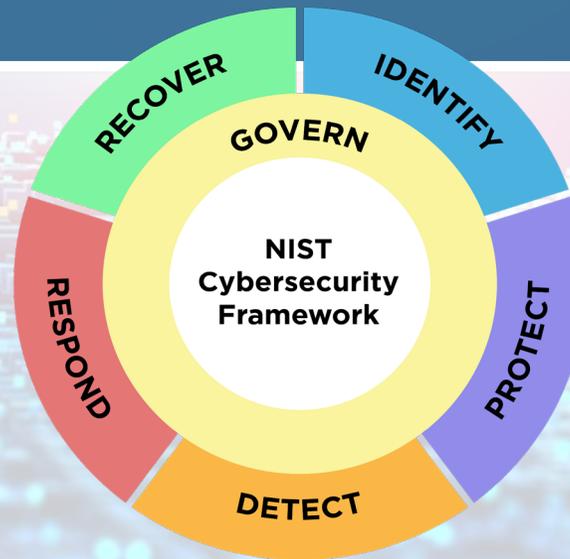




NIST Cybersecurity Framework 2.0: Guía de inicio rápido para pequeñas empresas



U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Publicación especial del NIST
NIST SP 1300
<https://doi.org/10.6028/NIST.SP.1300.spa>
Febrero de 2024

Marco de Seguridad Cibernética 2.0 del NIST: Guía de inicio rápido para pequeñas empresas

Finalidad

Esta guía proporciona a las pequeñas y medianas empresas (PYME), específicamente a aquellas que tienen planes de seguridad cibernética modestos o inexistentes, consideraciones para iniciar su estrategia de gestión de riesgos de seguridad cibernética utilizando el Marco de Seguridad Cibernética (CSF) 2.0 del NIST.

La guía también puede ayudar a otras organizaciones relativamente pequeñas, como organizaciones sin fines de lucro, agencias gubernamentales y escuelas. Es un suplemento al CSF del NIST y no pretende sustituirlo.

¿Qué es el Marco de seguridad cibernética del NIST?

El Marco de seguridad cibernética del NIST es una guía voluntaria que ayuda a las organizaciones -independientemente de su tamaño, sector o madurez- a **comprender, evaluar, priorizar y comunicar** mejor sus esfuerzos de seguridad cibernética.

El Marco no es un enfoque único para la gestión de los riesgos de seguridad cibernética.

Este suplemento y el CSF 2.0 completo pueden ayudar a organizaciones a considerar y registrar sus propias tolerancias de riesgo, prioridades, amenazas, vulnerabilidades, requisitos, etc.

Introducción al Marco de Seguridad Cibernética

El CSF organiza los resultados de la seguridad cibernética en seis funciones de alto nivel: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. Estas funciones, consideradas de forma conjunta, proporcionan una visión global de la gestión de los riesgos de seguridad cibernética. Las actividades enumeradas para cada función en esta guía pueden ofrecer un buen punto inicial para su empresa. Para obtener ejemplos específicos y orientados a la acción acerca de cómo lograr las actividades enumeradas, consulte los [Ejemplos de implementación del CSF 2.0](#). Si existen actividades contenidas en esta guía que no comprende o no se siente cómodo abordando por sí mismo, esta guía puede servirle como una guía de discusión con quien haya elegido para ayudarle a reducir sus riesgos de seguridad cibernética, como un proveedor de servicios de seguridad gestionada (MSSP).



EXPLORE MÁS RECURSOS DEL
MARCO DE SEGURIDAD
CIBERNÉTICA 2.0

nist.gov/cyberframework

Encuentre rápidamente
lo que necesita, entre
otros:

- ✓ Un conjunto de NUEVAS guías de inicio rápido
 - ✓ Ejemplos de implementación
 - ✓ Herramientas de búsqueda
- ✓ Preguntas frecuentes
 - ✓ ¡Y mucho más!

GOBERNAR



La función Gobernar le ayuda a establecer y monitorear la estrategia, las expectativas y la política de gestión de riesgos de seguridad cibernética de su empresa.

