El Marco de Seguridad Cibernética (CSF) 2.0 del NIST

National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
Esta publicación está disponible de forma gratuita en: https://doi.org/10.6028/NIST.CSWP.29.spa

Febrero 26, 2024

NIST | NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Resumen

El Marco de Seguridad Cibernética del NIST (CSF) 2.0 proporciona directrices a la industria, agencias gubernamentales y otras organizaciones para gestionar los riesgos de seguridad cibernética. Ofrece una taxonomía de resultados de seguridad cibernética de alto nivel que cualquier organización puede usar - sin importar su tamaño, sector o grado de madurez - para comprender mejor, evaluar, priorizar y comunicar sus esfuerzos de seguridad cibernética. El CSF no especifica cómo se deben lograr los resultados. Más bien, establece enlaces a recursos en línea que proporcionan orientación adicional sobre prácticas y controles que se podrían utilizar para lograr esos resultados. Este documento describe el CSF 2.0, sus componentes y algunas de las múltiples formas en que se puede utilizar.

Palabras clave

Seguridad cibernética; Marco de Seguridad Cibernética (CSF); gobernanza de riesgos de seguridad cibernética; gestión de riesgos de seguridad cibernética; gestión de riesgos empresariales; Perfiles; Niveles.

Audiencia

Las personas responsables de desarrollar y dirigir programas de seguridad cibernética son el público principal del CSF. Otras personas implicadas en la gestión de riesgos, como directivos, consejos de administración, profesionales de las adquisiciones, profesionales de la tecnología, gerentes de riesgos, abogados, especialistas en recursos humanos y auditores de seguridad cibernética y gestión de riesgos, también pueden utilizar el CSF para orientar sus decisiones relacionadas con la seguridad cibernética. Asimismo, el CSF puede ser útil para aquellos que elaboran e influyen en la política (por ejemplo, asociaciones, organizaciones profesionales, reguladores) que establecen y comunican las prioridades para la gestión de riesgos de seguridad cibernética.

Contenido complementario

El NIST continuará creando y albergando recursos adicionales para ayudar a las organizaciones a implementar el CSF, incluidas las Guías de Inicio Rápido y los Perfiles Comunitarios. Todos los recursos se ponen a disposición del público en el sitio web del CSF del NIST. Las sugerencias de recursos adicionales para hacer referencia en el sitio web de CSF del NIST siempre se pueden compartir con NIST en cyberframework@nist.gov.

Nota a los lectores

A menos que se indique lo contrario, los documentos citados, referenciados o extraídos en esta publicación no se incorporan en su totalidad a la misma.

Antes de la versión 2.0, el Marco de Seguridad Cibernética se llamaba “Marco para Mejorar la Seguridad Cibernética de las Infraestructuras Críticas”. Este título no se utiliza para el CSF 2.0.

Agradecimientos

El CSF es el resultado de un esfuerzo de colaboración de varios años entre la industria, el mundo académico y el gobierno de los Estados Unidos y de todo el mundo. El NIST reconoce y agradece a todos aquellos que contribuyeron a este CSF revisado. Puede obtener información sobre el proceso de desarrollo del CSF en el sitio web del CSF del NIST. Las lecciones aprendidas sobre el uso del CSF se pueden compartir siempre con el NIST en cyberframework@nist.gov.

Traducción realizada por TaikaTranslations LLC bajo contrato con NIST [133ND23PNB770271]. Traducción oficial del Gobierno de EE.UU.
Translated by TaikaTranslations LLC under contract with NIST [133ND23PNB770271]. Official U.S. Government translation.

Esta publicación está disponible gratuitamente en inglés en el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés): https://doi.org/10.6028/NIST.CSWP.29.
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.29.

Índice

Lista de Imágenes

Prólogo

El Marco de Seguridad Cibernética (CSF) 2.0 está diseñado para ayudar a las organizaciones de todos los tamaños y sectores – lo que incluye a la industria, el gobierno, la academia y las organizaciones sin fines de lucro - para gestionar y reducir sus riesgos de seguridad cibernética. Es útil sin importar el nivel de madurez y sofisticación técnica de los programas de seguridad cibernética de una organización. Sin embargo, el CSF no adopta un enfoque de una talla que sirve para todos. Cada organización tiene riesgos comunes y únicos, así como diferentes preferencias y tolerancias de riesgo, misiones específicas y objetivos para lograr esas misiones. El modo en que las organizaciones apliquen por necesidad el CSF variará.

Idealmente, el CSF se utilizará para abordar los riesgos de seguridad cibernética junto con otros riesgos de la empresa, como los de índole financiera, de privacidad, de cadena de suministro, de reputación, tecnológica o física.

El CSF describe los resultados deseados que pretenden ser entendidos por una amplia audiencia, lo que incluye directivos, gerentes y profesionales, sin importar su experiencia en seguridad cibernética. Dado que estos resultados son neutrales con respecto al sector, el país y la tecnología, proporcionan a una organización la flexibilidad necesaria para abordar sus riesgos, tecnologías y consideraciones de misión únicos. Los resultados se asignan directamente a una lista de posibles controles de seguridad para su consideración inmediata con el fin de mitigar los riesgos de seguridad cibernética.

Aunque no es obligatorio, el CSF ayuda a sus usuarios a conocer y seleccionar resultados específicos. Las sugerencias sobre cómo se pueden lograr resultados específicos se proporcionan en un conjunto cada vez mayor de recursos en línea que complementan el CSF, entre los que se incluye una serie de Guías de Inicio Rápido (QSG). Asimismo, varias herramientas ofrecen formatos descargables para ayudar a las organizaciones que decidan automatizar algunos de sus procesos. Las QSG sugieren maneras iniciales de utilizar el CSF e invitan al lector a explorar el CSF y los recursos relacionados en mayor detalle. Disponible a través del CSF del sitio web de NIST, sitio web del CSF del NIST, el CSF y estos recursos complementarios del NIST y otros deben considerarse como una "cartera del CSF" para ayudar a gestionar y reducir los riesgos. Sin importar cómo se aplique, el CSF insta a sus usuarios a considerar su postura de seguridad cibernética en contexto y luego adaptar el CSF a sus necesidades específicas.

Sobre la base de versiones anteriores, el CSF 2.0 contiene nuevas características que destacan la importancia de la *gobernanza* y las *cadenas de suministro*. Se presta especial atención a los QSG a fin de garantizar que el CSF sea pertinente y fácilmente accesible tanto para las organizaciones más pequeñas como para sus pares de mayor tamaño. El NIST proporciona ahora *Ejemplos de implementación* y *Referencias informativas*, que están disponibles en línea y se actualizan periódicamente. La creación de *Perfiles Organizativos* de estado actual y de estado objetivo ayuda a que las organizaciones comparen dónde están frente a dónde quieren o necesitan estar y les permite implementar y evaluar los controles de seguridad más rápidamente.

Los riesgos de seguridad cibernética están en constante expansión, y la gestión de esos riesgos debe ser un proceso continuo. Esto es cierto tanto si una organización está empezando a enfrentarse a sus desafíos de seguridad cibernética como si ha estado activa durante muchos años con un equipo de seguridad cibernética sofisticado y bien dotado de recursos. El CSF está diseñado para ser útil para cualquier tipo de organización y se espera que proporcione la orientación adecuada durante mucho tiempo.

1. Visión general del Marco de Seguridad Cibernética (CSF)

Este documento es la versión 2.0 del Marco de Seguridad Cibernética del NIST (*Marco* o *CSF*). Incluye los siguientes componentes:

- ***CSF Core***, el núcleo del CSF, que es una taxonomía de resultados de seguridad cibernética de alto nivel que puede ayudar a cualquier organización a gestionar sus riesgos de seguridad cibernética. Los componentes del CSF Core son una jerarquía de Funciones, Categorías y Subcategorías que detallan cada resultado. Estos resultados pueden ser comprendidos por una amplia audiencia, lo que incluye directivos, gerentes y profesionales, independientemente de su experiencia en ciberseguridad. Dado que los resultados son neutrales con respecto al sector, país y tecnología, proporcionan a una organización la flexibilidad necesaria para abordar sus riesgos, tecnologías y consideraciones de misión únicos.
- ***Los perfiles organizativos de CSF,*** que son un mecanismo para describir la postura de seguridad cibernética actual y/u objetiva de una organización en términos de los resultados del Núcleo CSF.
- ***Los niveles de CSF,*** que pueden aplicarse a los Perfiles Organizativos de CSF para caracterizar el rigor de las prácticas de gobierno y gestión de riesgos de seguridad cibernética de una organización. Los niveles también pueden proporcionar el contexto de cómo una organización ve los riesgos de seguridad cibernética y los procesos establecidos para gestionar esos riesgos.

