FACULTAD DE INGENIERÍA

CIBERSEGURIDAD INTEGRAL

Estrategia, riesgo, tecnología y cultura organizacional

LORENZO ELGUEA FERNÁNDEZ

UNIVERSIDAD Panamericana

CIBERSEGURIDAD
INTEGRAL

Estrategia, riesgo, tecnología y cultura organizacional

Primera edición electrónica, 2026

Título: **Ciberseguridad integral:**
Estrategia, riesgo, tecnología y cultura organizacional
Autor: Lorenzo Miguel Elguea Fernández
Facultad de Ingeniería

Responsable editorial: Manuel Bernal Coronel
Diseño de portada: Ivonne Lara Alba
Cuidado editorial: Santi Ediciones

ISBN: 978-607-8826-95-7

Universidad Panamericana, Campus México
Jerez 10, Insurgentes Mixcoac, Benito Juárez,
Ciudad de México, México, C.P. 03920
Conmutador: +52 55 5482 1600
www.up.edu.mx

Impreso en México / *Printed in Mexico*.

CIBERSEGURIDAD
INTEGRAL

Estrategia, riesgo, tecnología y cultura organizacional

LORENZO ELGUEA FERNÁNDEZ

FACULTAD DE INGENIERÍA

UNIVERSIDAD
Panamericana

A mi familia, por su apoyo incondicional.

Para todos mis amigos.

A mis compañeros del trabajo, los que siempre me apoyan con las vulnerabilidades y los que solo a veces.

A la IA generativa, quien me ayudó en algunas partes de este trabajo.

CONTENIDO

GLOSARIO

AES	(*Advanced Encryption Standard*), también conocido como Rijndael, es el algoritmo de cifrado simétrico más utilizado y seguro en el mundo actualmente. Fue adoptado por el gobierno de los Estados Unidos en 2001 –bajo el estándar FIPS 197– (NIST, 2001a) tras un concurso público para sustituir al antiguo y ya vulnerable DES. Al ser un cifrado simétrico, utiliza la misma llave tanto para cifrar el mensaje como para descifrarlo. Es el estándar de facto para proteger datos en reposo (discos duros) y datos en tránsito (como en las redes wi-fi WPA2/WPA3 y el protocolo HTTPS).
Algoritmo	Conjunto de pasos para resolver un problema.
BIA	(*Business Impact Analysis*; en español: análisis de impacto al negocio), es el proceso fundamental de la gestión de la continuidad que permite determinar qué tan graves serían las consecuencias de una interrupción en las actividades de una organización. Estrechamente relacionado con el DRP.
BIOS	(*Basic Input/Output System*; en español: sistema básico de entrada y salida) es el primer programa que se ejecuta al encender una

	computadora. Es un firmware instalado en un chip dedicado de la placa base (*motherboard*) y su función es actuar como el puente fundamental entre el hardware del equipo y el sistema operativo.
CIEM	(*Cloud Infrastructure Entitlement Management*) es una tecnología de seguridad enfocada exclusivamente en gestionar y asegurar las identidades y sus permisos en entornos de nube pública. Si el CSPM se encarga de que la "puerta" esté bien cerrada, el CIEM se encarga de que solo las personas (y máquinas) adecuadas tengan la "llave" correcta y no puedan hacer más de lo estrictamente necesario.
Cifrado homomórfico	Es una técnica de criptografía avanzada que permite realizar cálculos directamente sobre datos cifrados, sin necesidad de descifrarlos previamente. El resultado de esos cálculos, una vez descifrado, es idéntico al que se obtendría si las operaciones se hubieran realizado sobre los datos en claro.
CSPM	(*Cloud Security Posture Management*) es una categoría de herramientas de seguridad diseñadas para identificar y corregir automáticamente errores de configuración y riesgos de cumplimiento en la nube. Si el cifrado protege el dato, el CSPM protege el "contenedor" donde vive ese dato, asegurándose de que las puertas y ventanas de tu infraestructura digital no se queden abiertas por accidente.
CVE	(*Common Vulnerabilities and Exposures*; en español vulnerabilidades y exposiciones comunes) es un sistema estandarizado que asigna identificadores únicos a vulnerabilidades de seguridad en software y hardware.

CVSS	(*Common Vulnerability Scoring System*) es el estándar industrial global para evaluar la severidad de una vulnerabilidad de seguridad informática.
DLP	(*Data Loss Prevention*) es una solución de seguridad diseñada para identificar, monitorear y proteger la información sensible de una organización, evitando que sea maltratada o robada, ya sea por error humano o por ataques malintencionados.
Ecosistémica	Se refiere a una visión integral y multidimensional que reconoce que la seguridad de una organización depende de la interdependencia entre sus componentes internos (personas, procesos y tecnología) y sus influencias externas (regulaciones, proveedores, amenazas y mercado). Bajo este enfoque, cualquier cambio o vulnerabilidad en un nodo del sistema afecta inevitablemente a la estabilidad del conjunto, obligando a que la gestión del riesgo sea holística, dinámica y adaptativa en lugar de estática y perimetral.
EDR	(*Endpoint Detection and Response*) es una solución de seguridad avanzada diseñada para proteger los dispositivos finales (*endpoints*), como computadoras, laptops y servidores, mediante el monitoreo continuo y la respuesta automatizada ante amenazas. A diferencia de un antivirus tradicional, que se basa principalmente en firmas de virus conocidos, el EDR se centra en el análisis de comportamiento.
Gobernanza	La gobernanza es más amplia que el Gobierno. Es el conjunto de procesos, políticas, principios, normas y mecanismos que aseguran que la organización tome buenas decisiones alineadas a sus objetivos, ética, gestión de

	riesgos y cumplimiento. Se refiere a cómo se gobierna. Incluye: a) Políticas; b) Estrategia de gestión de riesgos; c) Métricas y supervisión; d) Marcos normativos; e) Responsabilidades claras; f) Supervisión continua, y g) Mecanismos de control.
Gobierno	En el ámbito organizacional (no político), gobierno se refiere a: La estructura formal que toma decisiones. Las autoridades y roles asignados. Quién tiene el poder y la responsabilidad de dirigir. Es decir: quién manda, quién decide, quién aprueba. Ejemplos: a) Junta directiva; b) Alta dirección; c) Comité de riesgos, y d) CISO como autoridad designada.
Hardware	El hardware es toda la parte física y tangible de una computadora o dispositivo electrónico. Es decir, todo lo que puedes ver y tocar (a diferencia del software, que es la parte lógica).
Hash	Un hash es una huella digital de un dato, siempre tiene la misma longitud, sin importar el tamaño del dato original, es irreversible: no puedes obtener el dato original a partir del hash y si cambias un solo carácter en la entrada, cambia completamente el hash..
Malware	Proviene de la combinación de las palabras en inglés *malicious software* (software malicioso). Se define como cualquier programa, código o aplicación diseñada específicamente para infiltrarse, dañar, alterar o extraer información de un dispositivo (computadora, smartphone, servidor o red) sin el consentimiento del usuario. A diferencia de un error de software común, el *malware* tiene una intención negativa. Sus objetivos

	suelen ser el robo de datos financieros, el espionaje, la extorsión o simplemente causar caos operativo.
MFA	(*Multi-Factor Authentication o Autenticación de Doble Factor*) es un sistema de seguridad que requiere que un usuario proporcione dos o más pruebas de identidad diferentes antes de concederle acceso a una cuenta o sistema. Su objetivo es simple: si un atacante logra robar tu contraseña (el primer factor), no podrá entrar a tu cuenta porque aún le faltará el segundo factor, que solo tú posees.
MITRE	ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es un marco de conocimiento global que recopila, organiza y describe de manera detallada las tácticas, técnicas y procedimientos (TTPs) que usan los atacantes en el mundo real. Fue creado por MITRE, una organización sin fines de lucro que apoya investigación y desarrollo en seguridad.
MTD	Es el periodo máximo de tiempo que un proceso, servicio o sistema puede permanecer inactivo antes de que la interrupción cause daños inaceptables.
NIST	(*National Institute of Standards and Technology*) es una agencia del Departamento de Comercio de EE. UU. dedicada a desarrollar estándares, mediciones y tecnologías para garantizar calidad, seguridad y precisión.
PCI DSS	(*Payment Card Industry Data Security Standard*) es un conjunto de normas de seguridad diseñadas para garantizar que todas las empresas que procesan, almacenan o transmiten datos de tarjetas de crédito o débito mantengan un entorno seguro.

Pentest	Pruebas de penetración.
Phishing	Es una técnica de ingeniería social utilizada por ciberdelincuentes para engañar a las personas y obtener información sensible, como contraseñas, números de tarjetas de crédito o datos bancarios. El atacante se hace pasar por una entidad de confianza (un banco, una red social, un compañero de trabajo o una institución gubernamental) a través de canales de comunicación digital.
Ransomware	Tipo de *malware* (software malicioso) que bloquea o cifra los archivos de una computadora o dispositivo y luego exige un pago (un "rescate") para devolver el acceso.
RPO	(*Recovery Point Objective*) es la cantidad máxima de datos que la institución está dispuesta a perder. Responde a la pregunta: ¿hasta qué punto en el pasado debemos recuperar la información?
RTO	(*Recovery Time Objective*) es el tiempo máximo que la institución puede permitirse estar sin el servicio. Responde a la pregunta: ¿cuánto tiempo tardamos en volver a funcionar?
SHA	(Secure Hash Algorithm), SHA-1 usa una longitud del hash: 160 bits (40 caracteres hexadecimales). y los demás, por ejemplo SHA-512 usan 512 bits.
SIEM	(*Security Information and Event Management*) es una plataforma tecnológica que centraliza, correlaciona y analiza los eventos y registros (logs) de seguridad generados en una organización, con el objetivo de detectar amenazas, generar alertas y apoyar la respuesta a incidentes.

SOC	(*Security Operations Center*; en español: Centro de Operaciones de Seguridad) es una unidad centralizada dentro de una organización –o un servicio externo– que se encarga de monitorizar, detectar, analizar y responder a incidentes de ciberseguridad las 24 horas del día, los 7 días de la semana.
Software	Es el conjunto de programas, aplicaciones y datos que permiten que una computadora, teléfono u otro dispositivo electrónico funcione y realice tareas. Es la "parte lógica" o intangible de un sistema (a diferencia del hardware, que es la parte física).
TKS	(*Tasks, Knowledge, Skills*) es un acrónimo práctico que agrupa los tres elementos fundamentales que describen lo que una persona debe hacer (*tasks*), saber (*knowledge*) y saber aplicar (*skills*) para desempeñar un rol de ciberseguridad.
TPM	(*Trusted Platform Module*) es un chip de seguridad que viene integrado en muchas computadoras modernas. Su función principal es proteger información sensible y garantizar la integridad del sistema..
UEFI	(*Unified Extensible Firmware Interface*) es el software básico que actúa como puente entre el hardware de tu computadora y el sistema operativo. Es el sucesor moderno del antiguo BIOS (desde el 2012 aprox.) y es lo primero que se ejecuta al presionar el botón de encendido.
Vulnerabilidad	Es una debilidad en un sistema –como software, hardware, redes o procesos, incluso humana–, que puede ser aprovechada por un atacante para causar daño.

WAF (*Web Application Firewall*; en español: cortafuegos de aplicaciones web) es una solución de seguridad diseñada específicamente para proteger aplicaciones web mediante el filtrado y monitoreo del tráfico HTTP/HTTPS entre la aplicación y el internet. A diferencia de un firewall tradicional que actúa como una barrera en las puertas de la red (capas 3 y 4 del modelo OSI), el WAF opera en la capa 7 (capa de aplicación). Esto le permite inspeccionar el contenido de los mensajes y detener ataques que los firewalls convencionales no pueden ver.

PRÓLOGO

Si hace apenas un par de décadas nos hubieran preguntado cómo reforzar la seguridad institucional, probablemente habríamos pensado en bardas más altas, muros más gruesos, cámaras de vigilancia o personal de seguridad mejor capacitado. La noción de protección estaba asociada, casi exclusivamente, al resguardo físico de los espacios y los bienes. Hoy, ese paradigma resulta claramente insuficiente. En el contexto actual, no existe una estrategia de seguridad sólida que no incorpore de manera central la protección de la información, los datos y los activos digitales de las organizaciones.

La ciberseguridad ha adquirido un protagonismo incuestionable y su relevancia ha crecido de forma exponencial en los últimos años. Todos los días se registran miles de ciberataques en todo el mundo y, lamentablemente, muchos de ellos logran su objetivo de interrumpir operaciones, comprometer información crítica o generar pérdidas económicas y reputacionales de gran escala.

De acuerdo con estimaciones de Cybersecurity Ventures y del Foro Económico Mundial, el costo global del cibercrimen superará los 10 billones de dólares anuales en 2026. Si el cibercrimen fuera una economía nacional, sería equiparable a la tercera más grande del mundo, solo por detrás de Estados Unidos y China. Estas cifras explican por qué la ciberseguridad se ha convertido en un asunto estratégico para la protección no solo de organizaciones, sino también de países.

Los ejemplos recientes son contundentes. En 2022, el Gobierno de Costa Rica sufrió un ciberataque de tal magnitud que lo llevó a declarar un estado de emergencia nacional, paralizando servicios públicos e impactando sectores clave de su economía. En Estados Unidos, el ataque a Change Healthcare interrumpió servicios médicos esenciales, afectando hospitales y pacientes en todo el país. Casos como los de Colonial Pipeline, Jaguar Land Rover o

IBM evidencian que ninguna industria ni organización –pública o privada– está exenta de enfrentar este tipo de amenazas.

Sin embargo, los efectos de los ciberataques no se limitan al daño a servidores, infraestructuras tecnológicas o pérdidas económicas. Con frecuencia, el impacto más profundo se da en el ámbito humano, pues la extracción y exposición de datos personales, información médica, financiera o estratégica deja a personas en situación de vulnerabilidad frente a redes criminales cada vez más sofisticadas. En este sentido, la ciberseguridad es también una cuestión de responsabilidad social y de protección de la dignidad de los seres humanos.

