UNMSM
Fundación
SAN MARCOS
*Por el desarrollo de la Ciencia y la Cultura*

# DIPLOMADO DE ESPECIALIZACIÓN

# GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

## El Marco de la Seguridad Cibernética (CSF) 2.0 del NIST

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

# RESUMEN EJECUTIVO

## El Marco de Seguridad Cibernética (CSF) 2.0 del NIST

*Elaborado a partir de la versión oficial en español proporcionada como lectura.*

*El presente resumen sintetiza los principales planteamientos, estructura y utilidad práctica del NIST Cybersecurity Framework (CSF) 2.0. No pretende sustituir el documento original ni convertirlo en una lista de controles; busca facilitar su comprensión y servir como material de lectura ejecutiva.*

*National Institute of Standards and Technology. (2024). El Marco de Seguridad Cibernética (CSF) 2.0 del NIST (NIST Cybersecurity White Paper NIST CSWP 29 spa). Gaithersburg, MD: U.S. Department of Commerce. Publicado el 26 de febrero de 2024.*

## 1. Contexto, propósito y alcance del CSF 2.0

El Marco de Seguridad Cibernética (CSF) 2.0 del National Institute of Standards and Technology (NIST) constituye una referencia de alto nivel para gestionar los riesgos de seguridad cibernética. Su principal aporte no consiste en imponer una metodología única ni en definir un conjunto cerrado de controles técnicos, sino en proporcionar una estructura común para comprender, evaluar, priorizar y comunicar el riesgo. Esta orientación resulta especialmente relevante en organizaciones donde la ciberseguridad ya no puede tratarse como una responsabilidad exclusiva del área de tecnología.

El documento señala expresamente que el CSF 2.0 está dirigido a organizaciones de todos los tamaños y sectores, incluyendo industria, gobierno, academia y organizaciones sin fines de lucro. También reconoce que cada organización posee una combinación particular de amenazas, vulnerabilidades, objetivos, misión, recursos y tolerancia al riesgo. Por ello, el marco evita el enfoque de “talla única” y permite adaptar sus resultados al contexto de cada entidad.

Un aspecto importante es que la versión 2.0 amplía el enfoque respecto de versiones anteriores. La gobernanza adquiere una posición explícita y central, y la gestión de riesgos de la cadena de suministro recibe una atención específica. El marco también se concibe como aplicable a tecnologías y entornos diversos, incluyendo TI, IoT, tecnología operativa, servicios en la nube, dispositivos móviles e inteligencia artificial.

Desde una perspectiva ejecutiva, la idea central puede resumirse así: una organización no mejora su seguridad simplemente acumulando herramientas. Primero debe comprender qué debe proteger, por qué es importante, qué riesgos enfrenta, qué resultados necesita alcanzar y cómo esos resultados se relacionan con su misión. El CSF ofrece el lenguaje y la estructura para ordenar esa conversación.

El CSF es, además, voluntario como marco fundamental, aunque puede ser incorporado a políticas o mandatos gubernamentales. El NIST recomienda utilizarlo junto con otros marcos, normas, directrices y prácticas. Por tanto, su valor aumenta cuando funciona

como una capa de integración entre gobierno, gestión de riesgos y ejecución técnica.

En términos de gestión, el CSF permite pasar de una visión fragmentada de la ciberseguridad a una visión basada en riesgo. El objetivo no es demostrar que todos los controles existen, sino determinar si la organización está alcanzando los resultados de seguridad que necesita y si sus inversiones responden a sus prioridades reales.

## 2. La arquitectura del CSF: Core, Perfiles y Niveles

El CSF 2.0 se articula alrededor de tres componentes principales: el CSF Core, los Perfiles Organizativos y los Niveles del CSF. Estos elementos cumplen funciones diferentes, pero se complementan para construir una visión práctica de la postura de seguridad cibernética.

