor claridad posible. El plan debe reconocer que es probable que esas consideraciones y requisitos evolucionen durante el resto del ciclo de vida. La fase de diseño debe tener en cuenta los requisitos de seguridad cibernética como parte de un proceso de ingeniería de sistemas multidisciplinarios más amplio.[10] Un hito clave de la fase de diseño es la validación de que las especificaciones de seguridad cibernética del sistema coinciden con las necesidades y la disposición de riesgo de la organización según lo capturado en un Perfil de Marco. Los resultados deseados de seguridad cibernética priorizados en un Perfil Objetivo deben incorporarse cuando a) desarrolle el sistema durante la fase de construcción y b) compre o externalice el sistema durante la fase de compra. Ese mismo Perfil Objetivo sirve como una lista de características de seguridad cibernética del sistema que debe ser evaluado al implementar el sistema para verificar que todas las características estén implementadas. Los resultados de seguridad cibernética que se determinan mediante el uso del Marco entonces servirán como base para la operación continua del sistema. Esto incluye reevaluaciones ocasionales que capten los resultados en un Perfil Actual para verificar que los requisitos de seguridad cibernética aún se cumplan. Típicamente, una red compleja de dependencias (por ejemplo, controles comunes y de compensación) entre sistemas significa que los resultados documentados en los Perfiles Objetivo de los sistemas relacionados deben ser considerado cuidadosamente a medida que los sistemas se retiran.

Las siguientes secciones presentan diferentes formas en que las organizaciones pueden utilizar el Marco.

3.1 Revisión básica de prácticas de seguridad cibernética

El Marco puede ser utilizado para comparar las actividades de seguridad cibernética actuales de una organización con las delineadas en el Núcleo del Marco. Mediante la creación de un Perfil Actual, las organizaciones pueden examinar en qué medida están logrando los resultados descritos en las Categorías y Subcategorías principales, alineadas con las cinco Funciones de alto nivel: Identificar, Proteger, Detectar, Responder y Recuperar. Una organización puede descubrir que ya está logrando los resultados deseados,

[10] Publicación especial de NIST 800-160 Volumen 1, *Ingeniería de seguridad del sistema, consideraciones para un enfoque multidisciplinario en la ingeniería de sistemas seguros confiables*, Ross et al, noviembre de 2016 (actualizado el 21 de marzo de 2018), https://doi.org/10.6028/NIST.SP.800-160v1.

manejando así la seguridad cibernética en una manera conmensurado con el riesgo conocido. Como alternativa, una organización puede determinar que puede (o necesita) mejorar. La organización puede utilizar esa información para desarrollar un plan de acción para fortalecer las prácticas existentes de seguridad cibernética y reducir el riesgo de seguridad cibernética. Además, una organización puede encontrar que está invirtiendo demasiado para lograr ciertos resultados. La organización puede utilizar esta información para volver a priorizar los recursos.

Si bien no reemplazan un proceso de gestión de riesgos, estas cinco Funciones de alto nivel proporcionarán una forma concisa para que los altos ejecutivos y otros destilen los conceptos fundamentales del riesgo de seguridad cibernética para que puedan evaluar cómo se gestionan los riesgos identificados y cómo está su organización de alto nivel en comparación con los estándares, directrices y prácticas de seguridad cibernética existentes. El Marco también puede ayudar a una organización a responder preguntas fundamentales, incluida "¿Cómo estamos?". Luego, pueden moverse de una manera más informada para fortalecer sus prácticas de seguridad cibernética donde y cuando lo consideren necesario.

3.2 Establecimiento o mejora de un programa de seguridad cibernética

Los siguientes pasos ilustran cómo una organización podría utilizar el Marco para crear un nuevo programa de seguridad cibernética o mejorar un programa existente. Estos pasos deben repetirse según sea necesario para mejorar continuamente la seguridad cibernética.

Paso 1: Priorización y Alcance. La organización identifica sus objetivos empresariales o de misión y las prioridades organizacionales de alto nivel. Con esta información, la organización toma decisiones estratégicas con respecto a las implementaciones de seguridad cibernética y determina el alcance de los sistemas y activos que respaldan la línea o proceso comercial seleccionado. Se puede adaptar El Marco para admitir las diferentes líneas de negocio o procesos dentro de una organización, que pueden tener diferentes necesidades empresariales y la tolerancia al riesgo asociada. Las tolerancias de riesgo pueden reflejarse en un Nivel de Implementación Objetivo.

Paso 2: Orientación. Una vez que se ha determinado el alcance del programa de seguridad cibernética para la línea de negocio o el proceso, la organización identifica los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general. La organización luego consulta las fuentes para identificar las amenazas y vulnerabilidades aplicables a esos sistemas y activos.

Paso 3: Crear un Perfil Actual. La organización desarrolla un Perfil Actual en que indica qué resultados de categoría y subcategoría del Núcleo del Marco se están logrando actualmente. Si se logra parcialmente un resultado, tomar nota de este hecho ayudará a respaldar los pasos posteriores al proporcionar información de referencia.