Ante este escenario, la ciberseguridad ha escalado posiciones hasta convertirse en una prioridad en las agendas corporativas. Sistemas de monitoreo continuo, adquisición de software especializado, inversiones en infraestructura tecnológica y la subcontratación de servicios técnicos avanzados son hoy una constante en las áreas de tecnología y en los niveles más altos de la dirección. No obstante, estas medidas, por sí solas, resultan insuficientes.

La experiencia demuestra que ninguna estrategia de ciberseguridad es verdaderamente eficaz si no está acompañada de una visión integral, de un liderazgo comprometido y de una cultura organizacional sólida. Cuando los controles tecnológicos no se integran en un marco estratégico claro; cuando la compra de herramientas no responde a una comprensión holística del riesgo; o cuando la estrategia no permea en los comportamientos cotidianos de las personas, la organización sigue expuesta. De hecho, el Verizon Data Breach Investigations Report señala de manera consistente que entre el 68 % y el 82 % de las brechas de seguridad involucran, de alguna forma, el factor humano.

Es precisamente en este punto donde cobra especial relevancia la obra *Ciberseguridad integral: estrategia, riesgo, tecnología y cultura organizacional*; su oportunidad no radica únicamente en ofrecer herramientas prácticas para fortalecer los sistemas de protección, sino en su capacidad para articular la ciberseguridad como un desafío estratégico y cultural. El libro pone en el centro a las personas, aborda la gestión del riesgo desde una perspectiva amplia y conecta la tecnología con la toma de decisiones al más alto nivel organizacional, un enfoque tan necesario como frecuentemente ausente en la literatura técnica.

El doctor Lorenzo Elguea Fernández reúne dos cualidades que lo acreditan de manera sobresaliente para abordar este tema. Por un lado, posee un conocimiento técnico profundo en materia de ciberseguridad. Por otro lado, cuenta con una amplia experiencia como directivo de alto nivel en áreas tecnológicas y actualmente se desempeña como máximo responsable de ciberseguridad en la Universidad Panamericana. Esta combinación de rigor técnico y experiencia práctica se refleja con claridad a lo largo de la obra.

Así como nadie puede afirmar que está completamente exento de sufrir un accidente en la carretera, ninguna persona, empresa, universidad o entidad pública puede asegurar que jamás enfrentará un incidente de ciberseguridad. Lo que sí está en nuestras manos es reducir de manera significativa los riesgos al fortalecer protocolos, capacitar a las personas, elevar la conversación estratégica al más alto nivel organizacional y generar conciencia con auténtica sensibilidad humana.

Desde esta perspectiva, la lectura de este libro no solo resulta de gran interés, también es una herramienta clave para quienes tienen la responsabilidad de proteger organizaciones en un entorno digital cada vez más complejo, interconectado y desafiante.

Dr. Santiago García Álvarez
Rector Universidad Panamericana
Ciudad de México, enero de 2026

INTRODUCCIÓN

El objetivo de esta obra es guiarte en la implementación de una estrategia de ciberseguridad robusta en tu institución. La premisa fundamental es que la seguridad digital es universal: no importa el tamaño de la organización, ni la cantidad de usuarios o dispositivos conectados. El contenido está estructurado pedagógicamente: primero se exponen las herramientas, metodologías y marcos de referencia, para luego facilitar su adecuación e implementación práctica.

Reconocemos que la robustez de estos marcos varía. Una PYME puede iniciar con los controles básicos del Center for Internet Security (CIS, 2025a)[1] y evaluar progresivamente la adopción del NIST CSF 2.0 (NIST, 2024b).

Una estrategia de ciberseguridad es fundamental para proteger los activos más valiosos de una organización: la información, la continuidad operativa y la confianza de sus clientes y usuarios. En un entorno donde las amenazas digitales evolucionan constantemente, las empresas e instituciones necesitan un enfoque preventivo que permita identificar riesgos, anticiparse a posibles ataques y reducir vulnerabilidades antes de que puedan ser explotadas.

Para mantener un entorno protegido y resiliente es clave la implementación de controles de seguridad –técnicos, administrativos y físicos–. Estos controles permiten regular cómo se accede a la información, detectar actividades sospechosas y responder de manera oportuna ante incidentes. Además, estandarizan procedimientos, fortalecen la trazabilidad y garantizan el cumplimiento de normativas y buenas prácticas, lo que contribuye a un entorno más seguro y organizado.

[1] Los Controles CIS consisten en salvaguardas que requieren que usted haga una sola cosa. Este enfoque simplificado de ciberseguridad ha demostrado ayudarle a protegerse contra las principales amenazas actuales.

Por su parte, la implementación de controles específicos es el mecanismo que transforma esa estrategia en una defensa activa y tangible. Al establecer barreras técnicas, administrativas y físicas (como la autenticación multifactor, la segmentación de redes o las políticas de acceso estricto), una institución adopta de un enfoque reactivo a uno proactivo. Estos controles no solo mitigan el riesgo de robo de datos o secuestro de información (*ransomware*), sino que también garantizan el cumplimiento de normativas legales y de privacidad cada vez más estrictas. Sin estos controles, cualquier brecha de seguridad se convierte en una crisis de confianza que puede destruir en minutos la reputación construida durante años.

Adoptar una cultura de seguridad integral otorga una ventaja competitiva y fomenta la ciberresiliencia. En un mercado donde los clientes y socios comerciales son cada vez más conscientes de los riesgos, demostrar que se cuenta con una infraestructura protegida y controles rigurosos genera confianza y credibilidad. La ciberseguridad, por tanto, no debe verse como un gasto a fondo perdido, sino como una inversión estratégica que habilita la innovación segura y garantiza la sostenibilidad y longevidad de la institución frente a la incertidumbre del futuro digital.

Finalmente, una estrategia de ciberseguridad madura y bien implementada mejora la reputación institucional y aumenta la confianza de clientes, socios y público en general. Las organizaciones que invierten en protegerse no solo evitan pérdidas económicas y daños operativos, sino que también se posicionan como responsables y preparadas frente a un panorama digital cada vez más complejo. Esto la convierte en un componente indispensable para la sostenibilidad y el éxito a largo plazo.

Justificación

Existe el mito de que los ciberdelincuentes atacan a grandes corporativos o bancos. La ciberseguridad no depende del tamaño de la nómina, ni de la cantidad de sucursales, sino del valor de los datos que manejas y de tu conexión a internet. El tamaño es irrelevante para la necesidad, aunque sí definirá la complejidad de la estrategia:

1. *Los ataques son automatizados* (*bots):* a los hackers no les importa si eres una PYME o una multinacional. Utilizan

bots (programas automáticos) que escanean internet buscando puertas abiertas. Si tu pequeña empresa tiene una vulnerabilidad, el bot entrará. No es algo personal, es un juego de números.

2. *El eslabón más débil* (*la cadena de suministro):* grandes empresas invierten millones en su seguridad, convirtiéndose en fortalezas difíciles de penetrar. En ese caso, los atacantes buscan a los proveedores pequeños (contadores, agencias de marketing, consultores) que tengan acceso a los sistemas de la empresa grande. Si tú eres ese proveedor pequeño y no tienes seguridad, te usarán como caballo de Troya para atacar a tus clientes grandes.

3. *La capacidad de supervivencia:* el punto más crítico. Una empresa grande puede sobrevivir a una pérdida millonaria o a una multa por protección de datos. Una PYME no tiene ese margen. Según estadísticas de la industria, aproximadamente el 60 % de las pequeñas empresas que sufren un ciberataque grave cierran sus operaciones en los seis meses siguientes debido a los costos de recuperación y la pérdida de reputación.

Tabla 1. Implementación de ciberseguridad según el tamaño de la empresa

Tamaño de la empresa	Enfoque de la estrategia	Controles típicos
Micro/freelance: 1-10 empleados	Higiene básica	Antivirus, contraseñas fuertes y doble factor de autenticación (MFA). Copias de seguridad en la nube. MFA (doble factor) en todo.
Pequeña: 11-100 empleados.	Prevención y perímetro	Firewall, VPN para trabajo remoto. Control de acceso a datos. Capacitación a empleados. Póliza de ciberseguro. Antivirus centralizado.

Tamaño de la empresa	Enfoque de la estrategia	Controles típicos
Mediana/ grande: 100-1000 empleados	Detección y gestión	Equipo dedicado (CISO). Monitoreo 24/7 (SOC). Segmentación de Red (EDR/XDR). Pruebas de penetración (Hacking ético). Cumplimiento normativo (ISO 27001).
Corporativo: +1000 empleados	Gobernanza y resiliencia	SOC 24/7. Director de Ciberseguridad. Inteligencia de amenazas. Cumplimiento avanzado. Certificaciones (ISO, PCI, GDPR). Auditoría continua.

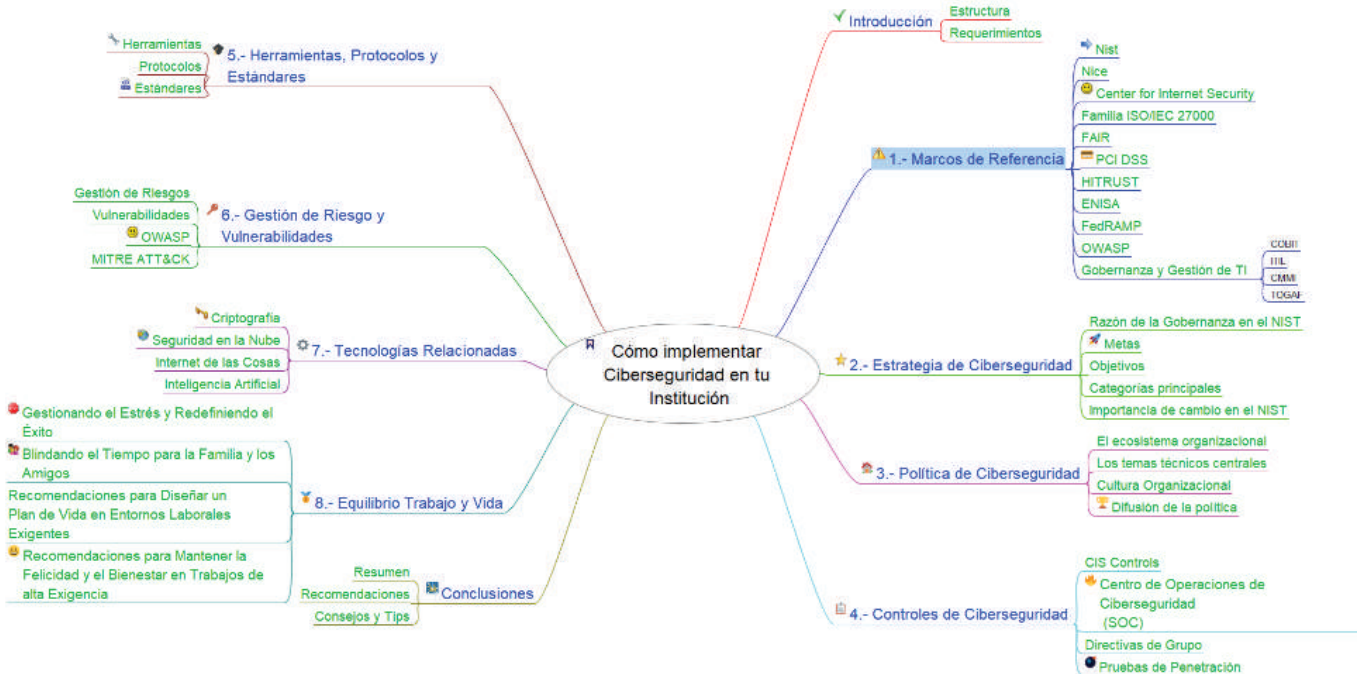
Fuente: elaboración propia.

Estructura de la obra

En el primer capítulo se presentarán algunos marcos de ciberseguridad. En el segundo, se profundizará en la importancia de definir una estrategia propia, siguiendo los pasos del NIST, en su sección de gobernanza. En el tercer capítulo elaborarás tu política de ciberseguridad, incluyendo todo tu ecosistema. Después de los pasos anteriores, definirás los controles (capítulo 4), y las herramientas, protocolos y estándares (capítulo 5) para cumplir tu estrategia y alinearte a los objetivos del negocio.

El capítulo 6 aborda los riesgos, su mitigación, vulnerabilidades y OWASP. El capítulo 7 trata sobre las tecnologías relacionadas, mientras que el capítulo 8 explica la importancia del equilibrio entre trabajo y vida personal. Y para terminar, en las conclusiones, se encuentran recomendaciones, consejos y tips, junto con un resumen que pueden ser de ayuda.

Figura 1. Mapa mental de la estructura del libro



Fuente: elaboración propia.

Requerimientos

Es fundamental definir de manera precisa la visión, misión y valores institucionales. La ciberseguridad no es un fin en sí mismo, es un medio para habilitar y proteger lo que la institución quiere lograr.

1. **La misión. Protegiendo lo que haces hoy:** define la razón de ser de la empresa, qué hace y para quién. La ciberseguridad debe garantizar que esa operación no se detenga.

   Identificación de lo que es valioso para tu institución: si tu misión es "proveer servicios financieros seguros", tu activo más crítico es la integridad de los datos transaccionales. Si tu misión es "innovar en diseño gráfico", tu activo crítico es la propiedad intelectual. La misión te dice qué proteger con mayor intensidad.

   Continuidad del negocio: los controles no deben entorpecer la misión. Si tu misión requiere velocidad y entrega en tiempo real, controles de seguridad excesivamente burocráticos matarán tu operación.

   La visión. Preparando la seguridad para el futuro: la visión establece hacia dónde quiere ir la organización a largo plazo (por ejemplo, ser la empresa líder en ventas digitales en 5 años).

   Escalabilidad: si la visión implica una expansión global o migración a la nube, la estrategia de seguridad no puede basarse en servidores físicos locales y rígidos. Debe ser una seguridad flexible y escalable.

   Gestión del cambio: si la visión es ser disruptivos tecnológicamente, la seguridad debe enfocarse en DevSecOps (seguridad en el desarrollo) y no en bloqueos tradicionales que frenen la innovación.

2. **Los valores. Definiendo la cultura de seguridad:** los valores dictan el comportamiento ético y la cultura organizacional. Estos definen el "apetito de riesgo".