Acciones que deben considerarse

Entender

- Comprenda cómo los riesgos de seguridad cibernética pueden interrumpir el cumplimiento de la misión de su empresa. (GV.OC-01)
- Comprenda sus requisitos legales, normativos y contractuales en materia de seguridad cibernética. (GV.OC-03)
- Comprenda quién dentro de su empresa será responsable de elaborar y ejecutar la estrategia de seguridad cibernética. (GV.RR-02)

Evaluar

- Evaluar el impacto potencial de una pérdida total o parcial de los activos y operaciones críticos de la empresa. (GV.OC-04)
- Evalúe si un seguro de seguridad cibernética es adecuado para su empresa. (GV.RM-04)
- Evalúe los riesgos de seguridad cibernética que plantean los proveedores y otros terceros antes de entablar relaciones formales. (GV.SC-06)

Establezca prioridades

- Dé prioridad a la gestión de los riesgos de seguridad cibernética junto con otros riesgos empresariales.

Comunicar

- Comunique el apoyo de la dirección a una cultura consciente de los riesgos, ética y de mejora continua. (GV.RR-01)
- Comunique, aplique y mantenga políticas para gestionar los riesgos de seguridad cibernética. (GV.PO-01)
- Establecimiento del contexto organizativo

Introducción a la gobernanza de la seguridad cibernética

Puede utilizar estas tablas para empezar a pensar en su estrategia de gobernanza de la seguridad cibernética.

Establecimiento del contexto organizativo	
Nuestra misión empresarial:	
¿Qué riesgos de seguridad cibernética pueden impedirnos lograr esta misión?	

Documentación de los requisitos de seguridad cibernética	
Enumere sus requisitos legales:	
Enumere sus requisitos normativos:	
Enumere sus requisitos contractuales:	

Profundización técnica: [Escenificación de los riesgos de seguridad cibernética para la gestión del riesgo empresarial y la supervisión de la gobernanza](#)

Preguntas que debe plantearse

A medida que crece nuestra empresa, ¿con qué frecuencia revisamos nuestra estrategia de seguridad cibernética?

- ¿Necesitamos mejorar las competencias de nuestro personal actual, contratar talentos o contratar a un colaborador externo que nos ayude a establecer y gestionar nuestro plan de seguridad cibernética?
- ¿Disponemos de políticas de uso aceptable para la empresa y para los dispositivos propiedad de los empleados que acceden a los recursos de la empresa? ¿Se ha informado a los empleados sobre estas políticas?

Recursos relacionados

- [Manual de recursos para proteger las cadenas de suministro pequeñas y medianas](#)
- [Elección de un vendedor/proveedor de servicios](#)

[Ver todos los recursos NIST CSF 2.0 aquí](#)

IDENTIFICAR



La función Identificar le ayuda a determinar el riesgo actual de seguridad cibernética para la empresa.

Acciones que deben considerarse

Entender

- Comprenda en qué activos confía su empresa creando y manteniendo un inventario de hardware, software, sistemas y servicios. *(ID.AM-01/02/04)*

Evaluar

- Evalúe sus activos (informáticos y físicos) en busca de posibles vulnerabilidades. *(ID.RA-01)*
- Evalúe la eficacia del programa de seguridad cibernética de la empresa para identificar las áreas que necesitan mejoras. *(ID.IM-01)*

Establezca prioridades

- Priorice el inventario y la clasificación de sus datos empresariales. *(ID.AM-07)*
- Priorice la documentación de las amenazas internas y externas a la seguridad cibernética y las respuestas asociadas mediante un registro de riesgos. *(ID.RA)*

Comunicar

- Comunique los planes, las políticas y las mejores prácticas de seguridad cibernética a todo el personal y a los terceros pertinentes. *(ID.IM-04)*
- Comunique al personal la importancia de identificar las mejoras necesarias en los procesos, procedimientos y actividades de gestión de riesgos de seguridad cibernética. *(ID.IM)*

Cómo empezar a identificar el riesgo actual de seguridad cibernética para su empresa

Antes de que pueda proteger sus activos, necesita identificarlos. Entonces puede determinar el nivel apropiado de protección para cada activo basado en su sensibilidad y criticidad para la misión de su negocio. Puede utilizar esta tabla de muestra para empezar a realizar su inventario de activos de tecnología de la información (TI). A medida que su empresa vaya madurando, puede plantearse utilizar una solución automatizada de inventario de activos o un proveedor de servicios de seguridad gestionada que le ayude a gestionar todos sus activos empresariales.