Este documento describe a *qué* resultados deseables puede aspirar una organización. No *establece* resultados ni cómo se pueden lograrse. Las descripciones de cómo una organización puede lograr esos resultados se proporcionan en un conjunto de recursos en línea que complementan el CSF y están disponibles a través del sitio web del CSF de NIST. Estos recursos ofrecen orientación adicional sobre las prácticas y controles que podrían utilizarse para lograr los resultados y tienen como objetivo ayudar a una organización a comprender, adoptar y utilizar el CSF. Entre ellos se incluyen:

- *Referencias informativas* que apuntan a fuentes de orientación sobre cada resultado a partir de normas, directrices, marcos, reglamentos, políticas, etc. existentes a nivel mundial.
- *Ejemplos de aplicación* que ilustran posibles formas de lograr cada resultado
- *Guías de inicio rápido* que ofrecen orientación práctica sobre el uso del CSF y sus recursos en línea, incluida la transición de las versiones anteriores del CSF a la versión 2.0.
- *Perfiles comunitarios y plantillas de perfiles organizativos* que ayudan a una organización a poner en práctica el CSF y a establecer prioridades para la gestión de los riesgos de seguridad cibernética

Una organización puede utilizar el Núcleo, los Perfiles y los Niveles del CSF con los recursos adicionales para comprender, evaluar, priorizar y comunicar los riesgos de seguridad cibernética.

- **Comprender y evaluar:** Describir la postura de la seguridad cibernética actual u objetivo de parte o de toda una organización, determinar las brechas y evaluar el progreso para abordar esas brechas.
- **Priorizar:** Identificar, organizar y priorizar las acciones para gestionar los riesgos de seguridad cibernética que se alinean con la misión de la organización, los requisitos legales y normativos, y las expectativas de gestión de riesgos y gobernanza.
- **Comunicar:** Proporcionar un lenguaje común para la comunicación dentro y fuera de la organización acerca de los riesgos de seguridad cibernética, capacidades, necesidades y expectativas.

El CSF fue diseñado para que sea utilizado por organizaciones de todos los tamaños y sectores, lo que incluye a la industria, el gobierno, el mundo académico y las organizaciones sin fines de lucro, sin importar el nivel de madurez de sus programas de seguridad cibernética. El CSF es un recurso fundamental que se puede adoptar voluntariamente y a través de políticas y mandatos gubernamentales. La taxonomía del CSF y las normativas, directrices y prácticas referenciadas no son específicas de un país, y las versiones anteriores del CSF fueron aprovechadas con éxito por diversos gobiernos y otras organizaciones tanto dentro como fuera de los Estados Unidos.

El CSF se debe utilizar junto con otros recursos (p. ej., marcos, normas, directrices, prácticas principales) para gestionar mejor los riesgos de seguridad cibernética e informar la gestión general de los riesgos de la tecnología de la información y las comunicaciones (ICT) a nivel empresarial. El CSF es un marco flexible que se ha diseñado para su uso por parte de todas las organizaciones, sin importar su tamaño. Las organizaciones seguirán teniendo riesgos únicos - incluidas las diferentes amenazas y vulnerabilidades- y tolerancias al riesgo, así como objetivos y requisitos de misión únicos. Por lo tanto, los enfoques de las organizaciones para gestionar los riesgos y sus implementaciones del CSF variarán.

El resto de este documento tiene la siguiente estructura:

- La sección 2 explica los fundamentos del CSF Core: Funciones, Categorías y Subcategorías.
- La sección 3 define los conceptos de perfiles y niveles del CSF.
- Esta sección 4 proporciona una visión general de determinados componentes del conjunto de recursos en línea del CSF: Referencias informativas, ejemplos de aplicación y guías de inicio rápido.
- La sección 5 trata sobre cómo una organización puede integrar el CSF con otros programas de gestión de riesgos.
- Appendix A es el CSF Core.
- Appendix B contiene una ilustración teórica de los niveles del CSF.
- Appendix C es un glosario de terminología del CSF.

2. Introducción al CSF Core

Appendix A es el CSF Core - un conjunto de resultados de seguridad cibernética ordenados por función, luego categoría y finalmente subcategoría, como se muestra en Fig. 1. Estos resultados no son una lista de verificación de acciones que hay que realizar; las acciones específicas que se tomen para lograr un resultado variarán en función de la organización y el caso de uso, al igual que la persona responsable de dichas acciones. Asimismo, el orden y el tamaño de las Funciones, las Categorías y las Subcategorías del Core no implican la secuencia o la importancia de su consecución. La estructura del Core está diseñada para que tenga mayor resonancia entre los encargados de hacer operativa la gestión de riesgos dentro de una organización.

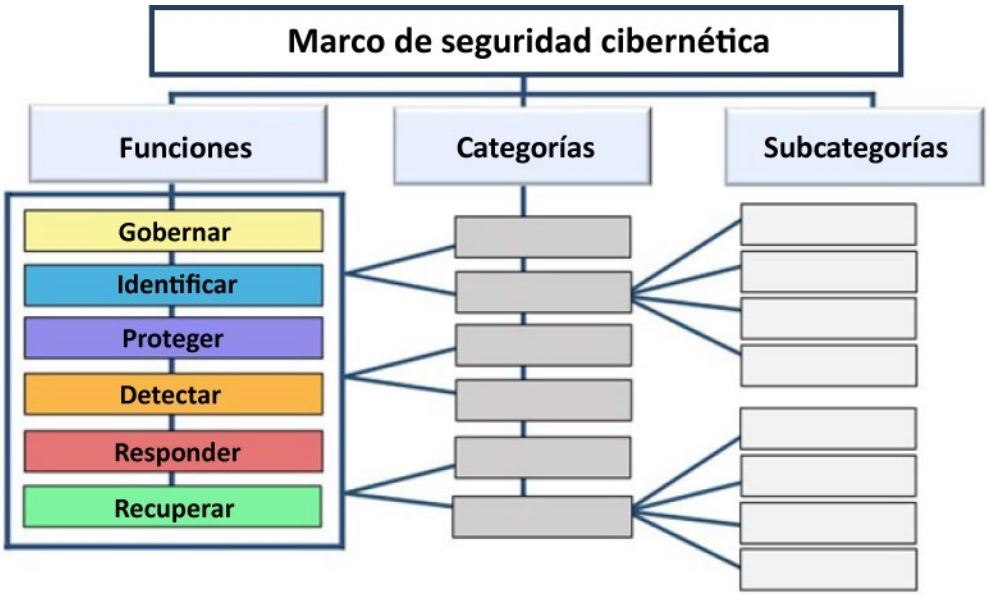

Fig. 1. Estructura de CSF Core

Las Funciones Básicas del CSF — Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar — organizan los resultados de la seguridad cibernética en su nivel más alto.

- **Gobernar (GV)** — *La estrategia, las expectativas y la política de gestión de riesgos de seguridad cibernética de la organización se establecen, comunican y supervisan.* La función de gobernanza proporciona resultados para informar acerca de lo que una organización puede hacer para lograr y priorizar los resultados de las otras cinco funciones en el contexto de su misión y las expectativas de las partes interesadas. Las actividades de gobernanza son fundamentales para incorporar la seguridad cibernética en la estrategia más amplia de gestión de riesgos empresariales (ERM) de una organización. La gobernanza aborda una comprensión del contexto organizativo; el establecimiento de la estrategia de seguridad cibernética y la gestión de riesgos de la cadena de suministro de seguridad cibernética; las funciones, las responsabilidades y las autoridades; la política; y la supervisión de la estrategia de seguridad cibernética.
- Identificar (ID) — Se conocen los riesgos actuales de seguridad cibernética de la organización. Comprender los activos de la organización (p. ej., datos, hardware, software, sistemas, instalaciones, servicios, personas), los proveedores y los riesgos de

seguridad cibernética relacionados permite a una organización priorizar sus esfuerzos de acuerdo con su estrategia de gestión de riesgos y las necesidades de la misión identificadas en el marco de la Gobernanza. Esta Función también incluye la identificación de oportunidades de mejora para las políticas, los planes, los procesos, los procedimientos y las prácticas de la organización que apoyan la gestión de riesgos de seguridad cibernética para informar los esfuerzos en el marco de las seis Funciones.

- **Proteger (PR)** — *Se utilizan medidas de protección para gestionar los riesgos de seguridad cibernética de la organización.* Una vez que se hayan identificado y priorizado los activos y los riesgos, Proteger contribuye a la capacidad de proteger dichos activos para evitar o reducir la probabilidad y el impacto de los eventos adversos de seguridad cibernética, así como para aumentar la probabilidad y el impacto de aprovechar las oportunidades. Los resultados contemplados en esta función incluyen la gestión de identidades, la autenticación y el control de acceso; la concienciación y la formación; la seguridad de los datos; la seguridad de las plataformas (es decir, la seguridad del hardware, el software y los servicios de las plataformas físicas y virtuales); y la resiliencia de la infraestructura tecnológica.
- **Detectar (DE)** — *Se detectan y analizan posibles ataques y situaciones comprometedoras en materia de seguridad cibernética.* Detectar permite el descubrimiento y el análisis oportunos de anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos que pueden indicar que se están produciendo ataques e incidentes de seguridad cibernética. Esta Función apoya el éxito de las actividades de respuesta y recuperación de incidentes.
- **Responder (RS)** — *Se toman medidas en relación con un incidente de seguridad cibernética detectado.* Responder apoya la capacidad de contención de los efectos de los incidentes de seguridad cibernética. Los resultados de esta función abarcan la gestión, el análisis, la mitigación, la notificación y la comunicación de incidentes.
- **Recuperación (RC)** — *Se restauran los activos y las operaciones afectados por un incidente de seguridad cibernética.* La recuperación contribuye al restablecimiento oportuno de las operaciones normales para reducir los efectos de los incidentes de seguridad cibernética y permitir una comunicación adecuada durante los esfuerzos de recuperación.