   Confianza vs. agilidad: si un valor central es la "confidencialidad" (por ejemplo, un banco o un hospital), los controles de acceso serán estrictos, aunque sean incómodos. Si un valor es la "transparencia y colaboración" (por ejemplo, una startup tecnológica), los controles deben ser invisibles y permitir el flujo libre de ideas, enfocándose más en el monitoreo que en la restricción.

   Reputación: la "honestidad" es un valor, la estrategia de ciberseguridad debe incluir protocolos claros de comunicación transparente en caso de una brecha de datos, para evitar intentar ocultarla.

Si no se conoce esto se corre el riesgo de implementar controles que no aportan valor, que dificultan operaciones o que no protegen lo importante. Los valores institucionales como transparencia, responsabilidad, orientación al usuario o innovación definen:

» El apetito y tolerancia al riesgo.
» La postura ética frente al manejo de datos.
» La importancia de construir confianza con clientes, empleados o ciudadanos.

MARCOS DE REFERENCIA

Los marcos de referencia de ciberseguridad surgen ante la necesidad de orientar a las organizaciones en un entorno donde las amenazas digitales evolucionan con rapidez y complejidad creciente. Ante la dificultad de definir controles desde cero, estos marcos proporcionan un conjunto estructurado de buenas prácticas, principios y requisitos que permiten gestionar los riesgos de manera consistente.

Su existencia responde a la necesidad de uniformidad, estandarización y alineación con el negocio, especialmente en organizaciones donde la ciberseguridad debe integrarse tanto en procesos técnicos como en operativos, legales y estratégicos.

Estos marcos ayudan a las empresas a evaluar su nivel de madurez, priorizar inversiones, demostrar cumplimiento normativo y mejorar la resiliencia frente a incidentes. Proporcionan un lenguaje común entre equipos técnicos, ejecutivos, auditores y proveedores, lo que facilita la toma de decisiones informadas y coherentes. En esencia, funcionan como una guía práctica para transformar la ciberseguridad en un proceso gestionable, medible y adaptable, permitiendo a las organizaciones proteger sus activos críticos con mayor eficacia bajo estándares reconocidos globalmente.

En la práctica, actúan como una brújula de navegación que permite a las empresas evaluar objetivamente su madurez actual, identificar puntos ciegos en su defensa y priorizar recursos hacia los riesgos más críticos.

Tipos de marcos de referencia

Algunas páginas muestran "sus" propios Top Cybersecurity Frameworks (por ejemplo, Mutune, 2019), sin embargo, creo que estos son los más útiles para instituciones mexicanas de cualquier tamaño.

NIST CSF 2.0

El National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, conocido como NIST CSF 2.0, es la versión evolucionada del Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología, diseñado como una herramienta flexible y estratégica para que cualquier tipo de organización, independientemente de su sector o tamaño, pueda reducir su exposición a riesgos digitales. A diferencia de su predecesor, esta actualización introduce la función de gobernanza como eje central, enfatizando que la ciberseguridad debe ser una prioridad de la alta dirección y no solo una tarea técnica, además de ampliar su alcance global para facilitar la comunicación y la gestión de riesgos en las cadenas de suministro (NIST, 2024b).

Antecedentes

El NIST CSF 1.0 nació a partir de una necesidad en Estados Unidos y tenía una finalidad muy clara. Se originó debido a una orden ejecutiva del presidente Barack Obama de Estados Unidos, Orden No. 13636, Improving Critical Infrastructure Cybersecurity, 12 de febrero de 2013.

El gobierno de EE.UU. pidió al NIST que desarrollara un marco de ciberseguridad que ayudara a:

- Proteger la infraestructura crítica (energía, agua, transporte, salud, financiero, etcétera).
- Crear un lenguaje común de ciberseguridad.
- Establecer mejores prácticas sin depender de una regulación estricta.

El NIST trabajó con industria, expertos, academia y gobierno, y en febrero de 2014 publicó oficialmente el CSF versión 1.0 (NIST, 2025a). Su finalidad era crear un marco voluntario, basado en riesgos, flexible, con un lenguaje común, para mejorar la ciberseguridad y resiliencia de las organizaciones públicas y privadas.

Posteriormente se publicó la NIST CSF versión 1.1 el 16 de abril de 2018 y fue una actualización de la versión 1.0, enfocada en aclaraciones y mejoras (sin cambiar la estructura principal).

Versión actual

Finalmente, el NIST CSF versión 2.0 se publicó el 26 de febrero de 2024, que es una actualización mayor, con cambios estructurales importantes, una nueva función (*Govern*), guías más extensas y mayor alcance para todo tipo de organizaciones.

NIST CSF 2.0 = *CSF* 1.1 + *Gobernanza* + *Alcance ampliado* + *Ejemplos prácticos* + *Supply chain* + *Modernización*
(Representación componentes del NIST CSF 2.0)

Los seis componentes del CSF 2.0 son:

Figura 2. Evolución del NIST CSF 1.1 al 2.0

Fuente: NIST (2025b).

1. El marco está compuesto por *core* (núcleo), con funciones, categorías y subcategorías.
2. Perfiles (*profiles*), perfil actual (*current profile*) y perfil objetivo (*target profile*).
3. Los ejemplos de implementación (*implementation examples*) son ejemplos prácticos de implementación por subcategoría.
4. Los niveles de implementación (*tiers*) evalúan el nivel de madurez y gobernanza del riesgo.
5. Las referencias informativas (*informative references*) están compuestas por normas, marcos de trabajo y controles de referencia.

6. Los documentos de orientación (*guidance documents*) son guías complementarias por sector, tamaño y necesidad.

Núcleo (core)

El núcleo está formado por las seis funciones:

1. *Gobernar (GV)*: la estrategia, políticas y gestión de riesgos organizacional –"el cerebro"–.
2. *Identificar (ID)*: comprender los activos, datos y riesgos actuales.
3. *Proteger (PR)*: implementar salvaguardas para contener el impacto de un evento.
4. *Detectar (DE)*: encontrar incidentes cuando ocurren.
5. *Responder (RS)*: tomar acción ante un incidente detectado.
6. *Recuperar (RC)*: restaurar capacidades y servicios dañados.

Cada función se divide en categorías que representan resultados de seguridad más específicos (23 categorías en total) y cada categoría se desglosa en subcategorías, que representan resultados aún más detallados y ejecutables (106 subcategorías en total).

Adicionalmente, en el Núcleo, están los ejemplos de implementación (*implementation examples*), que es un elemento nuevo y clave en CSF 2.0. buscando hacer el *core* mucho más práctico y fácil de adoptar.

Cada subcategoría ahora viene acompañada de ejemplos prácticos, como:

» Controles sugeridos.
» Procesos recomendados.
» Herramientas o prácticas comunes.
» Actividades específicas que ayudan a cumplir la subcategoría.

El *core* también incluye referencias informativas (*informative references*) a otros estándares que se alinean con cada subcategoría que ayudan a conectar el CSF con marcos regulatorios o técnicos ya existentes como:

» ISO/IEC 27001.

- » COBIT.
- » CIS Controls.
- » SP 800-53.
- » SOC 2.
- » ISA/IEC 62443.

Tabla 2. Funciones y categorías del NIST CSF 2.0

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	**CSF 2.0 Category**	**CSF 2.0 Category Identifier**
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identity (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Fuente: NIST (2025b).

Perfiles (profiles)

Los perfiles (*profiles*) en el NIST CSF 2.0 son la herramienta que permite que el marco deje de ser un estándar teórico y se convierta en

un plan de acción real para tu institución. Un perfil es un mapeo de cómo la organización aplica el CSF según sus necesidades, riesgos y objetivos. El NIST CSF no obliga a implementar todo; los perfiles ayudan a elegir lo que sí es necesario, en qué nivel y en qué momento.

Existen dos tipos de perfiles principales:

1. Perfil actual (*current profile*), que refleja lo que la organización hace hoy respecto a cada subcategoría del CSF. Incluye:

    » Controles existentes.
    » Políticas actuales.
    » Procesos vigentes.
    » Nivel real de madurez o efectividad.
    » Riesgos presentes.
    » Brechas identificadas.

    Es una evaluación diagnóstica.

2. Perfil objetivo (*target profile*) refleja el nivel de ciberseguridad que la organización desea alcanzar, considerando:

    » Objetivos estratégicos.
    » Misión, visión y valores.
    » Apetito de riesgo.
    » Regulaciones aplicables.
    » Nivel de madurez esperado
    » Capacidades y presupuesto.

Es la meta futura. Una gran mejora en la versión 2.0 es el énfasis en los perfiles comunitarios. Antes, cada empresa tenía que crear su perfil objetivo desde cero, lo cual era difícil. Ahora, el NIST y varias asociaciones están publicando perfiles prediseñados para sectores específicos.

Niveles de implementación (tiers)

Los niveles de implementación representan el grado en que una organización incorpora y gestiona la ciberseguridad dentro de sus procesos, su gobernanza y su cultura. No son niveles de madurez técnica, sino una medida del enfoque organizacional hacia la gestión del riesgo, considerando factores como la formalidad de los procesos, la toma de decisiones basada en riesgo y la integración de la ciberseguridad con la dirección y la estrategia corporativa. Los niveles van desde el *Tier 1* (parcial), donde las prácticas son reactivas y poco consistentes, hasta el *Tier 4* (adaptativo), donde la organización anticipa amenazas y optimiza sus controles de manera continua (NIST, 2024b).

Nivel 1 **Parcial (*partial*) gestión de riesgos:** informal y reactiva. No existe un proceso estructurado para priorizar las actividades de ciberseguridad.

Cultura: la conciencia sobre el riesgo de ciberseguridad es limitada a nivel organizacional.

Participación externa: la organización no colabora activamente con otras entidades ni comparte información sobre amenazas.

Nivel 2 **Riesgo informado (*risk informed*) gestión de riesgos:** existe una aprobación de los procesos de gestión de riesgos por parte de la dirección, pero no se aplican de forma constante en toda la empresa.

Cultura: hay conciencia de los riesgos, pero el flujo de información es fragmentado.

Participación externa: la organización conoce su lugar en el ecosistema, pero su colaboración es inconsistente.

Nivel 3 **Repetible (*repeatable*) gestión de riesgos:** los procesos están formalmente aprobados y se expresan como políticas. Se actualizan regularmente en función de los cambios en el entorno de amenazas.

Cultura: existe un enfoque en toda la organización para gestionar el riesgo. El personal tiene los conocimientos y las habilidades necesarias.

Participación externa: la organización colabora activamente con socios y recibe información sobre amenazas para mejorar su postura.

Nivel 4 **Adaptable (*adaptive*) gestión de riesgos:** la organización adapta sus prácticas de ciberseguridad basándose en lecciones aprendidas y en indicadores predictivos. La ciberseguridad es parte del ADN de la toma de decisiones.

Cultura: existe una cultura de mejora continua y una respuesta rápida ante incidentes y cambios tecnológicos.

Participación externa: la organización no solo recibe información, sino que contribuye activamente al ecosistema global, ayudando a otros a entender nuevas amenazas.

En el NIST CSF 2.0, los tiers ayudan a que la organización determine qué tan alineada está su gestión de ciberseguridad con sus objetivos y necesidades, y sirven como referencia para definir metas realistas dentro del perfil objetivo (*Target profile*). Elegir un tier adecuado no significa aspirar siempre al nivel más alto, sino seleccionar el que mejor se ajuste al contexto, recursos y apetito de riesgo de la institución. Así, los niveles se convierten en una herramienta estratégica que guía la priorización de mejoras y la evolución progresiva de la postura de ciberseguridad.

Los niveles de implementación (*tiers*) describen el grado de rigor, sofisticación y formalidad con el que tu organización gestiona los riesgos de ciberseguridad. Se dividen en cuatro niveles que van desde el *Tier 1* (parcial), donde la gestión es reactiva, improvisada y "ad hoc", hasta el Tier 4 (adaptativo), donde la ciberseguridad está totalmente integrada en la cultura organizacional, utiliza aprendizaje continuo y responde activamente a amenazas avanzadas.

Básicamente, miden qué tan maduros son tus procesos para tomar decisiones de seguridad, no solo qué herramientas tecnológicas tienes instaladas.

Es crucial entender que no todas las organizaciones necesitan llegar al *Tier 4*. El nivel ideal depende de tu misión, presupuesto y apetito de riesgo.

NICE

El marco NICE es un estándar que define las competencias, roles y habilidades necesarias en la fuerza laboral de ciberseguridad. No trata de controles técnicos ni de gestión de riesgos; se centra en personas y capacidades profesionales. También es del NIST (Wetzel et al., 2020).

Enfoque del NICE:

» Roles de ciberseguridad (SOC, analistas, administradores, etcétera).
» Conocimientos, habilidades y tareas necesarias.
» Competencias laborales.
» Planificación de fuerza laboral.
» Formación, certificaciones y desarrollo profesional Se enfoca en personas, talento y formación en ciberseguridad.

Aunque son distintos, se integran muy bien:

» El CSF 2.0 puede identificar que la institución necesita mejorar detección o respuesta.
» El NICE ayuda a definir qué profesionales, con qué habilidades, se necesitan para lograrlo.
» Ejemplo: Si el CSF detecta brechas en monitoreo -+ NICE indica qué competencias debe tener un analista SOC, *Threat Hunter* o *Incident Responder* (tabla 3).

Estructura del NICE (NICE Framework)

Define una estructura común para describir el trabajo en ciberseguridad, organizando la fuerza laboral en siete categorías que repre-

sentan áreas amplias de actividad (como "defensa y protección" o "análisis"). Estas categorías ayudan a entender el panorama general de las funciones de ciberseguridad dentro de una organización y sirven como punto de partida para planificar equipos y roles. Son la vista de más alto nivel del marco (figura 3).

Dentro de esas categorías, el NICE describe *Work Roles*, que son los roles laborales específicos de ciberseguridad, cada uno con tareas claramente definidas. Estos roles representan puestos como Analista de ciberseguridad, Administrador de sistemas, Forense digital, Gestor de riesgos o Especialista en inteligencia de amenazas. Cada *Work Role* se compone de un conjunto de tareas que describen lo que la persona debe hacer en su día a día, lo que permite establecer descripciones de puesto precisas y comparables entre organizaciones.