Software/hardware/sistema/servicio	Uso oficial del activo	Administrador o propietario del activo:	Identifique los datos sensibles a los que tiene acceso el activo:	¿Se requiere autenticación de múltiples factores para acceder a este activo?	Riesgo para la empresa si perdemos el acceso a este activo

Profundización técnica: [Integración de la seguridad cibernética y la gestión de riesgos empresariales](#)

Preguntas que debe plantearse

- ¿Cuáles son nuestros activos empresariales más críticos (datos, hardware, software, sistemas, instalaciones, servicios, personas, etc.) que necesitamos proteger?
- ¿Cuáles son los riesgos de seguridad cibernética y privacidad asociados con cada activo?
- ¿Qué tecnologías o servicios utiliza el personal para realizar su trabajo? ¿Estos servicios o tecnologías son seguros y están aprobados para su uso?

Recursos relacionados

- [Plantilla de registro de riesgos del NIST](#)
- [Haga un inventario. Sepa qué información sensible tiene](#)
- [Evalúe su resiliencia operativa y sus prácticas de seguridad cibernética](#)

[Ver todos los recursos NIST CSF 2.0 aquí](#)

PROTEGER



La función Proteger apoya su capacidad de utilizar salvaguardas para prevenir o reducir los riesgos de seguridad cibernética.

Acciones que deben considerarse

Entender

- Comprenda a qué información deben tener o tienen acceso los empleados. Restrinja el acceso a la información sensible sólo a aquellos empleados que la necesiten para realizar su trabajo. *(PR.AA-05)*

Evaluar

- Evalúe la puntualidad, la calidad y la frecuencia de la capacitación en materia de seguridad cibernética que imparte su empresa a los empleados. *(PR.AT-01/02)*

Establezca prioridades

- Dé prioridad al requisito de autenticación de múltiples factores en todas las cuentas que lo ofrezcan y considere el uso de gestores de contraseñas para ayudarle a usted y a su personal a generar y proteger contraseñas seguras. *(PR.AA-03)*
- Dé prioridad al cambio de las contraseñas predeterminadas del fabricante. *(PR.AA-01)*
- Priorice la actualización periódica y la aplicación de parches en el software y los sistemas operativos. Active las actualizaciones automáticas para recordarlas. *(PR.PS-02)*
- Dé prioridad a la realización periódica de copias de seguridad de sus datos y a la comprobación de las mismas. *(PR.DS-11)*
- Priorice la configuración de sus tabletas y portátiles para activar el cifrado de disco completo para proteger los datos. *(PR.DS-01)*

Comunicar

- Comunique a su personal cómo reconocer ataques comunes, informar sobre ataques o actividades sospechosas y realizar tareas básicas de higiene cibernética. *(PR.AT-01/02)*

Cómo empezar a proteger su empresa

Habilitar la autenticación de múltiples factores (MFA) es una de las formas más rápidas y económicas de proteger sus datos. Comience con las cuentas que pueden acceder a la información más sensible. Utilice esta lista de verificación para empezar, pero recuerde que su propia lista será más larga que ésta: :

Account	MFA habilitado (sí/no)
Cuenta(s) bancaria(s)	
Cuenta(s) contable(s) y fiscal(es)	
Cuenta(s) comercial(es)	
Cuentas de Google, Microsoft y/o ID de Apple	
Cuenta(s) de correo electrónico	
Gestor(es) de contraseñas	
Cuentas de sitios web	

Profundización técnica: [Directrices del NIST sobre identidad digital](#)

Preguntas que debe plantearse

- ¿Estamos restringiendo el acceso y los privilegios sólo a aquellos que lo necesitan? ¿Estamos eliminando el acceso cuando ya no lo necesitan?
- ¿Cómo estamos limpiando y destruyendo de forma segura los datos y los dispositivos de almacenamiento de datos cuando ya no son necesarios?
- ¿Poseen los empleados los conocimientos y habilidades necesarios para realizar su trabajo teniendo en cuenta la seguridad?