Aunque muchas actividades de gestión de riesgos de seguridad cibernética se centran en evitar que se produzcan acontecimientos negativos, también pueden apoyar el aprovechamiento de oportunidades positivas. Las acciones para reducir el riesgo de seguridad cibernética pueden beneficiar a una organización de otras maneras, como el aumento de los ingresos (p. ej., primero ofreciendo el exceso de espacio de las instalaciones a un proveedor de alojamiento comercial para alojar sus propios centros de datos y los de otras organizaciones, y luego trasladando un importante sistema financiero del centro de datos interno de la organización al proveedor de alojamiento para reducir los riesgos de seguridad cibernética).

Figure 2 muestra las Funciones del CSF como una rueda porque todas las Funciones se relacionan entre sí. Por ejemplo, una organización categorizará los activos en Identificar y tomará medidas para asegurar esos activos en Proteger. Las inversiones en planificación y pruebas en las funciones de gobernanza e identificación permitirán la detección oportuna de acontecimientos inesperados en la función de detección, así como la adopción de medidas de respuesta y recuperación ante incidentes de seguridad cibernética en las funciones de respuesta y recuperación. La gobernanza está en el centro de la rueda porque informa sobre cómo una organización implementará las otras cinco Funciones.

Fig. 2. Funciones del CSF

Las funciones deben abordarse simultáneamente. Las acciones que dan apoyo a Gobernar, Identificar, Proteger y Detectar deben ocurrir continuamente, y las acciones que dan apoyo a Responder y Recuperar deben estar listas en todo momento y ocurrir cuando ocurran incidentes de seguridad cibernética. Todas las funciones tienen roles vitales relacionados con los incidentes de seguridad cibernética. Los resultados de Gobernar, Identificar y Proteger ayudan a prevenir y preparar los incidentes, mientras que los resultados de Gobernar, Detectar, Responder y Recuperar ayudan a descubrir y gestionar los incidentes.

Cada Función recibe el nombre de un verbo que resume su contenido. Cada función se divide en *Categorías*, que son los resultados de seguridad cibernética relacionados que componen colectivamente la función. Las *subcategorías* dividen a su vez cada categoría en resultados más específicos de actividades técnicas y de gestión. Las subcategorías no son exhaustivas, pero describen resultados detallados que apoyan cada categoría.

Las Funciones, Categorías y Subcategorías se aplican a todas las ICT utilizadas por una organización, incluidas la tecnología de la información (TI), el Internet de las Cosas (IoT) y la Tecnología Operativa (OT). También se aplican a todos los tipos de entornos tecnológicos, incluidos los sistemas en la nube, móviles y de inteligencia artificial. El CSF Core está orientado al futuro y su objetivo es aplicarse a futuros cambios en tecnologías y entornos.

3. Introducción a los perfiles y niveles del CSF

Esta sección define los conceptos de perfiles y niveles de CSF.

3.1. Perfiles de CSF

Un *Perfil Organizativo de CSF* describe la postura de seguridad cibernética actual u objetivo de una organización en términos de los resultados del Core. Los Perfiles Organizativos se utilizan para comprender, adaptar, evaluar, priorizar y comunicar los resultados del Core teniendo en cuenta los objetivos de la misión de una organización, las expectativas de las partes interesadas, el panorama de amenazas y los requisitos. Una organización puede entonces priorizar sus acciones para lograr resultados específicos y comunicar esa información a las partes interesadas.

Cada perfil organizativo incluye uno o ambos de los siguientes elementos:

1. Un *Perfil Actual* especifica los resultados esenciales que una organización está logrando actualmente (o intentando lograr) y caracteriza cómo o en qué medida se está logrando cada resultado.
2. Un *Perfil Objetivo* especifica los resultados deseados que una organización ha seleccionado y priorizado para alcanzar sus objetivos de gestión de riesgos de seguridad cibernética. Un Perfil Objetivo considera cambios anticipados a la postura de seguridad cibernética de la organización, tales como nuevos requerimientos, adopción de nuevas tecnologías, y tendencias de inteligencia de amenazas.

Un *Perfil Comunitario* es una línea base de resultados de CSF que se crea y publica para abordar intereses y objetivos compartidos entre varias organizaciones. Un perfil comunitario se desarrolla normalmente para un sector, subsector, tecnología, tipo de amenaza u otro caso de uso en particular. Una organización puede utilizar un Perfil Comunitario como base para su propio Perfil Objetivo. Se pueden encontrar ejemplos de perfiles comunitarios en el sitio web del CSF del NIST.

Los pasos mostrados en la Fig. 3 y resumidos a continuación ilustran una forma en que una organización podría utilizar un Perfil Organizativo para ayudar a informar la mejora continua de su seguridad cibernética.

Fig. 3. Pasos para crear y utilizar un Perfil Organizativo de CSF

1. **Alcance del Perfil Organizativo.** Documentar los hechos y suposiciones de alto nivel en los que se basará el perfil para definir su alcance. Una organización puede tener tantos Perfiles Organizativos como desee, cada uno con un alcance diferente. Por ejemplo, un perfil puede abarcar toda una organización o limitarse a los sistemas financieros de una organización o a combatir amenazas de ransomware y manejar incidentes de ransomware que involucren esos sistemas financieros.
2. **Recopile la información necesaria para preparar el Perfil Organizativo.** Ejemplos de información pueden incluir políticas organizativas, prioridades y recursos de gestión de riesgos, perfiles de riesgo empresarial, registros de análisis de impacto en el negocio (BIA), requisitos y estándares de seguridad cibernética seguidos por la organización, prácticas y herramientas (p. ej., procedimientos y salvaguardas), y roles de trabajo.
3. **Crear el perfil organizativo.** Determine qué tipos de información debe incluir el Perfil para los resultados seleccionados del CSF, y documente la información necesaria. Considere las implicaciones de riesgo del Perfil Actual para informar la planificación y priorización del Perfil Objetivo. Asimismo, considere el uso de un Perfil Comunitario como base para el Perfil Objetivo.
4. **Analice las brechas entre el Perfil Actual y el Perfil Objetivo, y cree un plan de acción.** Realice un análisis de brechas para identificar y analizar las diferencias entre el Perfil Actual y el Perfil Objetivo, y desarrolle un plan de acción priorizado (por ejemplo, registro de riesgos, informe detallado de riesgos, Plan de Acción e Hitos [POA&M]) para abordar esas brechas.
5. **Implemente el plan de acción y actualice el perfil organizativo.** Siga el plan de acción para abordar las brechas y mover la organización hacia el Perfil Objetivo. Un plan de acción puede tener un plazo global o ser continuo.

Dada la importancia de la mejora continua, una organización puede repetir estos pasos tantas veces como sea necesario.

Existen otros usos para los Perfiles Organizativos. Por ejemplo, se puede usar un Perfil Actual para documentar y comunicar las capacidades de seguridad cibernética de la organización y las oportunidades conocidas de mejora con las partes interesadas externas, tales como socios de

negocios o clientes potenciales. También, un Perfil Objetivo puede ayudar a expresar los requisitos y expectativas de gestión de riesgos de seguridad cibernética de la organización a los proveedores, colaboradores y otras terceras partes como un objetivo a alcanzar por esas partes.

3.2. Niveles de CSF

Una organización puede elegir utilizar los Niveles para informar sus Perfiles Actual y Objetivo. Los *niveles* caracterizan el rigor de las prácticas de gobernanza y gestión de los riesgos de seguridad cibernética de una organización, y proporcionan el contexto de cómo una organización ve los riesgos de seguridad cibernética y los procesos establecidos para gestionar esos riesgos. Los niveles, tal y como se muestran en Fig. 4 e ilustran teóricamente en Appendix B, reflejan las prácticas de una organización para gestionar los riesgos de seguridad cibernética como Parcial (Nivel 1), Informado sobre el Riesgo (Nivel 2), Repetible (Nivel 3) y Adaptativo (Nivel 4). Los niveles describen una evolución desde respuestas informales y ad hoc hasta enfoques ágiles, informados sobre el riesgo y en continua mejora. La selección de niveles ayuda a establecer el tono general de cómo una organización gestionará sus riesgos de seguridad cibernética.

Fig. 4. Los niveles de los CSF para el gobierno y la gestión de los riesgos de seguridad cibernética

Los niveles deben complementar la metodología de gestión de riesgos de seguridad cibernética de una organización en lugar de reemplazarla. Por ejemplo, una organización puede utilizar los niveles para comunicarse internamente como punto de referencia para un enfoque[1] de toda la organización para gestionar los riesgos de seguridad cibernética. La progresión a niveles superiores se fomenta cuando los riesgos o mandatos son mayores o cuando un análisis de costos y beneficios indica una reducción factible y rentable de los riesgos negativos de seguridad cibernética.

El sitio web del CSF del NIST proporciona información adicional sobre el uso de perfiles y niveles. Incluye punteros a plantillas de Perfiles Organizativos alojadas en el NIST y un repositorio de Perfiles Comunitarios en una variedad de formatos legibles por máquina y por el ser humano.

[1] Para los fines de este documento, los términos “toda la organización” y “empresa” tienen el mismo significado.