### CSF Core

El Core es una taxonomía de resultados de seguridad cibernética de alto nivel. Su estructura se organiza en Funciones, Categorías y Subcategorías. Es importante comprender que estos resultados no constituyen una lista de verificación de acciones obligatorias. El NIST deja margen para que cada organización determine cómo alcanzar los resultados según su contexto y caso de uso.

La estructura superior está conformada por seis Funciones: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar. La organización de estas funciones no representa una secuencia rígida. El propio documento explica que deben abordarse de manera simultánea y que las actividades de gobierno, identificación, protección y detección deben mantenerse continuamente, mientras que las capacidades de respuesta y recuperación deben estar preparadas para actuar cuando ocurran incidentes.

### Perfiles Organizativos

Los Perfiles permiten describir la postura actual y la postura objetivo de una organización utilizando los resultados del Core. El Perfil Actual muestra qué resultados se están logrando y en qué medida; el Perfil

Objetivo recoge los resultados que la organización ha seleccionado y priorizado para alcanzar sus objetivos de gestión del riesgo.

La comparación entre ambos perfiles permite visualizar brechas y convertirlas en acciones. Este enfoque evita que la planificación de ciberseguridad se limite a declaraciones generales. La organización puede identificar qué necesita cambiar, por qué debe hacerlo, qué prioridad tiene y cómo comprobará el avance.

### Niveles

Los Niveles caracterizan el rigor de las prácticas de gobierno y gestión del riesgo. El CSF reconoce cuatro: Nivel 1, Parcial; Nivel 2, Informado sobre el Riesgo; Nivel 3, Repetible; y Nivel 4, Adaptativo. No se presentan como una certificación ni como una obligación de llegar siempre al nivel máximo. Deben utilizarse como contexto para comprender la forma en que una organización gestiona sus riesgos.

## 3. Gobernar: el cambio más relevante del CSF 2.0

La incorporación explícita de la función Gobernar representa uno de los cambios conceptuales más significativos del CSF 2.0. La ciberseguridad deja de aparecer únicamente como un conjunto de actividades operativas y pasa a formar parte visible de la gestión estratégica del riesgo.

Gobernar comprende el establecimiento, comunicación y supervisión de la estrategia, las expectativas y las políticas de gestión del riesgo de seguridad cibernética. El NIST vincula esta función con el contexto organizativo, la estrategia de riesgo, las funciones y responsabilidades, las políticas, la supervisión y la gestión del riesgo de la cadena de suministro.

El contexto organizativo obliga a considerar la misión, las expectativas de las partes interesadas, las dependencias y los requisitos legales, regulatorios y contractuales. En la práctica, esto significa que una decisión de seguridad debe entenderse en función de lo que la organización necesita cumplir y proteger, y no solamente en función de las capacidades de una herramienta tecnológica.

La estrategia de gestión de riesgos incorpora prioridades, restricciones, apetito y tolerancia al riesgo. Esta dimensión es

particularmente importante para la alta dirección porque permite discutir cuánto riesgo está dispuesta a aceptar la organización y qué riesgos requieren tratamiento prioritario.

El CSF también establece que las funciones, responsabilidades y autoridades deben ser claras. El liderazgo organizacional debe asumir responsabilidad por los riesgos de ciberseguridad, promover una cultura consciente del riesgo y asegurar recursos adecuados. La seguridad cibernética debe, además, incorporarse a determinadas prácticas de recursos humanos.

La política debe mantenerse alineada con los cambios en requisitos, amenazas, tecnología y misión. La supervisión, por su parte, utiliza los resultados y el desempeño de la gestión del riesgo para ajustar la estrategia.

### La cadena de suministro como responsabilidad de gobierno

La categoría GV.SC incorpora la gestión de riesgos de la cadena de suministro cibernética. El marco propone conocer y priorizar proveedores por criticidad, establecer requisitos en contratos, realizar diligencia debida antes de iniciar relaciones, monitorear riesgos durante la relación y considerar a proveedores y terceros en la planificación, respuesta y recuperación de incidentes.