Paso 4: Realizar una evaluación de riesgos. Esta evaluación podría estar guiada por el proceso de gestión de riesgos general de la organización o actividades previas de evaluación de riesgos. La organización analiza el entorno operativo para discernir la probabilidad de un evento de seguridad cibernética y el impacto que el evento podría tener en la organización. Es importante que las organizaciones identifiquen los riesgos emergentes y utilicen la información de amenazas de seguridad cibernética de fuentes internas y externas para obtener una mejor comprensión de la probabilidad y el impacto de los eventos de seguridad cibernética.

Paso 5: Crear un Perfil objetivo. La organización crea un Perfil Objetivo que se centra en la evaluación de las Categorías y Subcategorías del Marco que describen los resultados deseados de seguridad cibernética de la organización. Las organizaciones también pueden desarrollar sus propias Categorías adicionales y

Subcategorías para tener en cuenta los riesgos únicos de la organización. La organización también puede considerar las influencias y los requisitos de las partes interesadas externas, como las entidades del sector, los clientes y los socios empresariales, al crear un Perfil objetivo. El Perfil Objetivo debe reflejar adecuadamente los criterios dentro del Nivel de Implementación objetivo.

Paso 6: Determinar, analizar y priorizar brechas. La organización compara el Perfil Actual y el Perfil Objetivo para determinar las brechas. A continuación, crea un plan de acción priorizado para abordar las brechas (que reflejan los impulsores, los costos y los beneficios, y los riesgos de la misión) para lograr los resultados en el Perfil Objetivo. Luego, la organización determina los recursos necesarios para abordar las brechas, que incluyen los fondos y la fuerza laboral. El uso de Perfiles de esta manera alienta a la organización a tomar decisiones informadas sobre las actividades de seguridad cibernética, respalda la gestión de riesgos y permite a la organización realizar mejoras específicas y rentables.

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

Una organización repite los pasos según sea necesario para evaluar y mejorar continuamente su seguridad cibernética. Por ejemplo, las organizaciones pueden encontrar que una repetición más frecuente del paso orientación mejora la calidad de las evaluaciones de riesgos. Además, las organizaciones pueden supervisar el progreso a través de actualizaciones iterativas al Perfil Actual, y luego compararlo con el Perfil Objetivo. Las organizaciones también pueden utilizar este proceso para alinear su programa de seguridad cibernética con su Nivel de Implementación del Marco deseado.

3.3 Comunicación de requisitos de seguridad cibernética a las partes interesadas

El Marco proporciona un lenguaje común para comunicar los requisitos entre las partes interesadas interdependientes responsables de la entrega de productos y servicios esenciales de infraestructura crítica. Por ejemplo:

- Una organización puede utilizar un Perfil Objetivo para expresar los requisitos de gestión de riesgos de seguridad cibernética a un proveedor de servicios externo (por ejemplo, un proveedor de la nube al que está exportando datos).
- Una organización puede expresar su estado de seguridad cibernética a través de un Perfil Actual para informar resultados o comparar con los requisitos de adquisición.
- Un propietario u operador de infraestructura crítica, después de identificar un socio externo del que depende esa infraestructura, puede utilizar un Perfil Objetivo para transmitir Categorías y Subcategorías requeridas.
- Un sector de infraestructura crítica puede establecer un Perfil Objetivo que se pueda utilizar entre sus componentes como un Perfil de Referencia Inicial para construir sus Perfiles Objetivo personalizados.
- Una organización puede gestionar mejor el riesgo de seguridad cibernética entre sus partes interesadas mediante la evaluación de su posición en la infraestructura crítica y la economía digital más amplia al utilizar Niveles de implementación.

La comunicación es especialmente importante entre todas las partes interesadas dentro de las cadenas de suministro. Las cadenas de suministro son conjuntos de recursos y procesos complejos, distribuidos globalmente e interconectados entre múltiples niveles de organizaciones.

Las cadenas de suministro comienzan con el suministro de productos y servicios y se extienden desde el diseño, desarrollo, fabricación, procesamiento, manejo y entrega de productos y servicios hasta el usuario final. Dadas estas relaciones complejas e interconectadas, la gestión del riesgo de la cadena de suministro (SCRM) es una función organizativa crítica.[11]

La SCRM cibernética es el conjunto de actividades necesarias para gestionar el riesgo de seguridad cibernética asociado con partes externas. Más específicamente, la SCRM cibernética aborda tanto el efecto de la seguridad cibernética que una organización tiene en las partes externas como el efecto de seguridad cibernética que las partes externas tienen en una organización.

Un objetivo principal de la SCRM cibernética es identificar, evaluar y mitigar "los productos y servicios que pueden contener una funcionalidad potencialmente maliciosa, son falsificados o son vulnerables debido a malas prácticas de fabricación y desarrollo dentro de la cadena de suministro cibernética[12]". Las actividades de la SCRM cibernética pueden incluir las siguientes:

- Determinar los requisitos de seguridad cibernética para los proveedores.
- Promulgar requisitos de seguridad cibernética mediante un acuerdo formal (por ejemplo, contratos).
- Comunicar a los proveedores cómo se verificarán y validarán esos requisitos de seguridad cibernética.
- Verificar que los requisitos de seguridad cibernética se cumplan a través de una variedad de metodologías de evaluación.
- Gobernar y administrar las actividades anteriores.