4. Introducción a los recursos en línea que complementan el CSF

El NIST y otras organizaciones han producido un conjunto de recursos en línea que ayudan a las organizaciones a comprender, adoptar y utilizar el CSF. Dado que están alojados en línea, estos recursos adicionales pueden actualizarse con mayor frecuencia que este documento, que se actualiza con poca frecuencia para brindar estabilidad a sus usuarios, y estar disponibles en formatos legibles por máquinas. Esta sección ofrece una visión general de tres tipos de recursos en línea: Referencias informativas, ejemplos de aplicación y guías de inicio rápido.

Las referencias informativas son mapas que indican las relaciones entre el núcleo y las distintas normas, directrices, reglamentos y otros contenidos. Las Referencias Informativas ayudan a informar sobre cómo una organización puede lograr los resultados del Core. Las referencias informativas pueden ser específicas de un sector o de una tecnología. Pueden ser producidas por el NIST o por otra organización. Algunas referencias informativas tienen un alcance más limitado que una subcategoría. Por ejemplo, un control particular de SP 800-53, *Controles de Seguridad y Privacidad para Sistemas de Información y Organizaciones*, puede ser una de las muchas referencias necesarias para lograr el resultado descrito en una Subcategoría. Otras Referencias Informativas pueden ser de un nivel superior, como un requisito de una política que aborda parcialmente diversas Subcategorías. Al utilizar el CSF, una organización puede identificar las Referencias Informativas más relevantes.

Ejemplos de implementación proporcione ejemplos teóricos de pasos concisos y orientados a la acción para ayudar a lograr los resultados de las subcategorías. Los verbos utilizados para expresar los Ejemplos incluyen compartir, documentar, desarrollar, realizar, monitorear, analizar, evaluar y ejercer. Los Ejemplos no son una lista exhaustiva de todas las acciones que podría tomar una organización para lograr un resultado, ni representan una línea de base de las acciones necesarias para hacer frente a los riesgos de seguridad cibernética.

Las *Guías de Inicio Rápido (QSG)* son documentos concisos sobre temas específicos relacionados con los CSF y frecuentemente se adaptan a audiencias específicas. Las QSG pueden ayudar a una organización a implementar el CSF porque simplifican partes específicas del CSF en "primeros pasos" procesables que una organización puede considerar en el camino hacia la mejora de su postura de seguridad cibernética y la gestión de los riesgos asociados. Las guías se revisan en sus propios plazos, y se añaden nuevas guías según sea necesario.

Las sugerencias de nuevas referencias informativas para el CSF 2.0 siempre se pueden compartir con el NIST en olir@nist.gov. Las sugerencias sobre otros recursos de referencia en el sitio web del CSF del NIST, incluidos otros temas del QSG, se deben dirigir a cyberframework@nist.gov.

5. Mejora de la comunicación e integración de los riesgos de seguridad cibernética

El uso del CSF variará en función de la misión y los riesgos únicos de una organización. Al comprender las expectativas de las partes interesadas y el apetito y la tolerancia al riesgo (como se indica en la Gobernanza), una organización puede priorizar las actividades de seguridad cibernética para tomar decisiones informadas sobre los gastos y las acciones de seguridad cibernética. Una organización puede optar por gestionar el riesgo de una o más maneras -entre las que se incluyen mitigar, transferir, evitar o aceptar riesgos negativos y realizar, compartir, mejorar o aceptar riesgos positivos- dependiendo de los impactos y las probabilidades potenciales. Es importante destacar que una organización puede utilizar el CSF tanto internamente para gestionar sus capacidades de seguridad cibernética como externamente para supervisar o comunicarse con terceros.

Sin importar cómo se utilice el CSF, una organización se puede beneficiar del uso del CSF como guía para ayudarla a entender, evaluar, priorizar y comunicar los riesgos de seguridad cibernética y las acciones que gestionarán esos riesgos. Los resultados seleccionados pueden ser utilizados para enfocar e implementar decisiones estratégicas para mejorar las posturas de seguridad cibernética y mantener la continuidad de las funciones esenciales de la misión, teniendo en cuenta las prioridades y los recursos disponibles.

5.1. Cómo mejorar la comunicación de la gestión de riesgos

El CSF proporciona una base para mejorar la comunicación en relación con las expectativas, la planificación y los recursos de seguridad cibernética. El CSF fomenta el flujo bidireccional de información (como se muestra en la mitad superior de la Fig. 5) entre los directivos que se centran en las prioridades y la dirección estratégica de la organización y los gestores que gestionan los riesgos específicos de seguridad cibernética que podrían afectar a la concretización de dichas prioridades. El CSF también apoya un flujo similar (tal y como se muestra en la mitad inferior de la Fig. 5) entre los directivos y los profesionales que implementan y operan las tecnologías. La parte izquierda de la figura indica la importancia de que los profesionales compartan sus actualizaciones, percepciones e inquietudes con los gerentes y directivos.

Fig. 5. Cómo utilizar el CSF para mejorar la comunicación de la gestión de riesgos

Prepararse para crear y utilizar perfiles organizativos implica recopilar información sobre prioridades organizativas, recursos y dirección del riesgo por parte de los directivos. Posteriormente, los directivos colaboran con los profesionales para comunicar las necesidades empresariales y crear perfiles organizativos basados en el riesgo. Las acciones para cerrar cualquier brecha identificada entre los Perfiles Actuales y los Perfiles Objetivo serán implementadas por los directivos y los profesionales y proporcionarán información clave en los planes a nivel de sistema. A medida que se alcanza el estado objetivo en toda la organización —incluidos los controles y el monitoreo aplicados a nivel de sistema —, los resultados actualizados se pueden compartir a través de registros de riesgos e informes de progreso. Como parte de la evaluación continua, los gerentes obtienen información para realizar ajustes que reduzcan aún más los daños potenciales y aumenten los beneficios potenciales.

La función de gobernanza apoya la comunicación de los riesgos organizativos con los **directivos**. Las discusiones de los directivos tienen que ver con la estrategia, en particular con la forma en que las incertidumbres relacionadas con la seguridad cibernética podrían afectar al cumplimiento de los objetivos de la organización. Estas discusiones de gobierno apoyan el diálogo y el acuerdo sobre las estrategias de gestión de riesgos (lo que incluye al riesgo de la cadena de suministro de seguridad cibernética); funciones, responsabilidades y autoridades; políticas; y supervisión. A medida que los directivos establecen prioridades y objetivos de seguridad cibernética basados en esas necesidades, comunican las expectativas sobre el apetito de riesgo, la responsabilidad y los recursos. Los directivos también son responsables de integrar la gestión de riesgos de seguridad cibernética con los programas de ERM y los programas de gestión de riesgos de nivel inferior (consulte la Sec. 5.2). Las comunicaciones reflejadas en la mitad superior de la Fig. 5 pueden incluir consideraciones para ERM y los programas de nivel inferior y, por lo tanto, informar a los directivos y profesionales.

Los objetivos generales de seguridad cibernética establecidos por los directivos son informados por los **gerentes** y se transmiten en cascada a ellos. En una entidad comercial, se pueden aplicar

a una línea de negocio o división operativa. Para las entidades gubernamentales, pueden ser consideraciones a nivel de división o sucursal. Al aplicar el CSF, los gerentes se centrarán en cómo alcanzar los objetivos de riesgo a través de servicios comunes, controles y colaboración, tal como se expresa en el perfil de objetivos y se mejora a través de las acciones que se siguen en el plan de acción (p. ej., registro de riesgos, informe detallado de riesgos, POA&M).

Los **profesionales** se centran en implementar el estado objetivo y medir los cambios en el riesgo operativo para ayudar a planificar, llevar a cabo y monitorear actividades específicas de seguridad cibernética. A medida que se implementan los controles para gestionar el riesgo a un nivel aceptable, los profesionales proporcionan a los gerentes y directivos la información (p. ej., indicadores clave de rendimiento, indicadores clave de riesgo) que necesitan para comprender la postura de seguridad cibernética de la organización, tomar decisiones informadas y mantener o ajustar la estrategia de riesgo según corresponda. Los directivos también pueden combinar estos datos sobre riesgos de seguridad cibernética con información sobre otros tipos de riesgos de toda la organización. Las actualizaciones de las expectativas y prioridades se incluyen en Perfiles Organizativos actualizados a medida que se repite el ciclo.

5.2. Cómo mejorar la integración con otros programas de gestión de riesgos

Cada organización se enfrenta a numerosos tipos de riesgo de ICT (p. ej., privacidad, cadena de suministro, inteligencia artificial) y puede utilizar marcos y herramientas de gestión específicos para cada riesgo. Algunas organizaciones integran las ICT y todos los demás esfuerzos de gestión de riesgos a un alto nivel mediante el uso de ERM, mientras que otras mantienen los esfuerzos por separado para garantizar una atención adecuada a cada uno de ellos. Las pequeñas organizaciones, por su índole, pueden monitorear el riesgo a nivel de la empresa, mientras que las empresas más grandes pueden mantener esfuerzos separados de gestión de riesgos integrados en la ERM.

