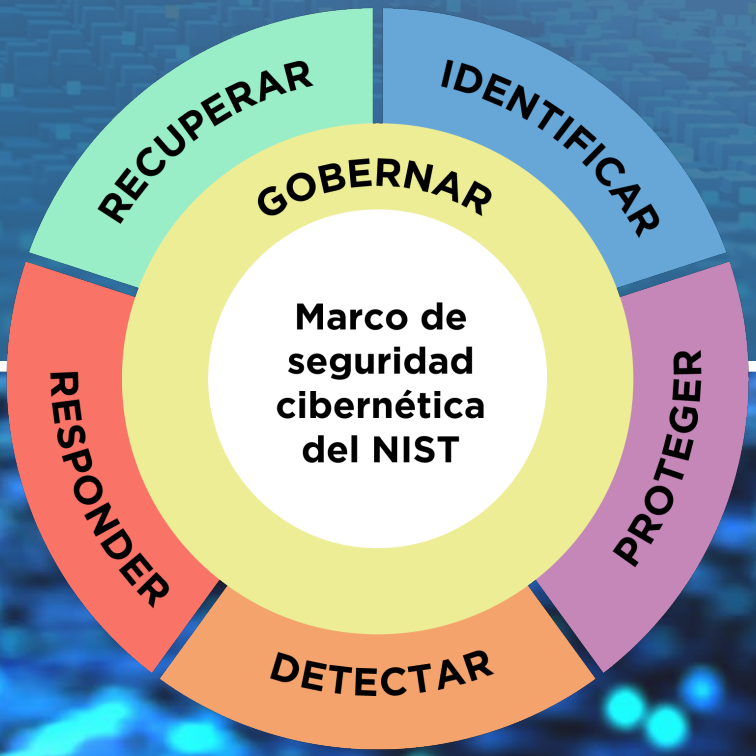
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0:
GUÍA DE RECURSOS Y DESCRIPCIÓN GENERAL



Publicación especial del NIST
NIST SP 1299 spa

https://doi.org/10.6028/NIST.SP.1299.spa
Febrero de 2024

NIST CSF 2.0:
GUÍA DE RECURSOS Y DESCRIPCIÓN GENERAL

¿QUÉ ES EL CSF 2.0... Y FORMAS POPULARES DE UTILIZARLO?

El Marco de seguridad cibernética (CSF) 2.0 del NIST puede ayudar a las organizaciones a gestionar y reducir sus riesgos de seguridad cibernética a medida que comienzan o mejoran su programa de seguridad cibernética. El CSF describe los resultados específicos que las organizaciones pueden lograr para abordar el riesgo. Otros recursos del NIST ayudan a explicar las acciones específicas que se pueden tomar para lograr cada resultado. *Esta guía es un complemento del CSF del NIST y no tiene como objetivo reemplazarlo.*

Las organizaciones pueden utilizar el CSF 2.0, junto con los recursos complementarios del NIST, para comprender, evaluar, priorizar y comunicar los riesgos de seguridad cibernética; es particularmente útil para fomentar la comunicación interna y externa entre equipos, así como para integrarse con estrategias de gestión de riesgos más amplias.

El CSF 2.0 está organizado por seis funciones - **Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.** En conjunto, estas funciones proporcionan una visión integral para gestionar el riesgo de seguridad cibernética. Esta *Guía de recursos y descripción general* ofrece detalles sobre cada función para servir como posibles puntos de partida.

El CSF 2.0 se compone de:

- **CSF principal** - una taxonomía de resultados de seguridad cibernética de alto nivel que puede ayudar a cualquier organización a gestionar sus riesgos de seguridad cibernética.
- **Perfiles organizativos del CSF -** un mecanismo para describir la postura de seguridad cibernética actual o futura de una organización en términos de los resultados del CSF principal.
- **Niveles del CSF** - se pueden aplicar a los perfiles organizativos del CSF para caracterizar el rigor de las prácticas de gestión y gobernanza de riesgos de Seguridad cibernética de una organización.

NIST CSF 2.0:
GUÍA DE RECURSOS Y DESCRIPCIÓN GENERAL

EXPLORAR MÁS RECURSOS DEL CSF 2.0

Referencias informativas	**Ver y crear asignaciones entre el CSF 2.0 y otros documentos.** ¿Desea enviar sus asignaciones a los documentos del NIST y que se muestren en nuestro sitio? Siga el enlace a la izquierda o envíe un correo electrónico a olir@nist.gov si tiene alguna pregunta.
Herramienta de referencia de privacidad y seguridad cibernética (CPRT)	Explore y descargue el contenido principal y mapeado de CSF 2.0. CPRT proporciona un mecanismo centralizado, estandarizado y modernizado para gestionar conjuntos de datos de referencia (y ofrece un formato consistente para acceder a los datos de referencia de varios estándares, pautas y marcos de Seguridad cibernética y privacidad del NIST).
Ejemplos de implementación	Vea y descargue ejemplos teóricos de pasos concisos y orientados a la acción para ayudar a lograr los resultados de las subcategorías de CSF 2.0, además de la orientación proporcionada en las Referencias informativas.
Herramienta de referencia de CSF 2.0	Acceda a versiones legibles por humanos y máquinas del contenido principal (en JSON y Excel). Asimismo puede ver y exportar partes del contenido principal utilizando términos de búsqueda clave.

