RESUMEN DE NORMA · CERT.GT

NIST CSF 2.0 en español

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Gerencia y responsables de seguridad de organizaciones de cualquier tamaño.

El Marco de Ciberseguridad del NIST organiza todo lo que una organización hace para manejar su riesgo de ciberseguridad en seis funciones fáciles de explicar a la gerencia. Es gratuito, voluntario y no se certifica. La versión 2.0 se publicó en febrero de 2024 y ya no está pensada sólo para infraestructura crítica.

Las seis funciones

Gobernar (GV)	Establecer la estrategia, las expectativas y la política de gestión de riesgos. Es la función nueva y sostiene a las demás.
Identificar (ID)	Saber qué tienes: activos, datos, proveedores y los riesgos que enfrentan.
Proteger (PR)	Aplicar salvaguardas: accesos, capacitación, seguridad de datos y de plataformas.
Detectar (DE)	Encontrar y analizar posibles ataques y compromisos.
Responder (RS)	Actuar ante un incidente detectado: gestionarlo, analizarlo, comunicarlo y mitigarlo.
Recuperar (RC)	Restaurar los activos y operaciones afectados.

Cómo está organizado

- Seis funciones, 22 categorías y 106 subcategorías. Cada subcategoría es un resultado esperado, no una instrucción.
- Gobernar: contexto organizacional, estrategia de riesgos, roles y responsabilidades, política, supervisión y riesgo de la cadena de suministro.
- Identificar: gestión de activos, evaluación de riesgos y mejora.
- Proteger: identidad y control de acceso, concientización, seguridad de datos, seguridad de plataformas y resiliencia de la infraestructura.
- Detectar: monitoreo continuo y análisis de eventos adversos.
- Responder: gestión, análisis, comunicación y mitigación de incidentes.
- Recuperar: ejecución del plan de recuperación y comunicación.

Perfiles y niveles

- Perfil actual: qué resultados alcanzas hoy. Perfil objetivo: cuáles quieres alcanzar. La diferencia es tu plan de trabajo.
- Niveles (tiers) del 1 al 4 —parcial, informado por el riesgo, repetible y adaptativo— describen qué tan rigurosa es tu gestión del riesgo.
- Los niveles no son una calificación de madurez obligatoria: elige el que corresponda a tu riesgo y tu presupuesto.

Qué cambió frente a la versión 1.1

- Se agregó la función Gobernar, que lleva la ciberseguridad al nivel de la dirección.
- El alcance pasó de infraestructura crítica a todo tipo de organización.
- Mayor énfasis en la cadena de suministro.
- NIST publica ejemplos de implementación, guías de inicio rápido y referencias cruzadas con otros marcos.

Cómo empezar

- Usa la guía de inicio rápido para pequeñas empresas que publica NIST.
- Define el alcance: toda la organización o un servicio.
- Arma el perfil actual respondiendo, para cada categoría, si el resultado se cumple, se cumple en parte o no se cumple.
- Elige el perfil objetivo según tus riesgos principales, no según lo que hacen otros.
- Prioriza pocas brechas, asigna responsables y fechas, y repite el ejercicio cada año.

Cómo se relaciona con otras normas

- No compite con ISO 27001: el CSF da el lenguaje y las prioridades; ISO da el sistema de gestión certificable.
- Los CIS Controls sirven como lista concreta de acciones para cumplir las funciones Proteger y Detectar.
- NIST mantiene tablas de correspondencia con ISO 27001, CIS Controls y otros marcos.

Texto oficial

NIST Cybersecurity Framework 2.0 (NIST CSWP 29), gratuito en nist.gov/cyberframework.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Resumen elaborado por cert.gt con fines educativos; no es el texto oficial de la norma ni sustituye asesoría legal o de cumplimiento. No es un documento de una entidad gubernamental. Puedes copiarlo y adaptarlo citando la fuente (CC BY 4.0).