Las organizaciones pueden emplear un enfoque de ERM para equilibrar una *cartera* de consideraciones de riesgo, incluida la seguridad cibernética, y tomar decisiones informadas. Los directivos reciben información significativa sobre las actividades de riesgo actuales y previstas a medida que integran las estrategias de gobernanza y riesgo con los resultados de los usos anteriores del CSF. El CSF ayuda a las organizaciones a traducir su terminología sobre seguridad cibernética y gestión de riesgos de seguridad cibernética a un lenguaje general de gestión de riesgos que los directivos comprenderán.

Los recursos del NIST que describen la relación mutua entre la gestión de riesgos de seguridad cibernética y ERM incluyen:

- *Marco de seguridad cibernética 2.0 del NIST* - *Guía de inicio rápido de gestión de riesgos empresariales*
- Informe entre agencias (IR) 8286 del NIST, *Integración de la seguridad cibernética y la gestión de riesgos empresariales (ERM)*
- IR 8286A, *Identificación y estimación del riesgo de seguridad cibernética para la gestión del riesgo empresarial*

- IR 8286B, *Priorización del Riesgo de Seguridad Cibernética para la Gestión del Riesgo Empresarial*
- IR 8286C, *Clasificación de los riesgos de seguridad cibernética para la gestión de riesgos empresariales y la supervisión de la gobernanza*
- IR 8286D, *Uso del Análisis de Impacto en el Negocio para Informar la Priorización y Respuesta al Riesgo*
- SP 800-221, *Impacto Empresarial del Riesgo de las Tecnologías de la Información y las Comunicaciones: Gobernanza y Gestión de Programas de Riesgos de TIC dentro de una Cartera de Riesgos Empresariales*
- SP 800-221A, *Resultados de Riesgos de Tecnología de Información y Comunicaciones (ICT): Integración de los Programas de Gestión de Riesgos de ICT con la Cartera de Riesgos de la Empresa*

Una organización también puede considerar el CSF útil para integrar la gestión de riesgos de seguridad cibernética con programas individuales de gestión de riesgos de ICT, tales como:

- **Gestión y evaluación de riesgos de seguridad cibernética:** El CSF puede integrarse con programas establecidos de gestión y evaluación de riesgos de seguridad cibernética, como SP 800-37, Marco de gestión de riesgos para sistemas de información y organizaciones, y SP 800-30, Guía para realizar evaluaciones de riesgos del Marco de gestión de riesgos (RMF) del NIST. Para una organización que utilice el RMF del NIST y su conjunto de publicaciones, el CSF puede utilizarse para complementar el enfoque del RMF para seleccionar y priorizar los controles del SP 800-53, Controles de seguridad y privacidad para sistemas de información y organizaciones.
- **Riesgos de privacidad:** Si bien la seguridad cibernética y la privacidad son disciplinas independientes, sus objetivos se solapan en determinadas circunstancias, como se ilustra en Fig. 6.

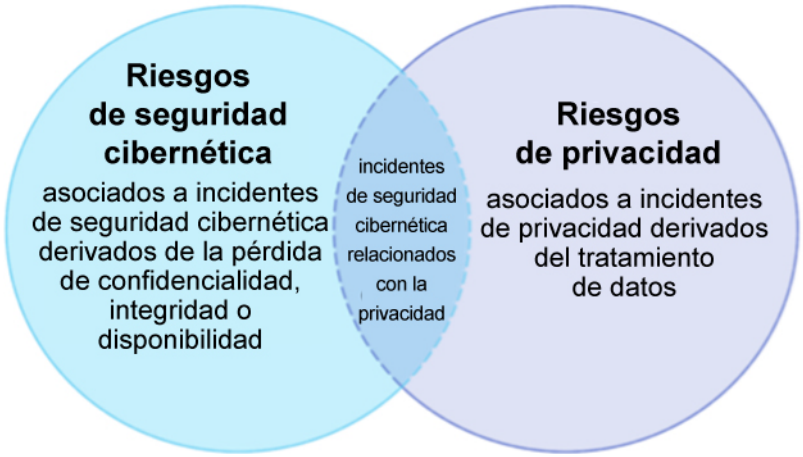

Fig. 6. Relación entre los riesgos de seguridad cibernética y privacidad

La gestión del riesgo de seguridad cibernética es esencial para abordar los riesgos de privacidad relacionados con la pérdida de confidencialidad, integridad y disponibilidad

de los datos de las personas. Por ejemplo, las violaciones de datos pueden conducir al robo de identidad. Sin embargo, los riesgos de privacidad también pueden surgir por medios no relacionados con incidentes de seguridad cibernética.

Una organización procesa datos para alcanzar objetivos de misión o de negocio, lo que a veces puede provocar *incidentes de privacidad* en los que los individuos pueden tener problemas como resultado del procesamiento de datos. Estos problemas se pueden expresar de varias maneras, pero el NIST los describe como efectos que van desde la dignidad (p. ej., vergüenza o estigma) a daños más tangibles (p. ej., discriminación, pérdida económica o daño físico). El Marco de Privacidad del NIST y el Marco de Seguridad Cibernética se pueden utilizar conjuntamente para abordar los diferentes aspectos de los riesgos de seguridad cibernética y privacidad. Además, la Metodología de Evaluación de Riesgos para la Privacidad (PRAM, por sus siglas en inglés) del NIST cuenta con un catálogo de problemas de ejemplo para su uso en evaluaciones de riesgos para la privacidad.

- **Riesgos de la cadena de suministro:** Una organización puede utilizar el CSF para fomentar la supervisión de los riesgos de seguridad cibernética y las comunicaciones con las partes interesadas a lo largo de las cadenas de suministro. Todos los tipos de tecnología dependen de un ecosistema de cadena de suministro complejo, distribuido a escala mundial, extenso e interconectado, con rutas geográficamente diversas y diversos niveles de subcontratación. Este ecosistema está compuesto por entidades de los sectores público y privado (p. ej., compradors, proveedores, desarrolladores, integradores de sistemas, proveedores de servicios de sistemas externos y otros proveedores de servicios relacionados con la tecnología) que interactúan para investigar, desarrollar, diseñar, fabricar, adquirir, entregar, integrar, operar, mantener, eliminar y utilizar o gestionar de otro modo productos y servicios tecnológicos Estas interacciones están determinadas e influidas por tecnologías, leyes, políticas, procedimientos y prácticas.

  Dadas las complejas e interconectadas relaciones de este ecosistema, la gestión de riesgos de la cadena de suministro (SCRM) es fundamental para las organizaciones. La SCRM de seguridad cibernética (C-SCRM) es un proceso sistemático para gestionar la exposición a los riesgos de seguridad cibernética a lo largo de las cadenas de suministro y desarrollar estrategias, políticas, procesos y procedimientos de respuesta adecuados. Las subcategorías dentro de la categoría CSF C-SCRM [GV.SC] proporcionan una conexión entre los resultados que se centran puramente en la seguridad cibernética y los que se centran en C-SCRM. SP 800-161r1 (Revisión 1), *Prácticas de Gestión de Riesgos de la Cadena de Suministro de seguridad cibernética para Sistemas y Organizaciones*, proporciona información en profundidad sobre C-SCRM.

- **Riesgos de las tecnologías emergentes:** A medida que surgen nuevas tecnologías y nuevas aplicaciones de la tecnología, aparecen nuevos riesgos. Un ejemplo actual es la inteligencia artificial (IA), que presenta riesgos de seguridad cibernética y privacidad, así como muchos otros tipos de riesgo. El Marco de Gestión de Riesgos de Inteligencia Artificial del NIST (AI RMF, por sus siglas en inglés) se desarrolló para ayudar a abordar estos riesgos. Tratar los riesgos de la IA junto con otros riesgos empresariales (p. ej.,

financieros, de seguridad cibernética, de reputación y de privacidad) producirá un resultado más integrado y una mayor eficiencia organizativa. Las consideraciones y los enfoques de gestión de riesgos de seguridad cibernética y privacidad son aplicables al diseño, desarrollo, despliegue, evaluación y uso de sistemas de IA. El AI RMF Core utiliza Funciones, Categorías y Subcategorías para describir los resultados de la IA y ayudar a gestionar los riesgos relacionados con la IA.

Appendix A. CSF Core

Este apéndice describe las Funciones, las Categorías y las Subcategorías del CSF Core. Table 1 enumera los nombres de las Funciones y Categorías del CSF 2.0 Core y los identificadores alfabéticos únicos. Cada nombre de función de la tabla está vinculado a su parte del apéndice. El orden de las Funciones, Categorías y Subcategorías del Core no es alfabético; su objetivo es que tenga mayor resonancia entre los encargados de hacer operativa la gestión de riesgos dentro de una organización. La numeración de las subcategorías no es secuencial de forma intencionada; las lagunas en la numeración indican las subcategorías del CSF 1.1 que se reubicaron en el CSF 2.0.