Recursos relacionados

- [Recursos de capacitación en seguridad cibernética](#)
- [Autenticación de múltiples factores](#)
- [Proteger su empresa del phishing](#)

[Ver todos los recursos del CSF del NIST 2.0 aquí](#)

DETECTAR



La función Detectar proporciona resultados que le ayudan a encontrar y analizar posibles ataques y compromisos de seguridad cibernética.

Acciones que deben considerarse

Entender

- Comprenda cómo identificar indicadores comunes de un incidente de seguridad cibernética. *(DE.CM)*

Evaluar

- Evalúe sus tecnologías informáticas y servicios externos en busca de desviaciones del comportamiento esperado o típico. *(DE.CM-06/09)*
- Evalúe su entorno físico en busca de signos de manipulación o actividad sospechosa. *(DE.CM-02)*

Establezca prioridades

- Dé prioridad a la instalación y el mantenimiento de software antivirus y antimalware en todos los dispositivos de la empresa, incluidos los servidores, las computadoras de escritorio y las portátiles. *(DE.CM-09)*
- Contrate a un proveedor de servicios para monitorear computadoras y redes en busca de actividad sospechosa si no cuenta con los recursos para hacerlo internamente. *(DE.CM)*

Comunicar

- Comuníquese con su respondedor de incidentes autorizado, como un MSSP, sobre los detalles pertinentes del incidente para ayudarlos a analizarlo y mitigarlo. *(DE.AE-06/07)*

Primeros pasos en la detección de incidentes

Algunos indicadores comunes de un incidente de seguridad cibernética son:

- Pérdida del acceso habitual a datos, aplicaciones o servicios
- Red inusualmente lenta
- Alertas de software antivirus cuando detecta que un host está infectado con malware
- Múltiples intentos fallidos de inicio de sesión
- Un administrador de correo electrónico observa muchos correos devueltos con contenido sospechoso
- Un administrador de red observa una desviación inusual de los flujos de tráfico de red típicos



Profundización técnica: [Guía de gestión de incidentes de seguridad informática del NIST](#)

Preguntas que debe plantearse

- ¿Los dispositivos que se utilizan para nuestro negocio, ya sean propiedad de la empresa o de los empleados, tienen instalado software antivirus?
- ¿Saben los empleados cómo detectar posibles ataques de seguridad cibernética y cómo denunciarlos?
- ¿Cómo monitorea nuestra empresa sus registros y alertas para detectar posibles incidentes cibernéticos?

Recursos relacionados

- [Protección y respuesta al ransomware](#)
- [Detección de una posible intrusión](#)
- [Recursos de capacitación en seguridad cibernética](#)

[Ver todos los recursos del CSF del NIST 2.0 aquí](#)

RESPONDER



La función Responder respalda su capacidad para tomar medidas en relación con un incidente de seguridad.

