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

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

Security and Privacy Controls for Information Systems and Organizations

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

NIST Special Publication 800-53, Revisión 5

Controles de seguridad y privacidad para sistemas de información y organizaciones

Nota de traducción: *Esta es una traducción/síntesis para fines académicos. La edición en inglés es la edición auténtica.*

1. Resumen ejecutivo

NIST Special Publication 800-53, Revisión 5, constituye uno de los catálogos de referencia más completos para diseñar, implementar, evaluar y mantener controles de seguridad y privacidad en sistemas de información y organizaciones. Su propósito central no es imponer una arquitectura tecnológica concreta, sino ofrecer un conjunto flexible de capacidades de protección que puedan adaptarse al contexto, al nivel de riesgo, a la misión de la organización y a las obligaciones legales y regulatorias aplicables.

La idea fundamental de la publicación es sencilla, aunque sus implicaciones son amplias: la ciberseguridad debe gestionarse como un problema de riesgo empresarial y no como una colección aislada de herramientas. Un firewall, un sistema de gestión de eventos, una solución de identidad o un antivirus son mecanismos que pueden contribuir a un control; por sí solos no constituyen un programa de seguridad completo. La protección efectiva requiere gobierno, personas, procesos, tecnología, evidencia y supervisión continua.

La Revisión 5 integra en un catálogo único los controles de seguridad y privacidad. Con ello reconoce que la protección de los sistemas y la protección de las personas cuyos datos son procesados están estrechamente relacionadas. Cuando una organización trata información de identificación personal (PII), las decisiones de seguridad pueden generar efectos sobre la privacidad y, a la inversa, las decisiones de privacidad pueden condicionar la arquitectura, el registro de eventos, el acceso y la conservación de la información.

Otro cambio relevante de la Revisión 5 es su orientación hacia resultados. Los controles describen capacidades de protección que deben conseguirse, dejando a la organización margen para determinar quién las implementa, con qué tecnología y con qué parámetros. Esta flexibilidad permite aplicar el catálogo a entornos tradicionales, nube, movilidad, IoT, sistemas ciberfísicos, sistemas industriales y otros escenarios tecnológicos.

La publicación organiza los controles en 20 familias. Entre ellas se encuentran control de acceso, concienciación y formación, auditoría, evaluación y autorización, gestión de configuración, continuidad,

identificación y autenticación, respuesta a incidentes, protección de medios, seguridad física, planificación, gestión del programa, seguridad del personal, privacidad, evaluación de riesgos, adquisición de sistemas y servicios, protección de comunicaciones, integridad de sistemas y gestión del riesgo de la cadena de suministro.

Para un profesional de ciberseguridad, la principal enseñanza de SP 800-53 es que un control debe entenderse dentro de un sistema de gestión de riesgos. Primero se determina qué se necesita proteger y qué consecuencias tendría una pérdida de confidencialidad, integridad o disponibilidad; después se seleccionan y adaptan los controles; posteriormente se implementan, se evalúan, se autorizan y se supervisan de forma continua. La seguridad, por tanto, no termina cuando un control se pone en producción.

2. Propósito, alcance y filosofía de la publicación

La publicación fue desarrollada por el National Institute of Standards and Technology (NIST) en el marco de sus responsabilidades vinculadas a la seguridad de la información del Gobierno federal de los Estados Unidos. Aunque su aplicación obligatoria se relaciona con el contexto federal estadounidense, NIST señala que las organizaciones no gubernamentales pueden utilizarla voluntariamente. Por su carácter general y adaptable, el catálogo se emplea también como referencia en numerosos programas de seguridad del sector privado.

El documento parte de una visión amplia de las amenazas. Los controles deben ayudar a enfrentar ataques deliberados, errores humanos, fallos estructurales, desastres naturales, amenazas de actores externos y riesgos asociados al tratamiento de información personal. Esta perspectiva evita reducir la ciberseguridad a la defensa frente a malware o intrusiones y obliga a considerar también disponibilidad, resiliencia, continuidad, personas, proveedores y procesos.