Tabla 3. Comparación entre NIST CSF 2.0 y NICE

Aspecto	NIST CSF 2.0	NICE
Propósito	Gestionar riesgos y fortalecer la ciberseguridad organizacional.	Definir roles y habilidades del personal de ciberseguridad.
Enfoque	Procesos, controles, gobernanza, resiliencia.	Personas, tareas, competencias.
Pregunta que responde	¿Qué debe hacer mi institución para estar segura?	¿Qué debe saber y hacer mi personal de ciberseguridad?
Uso principal	Crear estrategias, perfiles, planes y controles.	Diseñar equipos, capacitar, evaluar habilidades.
Aplicación	Organización.	Fuerza laboral (individual, equipos, RRHH).
Incluye	Categorías, subcategorías, ejemplos de implementación.	Roles, habilidades, conocimientos, tareas.

Fuente: elaboración propia.

Finalmente, el marco define los *Knowledge, Skills and Abilities* (KSAs) y las *Tasks* (T) asociadas a cada rol. Los KSAs representan los conocimientos, habilidades y capacidades específicas que un profesional necesita para desempeñar el rol, mientras que las tareas detallan las acciones concretas del trabajo. Esta sección es clave porque

permite planificar formación, evaluar competencias, identificar brechas en el talento y alinear certificaciones, programas educativos y necesidades organizacionales. En conjunto, estas tres partes hacen del NICE un marco imprescindible para estructurar, desarrollar y fortalecer la fuerza laboral en ciberseguridad. Esto se conoce como TKS.

El objetivo final del NICE es servir como un traductor universal entre tres mundos que suelen no entenderse: los empleadores (empresas), los proveedores de educación (universidades/cursos) y los candidatos/empleados. Al estandarizar el vocabulario, asegura que cuando un gerente pide "seguridad en la nube", el área de Recursos Humanos sepa qué buscar y el empleado sepa qué estudiar, facilitando la creación de planes de carrera y la retención del talento dentro de la institución.

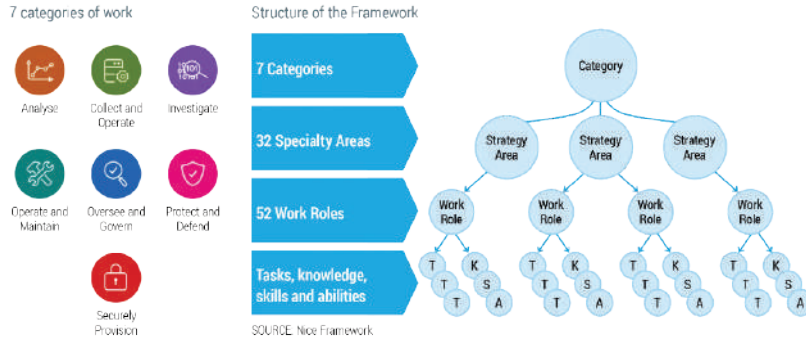
El NICE es especialmente valioso para:

» Empleadores:
- Ampliar la cartera de candidatos y aumentar la diversidad.
- Crear descripciones de puestos y evaluar a los candidatos.
- Monitorear y planificar las capacidades de la fuerza laboral.
- Desarrollar a los empleados (trabajo en equipo, capacitación).

» Estudiantes:
- Descubrir y planificar carreras en ciberseguridad.
- Desarrollo de conocimientos y habilidades.
- Demostrar capacidad y evidenciar competencia.

» Educadores:
- Desarrollar cursos y programas de aprendizaje que aborden las necesidades de los empleadores.
- Alinear la instrucción con el marco NICE.
- Realizar evaluaciones basadas en el desempeño.

Figura 3. Marco de referencia de NICE



Fuente: NIST (2025b).

Center for Internet Security (CIS)

El Center for Internet Security (CIS) es una organización sin fines de lucro dedicada a mejorar la ciberseguridad global mediante la creación de estándares, guías, configuraciones seguras y buenas prácticas que puedan aplicar organizaciones de cualquier tamaño. Es reconocido internacionalmente por sus controles CIS (CIS Controls) y los puntos de referencia del CIS (CIS Benchmarks), documentos ampliamente utilizados por instituciones públicas, privadas y educativas para fortalecer su postura de seguridad (CIS, 2026c).[2]

Los controles CIS son un conjunto priorizado de mejores prácticas de ciberseguridad diseñadas para detener los ataques más comunes. Son importantes porque están desarrollados por expertos del mundo real, basados en datos sobre ciberataques, y permiten a las organizaciones tener un camino claro, práctico y escalable para implementar seguridad sin necesidad de conocimientos avanzados o marcos complejos. Además, están organizados por niveles de implementación (*implementation groups*), lo que los hace accesibles tanto para organizaciones pequeñas como para grandes.

Por otro lado, los puntos de referencia del CIS (CIS Benchmarks) son guías detalladas de configuración segura para sistemas

[2] En general, los controles CIS son recomendaciones de buenas prácticas que consisten en un conjunto priorizado de acciones para defenderse de los ataques más comunes. En la versión 8.1 de los Controles, hay 18 Controles de nivel superior, seguidos de un subconjunto de 153 "acciones" denominadas Salvaguardias.

operativos, aplicaciones, servidores, bases de datos, servicios en la nube y dispositivos de red. Su importancia radica en que ofrecen configuraciones "listas para usar", respaldadas por una comunidad global de expertos, que reducen significativamente la superficie de ataque. Aplicar estos *benchmarks* permite asegurar que los sistemas estén configurados de manera robusta, coherente y alineada con estándares reconocidos, lo cual disminuye vulnerabilidades y aumenta la resiliencia frente a amenazas.

CIS Critical Security Controls

Los controles CIS (CIS Critical Security Controls) son un conjunto de 18 mejores prácticas prioritarias y ejecutables diseñadas para detener o mitigar los ciberataques más comunes y peligrosos (CIS, 2026a). A diferencia de otros marcos de trabajo que pueden ser muy teóricos, los controles CIS se centran en ofrecer una "higiene cibernética" esencial, organizando sus salvaguardas en grupos de implementación para que las empresas sepan exactamente qué pasos técnicos dar primero según su tamaño y recursos.

Su propósito principal es actuar como una hoja de ruta estratégica para fortalecer la postura de seguridad de toda la organización. Al implementar estos controles, las instituciones pueden reducir drásticamente su superficie de ataque, ya que cubren desde el inventario de activos y la protección de datos hasta la defensa contra *malware* y la respuesta ante incidentes, permitiendo además cumplir más fácilmente con normativas como GDPR, HIPAA o PCI DSS.

Control 1 Inventario y control de activos empresariales: saber qué dispositivos están conectados a tu red.

Control 2 *Inventario y control de activos de software:* gestionar todas las aplicaciones instaladas para evitar software no autorizado.

Control 3 *Protección de datos:* identificar, clasificar y proteger datos sensibles (cifrado, copias, etcétera).

Control 4 *Configuración segura de activos y software:* implementar el *hardening* –basado en los puntos de referencia del CIS (CIS Benchmarks)– en dispositivos y aplicaciones.

Control 5 *Gestión de cuentas:* gestionar el ciclo de vida de las cuentas de usuario y de administrador.

Control 6 *Gestión de control de acceso:* asegurar que solo las personas correctas tengan acceso a los datos (implementar MFA).

Control 7 *Gestión continua de vulnerabilidades:* escanear y remediar debilidades de seguridad de forma recurrente.

Control 8 *Gestión de registros de auditoría:* recolectar y analizar logs para detectar anomalías.

Control 9 *Protecciones de correo electrónico y navegadores web:* mitigar amenazas que llegan a través de la navegación o el *phishing*.

Control 10 *Defensas contra malware:* instalar y gestionar herramientas *antimalware* actualizadas.

Control 11 *Recuperación de datos:* mantener copias de seguridad adecuadas para recuperarse de ataques como el *ransomware*.

Control 12 *Gestión de infraestructura de red:* configurar de forma segura *firewalls*, routers y switches.

Control 13 *Monitoreo y defensa de la red:* vigilancia de la red para detectar intrusiones activas.

Control 14 *Concientización y capacitación en seguridad:* entrenar al personal para que sea la primera línea de defensa.

Control 15 *Gestión de proveedores de servicios:* evaluar la seguridad de los terceros que tienen acceso a tus datos.

Control 16 *Seguridad del software de aplicación:* prevenir vulnerabilidades en el software desarrollado internamente o por terceros.

Control 17 *Gestión de respuesta a incidentes:* tener un plan listo para reaccionar ante una brecha de seguridad.

Control 18 *Pruebas de penetración:* simular ataques reales para validar la efectividad de todas las defensas anteriores.

Los controles CIS (CIS Controls) están directamente alineados con MITRE ATT&CK (2024).

Puntos de referencia del CIS (CIS Benchmarks)

Los puntos de referencia del CIS (CIS Benchmarks) son guías de configuración específicas y detalladas (estándares de *hardening*) para endurecer sistemas tecnológicos particulares, como sistemas operativos, bases de datos o servicios en la nube. Mientras que los controles CIS (CIS Controls) te dicen qué proteger a nivel organizacional, los CIS Benchmarks te explican paso a paso cómo configurar de forma segura un producto específico para eliminar vulnerabilidades de fábrica y malas configuraciones. Por ejemplo, el documento para Windows 11, se encuentra en CIS (2026b):

- *Sistemas operativos:* son los más utilizados y cubren tanto versiones de escritorio como de servidor.
  - *Windows:* ya existen guías para Windows Server 2025 (lanzadas recientemente), además de Windows 11, 10 y versiones anteriores.

- *Linux: benchmarks* para distribuciones nuevas como RHEL 10, Rocky Linux 10, AlmaLinux 10, además de los clásicos Ubuntu, Debian y Amazon Linux.
- *Apple:* Guías actualizadas para macOS (incluyendo Sonoma y Sequoia) e iOS/iPadOS.

» *Infraestructura de nube* (*Cloud Foundations):* estos documentos son críticos para configurar la "base" de los proveedores de nube.
- *Principales:* AWS Foundations v5.0.0, Microsoft Azure Foundations v5.0.0 y Google Cloud Computing Platform.
- *Nuevos/específicos:* DigitalOcean Foundations, Oracle Cloud e IBM Cloud.
- *Servicios específicos: benchmarks* para servicios concretos como AWS End User Compute o bases de datos gestionadas en la nube.

» Software de servidor y bases de datos:
- *Bases de datos:* documentos para Oracle Database 23ai, MongoDB 8, PostgreSQL, MySQL 8.0 y SQL Server 2022.
- *Servidores web:* configuraciones para NGINX, Apache HTTP Server y Microsoft IIS.
- *Contenedores:* el *benchmark* de Docker v1.8.0 y guías para Kubernetes (incluyendo distribuciones como AKS de Azure y GKE de Google).

» Dispositivos de red y software de escritorio:
- *Redes:* guías para Cisco (IOS XE, NX-OS), Palo Alto Networks (PAN-OS 11), Fortinet y Juniper.
- *Aplicaciones:* navegadores (Google Chrome, Microsoft Edge v4.0.0, Firefox) y suites de productividad como Microsoft 365.

Las imágenes reforzadas del CIS (*CIS Hardened Images)*

Las imágenes reforzadas del CIS (CIS Hardened Images) son imágenes de sistemas operativos y plataformas en la nube que ya vienen

preconfiguradas según los CIS Benchmarks, aplicando ajustes de seguridad reforzada desde el primer arranque. Disponibles para servicios como AWS, Azure y Google Cloud, estas imágenes ofrecen un entorno endurecido y listo para usar, reduciendo significativamente la superficie de ataque y el riesgo asociado a configuraciones inseguras o inconsistentes. Su principal ventaja es que permiten a las organizaciones desplegar infraestructura segura de forma rápida y estandarizada, eliminando esfuerzos manuales de *hardening* y cumpliendo con buenas prácticas reconocidas internacionalmente desde el inicio.

CIS SecureSuite

El CIS SecureSuite no es un marco de ciberseguridad, sino un programa de membresía (suscripción) ofrecido por el Center for Internet Security (CIS) que proporciona acceso a herramientas, contenido, y recursos exclusivos para ayudar a las organizaciones a implementar y automatizar los CIS Controls y CIS Benchmarks. Incluye acceso a versiones avanzadas y descargables de los *benchmarks*, herramientas de evaluación automatizada (como CIS-CAT Pro), guías de mapeo con otros estándares, plantillas, documentación extendida y soporte especializado. Su propósito es facilitar que instituciones públicas y privadas adopten configuraciones seguras, evalúen su cumplimiento y mejoren continuamente su postura de ciberseguridad (CIS, 2025c).

El valor principal de CIS SecureSuite es que reduce tiempo, esfuerzo y complejidad en la implementación del *hardening* y de controles de seguridad, proporcionando herramientas para escanear sistemas, identificar desviaciones respecto a los *benchmarks* y generar reportes de cumplimiento detallados. Esto lo convierte en una solución muy atractiva para organizaciones que necesitan mejorar su seguridad de manera estructurada, cumplir requisitos regulatorios o administrar entornos grandes y heterogéneos sin tener que desarrollar procesos manuales desde cero.

Familia ISO/IEC 27000

El ISO es el acrónimo de la Organización Internacional de Normalización (International Organization for Standardization). A pesar de

que las siglas en inglés son IOS, se utiliza ISO, derivado de la palabra griega "isos" (igual), para reflejar que sus estándares son válidos y uniformes en todo el mundo (ISO–IEC, 2024).

Su función principal es crear y publicar estándares internacionales que definen las "mejores prácticas" para casi cualquier tipo de industria o proceso, desde la calidad de los productos hasta la gestión ambiental o la seguridad de la información (como la familia ISO/IEC 27000 que acabamos de mencionar). Estos estándares ayudan a garantizar la compatibilidad, la calidad, la seguridad y la eficiencia de bienes y servicios a nivel global, facilitando el comercio y la confianza entre países.