Los recursos adicionales incluyen los siguientes:

Perfiles de la comunidad y plantillas de perfiles (ayudan a las organizaciones a poner en práctica el CSF)

Herramientas de búsqueda (simplifican y agilizan la búsqueda de información específica)

Documentos conceptuales (obtenga más información sobre los distintos temas del CSF)

Preguntas frecuentes (vea lo que otros están preguntando y obtenga respuestas a las preguntas más importantes)

Explore el conjunto de recursos del CSF 2.0 del NIST

NIST CSF 2.0:
GUÍA DE RECURSOS Y DESCRIPCIÓN GENERAL

NAVEGACIÓN POR LAS GUÍAS DE INICIO RÁPIDO (QSG) DEL CSF 2.0 DEL NIST

Tipo de QSG	Descripción	Explorar
Pequeñas empresas (PYMES)	Proporciona a las PYMES, específicamente a aquellas que tienen planes de seguridad cibernética poco elaborados o carecen de ellos, consideraciones para poner en marcha su estrategia de gestión de riesgos de seguridad cibernética.	Consulte la Guía de inicio rápido
Creación y uso de perfiles organizativos	Proporciona a todas las organizaciones consideraciones para crear y usar perfiles actuales o de destino para implementar el CSF 2.0.	Consulte la Guía de inicio rápido
Uso de los niveles del CSF	Explica cómo cualquier organización puede aplicar los niveles del CSF a los perfiles organizativos para caracterizar el rigor de sus prácticas de gestión y gobernanza de riesgos de seguridad cibernética.	Consulte la Guía de inicio rápido
Proyecto de gestión de riesgos de la cadena de suministro de seguridad cibernética (C-SCRM)	Ayuda a todas las organizaciones a convertirse en compradores y proveedores inteligentes de productos y servicios tecnológicos mediante la mejora de sus procesos de C-SCRM.	Consulte la Guía de inicio rápido
Borrador de la gestión de riesgos empresariales (ERM, por sus siglas en inglés) para profesionales	Detalla cómo los profesionales de la gestión de riesgos empresariales pueden utilizar los resultados proporcionados en CSF 2.0 para mejorar la gestión de riesgos de seguridad cibernética organizativa.	Consulte la Guía de inicio rápido

...y más que surgirán en el futuro.

Consulte el repositorio QSG en línea actual

NIST CSF 2.0: GUÍA DE RECURSOS Y DESCRIPCIÓN GENERAL

GOBERNAR

Se establecen, comunican y monitorean la estrategia, las expectativas y la política de gestión de riesgos de seguridad cibernética de la organización.

Comprenda y evalúe las necesidades específicas de seguridad cibernética. Determine los riesgos y las necesidades únicos de su organización. Discuta el entorno de riesgo actual y previsto y la cantidad de riesgo que su organización está dispuesta a aceptar. Busque aportes e ideas de toda la organización. Comprenda qué ha funcionado o no ha funcionado bien en el pasado y coméntelo abiertamente.

Desarrolle una estrategia de riesgo de seguridad cibernética personalizada. Esto debe basarse en los objetivos de seguridad cibernética específicos de su organización, el entorno de riesgo y las lecciones aprendidas del pasado y de otros. Gestione, actualice y analice la estrategia a intervalos regulares. Los roles y las responsabilidades deben ser claros.

Establezca políticas de gestión de riesgos definidas. Las políticas deben ser aprobadas por la gerencia y deben ser para toda la organización, repetibles y recurrentes, y deben alinearse con el entorno de amenazas de seguridad cibernética actual, los riesgos (que cambiarán con el tiempo) y los objetivos de la misión. Incorpore políticas en la cultura de la empresa para ayudar a impulsar e inspirar la capacidad de tomar decisiones informadas. Tenga en cuenta las obligaciones legales, regulatorias y contractuales.

Desarrolle y comunique prácticas de seguridad cibernética organizativa. Estas deben ser sencillas y comunicarse regularmente. Deben reflejar la aplicación de la gestión de riesgos a los cambios en la misión o los requisitos comerciales, las amenazas y el panorama técnico general. Documente las prácticas y compártalas con espacio para la retroalimentación y la agilidad para cambiar el rumbo.