Tabla 1. CSF 2.0 Nombres e identificadores de funciones básicas y categorías

Función	Categoría	Identificador de Categoría
Gobernar (GV)	Contexto organizativo	GV.OC
	Estrategia de gestión de riesgos	GV.RM
	Funciones, responsabilidades y autoridades	GV.RR
	Política	GV.PO
	Supervisión	GV.OV
	Gestión de riesgos de la cadena de suministro en materia de seguridad cibernética	GV.SC
Identificar (ID)	Gestión de activos	ID.AM
	Evaluación de riesgos	ID.RA
	Mejora	ID.IM
Proteger (PR)	Gestión de identidades, autenticación y control de acceso	PR.AA
	Concienciación y capacitación	PR.AT
	Seguridad de datos	PR.DS
	Seguridad de plataformas	PR.PS
	Resistencia de la infraestructura tecnológica	PR.IR
Detectar (DE)	Monitoreo continuo	DE.CM
	Análisis de eventos adversos	DE.AE
Responder (RS)	Gestión de incidentes	RS.MA
	Análisis de incidentes	RS.AN
	Notificación y comunicación de la respuesta al incidente	RS.CO
	Mitigación de incidentes	RS.MI
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	RC.RP
	Comunicación de la recuperación del incidente	RC.CO

El CSF Core, las Referencias Informativas y los Ejemplos de Implementación están disponibles en el sitio web del CSF 2.0, y a través de la Herramienta de Referencia del CSF 2.0, que permite

que los usuarios los exploren y exporten en formatos legibles por humanos y máquinas. El núcleo del CSF 2.0 también está disponible en un formato legado similar al del CSF 1.1.

GOBERNAR (GV): Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de seguridad cibernética de la organización.

- **Contexto organizativo (GV.OC):** Se comprenden las circunstancias - misión, expectativas de las partes interesadas, dependencias y requisitos legales, normativos y contractuales - que afectan a las decisiones de gestión de riesgos de seguridad cibernética de la organización
  - **GV.OC-01:** Se comprende la misión de la organización y se informa sobre la gestión de riesgos de seguridad cibernética.
  - **GV.OC-02:** Las partes interesadas internas y externas son comprendidas, y sus necesidades y expectativas con respecto a la gestión de riesgos de seguridad cibernética son comprendidas y consideradas.
  - **GV.OC-03:** Se comprenden y gestionan los requisitos legales, normativos y contractuales relativos a la seguridad cibernética, incluidas las obligaciones en materia de privacidad y libertades civiles.
  - **GV.OC-04:** Se comprenden y comunican los objetivos, las capacidades y los servicios críticos de los que dependen las partes interesadas externas o que esperan de la organización
  - **GV.OC-05:** Se comprenden y comunican los resultados, capacidades y servicios de los que depende la organización

- **Estrategia de gestión de riesgos (GV.RM):** Se establecen, comunican y utilizan las prioridades, las restricciones, las declaraciones de tolerancia y apetito por el riesgo y los supuestos de la organización para respaldar las decisiones sobre el riesgo operativo
  - **GV.RM-01:** Los objetivos de la gestión de riesgos son establecidos y acordados por las partes interesadas de la organización
  - **GV.RM-02:** Se establecen, se comunican y se mantienen las declaraciones sobre el apetito de riesgo y la tolerancia al riesgo
  - **GV.RM-03:** Las actividades y los resultados de la gestión de riesgos de seguridad cibernética se incluyen en los procesos de gestión de riesgos de la empresa
  - **GV.RM-04:** Se establece y comunica una dirección estratégica que describa las opciones adecuadas de respuesta al riesgo.
  - **GV.RM-05:** Se establecen líneas de comunicación en toda la organización para los riesgos de seguridad cibernética, lo que incluye a los riesgos de proveedores y otros terceros.
  - **GV.RM-06:** Se establece y comunica un método estandarizado para calcular, documentar, categorizar y priorizar los riesgos de seguridad cibernética.

- **GV.RM-07:** Se caracterizan las oportunidades estratégicas (es decir, los riesgos positivos) y se incluyen en las discusiones sobre riesgos de seguridad cibernética de la organización.

- **Funciones, responsabilidades y autoridades (GV.RR):** Se establecen y comunican las funciones, las responsabilidades y las competencias en materia de seguridad cibernética para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua.
  - **GV.RR-01:** El liderazgo organizativo es responsable de los riesgos de seguridad cibernética y fomenta una cultura consciente de los riesgos, ética y de mejora continua.
  - **GV.RR-02:** Se establecen, comunican, comprenden y aplican las funciones, responsabilidades y autoridades relacionadas con la gestión de riesgos de seguridad cibernética.
  - **GV.RR-03:** Se asignan recursos adecuados de acuerdo con la estrategia de riesgos de seguridad cibernética, las funciones, las responsabilidades y las políticas.
  - **GV.RR-04:** La seguridad cibernética se incluye en las prácticas de recursos humanos

- **Política (GV.PO):** La política de seguridad cibernética de la organización es establecida, comunicada y aplicada.
  - **GV.PO-01:** La política de gestión de riesgos de seguridad cibernética se establece en base al contexto organizativo, la estrategia de seguridad cibernética y las prioridades, y es comunicada y aplicada
  - **GV.PO-02:** La política de gestión de riesgos de seguridad cibernética se revisa, actualiza, comunica y aplica para reflejar los cambios en los requisitos, las amenazas, la tecnología y la misión de la organización

- **Supervisión (GV.OV):** Los resultados de las actividades de gestión de riesgos de seguridad cibernética en toda la organización y el rendimiento se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos
  - **GV.OV-01:** Los resultados de la estrategia de gestión de riesgos de seguridad cibernética se revisan para informar y ajustar la estrategia y la dirección
  - **GV.OV-02:** La estrategia de gestión de riesgos de seguridad cibernética se revisa y ajusta para garantizar la cobertura de los requisitos y riesgos de la organización
  - **GV.OV-03:** El rendimiento de la gestión de riesgos de seguridad cibernética de la organización se evalúa y revisa para realizar los ajustes necesarios

- **Gestión de riesgos de la cadena de suministro de seguridad cibernética (GV.SC):** Las partes interesadas de la organización identifican, establecen, gestionan, supervisan y mejoran los procesos de gestión de riesgos de la cadena de suministro cibernética
  - **GV.SC-01:** Las partes interesadas de la organización establecen y acuerdan un programa, estrategia, objetivos, políticas y procesos de gestión de riesgos de seguridad cibernética en la cadena de suministro

- **GV.SC-02:** Se establecen, comunican y coordinan interna y externamente las funciones y responsabilidades de seguridad cibernética para proveedores, clientes y colaboradores
- **GV.SC-03:** La gestión de riesgos de la cadena de suministro de seguridad cibernética está integrada en la seguridad cibernética y la gestión de riesgos empresariales, la evaluación de riesgos y los procesos de mejora
- **GV.SC-04:** Los proveedores son conocidos y priorizados por criticidad
- **GV.SC-05:** Los requisitos para abordar los riesgos de seguridad cibernética en las cadenas de suministro se establecen, priorizan e integran en contratos y otros tipos de acuerdos con proveedores y otras terceras partes pertinentes
- **GV.SC-06:** Se llevan a cabo la planificación y la diligencia debida para reducir los riesgos antes de entablar relaciones formales con proveedores u otros terceros
- **GV.SC-07:** Los riesgos planteados por un proveedor, sus productos y servicios y otros terceros se comprenden, registran, priorizan, evalúan, responden y monitorean a lo largo de la relación
- **GV.SC-08:** Los proveedores pertinentes y otros terceros se incluyen en las actividades de planificación, respuesta y recuperación de incidentes
- **GV.SC-09:** Las prácticas de seguridad de la cadena de suministro se integran en los programas de seguridad cibernética y de gestión de riesgos empresariales, y su rendimiento se monitorea a lo largo del ciclo de vida de los productos y servicios tecnológicos
- **GV.SC-10:** Los planes de gestión de riesgos de la cadena de suministro de seguridad cibernética incluyen disposiciones para las actividades que ocurren después de la conclusión de un acuerdo de colaboración o servicio

IDENTIFICAR (ID): Se conocen los riesgos de seguridad cibernética actuales de la organización

- **Gestión de activos (ID.AM):** Los activos (p. ej., datos, hardware, software, sistemas, instalaciones, servicios, personas) que permiten a la organización alcanzar sus objetivos empresariales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización
  - **ID.AM-01:** Se mantienen inventarios del hardware gestionado por la organización
  - **ID.AM-02:** Se mantienen inventarios de software, servicios y sistemas gestionados por la organización
  - **ID.AM-03:** Se mantienen representaciones de la comunicación de red autorizada de la organización y de los flujos de datos de red internos y externos
  - **ID.AM-04:** Se mantienen inventarios de los servicios prestados por los proveedores

- **ID.AM-05:** Se priorizan los activos en función de su clasificación, criticidad, recursos e impacto en la misión
- **ID.AM-07:** Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados
- **ID.AM-08:** Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de vida

- **Evaluación de riesgos (ID.RA):** La organización comprende el riesgo de seguridad cibernética para la organización, los activos y los individuos
  - **ID.RA-01:** Se identifican, validan y registran las vulnerabilidades de los activos
  - **ID.RA-02:** Se recibe información sobre amenazas cibernéticas de foros y fuentes de intercambio de información
  - **ID.RA-03:** Se identifican y registran las amenazas internas y externas a la organización
  - **ID.RA-04:** Se identifican y registran los impactos potenciales y las probabilidades de que las amenazas exploten las vulnerabilidades
  - **ID.RA-05:** Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para comprender el riesgo inherente e informar sobre la priorización de la respuesta al riesgo
  - **ID.RA-06:** Se eligen, priorizan, planifican, controlan y comunican las respuestas al riesgo
  - **ID.RA-07:** Se gestionan los cambios y las excepciones, se evalúa su impacto en el riesgo, se registran y se realiza su seguimiento
  - **ID.RA-08:** Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades
  - **ID.RA-09:** Se evalúa la autenticidad e integridad del hardware y software antes de su adquisición y uso
  - **ID.RA-10:** Se evalúan los proveedores críticos antes de su adquisición

- **Mejora (ID.IM):** Se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos de seguridad cibernética de la organización en todas las funciones del CSF
  - **ID.IM-01:** Las mejoras se identifican a partir de evaluaciones
  - **ID.IM-02:** Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, lo que incluye a los realizados en coordinación con proveedores y terceros pertinentes
  - **ID.IM-03:** Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativos
  - **ID.IM-04:** Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de seguridad cibernética que afectan a las operaciones.