Como se muestra en la Figura 3, la SCRM cibernética abarca proveedores y compradores de tecnología, así como proveedores y compradores no tecnológicos, donde la tecnología se compone mínimamente de tecnología de la información (TI), sistemas de control industrial (ICS), sistemas ciber físicos (CPS) y dispositivos conectados en general, incluida la Internet de las cosas (IoT). La Figura 3 representa una organización en un solo punto en el tiempo. Sin embargo, a través del curso normal de las operaciones empresariales, la mayoría de las organizaciones serán tanto un proveedor como un comprador en relación con otras organizaciones o usuarios finales.

11 Comunicación de los requisitos de seguridad cibernética (Sección 3.3) y Decisiones de compra (Sección 3.4) abordan solo dos usos del Marco para la SCRM cibernética y no están destinados a abordar la SCRM cibernética de manera exhaustiva.

12 Publicación especial NIST 800-161, *Prácticas de gestión del riesgo de la cadena de suministro para sistemas y organizaciones federales de información*, Boyens et al, abril de 2015,https://doi.org/10.6028/NIST.SP.800-161.

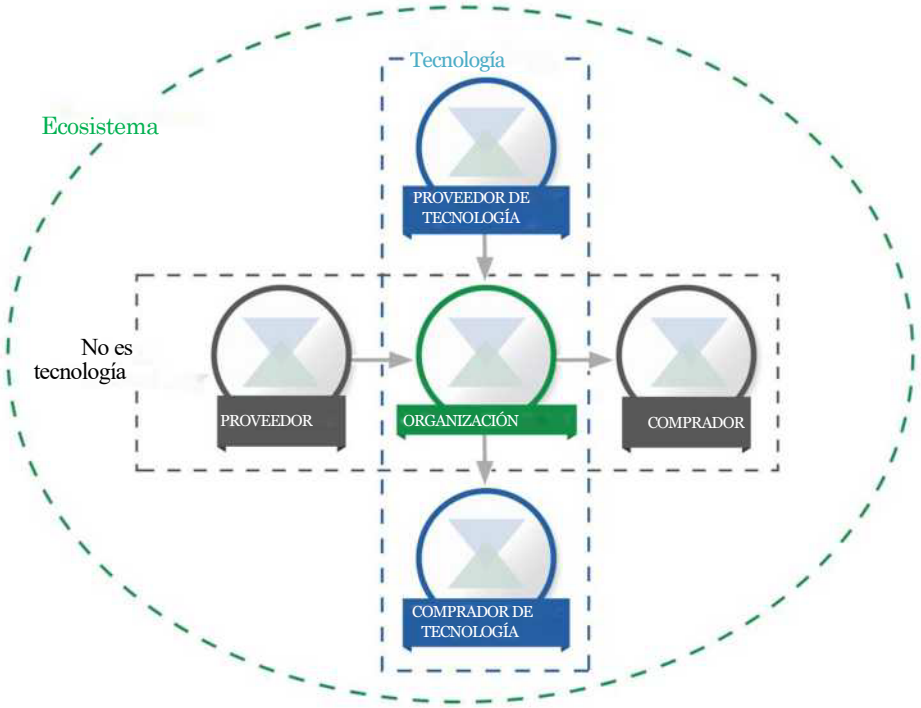

Figura 3: Relaciones de la cadena de suministro cibernética

Las partes descritas en la Figura 3 comprenden el ecosistema de seguridad cibernética de una organización. Estas relaciones destacan el papel crucial de la SCRM cibernética para abordar el riesgo de seguridad cibernética en la infraestructura crítica y la economía digital más amplia. Estas relaciones, los productos y servicios que brindan y los riesgos que presentan deben identificarse y tenerse en cuenta en las capacidades de protección y detección de las organizaciones, así como en sus protocolos de respuesta y recuperación.

En la figura anterior, el "Comprador" se refiere a las personas u organizaciones que consumen un determinado producto o servicio de una organización, incluidas las organizaciones con y sin fines de lucro. El "Proveedor" abarca a los proveedores de productos y servicios que una organización utiliza con fines internos (por ejemplo, la infraestructura de TI) o integrados en los productos o servicios proporcionados al Comprador. Estos términos son aplicables tanto para productos y servicios de base tecnológica como sin ella.