Se llama ISO/IEC porque las normas de tecnología, informática y comunicaciones son desarrolladas conjuntamente por dos organizaciones internacionales:

» *International Organization for Standardization* (*ISO):* organización que crea estándares internacionales en una gran variedad de industrias (calidad, seguridad, manufactura, etcétera).

» *International Electrotechnical Commission* (*IEC):* organización especializada en normas para electrotecnia, electrónica, tecnologías de la información y comunicaciones.

La familia de normas ISO/IEC 27000 es el principal conjunto de estándares internacionales dedicado a la gestión de la seguridad de la información. Su pieza central es la ISO/IEC 27001, la única norma de la familia que es certificable y que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI o ISMS). Este sistema no se enfoca solo en la tecnología, sino que aborda la seguridad de manera integral dentro de una organización, cubriendo personas, procesos y la infraestructura tecnológica, para asegurar que la gestión de los riesgos de seguridad sea un proceso continuo y sistemático.

La familia proporciona un marco robusto para proteger la confidencialidad, integridad y disponibilidad (C-I-D) de la información, el objetivo tripartito de la seguridad. Mientras que la norma 27001 específica qué debe hacer el SGSI (el requisito de gestión), la ISO/IEC 27002 actúa como un código de práctica, proporcionando

directrices detalladas y controles específicos para implementar esos requisitos (el cómo). Adoptar este marco permite a las instituciones mitigar riesgos de manera estructurada, cumplir con requisitos legales y contractuales, y obtener una certificación que demuestra confianza y compromiso con la seguridad a nivel mundial.

ISO/IEC 27001 y 27002

La ISO/IEC 27001 es la norma internacional más reconocida para la seguridad de la información, ya que establece los requisitos para crear, implementar y mejorar un sistema de gestión de seguridad de la información (SGSI). Al ser una norma certificable, permite a las empresas demostrar ante terceros que gestionan sus riesgos de forma profesional mediante un ciclo de mejora continua.

Por su parte, la ISO/IEC 27002 actúa como el catálogo detallado de controles; mientras que la 27001 dice qué requisitos cumplir, la 27002 ofrece una guía extensa de buenas prácticas sobre cómo implementar los controles técnicos, organizativos y físicos necesarios para proteger los activos de información.

La 27001 es certificable pero la 27002 no (ISO–IEC, 2022a, 2022b).

Tabla 4. Diferentes ISO/IEC de la familia 27000 y sus usos

Necesidad	ISO Recomendado
Implementar un sistema formal de seguridad	ISO/IEC 27001
Ver controles específicos	ISO/IEC 27002
Gestión de riesgos	ISO/IEC 27005
Seguridad en la nube	ISO/IEC 27017/27018
Ciberseguridad general	ISO/IEC 27032
Gestión de incidentes	ISO/IEC 27035
informática forense	ISO/IEC 27037-27043
Privacidad (GDPR)	ISO/IEC 27701
Continuidad del negocio	ISO 22301
Ciberseguridad en industria (OT)	IEC 62443
Ciberseguridad automotriz	ISO/SAE 21434

Fuente: elaboración propia.

ISO/IEC 27005

Gestión del riesgo en seguridad de la información. Esta norma proporciona las directrices para llevar a cabo la gestión de riesgos en seguridad de la información de manera sistemática (ISO-IEC, 2022c)[3]. Su importancia radica en que no impone una metodología rígida, sino que ofrece un marco que permite a las organizaciones identificar, evaluar y tratar las amenazas según su propio contexto. Es el complemento vital para la ISO 27001, ya que asegura que la inversión en seguridad esté alineada con los riesgos más críticos que enfrenta el negocio, evitando gastos innecesarios en controles que no son prioritarios.

ISO/IEC 27017 y ISO/IEC 27018

Estos estándares son para controles de seguridad en la nube (*Cloud Security*) y protección de datos personales en la nube (privacidad en servicios *cloud*) respectivamente.

Estas normas extienden los controles básicos de seguridad al entorno de computación en la nube. La ISO 27017 se enfoca en aspectos específicos de la nube (*cloud*), definiendo responsabilidades tanto para el proveedor como para el cliente; mientras que la ISO 27018 se especializa en la protección de los datos personales (PII) almacenados en nubes públicas. Juntas, ofrecen un marco de confianza esencial para que las organizaciones puedan migrar sus operaciones a servicios como AWS, Azure o Google Cloud garantizando que la privacidad y la seguridad técnica están alineadas con estándares globales.

ISO/IEC 27032 y ISO/IEC 27035

Enfoque específico de ciberseguridad: amenazas, ataques, defensa en ciberespacio. La ISO 27032 es la guía específica para la ciberseguridad, abordando amenazas que nacen en el ciberespacio como el *phishing*, *malware* y ataques de red, promoviendo la colaboración entre actores digitales.

En contraste, la ISO 27035 establece un marco estructurado para la gestión de incidentes; proporciona los procesos para

[3] Provee las directrices para alinear la gestión de riesgos con el contexto estratégico de la organización.

detectar, reportar y aprender de las brechas de seguridad. Ambas son fundamentales para la resiliencia operativa, asegurando que la empresa no solo intente prevenir ataques, sino que sepa cómo reaccionar de forma coordinada cuando estos ocurren.

ISO/IEC 27037, 27041, 27042, 27043

Familia sobre informática forense (*digital forensics*). Esta subfamilia de normas regula el ciclo de vida de las evidencias digitales, desde su identificación y recolección hasta su análisis y presentación. La ISO 27037 garantiza que la evidencia digital sea preservada de forma íntegra para ser válida en un juicio, mientras que las normas 27041 a 27043 estandarizan los métodos de investigación forense. Son documentos críticos para equipos legales y técnicos que deben demostrar la trazabilidad de un ataque o responder ante incidentes de fraude electrónico con rigor pericial.

ISO/IEC 27701

Extensión de 27001/27002 para privacidad (PIMS), orientada al cumplimiento tipo GDPR. La ISO 27701 es una extensión de la ISO 27001 que transforma el SGSI en un Sistema de Gestión de Información de Privacidad (PIMS). Su objetivo es integrar la protección de datos personales en la estructura de seguridad de la empresa, facilitando enormemente el cumplimiento de marcos legales complejos como el GDPR.

Al certificarse en esta norma, una organización demuestra que no solo protege la información como activo de negocio, sino que respeta los derechos de privacidad de los individuos de manera auditable y profesional.

Payment Card Industry Data Security Standard (PCI DSS)

El Payment Card Industry Data Security Standard (PCI DSS) es un estándar de seguridad global y obligatorio para cualquier organización que procese, transmita o almacene datos de tarjetas de pago (PCI Security Standards Council, 2022). A diferencia de marcos voluntarios como el NIST CSF, el PCI DSS es un estándar de cumplimiento técnico muy riguroso, impulsado por las principales marcas de tar-

jetas (Visa, Mastercard, AMEX). Su objetivo principal es reducir el fraude con tarjetas de crédito mediante la protección del entorno de datos de los titulares de tarjetas (CDE), exigiendo controles estrictos que van desde la seguridad de la red y el cifrado de datos hasta el desarrollo seguro de software y el monitoreo constante.

Desde la perspectiva de la gestión de riesgos, la versión más reciente (PCI DSS 4.0) ha evolucionado hacia un enfoque más dinámico y basado en resultados. Ya no se trata solo de cumplir con una lista de verificación anual, sino de demostrar que la seguridad es un proceso continuo. Este marco destaca por su nivel de detalle en los requisitos técnicos, obligando a las empresas a implementar medidas de autenticación multifactor (MFA) más robustas y a realizar escaneos de vulnerabilidades y pruebas de penetración con una frecuencia definida, lo que lo convierte en uno de los marcos de seguridad más prácticos (ejecutables) y exigentes del sector financiero.

La versión PCI DSS 4.0 representa el cambio más significativo en el estándar en casi una década. A diferencia de las versiones anteriores que eran muy rígidas, la 4.0 se diseñó para ser más flexible y adaptarse a las nuevas tecnologías (como la nube y los pagos móviles).

Los puntos más concretos y relevantes de esta actualización son:

1. *El enfoque personalizado* (*Customized Approach):* el cambio más radical. PCI DSS obligaba a cumplir un control de una forma específica (enfoque definido). La versión 4.0 permite a las organizaciones diseñar su propio control de seguridad para cumplir con el objetivo de control, siempre que puedan demostrar que su solución es igual de efectiva. Esto es ideal para empresas que usan tecnologías innovadoras que el estándar no preveía.

2. *Autenticación y contraseñas:* la seguridad de los accesos se ha endurecido considerablemente. MFA en todo: el uso de autenticación multifactor (MFA) ahora es obligatorio para todos los accesos al entorno de datos de tarjetas (CDE), no solo para administradores o accesos remotos. Contraseñas robustas: Se aumentó la longitud mínima de las contraseñas de 7 a 12 caracteres. Cuentas de servicio: se exige una gestión estricta de las contraseñas de aplica-

ciones y cuentas de sistema, prohibiendo las contraseñas "quemadas" en el código.

3. *Frecuencia basada en riesgo:* en lugar de decirte "haz esto cada tres meses", muchos requisitos ahora dicen que la organización debe definir la frecuencia basándose en su propio análisis de riesgos. Esto alinea a PCI DSS con marcos como ISO 27001 o NIST, obligando a la empresa a entender sus amenazas en lugar de solo seguir una lista de tareas.

4. *Nuevos controles técnicos específicos seguridad de scripts (e-commerce):* se añadieron requisitos para gestionar y autorizar todos los scripts que se ejecutan en el navegador del cliente (para evitar ataques tipo *magecart* o robo de datos en el carrito de compras). Revisiones de código: se enfatiza la seguridad en el desarrollo de software (DevSecOps), exigiendo revisiones manuales o automáticas de cualquier cambio en las aplicaciones que tocan pagos.

Factor Analysis of Information Risk (FAIR)

El modelo Factor Analysis of Information Risk conocido como modelo FAIR es el estándar internacional de referencia para la cuantificación del riesgo de ciberseguridad en términos financieros (The Open Group, 2020). A diferencia de otros marcos que utilizan escalas cualitativas (como alto, medio o bajo), FAIR descompone el riesgo en variables medibles, como la frecuencia de los eventos de amenaza y la magnitud de la pérdida probable. Esto permite a los CISO y directivos traducir las amenazas técnicas en dólares, euros o pesos, facilitando una toma de decisiones informada basada en el análisis de costo-beneficio y priorizando las inversiones donde realmente tendrán un mayor impacto económico para la organización.

HITRUST (Salud)

El Health Information Trust Alliance (HITRUST) es un marco de cumplimiento integral que unifica múltiples estándares (como HIPAA, NIST, ISO y PCI) en un solo modelo de control escalable

llamado HITRUST CSF. Aunque nació con un enfoque muy fuerte en el sector salud para garantizar la protección de datos médicos sensibles, su arquitectura se ha expandido a otras industrias debido a su riguroso proceso de certificación y su capacidad para "mapear" diferentes regulaciones en un solo lugar (HITRUST Alliance, 2023).

Obtener una certificación HITRUST es considerado uno de los logros más exigentes en ciberseguridad, ya que requiere una validación externa estricta que garantiza que los controles no solo existen, sino que operan de manera efectiva y medible.

Agencia de la Unión Europea para la Ciberseguridad (ENISA)

A diferencia de ser un único estándar rígido, el enfoque de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) funciona como el motor de la ciberseguridad en la Unión Europea, proporcionando marcos de certificación y directrices estratégicas que armonizan la protección digital en todos los Estados miembros. Su papel es fundamental para la implementación de la Directiva NIS2, ya que establece esquemas de certificación para productos y servicios TIC, además de ofrecer guías de higiene cibernética y marcos de competencias que permiten a las organizaciones europeas (especialmente infraestructuras críticas y PYMES) elevar su nivel de resiliencia frente a amenazas transfronterizas bajo un lenguaje común (ENISA, 2009, 2024).

ENISA desarrolla propuestas de esquemas de certificación de ciberseguridad (ENISA, 2026) a petición de la Comisión Europea o de los Estados miembros. El trabajo que la Agencia realiza a este fin cuenta con el apoyo de grupos de expertos (grupos de trabajo ad hoc). ENISA también colabora estrechamente con la comisión, las autoridades de los estados miembros y las partes interesadas pertinentes, tal como se define en la Ley de Ciberseguridad. Los esquemas de certificación a nivel de la UE establecen los requisitos técnicos, las normas y los procedimientos aplicables a los productos o servicios concretos.

La experiencia del sector, los comentarios constructivos y las opiniones consultivas del ecosistema de certificación se tienen en cuenta en cada etapa del proceso de desarrollo de los esquemas. El Programa de Trabajo Continuado de la Unión (PDU), un documento estratégico en el marco de la Ley de Ciberseguridad per-

mite a los fabricantes, las autoridades nacionales y los organismos de normalización estar bien preparados e informados sobre los próximos esquemas europeos de certificación de ciberseguridad y las prioridades regulatorias.

Federal Risk and Authorization Management Program (FedRAMP)

El Federal Risk and Authorization Management Program (FedRAMP) es el estándar para la seguridad en la nube del Gobierno de los Estados Unidos, diseñado para proporcionar un enfoque estandarizado y riguroso en la evaluación, autorización y monitoreo continuo de servicios *cloud* (FedRAMP, 2023, 2024). Su filosofía se basa en el principio de "evaluar una vez, reutilizar muchas", lo que permite que un proveedor de servicios en la nube (CSP) obtenga una autorización de seguridad (ATO) que sea válida para múltiples agencias federales.

Al estar fundamentado en los controles del NIST SP 800-53, FedRAMP garantiza que cualquier plataforma que maneje datos federales cumpla con niveles de seguridad extremadamente altos (bajo, moderado o alto), convirtiéndose en un requisito indispensable para los proveedores que desean operar en el sector público estadounidense.

OWASP SAMM y OWASP ASVS

El Open Worldwide Application Security Project (OWASP, son las siglas en inglés) es una organización internacional sin fines de lucro dedicada a mejorar la seguridad del software, especialmente de aplicaciones web y APIs y se distingue por ser una comunidad abierta y neutral dedicada a mejorar la seguridad del software a través de estándares, herramientas y guías prácticas. A diferencia de marcos de gobernanza como NIST o ISO, que ofrecen una visión organizacional de alto nivel, OWASP proporciona un enfoque técnico y operativo "en las trincheras", especializándose en proteger la capa de aplicación, que es el objetivo principal de la mayoría de los ciberataques actuales.

