MARCO DE CIBERSEGURIDAD
2.0 NIST

Guía para gestionar y reducir los riesgos de ciberseguridad

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Marco general

El Marco de Ciberseguridad del NIST (CSF) es una guía diseñada para ayudar a organizaciones de todos los tamaños a gestionar y reducir los riesgos de ciberseguridad. Ofrece un enfoque flexible para entender, evaluar, priorizar y comunicar los esfuerzos en ciberseguridad, adaptable a las necesidades y recursos específicos de cada organización.

Objetivo de la guía

La guía de inicio rápido para pequeñas empresas fue creada específicamente para las PYMES que cuentan con planes acotados o nulos en ciberseguridad. Esta guía proporciona un punto de partida y un instrumento de gestión continua de riesgos de ciberseguridad.

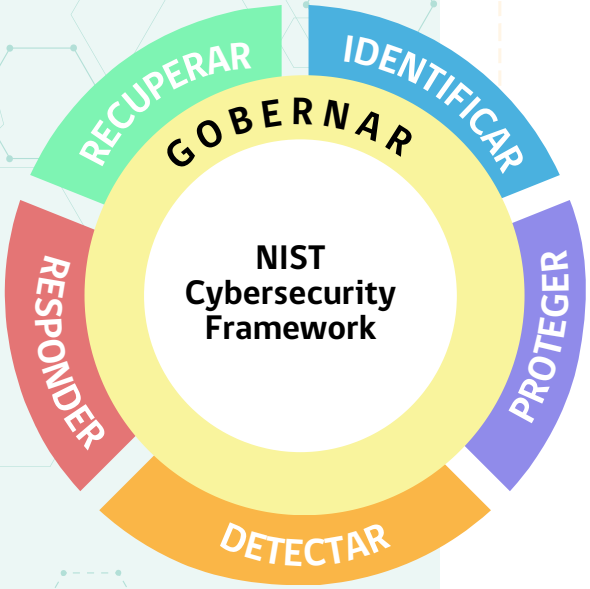
La publicación original está disponible aquí: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf

1 Organización

La guía está estructurada en torno a las 6 funciones del CSF: GOBERNAR, IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER y RECUPERAR. Cada función incluye:

ACCIONES A CONSIDERAR

Ofrece pasos para comprender, evaluar, priorizar y comunicar las iniciativas de ciberseguridad.



PRIMEROS PASOS

Esta sección incentiva a las empresas a reflexionar sobre cuestiones clave relacionadas con la gestión de riesgos de ciberseguridad, fomentando el diálogo interno o con proveedores de servicios de seguridad gestionada (MSSP).

PREGUNTAS PARA TENER EN CUENTA

Esta sección incentiva a las empresas a reflexionar sobre cuestiones clave relacionadas con la gestión de riesgos de ciberseguridad, fomentando el diálogo interno o con proveedores de servicios de seguridad gestionada (MSSP).

2 Síntesis por funciones

GOBERNAR

Ayuda a establecer y monitorear la estrategia, expectativas y políticas de gestión de riesgos de ciberseguridad del negocio.

Acciones	Definición (Identificador en el CSF 2.0)
Comprender	• Comprender cómo los riesgos de ciberseguridad pueden afectar el logro de la misión de tu negocio. (GV.OC-01) • Comprender los requisitos legales, regulatorios y contractuales de ciberseguridad. (GV.OC-03) • Comprender quién dentro de tu negocio será responsable de desarrollar y ejecutar la estrategia de ciberseguridad. (GV.RR-02)
Evaluar	• Evaluar el impacto potencial de la pérdida total o parcial de activos críticos del negocio y operaciones. (GV.0C-04) • Evaluar si el seguro de ciberseguridad es apropiado para tu negocio. (GV.RM-04) • Evaluar los riesgos de ciberseguridad que plantean los proveedores y otras terceras partes antes de establecer relaciones formales. (GV.SC-06)

Acciones	Definición (Identificador en el CSF 2.0)
Priorizar	Priorizar la gestión de riesgos de ciberseguridad junto con otros riesgos empresariales. (GV.RM-03)
Comunicar	Comunicar el apoyo del liderazgo a una cultura consciente de riesgos, ética y de mejora continua. (GV.RR-01)
	Comunicar, hacer cumplir y mantener políticas para la gestión de riesgos de ciberseguridad. (GV.PO-01)

Estrategia para comenzar la Gobernanza

Empieza planteando las siguientes preguntas en el contexto organizacional:

¿Cuál es nuestra declaración de misión empresarial?

¿Qué riesgos de ciberseguridad pueden impedirnos lograr esta misión?