Ya sea si se tienen en cuenta Subcategorías individuales del Núcleo o las consideraciones comprensivas de un Perfil, el Marco ofrece a las organizaciones y sus socios un método para ayudar a garantizar que el nuevo producto o servicio cumpla con los resultados fundamentales de seguridad. Al seleccionar primariamente los resultados que son relevantes para el contexto (por ejemplo, la transmisión de información de identificación personal (PII), la entrega de servicios de misión crítica, los servicios de verificación de datos, la integridad del producto o servicio), la organización puede evaluar a los socios según esos criterios. Por ejemplo, si se compra un sistema que monitorizará la tecnología operacional (OT) para comunicaciones anómalas en la red, la disponibilidad puede ser un objetivo de seguridad cibernética particularmente importante de conseguir y se debería impulsar una evaluación del Proveedor de Tecnología con respecto a las Subcategorías aplicables (p. ej., ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

3.4 Decisiones de compra

Dado que un Perfil Objetivo del Marco es una lista priorizada de requisitos de seguridad cibernética de la organización, los Perfiles Objetivo pueden utilizarse para informar las decisiones sobre la compra de productos y servicios. Esta transacción varía de comunicar los requisitos de seguridad cibernética a las partes interesadas (tratadas en la Sección 3.3) ya que quizás no es posible imponer un conjunto de requisitos de seguridad cibernética al proveedor. El objetivo debe ser tomar la mejor decisión de compra entre múltiples proveedores, dada una lista cuidadosamente determinada de requisitos de seguridad cibernética. A menudo, esto significa un cierto grado de intercambio, al comparar múltiples productos o servicios con brechas conocidos en el Perfil Objetivo.

Una vez que se compra un producto o servicio, el Perfil también se puede utilizar para rastrear y abordar el riesgo de seguridad cibernética residual. Por ejemplo, si el servicio o producto adquirido no cumplió con todos los objetivos descritos en el Perfil Objetivo, la organización puede abordar el riesgo residual a través de otras acciones de gestión. El Perfil también proporciona a la organización un método para evaluar si el producto cumple con los resultados de seguridad cibernética a través de revisiónes periódicos y mecanismos de prueba.

3.5 Identificación de oportunidades para referencias informativas nuevas o revisadas

El Marco se puede utilizar para identificar oportunidades para normas, pautas o prácticas nuevas o revisadas en las que referencias informativas adicionales ayudarían a las organizaciones a abordar las necesidades emergentes. Una organización que implementa una Subcategoría determinada o desarrolla una nueva Subcategoría podría descubrir que hay pocas Referencias Informativas, si las hay, para una actividad relacionada. Para abordar esa necesidad, la organización podría colaborar con los líderes tecnológicos o los organismos de normalización para redactar, desarrollar y coordinar estándares, directrices o prácticas.

3.6 Metodología para proteger la privacidad y las libertades civiles

Esta sección describe una metodología para abordar las implicaciones de la privacidad individual y las libertades civiles que pueden derivarse de la seguridad cibernética. Esta metodología pretende ser un conjunto general de consideraciones y procesos dado que las implicaciones de la privacidad y las libertades civiles pueden diferir por sector o con el tiempo, y las organizaciones pueden abordar estas consideraciones y procesos con una gama de implementaciones técnicas. No obstante, no todas las actividades en un programa de seguridad cibernética engendran consideraciones de privacidad y libertades civiles. Puede ser necesario desarrollar normas de privacidad técnicas, directrices y mejores prácticas adicionales para respaldar implementaciones técnicas mejoradas.

La privacidad y la seguridad cibernética tienen una fuerte conexión. Las actividades de seguridad cibernética de una organización también pueden crear riesgos para la privacidad y las libertades civiles cuando se usa, recopila, procesa, mantiene o divulga información personal. Algunos ejemplos incluyen: actividades de seguridad cibernética que resultan en la recopilación o retención excesiva de información personal; la divulgación o uso de información personal no relacionada con actividades de seguridad cibernética; y las actividades de mitigación de la seguridad cibernética que dan lugar a la denegación de servicios u otros impactos potencialmente adversos similares, incluidos algunos tipos de detección o monitoreo de incidentes que pueden inhibir la libertad de expresión o asociación.

El gobierno y sus agentes tienen la responsabilidad de proteger las libertades civiles derivadas de las actividades de seguridad cibernética. Como se menciona en la metodología a continuación, el gobierno o sus agentes que poseen u operan infraestructura crítica deben tener un proceso establecido para respaldar el cumplimiento de las actividades de seguridad cibernética con las leyes de privacidad, las reglamentaciones y los requisitos constitucionales aplicables.

Para abordar las implicaciones de privacidad, las organizaciones pueden considerar cómo su programa de seguridad cibernética podría incorporar principios de privacidad, tales como: la minimización de datos en la recopilación, divulgación y retención de material de información personal relacionado con el incidente de seguridad cibernética; usar limitaciones fuera de las actividades de seguridad cibernética en cualquier información recopilada específicamente para actividades de seguridad cibernética; la transparencia para ciertas actividades de seguridad cibernética; el consentimiento individual y la reparación de los impactos adversos derivados del uso de información personal en actividades de seguridad cibernética; calidad de los datos, integridad y seguridad; y rendición de cuentas y auditoría.

A medida que las organizaciones evalúan el Núcleo del Marco en el Apéndice A, los siguientes procesos y actividades pueden considerarse como un medio para abordar las implicaciones de la privacidad y las libertades civiles mencionadas anteriormente:

Gobernanza del riesgo de seguridad cibernética

- La evaluación del riesgo de seguridad cibernética de una organización y las respuestas ante el riesgo potencial consideran las implicaciones de la privacidad de su programa de seguridad cibernética.
- Las personas con responsabilidades de privacidad relacionadas con la seguridad cibernética trabajan para la gerencia apropiada y están debidamente capacitadas.
- Existe un proceso para apoyar el cumplimiento de las actividades de seguridad cibernética con las leyes de privacidad aplicables, las reglamentaciones y los requisitos constitucionales.
- Existe un proceso para evaluar la implementación de las medidas y los controles organizacionales anteriores.