La lectura ejecutiva es clara: la superficie de riesgo de una organización no termina en sus propios sistemas. Los servicios, proveedores, desarrolladores, integradores y terceros forman parte del ecosistema que debe ser gobernado.

## 4. Identificar: conocer antes de decidir

La función Identificar tiene como finalidad conocer los riesgos actuales de seguridad cibernética. Para ello, el CSF coloca en primer plano los activos, los proveedores, las vulnerabilidades, las amenazas y los posibles impactos. La lógica es sencilla: una organización difícilmente puede priorizar adecuadamente aquello que desconoce.

## Gestión de activos

El CSF plantea mantener inventarios de hardware, software, servicios y sistemas; representaciones de las comunicaciones y flujos de datos; inventarios de servicios proporcionados por terceros; clasificación y priorización de activos; inventarios de datos y gestión de activos durante todo su ciclo de vida.

No se trata únicamente de contar equipos. El enfoque incorpora datos, servicios, personas, sistemas y dependencias. La prioridad debe relacionarse con la criticidad y con el impacto que una interrupción, alteración o pérdida podría producir sobre la misión.

## Evaluación del riesgo

La organización debe identificar, validar y registrar vulnerabilidades; recibir información sobre amenazas; identificar amenazas internas y externas; estimar probabilidades e impactos; y utilizar esa información para comprender el riesgo inherente y priorizar respuestas.

El CSF también contempla la gestión de cambios y excepciones, la recepción y tratamiento de divulgaciones de vulnerabilidades, la evaluación de autenticidad e integridad del hardware y software antes de su adquisición y la evaluación de proveedores críticos.

## Mejora

La mejora es transversal. El marco reconoce que las oportunidades de mejora pueden surgir de evaluaciones, pruebas y ejercicios, actividades operativas y procesos de respuesta a incidentes. Los planes de respuesta y otros planes de seguridad deben establecerse, comunicarse, mantenerse y mejorarse.

Para una organización, esto cambia el sentido de la evaluación de seguridad. Una evaluación no debería terminar en un informe archivado, sino alimentar decisiones y acciones. La identificación debe producir conocimiento útil para gobernar, proteger, detectar, responder y recuperar.

## 5. Proteger: reducir la probabilidad y el impacto

Una vez identificados los activos y riesgos prioritarios, la función Proteger concentra las medidas destinadas a gestionar esos riesgos. El CSF agrupa aquí cinco áreas: gestión de identidades, autenticación y control de acceso; concienciación y capacitación; seguridad de datos; seguridad de plataformas; y resiliencia de la infraestructura tecnológica.

La gestión de identidades y accesos representa una barrera esencial frente al uso indebido de recursos. El enfoque del CSF no se limita a la existencia de mecanismos técnicos; se vincula con la necesidad de administrar quién puede acceder, bajo qué condiciones y con qué nivel de privilegio.

La concienciación y capacitación reconoce que las personas forman parte del sistema de seguridad. Una organización puede disponer de controles tecnológicos avanzados y, aun así, mantener una exposición considerable si sus usuarios no comprenden sus responsabilidades o los riesgos asociados con sus actividades.

La seguridad de los datos exige considerar su protección en función de los riesgos que afectan a la organización. Esto adquiere especial importancia cuando se procesan datos personales, información estratégica o información crítica para la continuidad de servicios.

La seguridad de plataformas comprende hardware, software y servicios de plataformas físicas y virtuales. El CSF adopta aquí una perspectiva amplia que permite aplicar los resultados a distintos modelos tecnológicos.

La resiliencia de la infraestructura busca que los componentes tecnológicos puedan soportar condiciones adversas y mantener o recuperar capacidades esenciales. Esta idea conecta la protección con la continuidad y la recuperación.

### Una protección basada en prioridades

El CSF no establece que todos los activos deban recibir exactamente el mismo nivel de protección. La protección debe responder a la criticidad, al contexto y a la estrategia de riesgo. Por ello, una inversión bien orientada no es necesariamente la que incorpora más

herramientas, sino la que reduce riesgos relevantes de forma coherente con los objetivos de la organización.