La principal fortaleza de OWASP radica en su capacidad para democratizar el conocimiento de seguridad mediante proyectos

emblemáticos como el OWASP Top 10, que identifica los riesgos más críticos para aplicaciones web, APIs y móviles. Su enfoque es puramente colaborativo y basado en datos reales del sector, lo que garantiza que sus recomendaciones sean actuales y relevantes. Además, ofrece marcos de trabajo avanzados como el ASVS (estándar de verificación para pruebas de seguridad) y el SAMM (modelo de madurez para el ciclo de vida de desarrollo), permitiendo que la seguridad se integre de forma natural en el desarrollo de software (DevSecOps) en lugar de ser un obstáculo externo.

Utilizar OWASP ofrece la ventaja competitiva de estandarizar la seguridad en todo el ciclo de vida del desarrollo, reduciendo drásticamente la probabilidad de brechas de datos costosas. Al ser recursos gratuitos y de código abierto, permite que organizaciones de cualquier tamaño implementen controles de alta calidad sin costos de licencias, facilitando además el cumplimiento de normativas rígidas como PCI DSS o GDPR, que suelen exigir pruebas de seguridad robustas en las aplicaciones. En resumen, OWASP transforma la ciberseguridad de una teoría abstracta en una serie de pasos accionables y medibles para los equipos técnicos.

Su proyecto más famoso, el OWASP Top 10, no es un marco de gobernanza (como NIST o ISO), sino un listado de riesgos críticos. En cambio, SAMM y ASVS sí lo son.

Software Assurance Maturity Model (OWASP SAMM)

Es un modelo de madurez diseñado para ayudar a las organizaciones a evaluar, formular e implementar una estrategia de seguridad de software que se integre en su ciclo de vida de desarrollo (SDLC) (OWASP Foundation, 2020):

> *¿Para qué sirve?:* permite que una institución sepa en qué nivel de seguridad está (del 0 al 3) y trace una hoja de ruta para mejorar.
>
> *Estructura:* se divide en cinco funciones de negocio (gobernanza, diseño, implementación, verificación y operaciones), y cada una tiene prácticas específicas.

Enfoque: estratégico, no te dice cómo programar una línea de código, sino cómo gestionar el equipo y los procesos para que el código sea seguro.

Application Security Verification Standard (*OWASP ASVS*)

Es un estándar de verificación que proporciona una lista detallada de requisitos y controles de seguridad técnicos. Es, esencialmente, una "guía de examen" para las aplicaciones (OWASP Foundation, 2021a):

¿Para qué sirve?: establece una base normalizada para probar los controles de seguridad técnica de una aplicación (como la autenticación, el manejo de errores o la criptografía).

Niveles: define tres niveles de seguridad:

- Nivel 1: seguridad básica (oportunista).
- Nivel 2: estándar para aplicaciones que manejan datos sensibles (defensa profunda).
- Nivel 3: para aplicaciones críticas (militar, salud, banca).

Enfoque: táctico y técnico, es la herramienta que usan los *pentesters* y desarrolladores para marcar una "lista de cotejo" (*checklist*) de seguridad.

Otros marcos de gobernanza y gestión de TI

Information Technology Infrastructure Library (*ITIL*)

Aunque es un marco de gestión de servicios de TI (ITSM), proporciona la estructura operativa necesaria para que la ciberseguridad sea sostenible y eficiente. A través de sus prácticas de gestión de incidentes, gestión de problemas y gestión de cambios, ITIL asegura que la seguridad no sea un esfuerzo aislado, sino una parte integral del ciclo de vida del servicio; esto permite que las respuestas ante ataques sean coordinadas, que los cambios en la infraestructura no introduzcan nuevas vulnerabilidades y que exista una mejora continua alineada siempre con las necesidades del negocio (AXELOS, 2019).

Control Objectives for Information and Related Technologies (COBIT)

El marco de Control Objectives for Information and Related Technologies (COBIT), actualmente en su versión COBIT 2019, se distingue de otros marcos de ciberseguridad porque no se enfoca únicamente en la protección técnica, sino en el gobierno y gestión de la información y la tecnología (I&T) en su totalidad. Desde la perspectiva de ciberseguridad, COBIT actúa como el paraguas que conecta los objetivos de negocio con las operaciones de seguridad, asegurando que las inversiones en tecnología estén alineadas con la estrategia de la empresa, que los riesgos sean optimizados y que los recursos se utilicen de manera eficiente (ISACA, 2018a).[4]

A diferencia del NIST CSF o los Controles CIS, que son más específicos en "qué hacer" para asegurar sistemas, COBIT define 40 objetivos de gobierno y gestión organizados en cinco dominios. Para un profesional de ciberseguridad, COBIT es fundamental porque proporciona la estructura necesaria para que la seguridad no sea un silo aislado, sino una parte integral del ciclo de vida de la empresa. Esto se logra mediante el uso de componentes como procesos, estructuras organizativas, flujos de información y, crucialmente, la cultura y el comportamiento, permitiendo que la seguridad sea auditable y medible desde la junta directiva.

Una de las mayores fortalezas de COBIT 2019 es su capacidad de personalización mediante "factores de diseño". Esto permite que una organización adapte su programa de ciberseguridad considerando su perfil de riesgo específico, el panorama de amenazas actual y sus requisitos de cumplimiento. Al implementar COBIT, una empresa puede integrar fácilmente otros estándares como ISO/IEC 27001 o NIST, utilizando a COBIT como el traductor que explica a los altos ejecutivos cómo esos controles técnicos están protegiendo realmente el valor del negocio.

Capability Maturity Model Integration (CMMI)

El Capability Maturity Model Integration (CMMI) es un modelo de mejora de procesos orientado a incrementar la madurez y capacidad organizacional en el desarrollo, adquisición y gestión de servicios

[4] Sostiene que las políticas son componentes del sistema de gobernanza y deben estar alineadas con las prioridades de la junta directiva.

y productos. A través de áreas de práctica como gestión de riesgos (*Risk Management*), gestión de procesos (*Process Management*) y aseguramiento de la calidad (*Quality Assurance*), CMMI promueve la estandarización, medición y mejora continua de los procesos críticos del negocio. Esto permite a las organizaciones reducir la variabilidad operativa, mejorar la previsibilidad y asegurar que las actividades se ejecuten de manera consistente y controlada (CMII, 2018).

En el ámbito de la ciberseguridad, CMMI contribuye indirectamente pero de forma significativa al fortalecer la gobernanza de procesos relacionados con la gestión de riesgos, la respuesta a incidentes y la protección de la información. Un mayor nivel de madurez implica que los controles de seguridad están definidos, documentados, medidos y mejorados de manera sistemática, lo que facilita la integración de prácticas de seguridad en el ciclo de vida de los sistemas y servicios, reduciendo la probabilidad y el impacto de incidentes de seguridad.

Open Group Architecture Framework (TOGAF)

El Open Group Architecture Framework (TOGAF) es un marco de referencia para el desarrollo y la gestión de arquitecturas empresariales (The Open Group, 2022), cuyo núcleo es el Architecture Development Method (ADM).

TOGAF permite alinear la estrategia del negocio con las arquitecturas de negocio, datos, aplicaciones y tecnología, proporcionando una visión integral y estructurada del ecosistema organizacional. Este enfoque facilita la toma de decisiones coherentes y sostenibles en entornos complejos y cambiantes.

Desde la perspectiva de la ciberseguridad, TOGAF integra la seguridad como un atributo transversal de la arquitectura empresarial, permitiendo diseñar controles de seguridad desde las fases tempranas del diseño arquitectónico (*Security by Design*). Al incorporar requisitos de seguridad en cada dominio arquitectónico, TOGAF ayuda a identificar riesgos, definir arquitecturas seguras y asegurar que las soluciones tecnológicas cumplan con políticas, normativas y objetivos de protección de la información, fortaleciendo así la postura de ciberseguridad de la organización.

ESTRATEGIA DE CIBERSEGURIDAD

En el entorno digital actual, donde la información se ha consolidado como el activo más crítico de cualquier organización, la implementación de una estrategia de ciberseguridad trasciende el ámbito técnico para convertirse en un imperativo de supervivencia y gobernanza corporativa.

Las estrategias de ciberseguridad son fundamentales para cualquier institución, ya que proporcionan una visión integral y de largo plazo sobre cómo proteger sus activos más críticos en un entorno digital cada vez más complejo. Su existencia responde a la necesidad de establecer una dirección clara, definir prioridades y articular un enfoque coherente frente a amenazas que evolucionan constantemente.

Sin una estrategia formal, las acciones de seguridad suelen ser reactivas, descoordinadas o insuficientes, lo que incrementa la exposición a riesgos operativos, financieros y reputacionales.

Además, una estrategia de ciberseguridad ayuda a las instituciones a alinear sus objetivos de protección con la misión del negocio, optimizar recursos, y garantizar que las decisiones de seguridad estén respaldadas por criterios de riesgo bien definidos. Facilita la asignación de responsabilidades, la adopción de tecnologías adecuadas y la implementación de controles efectivos.

También permite medir el progreso, fortalecer la resiliencia y asegurar el cumplimiento con regulaciones y marcos normativos. En conjunto, estas estrategias proporcionan un camino estructurado para construir un entorno seguro, confiable y sostenible a lo largo del tiempo.

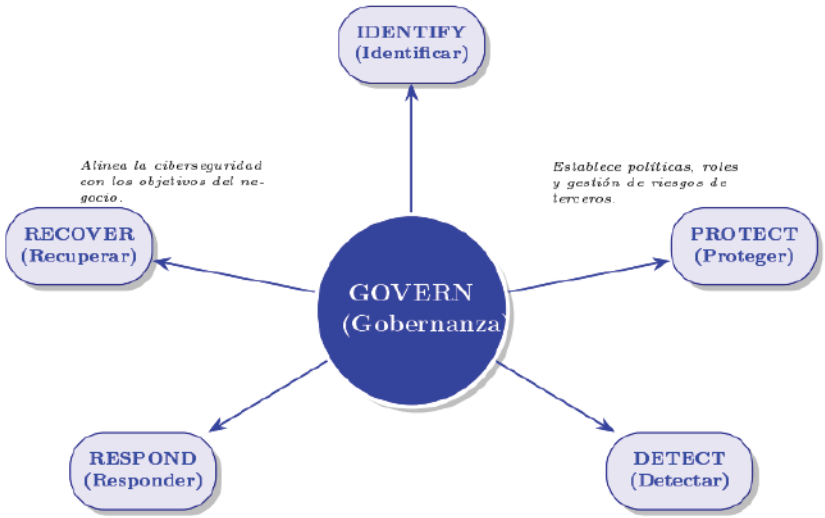
Como se vio en el capítulo anterior, el NIST, se compone de seis funciones en el *Core*, una de ellas la de gobernanza, poner la ciberseguridad enmarcada en la gobernanza del negocio.

Razón de la gobernanza en el NIST

Gobernanza significa que la organización define, comunica y supervisa su estrategia de gestión de riesgos cibernéticos, sus políticas, expectativas, y la toma de decisiones en seguridad y no se debe de confundir con gobierno[5] (NIST, 2024b).

Con su inclusión en CSF 2.0, la ciberseguridad deja de ser solo una cuestión técnica o de TI, se integra como una función de gobernanza empresarial, con visibilidad para la dirección, cumplimiento normativo, y toma de decisiones estratégicas.

Figura 4. GOV del NIST 2.0 y conexiones con las otras funciones



Fuente: elaboración propia.

Metas

EL NIST CSF 2.0 ayuda a tu estrategia de ciberseguridad con los siguientes puntos:

[5] El gobierno es quien tiene la autoridad; la gobernanza es el sistema de reglas y prácticas que se utiliza para ejercer esa autoridad de forma efectiva y transparente.

1. *Da una estructura ordenada:* te guía paso a paso para identificar riesgos, proteger activos, detectar incidentes, responder y recuperarte. Esto evita improvisaciones y alinea las acciones con los objetivos de negocio.
2. *Facilita la priorización:* te ayuda a invertir tiempo y recursos en los riesgos más críticos, según su impacto en tus operaciones.
3. *Promueve la mejora continua:* permite evaluar periódicamente tu madurez en ciberseguridad y ajustar la estrategia según los cambios tecnológicos o del negocio.
4. *Alinea la seguridad con la gestión empresarial:* la ciberseguridad se convierte en parte del gobierno corporativo, igual que las finanzas o la calidad.

Objetivos

Esta nueva función tiene como objetivo integrar la ciberseguridad en la toma de decisiones estratégicas. Incluye aspectos como:

- *Políticas y roles:* definir políticas claras y asignar responsabilidades de seguridad. Establece liderazgo y rendición de cuentas.
- *Gestión de riesgos:* integrar la ciberseguridad en la gestión general de riesgos del negocio. Permite equilibrar seguridad y objetivos comerciales.
- *Cumplimiento y regulaciones:* alinear la estrategia con normas legales y estándares. Reduce riesgos legales y reputacionales.
- *Cultura y capacitación:* fomentar la conciencia de seguridad en todo el personal. Fortalece la defensa humana ante ataques.
- *Supervisión y métricas:* medir y reportar el desempeño de la seguridad al liderazgo. Facilita la toma de decisiones informadas.

La función de gobernanza establece y monitorea la estrategia de gestión de riesgos de ciberseguridad, las expectativas y las políticas de la organización. Imagina que las otras cinco funciones (identificar, proteger, detectar, responder, recuperar) son el motor

y las ruedas del coche. La gobernanza es el volante y el conductor; define hacia dónde va el coche, a qué velocidad (apetito de riesgo) y quién es responsable de qué. Su objetivo principal es asegurar que la estrategia de seguridad esté alineada con la misión y los objetivos del negocio.

Categorías principales

En el NIST CSF 2.0, la función de gobernanza (GV) se divide en seis categorías principales (NIST, 2024b). Estas categorías están diseñadas para asegurar que la estrategia de ciberseguridad esté alineada con los objetivos de negocio y las obligaciones legales.