La publicación adopta una postura tecnológicamente neutral. En lugar de decir qué producto debe comprarse, describe la función de seguridad o privacidad que debe conseguirse. Esta característica es

especialmente importante para los profesionales que diseñan arquitecturas, redactan requisitos, gestionan proveedores o evalúan controles: el objetivo es verificar que existe una capacidad adecuada, no simplemente que una determinada herramienta está instalada.

3. Conceptos fundamentales

3.1 Requisitos frente a controles

Un requisito expresa una obligación, necesidad de protección o condición que debe satisfacerse. Puede provenir de una ley, regulación, política, contrato, necesidad de negocio, requisito de misión o evaluación de riesgos. El control es la capacidad de protección seleccionada e implementada para satisfacer ese requisito.

Esta distinción es esencial en un programa de cumplimiento. Cumplir un requisito no significa copiar literalmente un control del catálogo. La organización debe demostrar cómo el control elegido satisface la necesidad concreta y qué evidencia permite verificarlo.

3.2 Estructura de los controles

Cada control se presenta con una estructura común: identificador y nombre, declaración del control, discusión explicativa, controles relacionados, posibles mejoras del control y referencias. Los controles base definen una capacidad fundamental; las mejoras o control enhancements añaden funcionalidad o elevan el nivel de protección. Una mejora no se selecciona de forma independiente: requiere el control base correspondiente.

3.3 Parámetros y adaptación

Muchos controles contienen parámetros que la organización debe definir, por ejemplo la frecuencia de revisión de privilegios, el tiempo de bloqueo de una cuenta o el período de retención de registros. Esta característica permite adaptar el mismo control a diferentes niveles de riesgo. La adaptación o tailoring debe estar justificada por el contexto y documentada.

3.4 Formas de implementación

NIST contempla tres enfoques. Un control común puede ser implementado y administrado por una entidad que presta esa capacidad a varios sistemas; un control específico corresponde principalmente a un sistema concreto; y un control híbrido combina una parte común con otra específica. La elección debe hacerse según el contexto y con responsabilidades claramente asignadas.

3.5 Funcionalidad y aseguramiento

La funcionalidad responde a qué capacidad de seguridad o privacidad ofrece el sistema. El aseguramiento responde a qué grado de confianza existe en que esa capacidad está correctamente implementada, funciona como se espera y produce el resultado requerido. Esta diferencia es crítica: una organización puede tener una política de autenticación sólida en papel y, sin embargo, carecer de evidencia de que se aplica correctamente en los sistemas.

4. Gestión del riesgo como eje del modelo

SP 800-53 sitúa los controles dentro de un proceso de gestión de riesgos. El enfoque requiere comprender los activos, sistemas, procesos y datos, valorar las consecuencias de una pérdida o degradación, identificar amenazas y vulnerabilidades y determinar las medidas de protección apropiadas.

1. Definir el contexto y las necesidades de protección de la organización y de sus partes interesadas.
2. Categorizar los sistemas y la información de acuerdo con su impacto y criticidad.
3. Seleccionar controles y establecer los parámetros necesarios para el entorno concreto.
4. Implementar los controles, asignando responsables y generando evidencia.
5. Evaluar si los controles están correctamente implementados, funcionan como se espera y cumplen los requisitos.
6. Autorizar la operación considerando el riesgo residual y la capacidad de la organización para aceptarlo.
7. Supervisar continuamente los sistemas, controles, amenazas, cambios y resultados de las evaluaciones.

Este ciclo convierte la seguridad en un proceso dinámico. Un control adecuado hoy puede resultar insuficiente mañana debido a cambios en la arquitectura, nuevos servicios en la nube, incorporación de proveedores, vulnerabilidades, modificaciones regulatorias o cambios en el perfil de amenaza.