Enfoques para identificar, autenticar y autorizar a las personas a acceder a los activos y sistemas de la organización

- Se toman medidas para identificar y abordar las implicaciones de la privacidad de la gestión de la identidad y las medidas de control de acceso en la medida en que impliquen la recopilación, divulgación o uso de información personal.

Conciencia y acciones formativas

- La información aplicable de las políticas de privacidad de la organización se incluye en las actividades de capacitación y concientización de la fuerza de trabajo de seguridad cibernética.
- Los proveedores de servicios que proporcionan servicios relacionados con la seguridad cibernética para la organización están informados sobre las políticas de privacidad aplicables de la organización.

Detección de actividad anómala y monitoreo de sistemas y activos

- Existe un proceso para llevar a cabo una revisión de la privacidad de la detección de las actividades anómalas y la supervisión de seguridad cibernética de una organización.

Actividades de respuesta, incluido el intercambio de información u otros esfuerzos de mitigación

- Existe un proceso para evaluar y abordar si, cuándo, cómo y en qué medida la información personal se comparte fuera de la organización como parte de las actividades de intercambio de información de seguridad cibernética.
- Existe un proceso para llevar a cabo una revisión de la privacidad de los esfuerzos de mitigación de seguridad cibernética de una organización.

4.0 Autoevaluación del riesgo de seguridad cibernética con el Marco

El Marco de seguridad cibernética está diseñado para reducir el riesgo al mejorar la gestión del riesgo de seguridad cibernética para los objetivos de la organización. Idealmente, las organizaciones que usan el Marco podrán medir y asignar valores a su riesgo *junto con* el costo y los beneficios de los pasos tomados para reducir el riesgo a niveles aceptables. Mientras mejor sea capaz una organización de medir los riesgos, costos y beneficios de sus estrategias y pasos de seguridad cibernética, más racional, eficaz y valioso será su enfoque e inversiones en seguridad cibernética.

Con el tiempo, la autoevaluación y la medición deberían mejorar la toma de decisiones sobre las prioridades de inversión. Por ejemplo, medir, o al menos caracterizar robustamente, los aspectos del estado de seguridad cibernética de una organización y las tendencias a lo largo del tiempo puede permitirle a esa organización comprender y transmitir información de riesgo significativa a dependientes, proveedores, compradores y otras partes. Una organización puede lograr esto internamente o buscando una evaluación de un tercero. Si se hace de forma adecuada y con un conocimiento de las limitaciones, estas mediciones pueden proporcionar una base para relaciones de confianza sólidas, tanto dentro como fuera de una organización.

Para examinar la efectividad de las inversiones, una organización primero debe tener una comprensión clara de sus objetivos organizacionales, la relación entre esos objetivos y los resultados relacionados de seguridad cibernética, y cómo esos resultados discretos de seguridad cibernética se implementan y administran. Si bien las mediciones de todos esos puntos están fuera del alcance del Marco, los resultados de seguridad cibernética del nucleo del Marco apoyan la autoevaluación de la eficacia de la inversión y las actividades de seguridad cibernética en las siguientes maneras:

- Tomar decisiones sobre cómo las diferentes partes de la operación de seguridad cibernética deberían influir la selección de los Niveles de Implementación de objetivos.
- Evaluar el enfoque de la organización para la gestión del riesgo de seguridad cibernética al determinar los Niveles de Implementación actuales.
- Priorizar los resultados de seguridad cibernética mediante el desarrollo de Perfiles Objetivo.
- Determinar el grado en que los pasos específicos de seguridad cibernética logran los resultados de seguridad cibernética deseados mediante la evaluación de Perfiles Actuales.
- Medir el grado de implementación de los catálogos de controles o las guías técnicas enumerada como referencias informativas.

El desarrollo de las métricas de rendimiento de seguridad cibernética está evolucionando. Las organizaciones deben ser reflexivas, creativas y cuidadosas con la forma en que emplean las mediciones para optimizar el uso, al tiempo que evitan la dependencia en indicadores artificiales del estado actual y el progreso en la mejora de la gestión del riesgo de seguridad cibernética. Juzgar el riesgo cibernético requiere disciplina y debe revisarse periódicamente. Cada vez que se utilizan mediciones como parte del proceso del Marco, se alienta a las organizaciones a identificar claramente y saber por qué estas medidas son importantes y cómo contribuirán a la gestión general del riesgo de seguridad cibernética. También deben tener claro las limitaciones de las medidas que se utilizan.

Por ejemplo, el seguimiento de las medidas de seguridad y los resultados empresariales puede proporcionar información significativa sobre cómo los cambios en los controles de seguridad granulares afectan la finalización de los objetivos de la organización. Verificar el logro de algunos objetivos de la organización requiere analizar los datos solo *después* de que se haya logrado ese objetivo. Este tipo de medida de retraso es más absoluto.