Acciones que deben considerarse

Entender

- Comprenda cuál es su plan de respuesta a incidentes y quién tiene autoridad y responsabilidad para implementar los diversos aspectos del plan. *(RS.MA-01)*

Evaluar

- Evalúe su capacidad para responder a un incidente de seguridad cibernética. *(RS.MA-01)*
- Evalúe el incidente para determinar su gravedad, lo sucedido y su causa raíz. *(RS.AN-03, RS.MA-03)*

Establezca prioridades

- Dé prioridad a la adopción de medidas para contener y erradicar el incidente a fin de evitar daños mayores. *(RS.MI)*

Comunicar

- Comunique un incidente de seguridad cibernética confirmado a todas las partes interesadas internas y externas (p. ej., clientes, socios comerciales, organismos encargados de hacer cumplir la ley, organismos reguladores) según lo exijan las leyes, las regulaciones, los contratos o las políticas. *(RS.CO-02/03)*

Cómo empezar con un plan de respuesta a incidentes

Antes de que ocurra un incidente, debe estar preparado con un plan de respuesta básico. Éste se personalizará en función de la empresa, pero debe incluir:

- ✓ **Un líder empresarial:** Alguien responsable de elaborar y mantener su plan de respuesta a incidentes.
- ✓ **A quién llamar:** Enumere todas las personas que pueden formar parte de sus esfuerzos de respuesta a incidentes.
- ✓ Incluya su información de contacto, responsabilidades y autoridad.
- ✓ **Qué/cuándo/cómo comunicar:** Enumere las responsabilidades de comunicación/información de su empresa según lo exijan las leyes, regulaciones, contratos o políticas.

Profundización técnica : [Guía de gestión de incidentes de seguridad informática del NIST](#)

Preguntas que debe plantearse

- ¿Tenemos un plan de respuesta a incidentes de seguridad cibernética? En caso afirmativo, ¿lo hemos practicado para ver si es viable?
- ¿Sabemos quiénes son las principales partes interesadas y responsables internos y externos que nos ayudarán en caso de que se confirme un incidente de seguridad cibernética?

Recursos relacionados

- [Conceptos básicos del plan de respuesta a incidentes](#)
- [Centro de Denuncias de Delitos en Internet del FBI](#)
- [Respuesta a la violación de datos: Guía para empresas](#)
- [Mejores prácticas de respuesta a las víctimas y notificación de ciberincidentes](#)

Contacto	Teléfono
Responsable de la empresa:	
Contacto técnico:	
Policía Estatal:	
Legal:	
Banco:	
Seguro:	

[Ver todos los recursos del CSF del NIST 2.0 aquí](#)

RECUPERAR



La función Recuperar implica actividades para restaurar los activos y las operaciones que se vieron afectados por un incidente de seguridad cibernética.

Acciones que deben considerarse

Entender

- Comprenda quién tiene responsabilidades de recuperación dentro y fuera de su empresa. *(RC.RP-01)*

Evaluar

- Evalúe lo ocurrido preparando un informe posterior a la acción -por su cuenta o en consulta con un proveedor/colaborador- que documente el incidente, las medidas de respuesta y recuperación adoptadas y las lecciones aprendidas. *(RC.RP-06)*
- Evalúe la integridad de los datos y activos de las copias de seguridad antes de utilizarlos para la restauración. *(RC.RP-03)*

Establezca prioridades

- Priorice las acciones de recuperación en función de las necesidades de la organización, los recursos y los activos afectados. *(RC.RP-02)*

Comunicar

- Comuníquese de forma regular y segura con las partes interesadas internas y externas. *(RC.CO)*
- Comunique y documente la finalización del incidente y la reanudación de las actividades normales. *(RC.RP-06)*

Cómo empezar con un manual de recuperación

Un libro de jugadas suele incluir los siguientes elementos críticos:

- ✓ Un conjunto de procesos formales de recuperación
- ✓ Documentación de la criticidad de los recursos organizativos (p. ej., personas, instalaciones, componentes técnicos, servicios externos).
- ✓ Documentación de los sistemas que procesan y almacenan información de la organización, en particular activos clave. Esto ayudará a establecer el orden de prioridad de la restauración.
- ✓ Una lista del personal responsable de definir y aplicar los planes de recuperación.
- ✓ Un plan integral de comunicaciones de recuperación

Profundización técnica: [Guía del NIST para la recuperación de eventos de seguridad cibernética](#)

Preguntas que debe plantearse

- ¿Qué lecciones hemos aprendido? ¿Cómo podemos minimizar las posibilidades de que vuelva a ocurrir un incidente de seguridad cibernética en el futuro?
- ¿Cuáles son nuestras obligaciones legales, normativas y contractuales para comunicar a las partes interesadas internas y externas un incidente de seguridad cibernética?
- ¿Cómo nos aseguramos de que las medidas de recuperación que estamos tomando no están creando nuevas vulnerabilidades en nuestro negocio?