5. Las 20 familias de controles

ID	Familia	Enfoque principal
AC	Control de acceso	Gestiona quién puede acceder a qué recursos, bajo qué condiciones y con qué privilegios. Incluye cuentas, autorizaciones, separación de funciones, mínimo privilegio, control de sesiones y flujo de información.
AT	Concienciación y formación	Busca que usuarios, administradores y responsables comprendan sus obligaciones y desarrollen las competencias necesarias para operar de forma segura.
AU	Auditoría y responsabilidad	Establece capacidades para generar, proteger, revisar y analizar registros de auditoría, de modo que las acciones relevantes puedan atribuirse y utilizarse para detección, investigación y cumplimiento.
CA	Evaluación, autorización y supervisión	Conecta la implementación de controles con evaluaciones formales, autorización para operar y seguimiento continuo de la postura de seguridad.
CM	Gestión de configuración	Controla configuraciones, inventarios, cambios, software autorizado y parámetros técnicos para reducir desviaciones y superficies de ataque.
CP	Planificación de contingencias	Prepara a la organización para responder y recuperarse ante interrupciones, fallos y eventos que afecten la disponibilidad de sistemas y servicios.
IA	Identificación y autenticación	Establece mecanismos para identificar usuarios, dispositivos y procesos y verificar su identidad antes de conceder acceso.
IR	Respuesta a incidentes	Define capacidades para preparar, detectar, analizar, contener, erradicar y recuperar frente a incidentes, además de mejorar el programa a partir de las lecciones aprendidas.
MA	Mantenimiento	Regula las actividades de mantenimiento de sistemas, incluyendo acceso remoto, personal autorizado y medidas de protección durante intervenciones técnicas.

MP	Protección de medios	Protege soportes que contienen información durante su acceso, transporte, almacenamiento, sanitización y destrucción.
PE	Protección física y ambiental	Aborda instalaciones, acceso físico, energía, temperatura, detección de incendios y otras condiciones que pueden comprometer sistemas y equipos.
PL	Planificación	Integra los requisitos de seguridad y privacidad en planes, arquitectura, ciclo de vida, reglas de comportamiento y otros instrumentos de gobierno.
PM	Gestión del programa	Eleva la seguridad al nivel organizacional: estrategia, recursos, roles, métricas, coordinación, arquitectura, cultura y gestión de riesgos empresariales.
PS	Seguridad del personal	Gestiona riesgos asociados a las personas antes, durante y después de su relación con la organización, incluyendo selección, responsabilidades, transferencias y desvinculación.
PT	Tratamiento y transparencia de PII	Gestiona riesgos de privacidad derivados de la creación, recopilación, uso, tratamiento, conservación, divulgación y eliminación de información de identificación personal.
RA	Evaluación de riesgos	Identifica, analiza y actualiza riesgos relacionados con amenazas, vulnerabilidades, impacto, privacidad y condiciones del entorno.
SA	Adquisición de sistemas y servicios	Incorpora requisitos de seguridad y privacidad al desarrollo, compra, contratación, ingeniería, pruebas y gestión de proveedores de sistemas y servicios.
SC	Protección de sistemas y comunicaciones	Protege comunicaciones, fronteras de red, confidencialidad, integridad, criptografía, arquitectura y mecanismos de separación o aislamiento.
SI	Integridad de sistemas e información	Reduce riesgos asociados a software malicioso, vulnerabilidades, fallos, cambios no autorizados, errores y pérdida de integridad de la información.
SR	Gestión del riesgo de la cadena de suministro	Gestiona riesgos derivados de productos, servicios, proveedores, componentes, dependencias y procesos de adquisición y desarrollo a lo largo de la cadena de suministro.

6. Controles de especial relevancia para la práctica profesional

6.1 Identidad, autenticación y mínimo privilegio

La gestión de identidades es una de las primeras barreras contra el abuso de credenciales. SP 800-53 presta atención a la administración del ciclo de vida de las cuentas, la separación entre cuentas privilegiadas y no privilegiadas, la revisión periódica de privilegios, el bloqueo ante intentos fallidos, el bloqueo automático de dispositivos y la terminación de sesiones. El principio de mínimo privilegio exige que cada usuario o proceso disponga solo de los permisos necesarios para cumplir su función.