Sin embargo, a menudo es más valioso predecir si *puede* existir un riesgo de seguridad cibernética y el impacto que *podría* tener, utilizando una medida que provee una predicción.

Se alienta a las organizaciones a innovar y personalizar cómo incorporan las mediciones en su aplicación del Marco con un conocimiento completo de su utilidad y limitaciones.

Apéndice A: Núcleo del Marco

Este apéndice presenta el Núcleo del Marco: una lista de Funciones, Categorías, Subcategorías y Referencias Informativas que describen actividades específicas de seguridad cibernética que son comunes en todos los sectores de infraestructura crítica. El formato de presentación elegido para el Núcleo del Marco no sugiere un orden de implementación específico ni implica un grado de importancia de las Categorías, Subcategorías y Referencias Informativas. El Núcleo del Marco presentado en este apéndice representa un conjunto común de actividades para gestionar el riesgo de seguridad cibernética. Si bien el Marco no es exhaustivo, es extensible, lo que permite a las organizaciones, sectores y otras entidades utilizar Subcategorías y Referencias Informativas que son rentables y eficientes y que les permiten administrar sus riesgos de seguridad cibernética. Se pueden seleccionar las actividades desde el Núcleo del Marco durante el proceso de creación de Perfil y se pueden agregar Categorías adicionales, Subcategorías y Referencias Informativas al Perfil. Los procesos de gestión de riesgos de una organización, los requisitos legales o reglamentarios, los objetivos empresariales o de misión, y las limitaciones organizativas guían la selección de estas actividades durante la creación del Perfil. Se considera la información personal un componente de los datos o activos a los que se hace referencia en las Categorías al evaluar los riesgos de seguridad y las protecciones.

Si bien los resultados previstos identificados en las Funciones, Categorías y Subcategorías son los mismos para la TI y los ICS, los entornos operacionales y consideraciones para la TI y los ICS difieren. Los ICS tienen un efecto directo en el mundo físico, incluidos los riesgos potenciales para la salud y la seguridad de las personas y su impacto en el medioambiente. Además, los ICS tienen requisitos de rendimiento y confiabilidad únicos en comparación con la TI, y los objetivos de la seguridad pública y eficiencia deben ser considerados al implementar medidas de seguridad cibernética.

Para facilitar el uso, a cada componente del Núcleo del Marco se lo asigna un identificador único. Las funciones y las categorías tienen cada una un identificador alfabético único, como se muestra en la Tabla 1. Las Subcategorías dentro de cada Categoría se referencian numéricamente; el identificador único para cada Subcategoría se incluye en la Tabla 2.

Se puede encontrar material de apoyo adicional, incluyendo referencias informativas, relacionado con el Marco en el sitio web de NIST en http://www.nist.gov/cyberframework/.

Tabla 1: Identificadores únicos de función y categoría

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

Tabla 2: Núcleo del Marco

Función	Categoría	Subcategoría	Referencias informativas
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.	**CIS 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, PM-5
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	**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
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	**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
		ID.AM-4: Los sistemas de información externos están catalogados.	**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
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	**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
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Función	Categoría	Subcategoría	Referencias informativas
		(por ejemplo, proveedores, clientes, socios) están establecidas.	**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
	Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.	**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.BE-2: Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Cláusula 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las 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 funciones fundamentales para la entrega de servicios críticos.	**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
		ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	**COBIT 5** BAI03.02, 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-13, SA-14
	Gobernanza (ID.GV): Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la	**ID.GV-1:** Se establece y se comunica la política de seguridad cibernética organizacional.	**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

Función	Categoría	Subcategoría	Referencias informativas
	gestión del riesgo de seguridad cibernética.	**ID.GV-2:** Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	**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, PM-1, PM-2
		ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	**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
		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	**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, PM-9, PM-10, PM-11
	Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**ID.RA-1:** Se identifican y se documentan las vulnerabilidades de los activos.	**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** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	**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

Función	Categoría	Subcategoría	Referencias informativas
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	**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
		ID.RA-4: Se identifican los impactos y las probabilidades del negocio.	**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
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	**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
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Cláusula 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	**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
		ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	**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

Función	Categoría	Subcategoría	Referencias informativas
		ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	**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
	Gestión del riesgo de la cadena de suministro (ID.SC): 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.SC-1:** Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	**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, SA-12, PM-9
		ID.SC-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 evaluación de riesgos de la cadena de suministro cibernético.	**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 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-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.	**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
		ID.SC-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.	**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

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	**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, IR-3, IR-4, IR-6, IR-8, IR-9
PROTEGER (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	**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, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	**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, PE-8
		PR.AC-3: Se gestiona el acceso remoto.	**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

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	**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, AC-14, AC-16, AC-24
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	**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
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	**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, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-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).	**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

Función	Categoría	Subcategoría	Referencias informativas
			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** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-1:** Todos los usuarios están informados y capacitados.	**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
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	**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
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	**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
		PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.	**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 **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	**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

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13
	Seguridad de los datos (PR.DS): La información y los 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.DS-1:** Los datos en reposo están protegidos.	**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
		PR.DS-2: Los datos en tránsito están protegidos.	**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
		PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	**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
		PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	**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
		PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	**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,