Desde una perspectiva ejecutiva, Proteger debe entenderse como una inversión selectiva. La organización debe poder explicar qué protege, frente a qué amenazas, con qué prioridad y qué resultado espera obtener.

## 6. Detectar, Responder y Recuperar: capacidad para enfrentar incidentes

### Detectar

La función Detectar busca descubrir y analizar oportunamente anomalías, indicadores de compromiso y otros eventos potencialmente adversos. Su núcleo comprende el monitoreo continuo y el análisis de eventos adversos.

La detección conecta las capacidades preventivas con la realidad operativa. Una organización puede contar con políticas, inventarios y controles, pero necesita identificar rápidamente cuándo una situación se desvía de lo esperado. La oportunidad es fundamental: cuanto más tarde se identifica un incidente, mayor puede ser su impacto y más compleja su respuesta.

### Responder

Responder implica actuar frente a un incidente detectado. El CSF contempla la gestión, análisis, notificación y comunicación, así como la mitigación. El propósito es contener los efectos del incidente y coordinar las acciones necesarias para reducir daños.

La respuesta no es solamente técnica. Requiere decisiones, responsabilidades, canales de comunicación y coordinación con las partes interesadas. El marco también reconoce la importancia de involucrar a terceros pertinentes, especialmente cuando forman parte de la infraestructura o del servicio afectado.

### Recuperar

Recuperar se orienta a restaurar los activos y operaciones afectados y a reducir los efectos del incidente. Incluye la ejecución del plan de recuperación y la comunicación durante la recuperación.

La recuperación debe entenderse como una capacidad organizacional, no como una tarea aislada del área de TI. Cuando un incidente afecta servicios críticos, la organización necesita restablecer operaciones, comunicar el estado de la situación y extraer aprendizajes para evitar que las mismas debilidades vuelvan a producir impactos similares.

### La rueda del CSF

El NIST representa las seis funciones como una rueda porque se relacionan entre sí. Gobernar orienta las demás funciones; Identificar permite conocer qué debe protegerse; Proteger reduce exposición; Detectar permite descubrir eventos; Responder gestiona el incidente; y Recuperar restablece las operaciones. El ciclo, por tanto, no termina con la recuperación: los resultados deben retroalimentar la identificación y la mejora.

## 7. Perfiles Organizativos: convertir el marco en una hoja de ruta

Los Perfiles Organizativos constituyen uno de los mecanismos más útiles del CSF 2.0 para pasar de la teoría a la gestión. Permiten representar la situación actual y definir una situación objetivo en términos de resultados de seguridad.

El proceso sugerido por el NIST comienza delimitando el alcance. Una organización puede desarrollar un perfil para toda la entidad o para un ámbito concreto, como sistemas financieros, un servicio crítico o una amenaza específica. Esta flexibilidad permite evitar evaluaciones excesivamente amplias cuando la prioridad es resolver un riesgo determinado.

El segundo paso consiste en recopilar información relevante: políticas, prioridades, recursos, perfiles de riesgo empresarial, análisis de impacto en el negocio, requisitos y estándares aplicables, prácticas, herramientas, procedimientos y roles.

Con esa información se construye el Perfil Organizativo. Después se analiza la brecha entre el Perfil Actual y el Perfil Objetivo. La brecha debe transformarse en un plan de acción priorizado. El documento menciona como ejemplos un registro de riesgos, un informe detallado de riesgos o un Plan de Acción e Hitos (POA&M).

El paso siguiente es implementar el plan y actualizar el perfil. La mejora continua es una característica esencial: la organización puede repetir el ciclo tantas veces como sea necesario.

### Valor ejecutivo de los perfiles

El Perfil Actual permite comunicar capacidades y oportunidades de mejora. El Perfil Objetivo puede utilizarse para expresar requisitos y expectativas a proveedores, colaboradores y terceros. Así, el perfil deja de ser un documento exclusivamente interno y se convierte en una herramienta de comunicación y alineamiento.