6.2 Registro, monitoreo y trazabilidad

La auditoría no debe limitarse a almacenar logs. Los registros deben ser suficientes para reconstruir hechos relevantes, protegerse frente a modificación o destrucción, mantenerse durante el tiempo necesario y revisarse de acuerdo con el riesgo. La calidad de la evidencia condiciona la capacidad de detectar intrusiones, investigar incidentes y demostrar cumplimiento.

6.3 Configuración segura

La gestión de configuración reduce el riesgo de que cambios no controlados introduzcan vulnerabilidades. Esto implica mantener inventarios, establecer configuraciones de referencia, controlar modificaciones, identificar software autorizado y detectar desviaciones. Desde una perspectiva operativa, la configuración segura debe formar parte del ciclo de vida y no ser una tarea puntual posterior a la instalación.

6.4 Respuesta y recuperación

La respuesta a incidentes debe estar preparada antes de que ocurra el incidente. Esto supone disponer de procedimientos, responsables, mecanismos de reporte, capacidades de análisis, contención y recuperación, así como ejercicios y revisiones posteriores. La continuidad y la respuesta deben complementarse: una organización resiliente no solo intenta evitar incidentes, también limita su impacto y recupera las funciones críticas.

6.5 Protección de comunicaciones

La familia SC aborda la protección de las comunicaciones y de los límites de los sistemas. Incluye controles relacionados con arquitectura de red, control del tráfico, criptografía, protección de información en tránsito y mecanismos destinados a impedir accesos o flujos no autorizados. En entornos modernos, estas capacidades deben analizarse junto con nube, acceso remoto, dispositivos móviles, IoT y arquitecturas distribuidas.

6.6 Integridad y vulnerabilidades

La integridad requiere identificar cambios no autorizados, detectar software malicioso, gestionar vulnerabilidades y mantener mecanismos que permitan comprobar que los sistemas funcionan de manera confiable. La gestión de vulnerabilidades adquiere valor cuando se conecta con inventario, criticidad, exposición, inteligencia de amenazas y priorización basada en riesgo.

6.7 Cadena de suministro

La inclusión de la familia SR refleja una realidad: una organización puede tener controles internos maduros y, aun así, quedar expuesta por un proveedor, una dependencia de software, un componente comprometido o una práctica insegura de desarrollo. La gestión del riesgo de terceros debe comenzar antes de la contratación y continuar durante la relación, considerando requisitos, evaluación, monitoreo, cambios y condiciones de salida.

7. Seguridad y privacidad: una responsabilidad integrada

La Revisión 5 trata seguridad y privacidad dentro de un catálogo consolidado porque ambas disciplinas pueden perseguir objetivos distintos, pero se superponen cuando los sistemas procesan PII. La seguridad busca, entre otros objetivos, evitar acceso, uso, divulgación, modificación, interrupción o destrucción no autorizados. La privacidad se ocupa de los riesgos que el tratamiento de información puede generar para las personas.

Una medida de seguridad puede introducir un riesgo de privacidad si, por ejemplo, recopila más información de la necesaria, conserva registros durante períodos excesivos o utiliza mecanismos de

monitoreo sin considerar adecuadamente el propósito y la proporcionalidad. Por eso NIST plantea una colaboración estrecha entre los responsables de seguridad y privacidad.

8. Gobierno, responsabilidades y evidencia

Una característica decisiva del modelo es que los controles no deben quedar confinados al área técnica. La dirección establece prioridades y acepta o rechaza riesgos; los responsables de seguridad y privacidad definen políticas y supervisan; los propietarios de sistemas conocen el contexto operativo; los administradores implementan medidas; los usuarios cumplen las reglas; y los evaluadores comprueban la eficacia de los controles.

La evidencia es un elemento central. Las evaluaciones requieren artefactos que permitan determinar si un control existe, si está implementado correctamente, si opera como se espera y si satisface los requisitos. Políticas, procedimientos, configuraciones, registros, resultados de pruebas, tickets de cambio, informes de vulnerabilidades, actas de revisión y evidencias de formación pueden formar parte de ese conjunto.