Función	Categoría	Subcategoría	Referencias informativas
			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
		PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	**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, SI-7
		PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	**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
		PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	**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
	Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	**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, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3

Función	Categoría	Subcategoría	Referencias informativas
			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, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	**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
		PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	**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
		PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.	**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 son eliminados de acuerdo con las políticas.	**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

Función	Categoría	Subcategoría	Referencias informativas
		PR.IP-7: Se mejoran los procesos de protección.	**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** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	**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
		PR.IP-10: Se prueban los planes de respuesta y recuperación.	**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, IR-3, PM-14
		PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	**CIS CSC** 5, 16 **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.7.1.2, 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, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21

Función	Categoría	Subcategoría	Referencias informativas
		PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	**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** RA-3, RA-5, SI-2
	Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.	**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, MA-3, MA-5, MA-6
		PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	**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
	Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.	**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
		PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 **ISA 62443-3-3:2013** SR 2.3 **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

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	**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 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Las redes de comunicaciones y control están protegidas.	**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, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-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.	**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 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECTAR (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala	**DE.AE-1:** Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3

Función	Categoría	Subcategoría	Referencias informativas
	y se comprende el impacto potencial de los eventos.	los usuarios y sistemas.	**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
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	**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
		DE.AE-3: Cos datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	**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
		DE.AE-4: Se determina el impacto de los eventos.	**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, IR-4, RA-3, SI-4
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	**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** IR-4, IR-5, IR-8
	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia	**DE.CM-1:** Se monitorea la red para detectar posibles eventos de seguridad cibernética.	**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, CM-3, SC-5, SC-7, SI-4

Función	Categoría	Subcategoría	Referencias informativas
	de las medidas de protección.	**DE.CM-2:** Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	**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 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	**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 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Se detecta el código malicioso.	**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 **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Se detecta el código móvil no autorizado.	**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 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	**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
		DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	**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 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Se realizan escaneos de vulnerabilidades.	**CIS CSC** 4, 20

Función	Categoría	Subcategoría	Referencias informativas
			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 800-53 Rev. 4** RA-5
	Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-1:** Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	**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 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	**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 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Se prueban los procesos de detección.	**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 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Se comunica la información de la detección de eventos.	**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 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, APO12.06, 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 procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un incidente.	**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
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	**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, IR-3, IR-8
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	**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, IR-8
		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	**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 **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 realiza en consonancia con los planes de respuesta.	**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, IR-4, IR-8
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	**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

Función	Categoría	Subcategoría	Referencias informativas
	Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-1:** sSe investigan las notificaciones de los sistemas de detección.	**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
		RS.AN-2: Se comprende el impacto del incidente.	**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, IR-4
		RS.AN-3: Se realizan análisis forenses.	**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
		RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.	**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, IR-4, IR-5, IR-8
		RS.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).	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-1:** Los incidentes son contenidos.	**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

Función	Categoría	Subcategoría	Referencias informativas
			NIST SP 800-53 Rev. 4 IR-4
		RS.MI-2: Los incidentes son mitigados.	**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** IR-4
		RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Mejoras (RS.IM): Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta actuales y previas.	**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, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Se actualizan las estrategias de respuesta.	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECUPERAR (RC)	**Planificación de la recuperación (RC.RP):** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	**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
	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas.	**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, IR-4, IR-8
		RC.IM-2: Se actualizan las estrategias de recuperación.	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Cláusula 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Función	Categoría	Subcategoría	Referencias informativas
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	**RC.CO-1:** Se gestionan las relaciones públicas.	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Cláusula 7.4
		RC.CO-2: La reputación se repara después de un incidente.	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Cláusula 7.4
		RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Cláusula 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

La información sobre las referencias informativas descritas en el Apéndice A se puede encontrar en las siguientes lugares:

- 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 asignaciones entre las subcategorías del Núcleo del Marco y las secciones especificadas en las Referencias Informativas no tienen por objeto determinar definitivamente si las secciones especificadas en las Referencias Informativas proporcionan el resultado de Subcategoría deseado.

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

Apéndice B: Glosario

Este apéndice define los términos seleccionados que se utilizaron en la publicación.

Tabla 3: Glosario del Marco de trabajo

Comprador	Las personas u organizaciones que consumen un producto o servicio determinado.
Categoría	La subdivisión de una función en grupos de resultados de seguridad cibernética, estrechamente vinculada a las necesidades programáticas y a actividades particulares. Los ejemplos de categorías incluyen "Gestión de activos", "Gestión de identidad y control de acceso" y "Procesos de detección".
Infraestructura Crítica	Sistemas y activos, ya sean físicos o virtuales, tan importantes para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad cibernética, seguridad económica nacional, seguridad o salud pública nacional o cualquier combinación de esos asuntos.
Seguridad Cibernética	El proceso de protección de la información mediante la prevención, detección y respuesta a los ataques.
Evento de Seguridad Cibernética	Un cambio en la seguridad cibernética que puede tener un impacto en las operaciones de la organización (incluida la misión, las capacidades o la reputación).
Incidente de Seguridad Cibernética	Un evento de seguridad cibernética que se ha determinado que tiene un impacto en la organización, lo que provoca la necesidad de respuesta y recuperación.
Detectar (función)	Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética.
Marco de Trabajo	Un enfoque basado en el riesgo a fin de reducir el riesgo de seguridad cibernética compuesto por tres partes: el Núcleo, el Perfil y los Niveles de implementación del Marco. También conocido como el "Marco de seguridad cibernética".
Núcleo del Marco	Un conjunto de actividades y referencias de seguridad cibernética que son comunes a todos los sectores de infraestructura crítica y se organizan en torno a resultados particulares. El Núcleo del Marco comprende cuatro tipos de elementos: Funciones, Categorías, Subcategorías y Referencias Informativas.
Niveles de Implementación del Marco	Una lente a través de la cual se pueden ver las características del enfoque de riesgo de una organización: cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para administrar ese riesgo.