Contexto organizacional (GV.OC)

Aquí es donde la seguridad se encuentra con la realidad del negocio. No puedes proteger lo que no entiendes.

> *¿Qué define?:* la misión, visión y los valores de la organización.
>
> *Stakeholders:* identifica quiénes son las partes interesadas (clientes, reguladores, inversores) y qué esperan de la seguridad.
>
> *Dependencias:* entiende las dependencias críticas (legales, regulatorias, contractuales) que afectan las decisiones de ciberseguridad.

Estrategia de gestión de riesgos (GV.RM)

Esta categoría define las prioridades y cómo la empresa siente el riesgo.

> *Apetito y tolerancia al riesgo:* ¿cuánto riesgo estamos dispuestos a aceptar para lograr nuestros objetivos? (Por ejemplo, una *startup fintech* puede aceptar más riesgo en innovación que un banco central).

Priorización: establece qué riesgos deben tratarse primero basándose en su impacto potencial al negocio.

Roles, responsabilidades y autoridades (GV.RR)

Define el quién es quién en la ciberseguridad. El objetivo es eliminar la ambigüedad.

Liderazgo: asigna responsabilidades claras a la alta dirección y a la junta directiva (*Board*).

Operativo: define quién es responsable de ejecutar las tareas de seguridad y quién tiene la autoridad para tomar decisiones críticas (como apagar un servidor infectado).

Cultura: fomenta una cultura donde la ciberseguridad es responsabilidad de todos, no solo del departamento de TI.

Políticas (GV.PO)

Es el marco legal interno. Aquí se establecen, comunican y actualizan las reglas del juego.

Creación: desarrollo de políticas de seguridad alineadas con los riesgos (por ejemplo, Política de contraseñas, Política de acceso remoto).

Comunicación: asegurar que todos los empleados conozcan y entiendan estas políticas.

Revisión: actualizar las políticas regularmente para adaptarse a nuevas amenazas o cambios en la tecnología.

Supervisión (GV.OV)

Es el mecanismo de control. No basta con decir qué hacer, hay que verificar que se haga y que funcione.

Métricas y KPIs: monitoreo del desempeño de la estrategia de ciberseguridad.

Ajustes: si las métricas muestran que algo no funciona, la estrategia se ajusta.

Reporte: informar a la alta dirección sobre la postura de seguridad actual de manera clara y sin tecnicismos excesivos.

Gestión de riesgos en la cadena de suministro (GV.SC)

Esta es una adición crítica. Reconoce que el riesgo no termina en las paredes de tu empresa.

Proveedores: establece procesos para identificar, evaluar y gestionar los riesgos asociados con proveedores externos y socios.

Ciclo de vida: incluye requisitos de seguridad en los contratos y monitorea a los proveedores durante toda la relación comercial.

Importancia de este cambio en el NIST

Antes, la ciberseguridad se veía como algo que hace el equipo de TI en el sótano. Con la nueva función de gobernanza:

- *Involucra a la directiva:* obliga a los líderes de negocio a tomar decisiones sobre ciberseguridad.
- *Lenguaje común:* traduce los riesgos técnicos (vulnerabilidad en el puerto 80) a riesgos de negocio (posible pérdida de datos de clientes y multas regulatorias).
- *Responsabilidad compartida:* deja claro que la gestión de riesgos en la cadena de suministro (*Supply Chain*) es un tema de gobernanza estratégica, no solo de compras.

Tabla 5. Diferencia clave: gestión vs. gobernanza

Gestión	Gobernanza
Pregunta: ¿estamos haciendo las cosas correctamente?	Pregunta: ¿estamos haciendo las cosas correctas?
Enfoque: operativo/táctico	Enfoque: estratégico
Responsable: CISO Gerentes de TI, Analistas	Responsable: CEO Junta Directiva, Comité de Riesgos
Actividad: implementar controles, parchar, monitorear	Actividad: definir políticas, aprobar presupuesto, aceptar riesgo

Fuente: elaboración propia.

Preguntas para definir tu estrategia de ciberseguridad:

1. *Contexto organizacional:*
   Pregunta: ¿qué activos, procesos y servicios son esenciales para los objetivos del negocio?
   Define qué es lo más valioso para la organización (datos, sistemas, reputación, clientes).
   Esto te permite enfocar la estrategia en lo realmente crítico.

2. *Rol del liderazgo:*
   Pregunta: ¿quién tiene la responsabilidad final de la ciberseguridad dentro de la empresa?
   Determina roles: alta dirección, CISO, TI, cumplimiento, etcétera. Establece líneas claras de autoridad y comunicación.

3. *Políticas y principios:*
   Pregunta: ¿existen políticas de ciberseguridad documentadas y aprobadas por la dirección?
   Si no, crea un conjunto de políticas que definen comportamientos, accesos y controles mínimos.
   Asegúrate de que estén alineadas con los objetivos del negocio.

4. *Integración con la gestión de riesgos empresariales:*
   Pregunta: ¿cómo se integra la ciberseguridad en el marco general de gestión de riesgos corporativos?
   Evalúa si los riesgos cibernéticos se gestionan igual que los financieros u operativos. Promueve que el riesgo cibernético sea tema de junta o comité de riesgo.

5. *Apetito y tolerancia al riesgo:*
   Pregunta: ¿qué nivel de riesgo cibernético está dispuesto a aceptar tu empresa?
   Define umbrales medibles (por ejemplo, tiempo máximo de inactividad, pérdidas financieras tolerables). Esto guiará decisiones sobre inversión en seguridad.

6. *Cumplimiento y regulaciones:*
   Pregunta: ¿qué leyes, normas o marcos aplican a tu negocio (por ejemplo, GDPR, ISO 27001, Ley de Protección de Datos)?
   Evalúa brechas y define un plan de cumplimiento.
   Esto asegura que la estrategia sea legalmente sólida y auditable.

7. *Cultura y concienciación:*
   Pregunta: ¿qué nivel de conocimiento de ciberseguridad tiene el personal?
   Desarrolla un plan de capacitación continuo con campañas, simulaciones y métricas. Una buena cultura reduce el riesgo humano.

8. *Medición y métricas:*
   Pregunta: ¿cómo se mide el desempeño y madurez de la ciberseguridad?
   Define indicadores clave (KPIs o KRIs): incidentes detectados, tiempo de respuesta, cumplimiento de políticas, etcétera.
   Permite monitorear progreso y justificar inversiones.

9. *Comunicación y reporte:*
   Pregunta: ¿cómo se informan los riesgos y resultados de seguridad al liderazgo y partes interesadas?
   Establece un formato de reporte periódico al directorio o comité. Esto mantiene la ciberseguridad visible y priorizada.

10. *Mejora continua y supervisión:*
    Pregunta: ¿con qué frecuencia se revisa y actualiza la estrategia de ciberseguridad?
    Programa revisiones anuales o tras cambios importantes. El entorno cambia, por eso el marco debe evolucionar.

Al responder estas diez preguntas y documentar tus respuestas, tendrás los pilares de una estrategia de ciberseguridad alineada con el NIST CSF 2.0 (función *Govern*):

- Gobernanza clara.
- Riesgos identificados y gestionados.
- Políticas actualizadas.
- Cultura organizacional fortalecida.

Resumen de una estrategia de ciberseguridad

Una estrategia de ciberseguridad debe abordar de forma integral los aspectos organizativos, técnicos y humanos de la seguridad de la información, alineándose con los objetivos del negocio y el perfil de riesgo de la organización.

Componentes principales

1. *Gobierno y liderazgo:*
   - Definición de roles y responsabilidades.
   - Políticas y marcos de referencia (NIST, ISO/IEC 27001).
   - Gestión de proveedores y terceros.

2. *Gestión de riesgos:*
   - Identificación y clasificación de activos.
   - Análisis de amenazas, vulnerabilidades e impacto.
   - Tratamiento y seguimiento del riesgo.

3. *Controles y arquitectura de seguridad:*
   - Controles preventivos, de detección y correctivos.
   - Gestión de identidades y accesos (IAM, MFA).
   - Seguridad de redes, aplicaciones y datos.

4. *Operaciones de seguridad:*
   - Monitoreo y correlación de eventos (SIEM/XDR).
   - Gestión de vulnerabilidades y parches.
   - Respuesta a incidentes de seguridad.

5. *Continuidad del negocio:*
   - Planes de continuidad y recuperación ante desastres.
   - Definición de RPO y RTO.
   - Pruebas periódicas de resiliencia.

6. *Personas y cultura:*
   - Programas de concienciación y capacitación.
   - Formación específica por rol.
   - Cultura de seguridad y reporte de incidentes.

7. *Cumplimiento y mejora continua:*
   - Cumplimiento normativo y auditorías.
   - Métricas, indicadores y lecciones aprendidas.
   - Revisión y actualización de la estrategia.

POLÍTICA DE CIBERSEGURIDAD

Las políticas de ciberseguridad no pueden existir sin un marco general de Gobernanza que diga (ISACA, 2018b; ISO/IEC, 2020; NIST, 2024b):

- Quién aprueba políticas.
- Quién las revisa y cada cuánto.
- Quién tiene autoridad para exigir cumplimiento.
- Quién es el dueño del riesgo (no siempre el área de TI).
- Estructura de roles: Junta directiva, CISO, áreas de negocio, auditoría.

Adicionalmente se debe incluir estos dos componentes: el ecosistema organizacional y los temas técnicos centrales.

El ecosistema organizacional

Representa la intrincada red de relaciones, procesos y actores que definen cómo una institución interactúa con el riesgo digital. Ya no es posible visualizar la seguridad de la información como una barrera técnica aislada; en su lugar, debe entenderse como un organismo vivo donde convergen la cultura corporativa, los objetivos estratégicos y el cumplimiento normativo. En este entorno, cada colaborador, desde la alta dirección hasta el personal operativo, actúa como un nodo crítico cuya conciencia y comportamiento determinan la resiliencia general de la estructura frente a amenazas cada vez más sofisticadas.

Comprender este ecosistema implica reconocer que la política de ciberseguridad no opera en el vacío, sino que debe estar en simbiosis con el contexto dinámico de la organización. Esto incluye la gestión de las expectativas de las partes interesadas, la integra-

ción transparente con los proveedores de la cadena de suministro y la adaptación constante a un marco legal en evolución. Al adoptar una visión ecosistémica, la organización deja de reaccionar de forma fragmentada ante los incidentes y comienza a cultivar un entorno de gobernanza robusto, donde la seguridad es un habilitador del negocio y no un obstáculo para la innovación.

Alineación estratégica y gestión de riesgos

Antes de escribir una sola regla, necesitas definir el por qué y el cuánto.

> *Apetito de riesgo* (*Risk Appetite):* ¿cuánto riesgo está dispuesta a tolerar la organización para alcanzar sus objetivos? No se puede blindar todo al 100 %; definir esto ayuda a priorizar presupuestos.
>
> *Clasificación de activos:* no toda la información vale lo mismo. Necesitas una política de clasificación de la información (por ejemplo, pública, interna, confidencial, secreta). Sin esto, aplicarás medidas costosas a datos irrelevantes o medidas débiles a datos críticos.
>
> *Alineación con el negocio:* las políticas no deben impedir la operación. Deben estar alineadas con los objetivos comerciales para evitar que los usuarios busquen atajos (Shadow IT) (ISACA, 2019[6]; ISO/IEC, 2022c).

Marco normativo y cumplimiento (*Compliance)*

Las políticas no existen en el vacío, deben responder a leyes y estándares externos.

> Marcos de referencia (*Frameworks*): no inventes la rueda. Basa tus políticas en estándares reconocidos como ISO 27001, NIST CSF o CIS Controls. Esto da validez ante auditorías.

[6] Enfatiza la alineación entre el riesgo de TI y el riesgo empresarial (ERM).

Regulaciones locales e Internacionales: dependiendo de tu industria y ubicación, debes integrar requisitos de leyes como GDPR (Europa), LFPDPPP (México), HIPAA (Salud), o PCI-DSS (Pagos).

Respuesta y resiliencia

Asumir que nos van a atacar es más realista que pensar que vamos a bloquear todo.

Plan de respuesta a incidentes (IRP): ¿a quién se llama a las 3:00 AM si hay una brecha? La política debe definir roles, canales de comunicación y tiempos de respuesta.

Continuidad de negocio y recuperación (DRP): políticas sobre copias de seguridad (respaldos), pruebas de restauración y cómo operar si los sistemas principales caen.

El factor humano (cultura y sanciones)

Definir los diferentes tipos de usuarios.

Régimen sancionador: para que una política sea ley, debe haber consecuencias por incumplimiento. Esto debe estar alineado con Recursos Humanos y el departamento legal.

Ingeniería social y Concientización: política de formación continua. No basta con un curso al año; se requiere definir pruebas de *phishing* y métricas de capacitación.

Política de escritorio limpio y pantalla limpia: a menudo olvidada, pero crucial para la seguridad física en oficinas o trabajo híbrido.

Gestión del cambio y ciclo de vida

Frecuencia de actualización de las políticas.

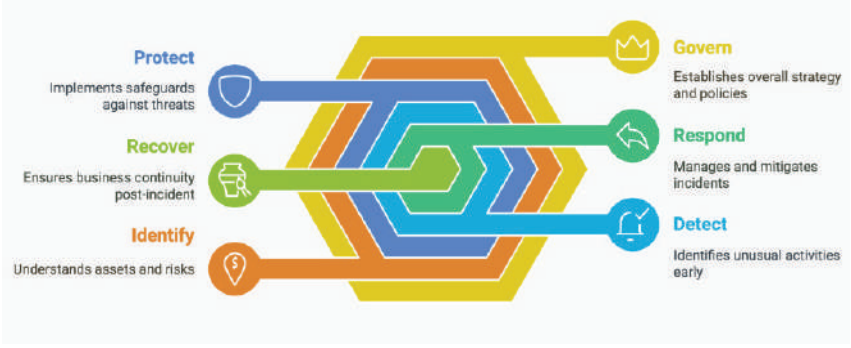
Gestión de cambios: política para asegurar que cualquier cambio en la infraestructura (actualizar un servidor, cambiar un *firewall*) pase por un proceso de aprobación y análisis de seguridad previo.