En términos prácticos, el Perfil Objetivo responde a una pregunta de dirección: ¿qué nivel de capacidad necesitamos alcanzar para gestionar nuestros riesgos de acuerdo con nuestra misión? El Perfil Actual responde a otra: ¿qué estamos logrando hoy? La diferencia entre ambos permite ordenar inversiones y decisiones.

## 8. Niveles del CSF y mejora de la madurez

Los cuatro Niveles del CSF describen la evolución de las prácticas de gobierno y gestión del riesgo. El Nivel 1, Parcial, representa respuestas informales y ad hoc. El Nivel 2, Informado sobre el Riesgo, muestra una gestión más consciente del riesgo. El Nivel 3, Repetible, supone prácticas establecidas y repetibles. El Nivel 4, Adaptativo, refleja enfoques ágiles, informados por el riesgo y orientados a la mejora continua.

El NIST advierte que los niveles no sustituyen una metodología de gestión de riesgos. Deben complementar el método utilizado por la organización y servir como referencia para comunicar cómo se gestiona el riesgo. Tampoco debe asumirse que toda organización necesita alcanzar el Nivel 4. La progresión debe justificarse por el nivel de riesgo, los mandatos aplicables y el análisis de costos y beneficios.

### Recursos que complementan el CSF

El documento distingue tres recursos principales: Referencias Informativas, Ejemplos de Implementación y Guías de Inicio Rápido. Las Referencias Informativas muestran relaciones entre resultados del Core y normas, directrices, reglamentos u otros contenidos

existentes. Los Ejemplos de Implementación presentan posibles pasos orientados a la acción. Las Guías de Inicio Rápido simplifican aspectos concretos del marco para facilitar los primeros pasos.

Esta arquitectura evita que el CSF se convierta en un documento aislado. El marco define resultados y permite vincularlos con controles, prácticas y normas que ya utiliza la organización. El resultado es una estructura de integración, no una sustitución automática de las metodologías existentes.

### Implicación para programas de ciberseguridad

Una organización madura debería utilizar los niveles como lenguaje de gestión y los perfiles como instrumento de planificación. El objetivo es que la madurez no se mida solamente por cantidad de controles, sino por la consistencia con que la organización gobierna, comprende, trata y revisa sus riesgos.

## 9. Integración con riesgos empresariales, privacidad, proveedores e IA

Uno de los aportes más importantes del CSF 2.0 es su orientación hacia la integración. El NIST plantea que la seguridad cibernética debe gestionarse junto con otros riesgos empresariales, como los financieros, de privacidad, cadena de suministro, reputación, tecnológicos o físicos.

### Gestión del riesgo empresarial

El CSF puede integrarse con programas de Enterprise Risk Management (ERM) y con metodologías específicas de gestión de riesgos de TIC. El documento menciona su relación con publicaciones del NIST como SP 800-37 y SP 800-30 y señala que puede complementar el enfoque del Risk Management Framework para seleccionar y priorizar controles de SP 800-53.

El valor de esta integración es principalmente de gestión: permite traducir conceptos de ciberseguridad a un lenguaje comprensible para quienes toman decisiones sobre la cartera general de riesgos. La dirección puede así comparar riesgos tecnológicos con otras exposiciones de la organización y decidir dónde asignar recursos.

### Privacidad

El NIST diferencia seguridad cibernética y privacidad, pero reconoce que existen áreas de solapamiento. La pérdida de confidencialidad, integridad o disponibilidad de datos personales puede generar riesgos de privacidad, como ocurre con determinadas violaciones de datos. Sin embargo, también existen riesgos de privacidad que pueden aparecer sin un incidente de ciberseguridad, derivados del propio procesamiento de información.

Por ello, el documento plantea que el CSF y el Marco de Privacidad del NIST pueden utilizarse conjuntamente. La conclusión es relevante: proteger información no equivale automáticamente a gestionar todos los riesgos de privacidad.