Luego, puedes continuar enumerando los requisitos de ciberseguridad, como:

- Legales
- Regulatorios
- Contractuales

Otras preguntas para realizar un análisis y evaluación:

- ¿Con qué frecuencia revisamos nuestra estrategia de ciberseguridad?
- ¿Necesitamos mejorar las habilidades de nuestro personal actual, contratar talento o a un socio externo para establecer y gestionar nuestro plan de ciberseguridad?
- ¿Tenemos políticas de uso aceptable para los dispositivos empresariales y de uso personal con el que acceden a recursos empresariales? ¿Los trabajadores han sido educados sobre estas políticas?

IDENTIFICAR

Ayuda a determinar el riesgo actual de ciberseguridad para el negocio.

Acciones	Definición (Identificador en el CSF 2.0)
Comprender	• Comprender en qué activos depende tu negocio creando y manteniendo un inventario de hardware, software, sistemas y servicios. (ID.AM-01/02/04)
Evaluar	• Evaluar tus activos (TI y físicos) para identificar posibles vulnerabilidades. (ID.RA-01) • Evaluar la efectividad del programa de ciberseguridad del negocio para identificar áreas que necesitan mejoras. (ID.IM-01)
Priorizar	• Priorizar el inventario y la clasificación de los datos de tu negocio. (ID.AM-07) • Priorizar la documentación de amenazas de ciberseguridad internas y externas y las respuestas asociadas utilizando un registro de riesgos. (ID.RA)
Comunicar	• Comunicar los planes, políticas y mejores prácticas de ciberseguridad a todo el personal y terceros relevantes. (ID.IM-04) • Comunicar al personal la importancia de identificar mejoras necesarias en los procesos, procedimientos y actividades de gestión de riesgos de ciberseguridad. (ID.IM)

Identificar el riesgo de ciberseguridad del negocio

Antes de poder proteger tus activos, necesitas identificarlos y luego determinar el nivel adecuado de protección para cada uno, según su sensibilidad y criticidad.

Para realizar un inventario puedes considerar:

- Software/hardware/sistema/ servicios
- Uso oficial del activo
- Identificar los datos confidenciales a los que tiene acceso el activo.
- ¿Se requiere autenticación multifactorial para acceder a este activo?
- Riesgo para la empresa si perdemos el acceso a este activo.

Otras preguntas para realizar un análisis y evaluación:

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

PROTEGER

Ayuda a respaldar tu capacidad para usar salvaguardas que prevengan o reduzcan los riesgos de ciberseguridad.

Acciones	Definición (Identificador en el CSF 2.0)
Comprender	Comprender qué información los empleados deben o pueden acceder. Restringir el acceso a información sensible solo a aquellos empleados que lo necesiten para realizar su trabajo. (PR.AA-05)
Evaluar	Evaluar la puntualidad, calidad y frecuencia de la capacitación en ciberseguridad para los empleados de tu empresa. (PR.AT-01/02)
Priorizar	Priorizar el uso de autenticación multifactorial en todas las cuentas que lo ofrezcan y considerar el uso de administradores de contraseñas para ayudarte a ti y a tu personal a generar y proteger contraseñas seguras. (PR.AA-03)
	Priorizar el cambio de contraseñas predeterminadas de los fabricantes. (PR.AA-01)
	Priorizar la actualización y el parcheo regular de software y sistemas operativos, así como habilitar actualizaciones automáticas para ayudarte a recordarlo. (PR.PS-02)

Priorizar	Priorizar la realización de copias de seguridad regulares de tus datos y la prueba de esas copias de seguridad. (PR.DS-11) Priorizar la configuración de tus tablets y portátiles para habilitar el cifrado de disco completo y proteger los datos. (PR.DS-01)
Comunicar	Comunicar a tu personal cómo reconocer ataques comunes, informar sobre ataques o actividades sospechosas, y realizar tareas básicas de higiene cibernética. (PR.AT-01/02)

Estrategia para comenzar con la protección de tu negocio

Habilitar la autenticación multifactorial (MFA) es una forma rápida y económica de proteger tus datos. Comienza con cuentas que puedan acceder a la información más sensible, como por ejemplo:

- Cuentas bancarias
- Cuentas de contabilidad e impuestos.
- ID de cuentas de Google, Microsoft y/o Apple.
- Cuentas de correo electrónico.
- Administradores de contraseñas.
- Cuentas de sitios web.

Otras preguntas para realizar un análisis y evaluación:

- ¿Estamos restringiendo el acceso y los privilegios solo a aquellos que lo necesitan? ¿Estamos eliminando el acceso cuando ya no lo necesitan?
- ¿Los funcionarios tienen el conocimiento y las habilidades necesarias para realizar su trabajo con seguridad?

DETECTAR

Ayuda a proporcionar resultados para encontrar y analizar posibles ataques cibernéticos y compromisos de seguridad.