Establezca y monitoree la gestión de riesgos de la cadena de suministro de seguridad cibernética. Establezca una estrategia, una política y roles y responsabilidades, incluida la supervisión de proveedores, clientes y colaboradores. Incorpore requisitos en los contratos. Involucre a los colaboradores y proveedores en la planificación, la respuesta y la recuperación.

Implemente una supervisión y puntos de control continuos. Analice los riesgos a intervalos regulares y monitoréelos continuamente (tal como lo haría con los riesgos financieros).

IDENTIFICAR

Se comprenden los riesgos de seguridad cibernética actuales de la organización.

Identifique los procesos y activos comerciales críticos. Considere cuáles de las actividades de su organización deben seguir siendo viables. Por ejemplo, esto podría ser mantener un sitio web para recuperar pagos, proteger de forma segura la información de los clientes/pacientes o garantizar que la información crítica para su organización siga siendo accesible y precisa.

Mantenga inventarios de hardware, software, servicios y sistemas. Conozca qué computadoras y software utiliza su organización -incluidos los servicios prestados por los proveedores- porque con frecuencia son los puntos de entrada de los actores maliciosos. Este inventario podría ser tan simple como una hoja de cálculo. Considere incluir dispositivos y aplicaciones propios, alquilados y personales de los empleados.

Documente los flujos de información. Considere qué tipo de información recopila y usa su organización (y dónde se encuentran los datos y cómo se usan), especialmente cuando existen contratos y colaboradores externos involucrados.

Identifique amenazas, vulnerabilidades y riesgos para los activos. Basándose en el conocimiento de las amenazas internas y externas, los riesgos deben ser identificados, evaluados y documentados. Algunos ejemplos de formas de documentarlos incluyen registros de riesgos: repositorios de información sobre riesgos, incluidos datos sobre los riesgos con el paso del tiempo. Asegúrese de que se identifiquen, prioricen y ejecuten las respuestas a los riesgos, y de que se controlen los resultados.

Las lecciones aprendidas se utilizan para identificar mejoras. Al realizar las operaciones comerciales diarias, es importante identificar formas de refinar o mejorar aún más el rendimiento, incluidas las oportunidades para administrar y reducir mejor los riesgos de seguridad cibernética. Esto requiere un esfuerzo deliberado por parte de su organización a todos los niveles. Si hay un incidente, evalúe lo que sucedió. Prepare un informe posterior a la acción que documente el incidente, la respuesta, las acciones de recuperación tomadas y las lecciones aprendidas.

CSF 2.0 DEL NIST: GUÍA DE RECURSOS Y DESCRIPCIÓN GENERAL

PROTEGER

Se utilizan salvaguardas para gestionar los riesgos de seguridad cibernética de la organización.

Gestionar el acceso. Crear cuentas únicas para los empleados y asegurarse de que los usuarios solo tengan acceso a los recursos necesarios. Autenticar a los usuarios antes de que se les conceda acceso a la información, las computadoras y las aplicaciones. Gestionar y hacer un seguimiento del acceso físico a las instalaciones o los dispositivos.

Capacitar a los usuarios. Capacitar periódicamente a los empleados para asegurarse de que conocen las políticas y procedimientos de seguridad cibernética y de que tienen los conocimientos y habilidades para realizar tareas generales y específicas; explicar cómo reconocer los ataques comunes e informar sobre actividades sospechosas. Determinadas funciones pueden requerir capacitación adicional.

Proteger y supervisar los dispositivos. Considerar la posibilidad de utilizar productos de seguridad de puntos finales. Aplicar configuraciones uniformes a los dispositivos y controlar los cambios en las configuraciones de los dispositivos. Deshabilitar los servicios o las funciones que no admitan las funciones de la misión. Configurar los sistemas y los servicios para generar registros. Asegurarse de que los dispositivos se eliminen de forma segura.

Proteger los datos confidenciales. Asegurarse de que los datos confidenciales almacenados o transmitidos estén protegidos mediante cifrado. Considerar la posibilidad de utilizar la comprobación de integridad para que solo se realicen cambios aprobados en los datos. Eliminar o destruir de forma segura los datos cuando ya no sean necesarios o requeridos.

Gestionar y mantener el software. Actualizar periódicamente los sistemas operativos y las aplicaciones; activar las actualizaciones automáticas. Sustituir el software obsoleto por versiones compatibles. Considerar el uso de herramientas de software para escanear los dispositivos en busca de vulnerabilidades adicionales y remediarlas.