### Inteligencia artificial y tecnologías emergentes

La IA aparece como ejemplo de tecnología emergente que puede introducir riesgos de seguridad cibernética, privacidad y otros riesgos empresariales. El documento remite al AI Risk Management Framework del NIST y destaca que las consideraciones de seguridad y privacidad deben incorporarse al diseño, desarrollo, despliegue, evaluación y uso de sistemas de IA.

Esta perspectiva evita tratar la IA como un tema separado de la gestión de riesgos. Su gobernanza debe formar parte del mismo sistema general de decisión y supervisión.

## 10. Conclusiones ejecutivas y lectura estratégica

El CSF 2.0 del NIST propone una forma ordenada de gestionar la ciberseguridad sin imponer una receta tecnológica. Su mayor fortaleza es ofrecer un lenguaje común que conecta la dirección, los responsables de riesgo, los gestores y los profesionales que operan la tecnología. El marco parte de resultados deseados y permite que cada organización determine las prácticas y controles más apropiados para alcanzarlos.

La primera conclusión es que la ciberseguridad debe ser gobernada. Las decisiones sobre riesgo requieren contexto, responsables, recursos, políticas, supervisión y conexión con la misión. La inclusión

explícita de Gobernar y de la gestión de riesgos de la cadena de suministro refuerza esta visión.

La segunda conclusión es que la gestión comienza con conocimiento. Inventariar activos, comprender dependencias, identificar vulnerabilidades y amenazas y estimar impactos son condiciones necesarias para priorizar. Sin esta base, la inversión en seguridad corre el riesgo de responder a percepciones antes que a riesgos.

La tercera conclusión es que las seis funciones forman un sistema. Proteger no reemplaza Detectar; Detectar no reemplaza Responder; y Recuperar no puede ser improvisado después de un incidente. El valor del CSF aparece precisamente en la conexión entre las funciones y en la retroalimentación permanente.

La cuarta conclusión es que los Perfiles convierten el marco en una herramienta de gestión. Comparar un estado actual con un estado objetivo permite construir una agenda de mejora, priorizar brechas y comunicar avances. Esta lógica es especialmente útil para comités de dirección y programas de transformación de ciberseguridad.

La quinta conclusión es que la madurez debe responder al riesgo. Los Niveles 1 a 4 no deben utilizarse como una carrera automática hacia el nivel máximo. El nivel apropiado dependerá de los riesgos, mandatos, objetivos y análisis de costos y beneficios de cada organización.

La sexta conclusión es que el CSF funciona mejor integrado con otros instrumentos. El NIST contempla su relación con gestión de riesgos empresariales, RMF, controles de seguridad y privacidad, gestión de riesgos de cadena de suministro, privacidad e inteligencia artificial. Por ello, adoptarlo no significa abandonar los marcos existentes, sino utilizarlos dentro de una estructura común de resultados y prioridades.

## Conclusión final

Desde una perspectiva profesional, el CSF 2.0 puede entenderse como un sistema de dirección de la ciberseguridad basado en riesgo. Su utilidad no depende de implementar literalmente cada resultado, sino de utilizar su estructura para responder de manera consistente

cinco preguntas: qué es importante para la organización, qué puede afectar aquello que es importante, qué capacidades necesita para gestionar esos riesgos, qué brechas mantiene actualmente y cómo comprobará que está mejorando.

En consecuencia, una implementación efectiva debería comenzar por el contexto y el gobierno, continuar con la identificación de activos y riesgos, definir un Perfil Objetivo, priorizar las brechas y establecer acciones verificables. El ciclo debe mantenerse abierto, porque el riesgo cibernético cambia con las amenazas, las tecnologías, los proveedores y las prioridades institucionales.

En síntesis, el CSF 2.0 no debe verse como un catálogo de controles, sino como una estructura para tomar mejores decisiones de ciberseguridad. Su aporte principal es conectar estrategia, riesgo, operación y mejora continua, haciendo posible que la seguridad cibernética sea gestionada como una responsabilidad integral de la organización.