Acciones	Definición (Identificador en el CSF 2.0)
Comprender	Comprender cómo identificar los indicadores comunes de un incidente de ciberseguridad. (DE.CM)
Evaluar	Evaluar tus tecnologías informáticas y servicios externos para detectar desviaciones del comportamiento esperado o típico. (DE.CM-06/09)
	Evaluar tu entorno físico en busca de signos de manipulación o actividad sospechosa. (DE.CM-02)
Priorizar	Priorizar la instalación y mantenimiento de software antivirus y anti-malware en todos los dispositivos de la empresa, incluidos servidores, computadoras de escritorio y portátiles. (DE.CM-09)
	Priorizar la contratación de un proveedor de servicios para monitorear computadoras y redes en busca de actividad sospechosa si no tienes los recursos para hacerlo internamente. (DE.CM)

Comunicar

- Comunicarte con tu respondedor autorizado de incidentes, como un MSSP (Proveedor de Servicios de Seguridad Gestionada), sobre los detalles relevantes del incidente para ayudarles a analizarlo y mitigarlo. (DE.AE-06/07)

Indicadores comunes para detectar un incidentes

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

Otras preguntas para realizar un análisis y evaluación:

- ¿Tienen los dispositivos que se utilizan para nuestro negocio, ya sean propiedad de la empresa o de los empleados, software antivirus instalado?
- ¿Saben los empleados cómo detectar posibles ataques cibernéticos y cómo reportarlos?
- ¿Cómo está monitoreando nuestra empresa sus registros y alertas para detectar posibles incidentes cibernéticos?

RESPONDERR

Ayuda a respaldar su capacidad para tomar medidas en relación con un incidente de seguridad.

Acciones	Definición (Identificador en el CSF 2.0)
Comprender	Comprender 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	Evaluar tu capacidad para responder a un incidente de seguridad cibernética. (RS.MA-01) Evaluar el incidente para determinar su gravedad, lo sucedido y su causa raíz. (RS.AN-03, RS.MA-03)
Priorizar	Priorizar la adopción de medidas para contener y erradicar el incidente a fin de evitar daños mayores. (RS.MI)
Comunicar	Comunicar 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)

Un plan básico se personalizará según el negocio, pero al menos debe incluir:

- Un líder del negocio responsable de la ciberseguridad: Alguien que sea responsable de desarrollar y mantener tu plan de respuesta a incidentes.
- Un contacto a quién llamar: Enumera a todas las personas que pueden formar parte de tus esfuerzos de respuesta a incidentes. Incluye información de contacto, responsabilidades y cargo.
- Saber qué/cuándo/cómo reportar: Enumera las responsabilidades de comunicación/informe de tu empresa según lo exijan las leyes, regulaciones, contratos o políticas.

Otras preguntas para realizar un análisis y evaluación:

- ¿Tenemos un plan de respuesta a incidentes de ciberseguridad? Si es así, ¿lo hemos practicado para ver si es viable?
- ¿Sabemos quiénes son las partes interesadas y los responsables de la toma de decisiones clave, tanto internos como externos, que ayudarán si tenemos un incidente de ciberseguridad confirmado?

RECUPERAR

Involucra actividades para restaurar los activos y operaciones que fueron afectados por un incidente de ciberseguridad.

Acciones	Definición (Identificador en el CSF 2.0)
Comprender	Comprender quién dentro y fuera de la empresa tiene responsabilidades de recuperación. (RC.RP-01)
Evaluar	Evaluar lo que sucedió preparando un informe post-incidente—por tu cuenta o en consulta con un proveedor/socio—que documente el incidente, las acciones de respuesta y recuperación tomadas, y las lecciones aprendidas. (RC.RP-06) Evaluar la integridad de tus datos y activos respaldados antes de usarlos para la restauración. (RC.RP-03)
Priorizar	Priorizar tus acciones de recuperación basándote en las necesidades organizacionales, recursos y activos afectados. (RC.RP-02)
Comunicar	Comunicar regularmente y de manera segura con las partes interesadas internas y externas. (RC.CO) Comunicar y documentar la finalización del incidente y la reanudación de las actividades normales. (RC.RP-06)

¿Cómo empezar un playbook de recuperación?

El documento debe contener los siguientes elementos críticos:

- Procesos formales de recuperación.
- Documentación de la importancia de los recursos organizacionales (por ejemplo, personas, instalaciones, componentes técnicos, servicios externos)
- Documentación de los sistemas que procesan y almacenan la información organizacional, particularmente los activos clave. Esto ayudará a informar el orden de prioridad para la restauración.
- Una lista del equipo responsable de definir e implementar los planes de recuperación.
- Un plan de comunicación de recuperación integral.

Otras preguntas para realizar un análisis y evaluación:

- ¿Cuáles son nuestras lecciones aprendidas? ¿Cómo podemos minimizar las posibilidades de que ocurra un incidente de ciberseguridad en el futuro?
- ¿Cuáles son nuestras obligaciones legales, regulatorias y contractuales para comunicar a las partes interesadas internas y externas sobre un incidente de ciberseguridad?
- ¿Cómo aseguramos que los pasos de recuperación que adoptamos no introducen nuevas vulnerabilidades en nuestro negocio?

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

www.csirt.gob.cl

Noviembre 2024