Realizar copias de seguridad periódicas. Realizar copias de seguridad de los datos de acuerdo con los cronogramas acordados o utilizar las capacidades de copia de seguridad integradas; las soluciones de software y en la nube pueden automatizar este proceso. Mantener al menos un conjunto de datos respaldados con frecuencia fuera de línea para protegerlo contra el ransomware. Realizar pruebas para garantizar que los datos respaldados se puedan restaurar correctamente en los sistemas.

DETECTAR

Se detectan y analizan posibles ataques y vulneraciones de seguridad cibernética.

Monitorear las redes, los sistemas y las instalaciones de forma continua para encontrar eventos potencialmente adversos. Desarrollar y probar procesos y procedimientos para detectar indicadores de un incidente de Ssguridad cibernética en la red y en el entorno físico. Recopilar información de registros de diversas fuentes organizativas para ayudar a detectar actividades no autorizadas.

Determinar y analizar el impacto estimado y el alcance de los eventos adversos. Si se detecta un evento de seguridad cibernética, su organización debe trabajar de manera rápida y exhaustiva para comprender el impacto del incidente. Comprender los detalles sobre los incidentes de seguridad cibernética ayudará a informar la respuesta.

Brindar información sobre eventos adversos al personal y las herramientas autorizados. Cuando se detecten eventos adversos, brinde información sobre el evento internamente al personal autorizado para garantizar que se tomen las medidas de respuesta a incidentes adecuadas.

CSF DEL NIST 2.0: GUÍA DE RECURSOS Y DESCRIPCIÓN GENERAL

RESPONDER

Se toman medidas con respecto a un incidente de seguridad cibernética detectado.

Ejecute un plan de respuesta a incidentes una vez que se declare un incidente, en coordinación con terceros relevantes.
Con el fin de ejecutar correctamente un plan de respuesta a incidentes, asegúrese de que todos conocen sus responsabilidades; esto incluye comprender cualquier requisito (p. ej., reglamentario, de notificación legal y de intercambio de información).

Categorizar y priorizar los incidentes y escalarlos o elevarlos según sea necesario. Analizar lo que ha estado ocurriendo, determinar la causa raíz del incidente y priorizar qué incidentes requieren primero la atención de su organización. Comunique esta priorización a su equipo y asegúrese de que todos entienden a quién debe comunicarse la información relativa a un incidente priorizado cuando se produzca.

Recopilar datos de incidentes y preservar su integridad y procedencia. Recopilar información de manera segura ayudará a su organización en la respuesta a un incidente. Asegúrese de que los datos sigan estando seguros después del incidente para mantener la reputación de su organización y la confianza de las partes interesadas. Almacenar esta información de manera segura también puede ayudar a informar los planes de respuesta actualizados y futuros para que sean aún más efectivos.

Notifique a las partes interesadas internas y externas sobre cualquier incidente y comparta la información del incidente con ellas, siguiendo las políticas establecidas por su organización. Comparta información de manera segura de acuerdo con los planes de respuesta y los acuerdos de intercambio de información. Notifique a los colaboradores comerciales y clientes sobre incidentes de acuerdo con los requisitos contractuales.

Contener y erradicar incidentes. Ejecutar un plan de respuesta desarrollado y probado ayudará a su organización a contener los efectos de un incidente y erradicarlo. Una coordinación y comunicación significativas con las partes interesadas pueden dar como resultado una respuesta y mitigación del incidente más efectivas.

RESTAURAR

Se restauran los activos y las operaciones afectados por un incidente de seguridad cibernética.

Comprender los roles y las responsabilidades.
Comprenda quién, dentro y fuera de su empresa, tiene responsabilidades de recuperación. Sepa quién tiene acceso y autoridad para tomar decisiones para llevar a cabo sus esfuerzos de respuesta en nombre de la empresa.

Ejecute su plan de recuperación. Garantice la disponibilidad operativa de los sistemas y servicios afectados, y priorice y realice las tareas de recuperación.

Vuelva a comprobar su trabajo. Es importante garantizar la integridad de las copias de seguridad y otros activos de recuperación antes de emplearlos para reanudar las operaciones habituales de la empresa.

Comuníquese con las partes interesadas internas y externas. Tenga en cuenta cuidadosamente qué información se compartirá con las distintas partes interesadas, cómo y cuándo, de modo que todas ellas reciban la información que necesitan, pero no se comparta información inapropiada. Comunique a su personal las lecciones aprendidas y las revisiones de procesos, procedimientos y tecnologías (de acuerdo con las políticas ya establecidas por la organización). Este es un buen momento para capacitar, o reciclar, al personal en las mejores prácticas de seguridad cibernética.

Departamento de Comercio de EE.UU.
Gina M. Raimondo, Secretaria

Instituto Nacional de Estándares y Tecnología
Laurie E. Locascio, Directora del NIST y Subsecretaria de Comercio para Estándares y Tecnología