PROTEGER (PR): Se utilizan medidas de protección para gestionar los riesgos de seguridad cibernética de la organización

- **Gestión de identidades, autenticación y control de acceso (PR.AA):** El acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado
  - **PR.AA-01:** La organización gestiona las identidades y credenciales de los usuarios, servicios y equipos autorizados
  - **PR.AA-02:** Las identidades están comprobadas y vinculadas a credenciales basadas en el contexto de las interacciones
  - **PR.AA-03:** Los usuarios, servicios y hardware están autenticados
  - **PR.AA-04:** Las afirmaciones de identidad se protegen, transmiten y verifican
  - **PR.AA-05:** Los permisos de acceso, los derechos y las autorizaciones se definen en una política, se gestionan, se aplican y se revisan, e incorporan los principios de privilegio mínimo y separación de funciones
  - **PR.AA-06:** El acceso físico a los activos se gestiona, supervisa y aplica de forma proporcional al riesgo
- **Concienciación y capacitación (PR.AT):** Se proporciona al personal de la organización concienciación y capacitación en seguridad cibernética para que puedan realizar sus tareas relacionadas con la seguridad cibernética
  - **PR.AT-01:** Se sensibiliza y capacita al personal para que disponga de los conocimientos y habilidades necesarios para realizar tareas generales teniendo en cuenta los riesgos de seguridad cibernética
  - **PR.AT-02:** Se sensibiliza y capacita a las personas que desempeñan funciones especializadas para que posean los conocimientos y aptitudes necesarios para realizar las tareas pertinentes teniendo en cuenta los riesgos de seguridad cibernética
- **Seguridad de los datos (PR.DS):** Los datos se gestionan de forma coherente con la estrategia de riesgos de la organización para proteger la confidencialidad, integridad y disponibilidad de la información
  - **PR.DS-01:** La confidencialidad, la integridad y la disponibilidad de los datos en reposo están protegidas
  - **PR.DS-02:** La confidencialidad, la integridad y la disponibilidad de los datos en tránsito están protegidas
  - **PR.DS-10:** La confidencialidad, la integridad y la disponibilidad de los datos en uso están protegidas
  - **PR.DS-11:** Se crean, protegen, mantienen y comprueban copias de seguridad de los datos

- **Seguridad de la plataforma (PR.PS):** El hardware, el software (p. ej., firmware, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales se gestionan de acuerdo con la estrategia de riesgos de la organización para proteger su confidencialidad, integridad y disponibilidad
  - **PR.PS-01:** Se establecen y aplican prácticas de gestión de la configuración
  - **PR.PS-02:** Se mantiene, sustituye y elimina el software en función del riesgo
  - **PR.PS-03:** Se mantiene, sustituye y elimina el hardware en función del riesgo
  - **PR.PS-04:** Se generen registros y se pongan a disposición para una supervisión continua
  - **PR.PS-05:** Se impide la instalación y la ejecución de software no autorizado
  - **PR.PS-06:** Se integran prácticas seguras de desarrollo de software y se supervisa su rendimiento durante todo el ciclo de vida de desarrollo del software

- **Resiliencia de la infraestructura tecnológica (PR.IR):** Las arquitecturas de seguridad se gestionan con la estrategia de riesgos de la organización a fin de proteger la confidencialidad, la integridad y la disponibilidad de los activos, así como la resiliencia de la organización
  - **PR.IR-01:** Las redes y los entornos están protegidos contra el acceso lógico y el uso no autorizados
  - **PR.IR-02:** Los activos tecnológicos de la organización están protegidos de las amenazas del entorno
  - **PR.IR-03:** Se implementan mecanismos para lograr los requisitos de resiliencia en situaciones normales y adversas
  - **PR.IR-04:** Se mantiene una capacidad de recursos adecuada para garantizar la disponibilidad

DETECTAR (DE): Se detectan y analizan posibles ataques y situaciones comprometedoras en materia de seguridad cibernética.

- **Monitoreo continuo (DE.CM):** Los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos
  - **DE.CM-01:** Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos
  - **DE.CM-02:** Se monitorea el entorno físico para detectar posibles acontecimientos adversos
  - **DE.CM-03:** Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos

- **DE.CM-06:** Se monitorean las actividades y los servicios de los proveedores de servicios externos para detectar acontecimientos potencialmente adversos.
- **DE.CM-09:** Se monitorean el hardware y el software informáticos, los entornos de ejecución y sus datos para detectar posibles acontecimientos adversos

- **Análisis de acontecimientos adversos (DE.AE):** Se analizan anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos para caracterizarlos y detectar incidentes de seguridad cibernética
  - **DE.AE-02:** Los acontecimientos potencialmente adversos se analizan para comprender mejor las actividades asociadas
  - **DE.AE-03:** Se correlaciona la información procedente de diversas fuentes
  - **DE.AE-04:** Se comprende el impacto estimado y el alcance de los acontecimientos adversos
  - **DE.AE-06:** La información sobre acontecimientos adversos se proporciona al personal y a las herramientas autorizadas
  - **DE.AE-07:** La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis
  - **DE.AE-08:** Se declaran incidentes cuando los acontecimientos adversos cumplen con los criterios de incidente definidos

RESPONDER (RS): Se toman medidas en relación con un incidente de seguridad cibernética detectado

- **Gestión de incidentes (RS.MA):** Se gestionan las respuestas a los incidentes de seguridad cibernética detectados
  - **RS.MA-01:** Se ejecuta el plan de respuesta a incidentes en coordinación con los terceros pertinentes una vez que se declara un incidente
  - **RS.MA-02:** Se clasifican y validan los informes de incidentes
  - **RS.MA-03:** Se clasifican y priorizan los incidentes
  - **RS.MA-04:** Se escalan o elevan los incidentes según sea necesario
  - **RS.MA-05:** Se aplican los criterios para iniciar la recuperación de incidentes

- **Análisis de incidentes (RS.AN):** Se llevan a cabo investigaciones con el fin de garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación
  - **RS.AN-03:** Se realizan análisis para determinar lo que ocurrió durante un incidente y la causa raíz del mismo
  - **RS.AN-06:** Se registran las acciones realizadas durante una investigación y se preservan la integridad y la procedencia de los registros

- **RS.AN-07:** Se recopilan los datos y metadatos del incidente y se preservan su integridad y su procedencia
- **RS.AN-08:** Se estima y valida la magnitud de un incidente.

- **Notificación y comunicación de la respuesta al incidente (RS.CO):** Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según lo exijan las leyes, las normativas o las políticas
  - **RS.CO-02:** Se notifican los incidentes a las partes interesadas internas y externas
  - **RS.CO-03:** La información se comparte con las partes interesadas internas y externas designadas

- **Mitigación de incidentes (RS.MI):** Se llevan a cabo actividades a fin de evitar la expansión de un incidente y mitigar sus efectos
  - **RS.MI-01:** Se contienen los incidentes
  - **RS.MI-02:** Se erradican los incidentes

RECUPERACIÓN (RC): Se restauran los activos y las operaciones afectados por un incidente de seguridad cibernética

- **Ejecución del Plan de Recuperación de Incidentes (RC.RP):** Se realizan actividades de restauración que garantizan la disponibilidad operativa de los sistemas y servicios afectados por incidentes de seguridad cibernética
  - **RC.RP-01:** La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez que se inicia desde el proceso de respuesta a incidentes
  - **RC.RP-02:** Se seleccionan, delimitan, priorizan y llevan a cabo las acciones de recuperación
  - **RC.RP-03:** Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para la restauración
  - **RC.RP-04:** Se tienen en cuenta las funciones críticas de la misión y la gestión de riesgos de seguridad cibernética para establecer normas operativas posteriores al incidente
  - **RC.RP-05:** Se verifica la integridad de los activos restaurados, se restauran los sistemas y servicios y se confirma el estado operativo normal
  - **RC.RP-06:** Se declara el fin de la recuperación del incidente sobre la base de criterios y se completa la documentación relacionada con el incidente

- **Comunicación de la recuperación del incidente (RC.CO):** Se coordinan las actividades de restauración con las partes internas y externas

- **RC.CO-03:** Las actividades de recuperación y los progresos en el restablecimiento de las capacidades operativas se comunican a las partes interesadas internas y externas designadas
- **RC.CO-04:** Las actualizaciones públicas sobre la recuperación del incidente se comparten mediante el uso de métodos y mensajes aprobados

Appendix B. Niveles del CSF

Table 2 contiene una ilustración teórica de los niveles del CSF analizados en la Sec. 3. Los niveles caracterizan el rigor de las prácticas de gobernanza de riesgos de seguridad cibernética de una organización (Gobernar) y las prácticas de gestión de riesgos de seguridad cibernética (Identificar, Proteger, Detectar, Responder y Recuperar).