Recursos relacionados

- [Recursos de capacitación en seguridad cibernética](#)
- [Creación de un plan informático de recuperación en caso de catástrofe](#)
- [Copia de seguridad y recuperación de recursos](#)

[Ver todos los recursos del NIST CSF 2.0 aquí](#)

Perfiles y recursos adicionales



Uso de Perfiles Organizativos para Implementar el Marco de Seguridad Cibernética

Un *Perfil Organizativo del CSF* describe la postura de seguridad cibernética actual y/u objetivo de una organización en términos de los resultados de seguridad cibernética del Núcleo del CSF. Cada Perfil Organizativo incluye uno o ambos de los siguientes:

1. Un **Perfil Actual** especifica los resultados deseados 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 que una organización ha seleccionado y priorizado para alcanzar sus objetivos de gestión de riesgos de seguridad cibernética.
 - También puede utilizar un **Perfil Comunitario** como base para su Perfil Objetivo. Un Perfil Comunitario es una línea base de resultados objetivo para un sector, tecnología, tipo de amenaza u otro caso de uso en particular.
 - También puede optar por utilizar los **niveles del CSF** de Seguridad como base para la creación de su perfil. Los niveles caracterizan el rigor actual u objetivo de las prácticas de una organización según la función o categoría del CSF. Para obtener más información sobre los niveles y su uso, consulte la [Guía de inicio rápido para el uso de los niveles del CSF](#).

Vea la [Guía de inicio rápido para crear perfiles y usar perfiles organizativos](#) para obtener información más detallada sobre cómo empezar a crear perfiles actuales y objetivo para su organización.

Recursos adicionales

[La Herramienta de Referencia del Marco de Seguridad Cibernética del NIST](#) permite que los usuarios exploren el Núcleo del CSF 2.0 completo en versiones legibles por humanos y máquinas (en JSON y Excel), a la vez que mantiene recursos con información para ayudarlo a lograr los resultados deseados, tales como:

- [Mapeo](#): Las referencias informativas son mapas que indican las relaciones entre el MCE 2.0 y diversos estándares, directrices, regulaciones y otros contenidos. Ayudan a informar sobre cómo una organización puede lograr los resultados del núcleo.
- [Los ejemplos de implementación](#) ilustran pasos concisos y orientados a la acción para guiar a las organizaciones en el logro de los resultados del CSF. Los ejemplos no son una lista exhaustiva de todas las acciones que podría tomar una organización, ni son una línea de base de las acciones requeridas; son un conjunto de ejemplos útiles para que las organizaciones piensen en pasos concretos.

[La Herramienta de Referencia de Seguridad Cibernética y Privacidad del NIST \(CPRT\)](#) proporciona una forma sencilla de acceder a los datos de referencia de diversos estándares, directrices y marcos de seguridad cibernética y privacidad del NIST, descargables en formatos comunes (XLSX y JSON).

[NIST SP 800-53](#) proporciona un catálogo de controles de seguridad y privacidad entre los que se puede elegir. Los controles son flexibles, personalizables y se implementan como parte de un proceso de toda la organización para gestionar el riesgo. [Ver y exportar](#) desde la Herramienta de Referencia de Seguridad Cibernética y Privacidad (CPRT).

[El Marco de la fuerza laboral para la seguridad cibernética \(NICE Framework\)](#) ayuda a los empleadores a lograr los resultados del CSF 2.0 ayudándolos a identificar brechas críticas en el personal y las capacidades de seguridad cibernética; determinar y comunicar las responsabilidades de los puestos y las descripciones de los mismos; y proporcionar capacitación al personal e itinerarios profesionales.