Perfil del Marco	Una representación de los resultados que un sistema u organización particular ha seleccionado de las Categorías y Subcategorías del Marco de Trabajo.
Función	Uno de los principales componentes del Marco. Las funciones proporcionan el nivel más alto de estructura para organizar actividades básicas de seguridad cibernética en categorías y subcategorías. Las cinco funciones son Identificar, Proteger, Detectar, Responder y Recuperar.
Identificar (función)	Desarrollar la comprensión organizacional para gestionar el riesgo de seguridad cibernética para los sistemas, activos, datos y capacidades.
Referencia Informativa	Una sección específica de estándares, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustra un método para lograr los resultados asociados con cada Subcategoría. Un ejemplo de Referencia Informativa es ISO/IEC 27001 Control A.10.8.3, que respalda la Subcategoría "los datos en tránsito están protegidos" de la Categoría "seguridad de los datos" en la función "proteger".
Código móvil	Un programa (por ejemplo, script, macro u otra instrucción portátil) que se puede enviar sin cambios a una colección heterogénea de plataformas y ejecutarse con semántica idéntica.
Proteger (función)	Desarrollar e implementar las salvaguardas apropiadas para asegurar la entrega de servicios de infraestructura crítica.
Usuario privilegiado	Un usuario que está autorizado (y, por lo tanto, es de confianza) a realizar funciones relevantes para la seguridad que los usuarios normales no están autorizados a realizar.
Recuperar (función)	Desarrollar e implementar las actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto dañado debido a un evento de seguridad cibernética.
Responder (función)	Desarrollar e implementar las actividades apropiadas para tomar medidas con respecto a un evento de seguridad cibernética detectado.
Riesgo	Una medida del grado en el que una entidad se ve amenazada por una circunstancia o evento potencial y típicamente una función de: (i) los impactos adversos que surgirían si ocurriera la circunstancia o el evento; y (ii) la probabilidad de que ocurra.
Gestión de Riesgos	El proceso de identificar, evaluar y responder al riesgo.
Subcategoría	La subdivisión de una Categoría en resultados específicos de actividades técnicas o de gestión. Algunos ejemplos de subcategorías incluyen "Los sistemas de información externos se catalogan", "Los datos en reposo se protegen" y "Las notificaciones de los sistemas de detección se investigan".

Proveedor	Los proveedores de productos y servicios utilizados para los fines internos de una organización (por ejemplo, infraestructura de TI) o integrados en los productos de los servicios brindados a los compradores de esa organización.
Taxonomía	Un esquema de clasificación.

Apéndice C: Acrónimos

Este apéndice define los acrónimos seleccionados que se utilizaron en la publicación.

ANSI	American National Standards Institute (Instituto Nacional Estadounidense de Estándares)
CEA	Cybersecurity Enhancement Act of 2014 (Ley de Mejora de la Seguridad Cibernética de 2014)
CIS	Center for Internet Security (Centro para la Seguridad de Internet)
COBIT	Control Objectives for Information and Related Technology (Objetivos de Control para la Información y Tecnologías Relacionadas)
CPS	Cyber-Physical Systems (sistemas ciber físicos)
CSC	Critical Security Control (control de seguridad crítica)
DHS	Department of Homeland Security (Departamento de Seguridad Nacional de los Estados Unidos)
EO	Executive Order (Orden Ejecutiva)
ICS	Industrial Control Systems (sistemas de control industrial)
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional)
IoT	Internet of Things (Internet de las Cosas)
IR	Interagency Report (informe interinstitucional)
ISA	International Society of Automation (Sociedad Internacional de Automatización)
ISAC	Information Sharing and Analysis Center (Centro de Análisis e Intercambio de Información)
ISAO	Information Sharing and Analysis Organization (Organización de Análisis e Intercambio de Información)
ISO	International Organization for Standardization (Organización Internacional de Normalización)
TI	Tecnología Informática (Information Technology)
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
OT	Operational Technology (Tecnología Operacional)
PII	Personally Identifiable Information (información de identificación personal)
RFI	Request for Information (solicitud de información)
RMP	Risk Management Process (proceso de gestión de riesgos)
SCRM	Supply Chain Risk Management (gestión de riesgos en la cadena de suministro)
SP	Special Publication (Publicación Especial)