Tabla 2. Ilustración teórica de los niveles del CSF

Nivel	Gobernanza de riesgos de seguridad cibernética	Gestión de riesgos de seguridad cibernética
Nivel 1: Parcial	La aplicación de la estrategia de riesgos de seguridad cibernética de la organización se gestiona de manera ad hoc. La priorización es ad hoc y no se fundamenta formalmente en los objetivos o el entorno de amenazas.	Existe una conciencia limitada sobre los riesgos de seguridad cibernética a nivel organizativo. La organización implementa la gestión de riesgos de seguridad cibernética de forma irregular, caso por caso. Es posible que la organización no disponga de procesos que permitan compartir información en materia de seguridad cibernética dentro de la organización. La organización desconoce generalmente los riesgos de seguridad cibernética asociados a sus proveedores y a los productos y servicios que adquiere y utiliza.
Nivel 2: Conocimiento de los riesgos	Las prácticas de gestión de riesgos son aprobadas por la gerencia, pero pueden no estar establecidas como política para toda la organización. La priorización de las actividades de seguridad cibernética y las necesidades de protección se basan directamente en los objetivos de riesgo de la organización, el entorno de amenazas o los requisitos de negocio/misión.	Existe una conciencia sobre los riesgos de seguridad cibernética a nivel organizacional, pero no se estableció un enfoque de toda la organización para gestionar los riesgos de seguridad cibernética. La consideración de la seguridad cibernética en los objetivos y programas de la organización puede ocurrir en algunos, pero no en todos los niveles de la organización. La evaluación del riesgo cibernético de los activos organizativos y externos se produce, pero no suele ser repetible o recurrente. La información sobre seguridad cibernética se comparte dentro de la organización de manera informal. La organización es consciente de los riesgos de seguridad cibernética asociados con sus proveedores y los productos y servicios que adquiere y utiliza, pero no actúa de manera coherente o formal en respuesta a esos riesgos.
Nivel 3: Repetible	Las prácticas de gestión de riesgos de la organización se aprueban y expresan formalmente como política. Las políticas, los procesos y los procedimientos informados sobre los riesgos se definen, se aplican según lo previsto y se revisan.	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de seguridad cibernética. La información sobre seguridad cibernética se comparte de forma rutinaria en toda la organización. Existen métodos consistentes para responder de manera efectiva a los cambios en los riesgos. El personal dispone de los conocimientos y habilidades necesarios

Nivel	Gobernanza de riesgos de seguridad cibernética	Gestión de riesgos de seguridad cibernética
	Las prácticas de seguridad cibernética de la organización se actualizan periódicamente sobre la base de la aplicación de los procesos de gestión de riesgos a los cambios en los requisitos de negocio/misión, las amenazas y el panorama tecnológico.	para desempeñar las funciones y responsabilidades que le fueron asignadas. La organización supervisa de forma coherente y precisa los riesgos de seguridad cibernética de los activos. Los altos directivos de seguridad cibernética y no cibernética se comunican regularmente en relación con los riesgos de seguridad cibernética. Los directivos se aseguran de que la seguridad cibernética se considera a través de todas las líneas de operación en la organización. La estrategia de riesgos de la organización recibe información sobre los riesgos de seguridad cibernética asociados a sus proveedores y a los productos y servicios que adquiere y utiliza. El personal actúa formalmente sobre esos riesgos a través de mecanismos como acuerdos escritos para comunicar los requisitos básicos, estructuras de gobernanza (por ejemplo, consejos de riesgos), y aplicación y supervisión de políticas. Estas acciones se aplican de forma coherente y conforme a lo previsto, y se supervisan y revisan continuamente.
Nivel 4: Adaptable	Existe un enfoque a nivel de toda la organización para gestionar los riesgos de seguridad cibernética que utiliza políticas, procesos y procedimientos basados en los riesgos para hacer frente a posibles eventos de seguridad cibernética. La relación entre los riesgos de seguridad cibernética y los objetivos de la organización se entiende claramente y se tiene en cuenta a la hora de tomar decisiones. Los directivos supervisan los riesgos de seguridad cibernética en el mismo contexto que los riesgos financieros y otros riesgos organizativos. El presupuesto de la organización se basa en la comprensión del entorno de riesgo actual y previsto y en la tolerancia al riesgo. Las unidades de negocio implementan la visión ejecutiva y analizan los riesgos a nivel de sistema en el contexto de las tolerancias de riesgo de la organización. La gestión de riesgos de seguridad cibernética forma parte de la cultura organizativa. Evoluciona a partir de la concienciación sobre las actividades	La organización adapta sus prácticas de seguridad cibernética basándose en actividades de seguridad cibernética anteriores y actuales, incluidas las lecciones aprendidas y los indicadores predictivos. A través de un proceso de mejora continua que incorpora tecnologías y prácticas avanzadas de seguridad cibernética, la organización se adapta activamente a un panorama tecnológico cambiante y responde de manera oportuna y eficaz a las amenazas sofisticadas en evolución. La organización utiliza información en tiempo real o casi real para comprender los riesgos de seguridad cibernética asociados a sus proveedores y a los productos y servicios que adquiere y utiliza, y actuar de forma coherente al respecto. La información sobre seguridad cibernética se comparte constantemente en toda la organización y con terceros autorizados.

Nivel	Gobernanza de riesgos de seguridad cibernética	Gestión de riesgos de seguridad cibernética
	previas y la concienciación continua sobre las actividades en los sistemas y redes de la organización. La organización puede tener en cuenta de forma rápida y eficaz los cambios en los objetivos de negocio/misión en la forma de abordar y comunicar el riesgo.	

Appendix C. Glosario

Categoría de CSF
Un grupo de resultados de seguridad cibernética relacionados que colectivamente comprenden una Función de CSF.

Perfil de Comunidad de CSF
Una línea base de resultados de CSF que se crea y publica para abordar intereses y objetivos compartidos entre un número de organizaciones. Un perfil comunitario se desarrolla normalmente para un sector, subsector, tecnología, tipo de amenaza u otro caso de uso en particular. Una organización puede utilizar un Perfil Comunitario como base para su propio Perfil Objetivo.

CSF Core
Una taxonomía de resultados de seguridad cibernética de alto nivel que puede ayudar a cualquier organización a gestionar sus riesgos de seguridad cibernética. Sus componentes son una jerarquía de Funciones, Categorías y Subcategorías que detallan cada resultado.

Perfil Actual del CSF
Una parte de un Perfil Organizativo que especifica los resultados esenciales que una organización está logrando actualmente (o intentando lograr) y determina cómo o en qué medida se está logrando cada resultado.

Función de CSF
El mayor nivel de la organización para los resultados de seguridad cibernética. Hay seis funciones de CSF: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.

Ejemplo de implementación de un CSF
Una ilustración resumida, orientada a la acción y teórica de una forma de ayudar a lograr un resultado básico del CSF.

Referencia informativa del CSF
Un mapeo que indica una relación entre un resultado básico del CSF y una norma, directriz, regulación u otro contenido existente.

Perfil organizativo del CSF
Un mecanismo para describir la postura de seguridad cibernética actual u objetivo de una organización en términos de los resultados del CSF Core.

Guía de inicio rápido del CSF
Recurso complementario que proporciona una guía breve y práctica sobre temas específicos relacionados con el CSF.

Subcategoría del CSF
Un grupo de resultados más específicos de actividades técnicas y de gestión de seguridad cibernética que comprenden una categoría del CSF.

Perfil Objetivo del CSF
Una parte de un Perfil Organizativo que especifica los resultados esenciales deseados que una organización ha seleccionado y priorizado para lograr sus objetivos de gestión de riesgos de seguridad cibernética.

Nivel del CSF
Una caracterización del rigor de las prácticas de gobierno y gestión de riesgos de seguridad cibernética de una organización. Hay cuatro niveles: Parcial (Nivel 1), Riesgo Informado (Nivel 2), Repetible (Nivel 3) y Adaptativo (Nivel 4).

En este documento se identifican determinados equipos, instrumentos, software o materiales, comerciales o no comerciales, con el fin de especificar adecuadamente el procedimiento experimental. Dicha identificación no implica una recomendación o aprobación de cualquier producto o servicio por parte del NIST, ni implica que los materiales o equipos identificados sean necesariamente los mejores disponibles para ese fin.

Políticas de la Serie Técnica del NIST
Declaraciones sobre derechos de autor, uso y licencias
Sintaxis del identificador de publicación de la serie técnica del NIST

Cómo hacer referencia a esta publicación de la serie técnica del NIST:
Instituto Nacional de Estándares y Tecnología (2024) El Marco de Seguridad Cibernética (CSF) 2.0 del NIST. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 spa. https://doi.org/10.6028/NIST.CSWP.29.spa

Información de contacto
cyberframework@nist.gov

Instituto Nacional de Estándares y Tecnología
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Todos los comentarios están sujetos a publicación en virtud de la Ley de Libertad de Información (FOIA, por sus siglas en inglés).