Desde la perspectiva de auditoría, la pregunta correcta no es únicamente «¿tenemos el control?», sino «¿qué demuestra que el control funciona?». Esta diferencia separa un programa de cumplimiento documental de un programa de ciberseguridad operacional.

9. Aplicación práctica en una organización

Para aplicar SP 800-53 con criterio, una organización puede utilizar una secuencia de trabajo como la siguiente:

a. Identificar procesos críticos, activos, sistemas, datos y dependencias externas.
b. Determinar impactos y escenarios de riesgo, incluyendo riesgos para personas y privacidad.
c. Definir requisitos legales, regulatorios, contractuales, de negocio y de seguridad.
d. Seleccionar las familias y controles relevantes; establecer parámetros y justificaciones.

e. Decidir qué controles serán comunes, específicos o híbridos.
f. Implementar controles mediante políticas, procesos, configuraciones y tecnologías.
g. Definir indicadores y evidencias para cada control relevante.
h. Realizar evaluaciones independientes o internas según el nivel de riesgo.
i. Registrar deficiencias, priorizar acciones correctivas y aceptar formalmente el riesgo residual cuando corresponda.
j. Mantener monitoreo continuo y actualizar controles cuando cambien amenazas, sistemas, proveedores o requisitos.

El valor del catálogo aumenta cuando se integra con el ciclo de desarrollo y operación. Los requisitos de seguridad deben aparecer desde la arquitectura y adquisición, no únicamente durante una auditoría previa a la puesta en producción.

11. Conclusiones

NIST SP 800-53 Rev. 5 presenta una visión madura de la ciberseguridad: proteger sistemas y organizaciones exige gestionar riesgos de manera sistemática y mantener controles que sean adecuados al contexto, verificables y sostenibles. El catálogo aporta un lenguaje común para traducir necesidades de protección en capacidades concretas y para relacionar gobierno, arquitectura, operaciones, cumplimiento y privacidad.

La principal aportación para el estudiante de un diplomado es comprender que los controles no funcionan de manera aislada. Una autenticación robusta pierde valor si las cuentas no se administran correctamente; los registros pierden utilidad si no se protegen o revisan; un plan de contingencia es insuficiente si nunca se prueba; una política de proveedores no reduce el riesgo si no existen requisitos verificables; y una herramienta de seguridad no sustituye a la responsabilidad de la organización.

En consecuencia, la aplicación profesional de SP 800-53 debe comenzar por el riesgo y terminar en la evidencia y el monitoreo continuo. El objetivo no es acumular controles, sino construir una capacidad de protección coherente con la misión de la organización y suficientemente robusta para resistir, detectar, responder y recuperarse de eventos adversos.

12. Glosario esencial

Término	Definición
Control	Medida o capacidad de protección destinada a satisfacer requisitos de seguridad o privacidad.
Control enhancement	Mejora que amplía o fortalece un control base.
Tailoring / adaptación	Proceso de ajustar la selección, parámetros y aplicación de controles al contexto y riesgo.
PII	Información de identificación personal; datos que pueden vincularse o asociarse con una persona.
Mínimo privilegio	Principio por el cual se conceden solo los permisos necesarios para una función.
Control común	Control cuya capacidad puede ser heredada por varios sistemas o programas.
Control híbrido	Control cuya implementación se divide entre una capacidad común y otra específica del sistema.
Aseguramiento	Grado de confianza en que una capacidad de seguridad o privacidad está correctamente implementada y funciona como se espera.
Riesgo residual	Riesgo que permanece después de aplicar medidas de tratamiento o mitigación.
Monitoreo continuo	Supervisión periódica o continua de controles, sistemas, amenazas y cambios para mantener una visión actualizada del riesgo.

Fuente principal: National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, septiembre de 2020, con errata incorporada al 10 de diciembre de 2020.