Auditoría y revisión: definir cada cuánto tiempo se revisan las políticas (mínimo anualmente o tras cambios significativos) y quién es el responsable de auditarlas.

Los temas técnicos centrales

Diagrama NIST CSF 2.0

Figura 5. Funciones del NIST CSF 2.0



Fuente: Katai (2025).

Gestión de identidades y accesos (IAM)

La gestión de identidades y acceso (IAM, por sus siglas en inglés *Identity and Access Management*), es el conjunto de procesos, políticas y tecnologías que permiten: 1) identificar a los usuarios y sistemas; 2) autenticarlos (confirmar que son quienes dicen ser): 3) autorizar qué pueden hacer o a qué pueden acceder, y 4) Registrar y auditar sus acciones. En resumen: identificar, autenticar, autorizar y registrar.

Los componentes típicos de IAM son:

» Identidades (usuarios, roles, servicios, máquinas).
» Autenticación (*passwords*, MFA, biometría).
» Autorización (roles RBAC, permisos, políticas).
» Single Sign-On (SSO).
» Gestión del ciclo de vida de usuarios.
» Aprovisionamiento y desaprovisionamiento.
» Zero Trust aplicado a acceso.

En el anexo A.1.1 y A.1.2 se presenta dos ejemplos de almacén de contraseñas con SALT, usando los algoritmos de PBKDF2WithHmacSHA512 nativo en Java y el de Argon2 con la librería de org.bouncycastle.crypto (The Legion of the Buncy Castle, s.f.). El estándar técnico que utiliza Google Authenticator –el protocolo TOTP de la IETF– se encuentra disponible en internet (Google s.f.).[7]

Modelo CIA (Confidentiality, Integrity, Availability)

El modelo de confidencialidad, integridad y disponibilidad conocido como modelo CIA (*Confidentiality, Integrity, Availability*) es uno de los modelos fundamentales de la seguridad de la información (NIST, 2017; Stallings, 2017).

C.- Confidencialidad

La información solo puede ser accedida por personas o sistemas autorizados. Ejemplos: encriptación, control de accesos y clasificación de la información.

I.- Integridad

La información debe mantenerse correcta, completa y sin alteraciones no autorizadas. Ejemplos: *hashing*, control de versiones, firmas digitales y detección de manipulación.

[7] Más detalles en Tecnologías relacionadas/Validación multifactor de la presente obra.

A.- Disponibilidad

La información y los sistemas deben estar accesibles cuando se necesitan. Ejemplos: redundancia, respaldos (*backups*), protección contra DDoS, alta disponibilidad (HA).

Cultura organizacional

La cultura organizacional es, en última instancia, el sistema operativo invisible que determina si una política de ciberseguridad será un éxito o simplemente un documento olvidado en un cajón.

La cultura organizacional actúa como el catalizador crítico que transforma las directrices de seguridad de meras imposiciones normativas en hábitos operativos arraigados. En una organización donde la seguridad está integrada en los valores compartidos, los empleados no solo cumplen con las políticas por temor a sanciones, sino que las adoptan como parte de su responsabilidad profesional.

Esta "cultura de ciberseguridad" es la que permite que el personal se convierta en una red de sensores activos capaces de detectar anomalías y reportar incidentes de manera proactiva, cerrando la brecha entre la seguridad teórica definida por la gerencia y la ejecución técnica en el día a día.

Por el contrario, una cultura organizacional débil o indiferente puede neutralizar incluso las inversiones tecnológicas más sofisticadas. Si la alta dirección no proyecta un compromiso auténtico con la protección de los activos de información se genera una percepción de que la ciberseguridad es una carga burocrática o un obstáculo para la productividad. En este escenario, el factor humano deja de ser la primera línea de defensa para convertirse en el eslabón más vulnerable, donde el incumplimiento de las políticas se vuelve la norma y el riesgo se multiplica a través de acciones aparentemente inofensivas, pero sistémicamente peligrosas.

Factores clave de influencia

Los factores clave que influyen en la cultura de ciberseguridad pueden alinear a toda la plantilla hacia la resiliencia o, por el contrario, generar una inercia de negligencia difícil de revertir. El liderazgo ejemplar de la alta dirección establece el estándar ético y de

prioridad, mientras que los canales de comunicación determinan si las políticas son interpretadas como herramientas de empoderamiento o como manuales de restricción incomprensibles.

Al integrar incentivos positivos y mecanismos de retroalimentación en lugar de enfoques meramente punitivos, la organización logra que la ciberseguridad trascienda el cumplimiento técnico para convertirse en un fenómeno sociológico, donde la presión de grupo y el sentido de pertenencia actúan como los controles de seguridad más eficaces y menos costosos del sistema.

Los factores más importantes son:

» *Liderazgo con el ejemplo* (*Tone at the Top)*: si los directivos no usan MFA o comparten sus contraseñas, el resto de la organización no respetará la política.

» *Psicología del error:* una cultura que castiga el error humano severamente provoca que los empleados oculten los incidentes (como un clic en un link de *phishing*), impidiendo una respuesta rápida.

» *Comunicación interna:* las políticas deben redactarse en un lenguaje que el ecosistema organizacional entienda, alejándose del tecnicismo excesivo para lograr una verdadera apropiación.

Métricas y evaluación de la madurez cultural

La medición de la madurez en ciberseguridad no debe limitarse a indicadores técnicos de rendimiento (KPI), sino que debe incorporar indicadores de comportamiento y actitud que reflejen el estado real del ecosistema organizacional.

Un modelo de madurez robusto permite a la dirección visualizar la evolución desde un estado reactivo, donde la seguridad se percibe como un evento externo y punitivo, hacia un estado adaptativo o resiliente, donde la protección de la información es un valor intrínseco de la identidad corporativa. Esta transición es cuantificable mediante la observación de patrones de cumplimiento, la velo-

cidad de reporte de incidentes sospechosos y el nivel de autonomía de los colaboradores ante dilemas de seguridad (NIST, 2008).[8]

Para evaluar esta madurez de manera sistémica, las organizaciones pueden apoyarse en tres dimensiones de análisis:

Dimensión 1 *Dimensión cognitiva* (*conocimiento):* evalúa qué tanto comprenden los empleados los riesgos específicos de su rol y las políticas que los mitigan. No se mide solo con exámenes teóricos, sino con la capacidad de aplicar conceptos en situaciones simuladas.

Dimensión 2 *Dimensión afectiva* (*actitud):* mide la disposición y el compromiso emocional hacia la seguridad. Se evalúa mediante encuestas de percepción que revelan si los empleados consideran que la seguridad es una prioridad compartida o una barrera para su trabajo.

Dimensión 3 *Dimensión conductual* (*comportamiento):* métrica más crítica, pues registra las acciones reales. Se analiza a través de pruebas de ingeniería social controlada, auditoría de escritorio limpio y, fundamentalmente, la tasa de reportes voluntarios de anomalías.

[8] Provee un marco para el desarrollo y selección de métricas de seguridad.

Tabla 6. Niveles de madurez de la seguridad

Nivel de madurez	Percepción del empleado	Comportamiento típico
1. Inicial	La seguridad es el problema de TI.	Se ignoran las políticas; el error se oculta por miedo.
2. Definido	Sé que hay reglas, pero son molestas.	Cumplimiento mínimo para evitar sanciones.
3. Consciente	Entiendo mi rol en la protección.	Participación activa en capacitaciones y reportes.
4. Resiliente	La seguridad es parte de mi trabajo diario.	Vigilancia mutua y mejora continua de procesos.

Fuente: elaboración propia.

Difusión de la política

La difusión de la política de ciberseguridad representa el puente crítico entre la gobernanza estratégica y la realidad operativa. Una política que no se comunica de manera efectiva es, a efectos prácticos, una política inexistente. Por ello, la institución debe trascender la publicación pasiva y adoptar un modelo de comunicación proactivo y multicanal, donde el lenguaje técnico se traduzca en comportamientos cotidianos.

La meta de la difusión no es el conocimiento memorístico del documento, sino la internalización de sus principios, logrando que cada miembro de la organización comprenda no solo el "qué" de las reglas, sino el "por qué" de su importancia para la supervivencia del ecosistema común (Nacimba, 2024).

Para que una política de ciberseguridad sea efectiva dentro del ecosistema organizacional no basta con su existencia legal. Debe ser accesible, comprensible y estar presente en la cotidianidad del empleado. Su difusión debe ser un proceso estratégico de comunicación, no un simple envío masivo de correos.

Aquí tienes los métodos y canales más efectivos para publicar y difundir la política:

1. *Canales de publicación oficial:* la política debe tener un hogar permanente y conocido por todos:

- » *Intranet corporativa:* un repositorio centralizado donde resida la versión más reciente del documento. Debe ser fácil de encontrar (máximo a tres clics de la página principal).
- » *Manual de bienvenida* (*Onboarding):* la política debe ser uno de los primeros documentos que un nuevo colaborador lea y firme. Esto establece la seguridad desde el primer día.
- » *Repositorios de cumplimiento:* para instituciones reguladas, debe estar disponible en las plataformas de gestión de cumplimiento (GRC) para facilitar auditorías.

2. *Estrategias de difusión y sensibilización:* la difusión busca que el contenido de la política sea accionable (ejecutable) para el personal no técnico:
   - » *Cápsulas de información* (*Microlearning):* en lugar de enviar el PDF de 50 páginas, se deben enviar infografía o videos cortos que resuman puntos clave (por ejemplo, cómo gestionar tu contraseña según la nueva política).
   - » *Campañas de gamificación:* utilizar cuestionarios con recompensas o simulacros de *phishing* para reforzar lo que la política dicta sobre la detección de amenazas.
   - » *Fondos de pantalla y salvapantallas:* utilizar el entorno visual de las estaciones de trabajo para mostrar recordatorios breves de las normas de seguridad más críticas.

CONTROLES DE CIBERSEGURIDAD

En este capítulo veremos los siguientes controles:

a) Controles CIS (CIS Controls) (CIS, 2025b).9
b) NIST SP 800-53 (Security and Privacy Controls) (NIST, 2020).
c) ISO 27002 define "controles de seguridad" organizados en cuatro temas y 93 controles (versión 2022) (ISO–IEC, 2022b).

Se recomienda iniciar por los CIS Controls, ya que son controles muy concretos y cuenta con un mapa de ruta que te facilita la implementación (CIS, 2024).

Controles CIS (CIS Controls)

Los 153 controles del CIS se clasifican en 18 categorías (CIS, 2026d), que son las siguientes:

[9] Los Controles Críticos de Seguridad CIS® (CIS Controls®) comenzaron como una sencilla actividad de base para identificar los ciberataques más comunes e importantes del mundo real que afectan a las empresas a diario, traducir ese conocimiento y experiencia en acciones positivas y constructivas para los defensores y, posteriormente, compartir esa información con un público más amplio.

Tabla 7. Resumen de las 18 categorías de controles CIS

No.	Título	Descripción
1	Inventario y control de activos empresariales	Gestionar activamente (inventariar, rastrear y corregir) todos los activos empresariales (dispositivos de usuario final, incluyendo portátiles y móviles; dispositivos de red; dispositivos no informáticos/de Internet de las Cosas (IoT); y servidores) conectados a la infraestructura de forma física, virtual y remota, así como en entornos de nube, para conocer con precisión la totalidad de los activos que necesitan ser monitoreados y protegidos dentro de la empresa. Esto también permitirá identificar activos no autorizados y no administrados para su eliminación o remediación.
2	Inventario y control de activos de software	Gestionar activamente (inventariar, rastrear y corregir) todo el software (sistemas operativos y aplicaciones) en la red para que solo se instale y pueda ejecutar software autorizado, y para que se detecte y se evite la instalación o ejecución de software no autorizado y no administrado.
3	Protección de datos	Desarrollar procesos y controles técnicos para identificar, clasificar, gestionar, conservar y eliminar datos de forma segura.
4	Configuración segura de activos y software empresariales	Establecer y mantener la configuración segura de los activos empresariales (dispositivos de usuario final, incluyendo portátiles y móviles; dispositivos de red; dispositivos no informáticos/de Internet de las Cosas (IoT); y servidores) y el software (sistemas operativos y aplicaciones).

No.	Título	Descripción
5	Gestión de cuentas	Utilice procesos y herramientas para asignar y gestionar la autorización de credenciales para cuentas de usuario, incluyendo cuentas de administrador y cuentas de servicio, para activos y software empresariales.
6	Gestión del control de acceso	Utilice procesos y herramientas para crear, asignar, gestionar y revocar credenciales y privilegios de acceso para cuentas de usuario, administrador y servicio para activos y software empresariales.
7	Gestión continua de vulnerabilidades	Desarrolle un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos empresariales dentro de la infraestructura de la empresa, con el fin de remediar y minimizar la ventana de oportunidad para los atacantes. Supervise las fuentes públicas y privadas del sector para obtener nueva información sobre amenazas y vulnerabilidades.
8	Gestión de registros de auditoría	Recopile, alerte, revise y conserve registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.
9	Protección de correo electrónico y navegadores web	Mejore la protección y la detección de amenazas provenientes del correo electrónico y la web, ya que estas representan oportunidades para que los atacantes manipulen el comportamiento humano mediante interacción directa.
10	Defensa contra *malware*	Prevenga o controle la instalación, propagación y ejecución de aplicaciones, código o scripts maliciosos en los activos empresariales

No.	Título	Descripción
11	Recuperación de datos	Establezca y mantenga prácticas de recuperación de datos suficientes para restaurar los activos empresariales dentro del alcance a un estado de confianza previo al incidente.
12	Gestión de la infraestructura de red	Establecer, implementar y gestionar activamente (rastrear, informar y corregir) los dispositivos de red para evitar que los atacantes exploten los servicios de red y puntos de acceso vulnerables.
13	Monitoreo y defensa de la red	Implementar procesos y herramientas para establecer y mantener una supervisión integral de la red y una defensa contra amenazas de seguridad en toda la infraestructura de red y la base de usuarios de la empresa.
14	Capacitación en seguridad y concientización	Establecer y mantener un programa de concienciación sobre seguridad para influir en el comportamiento del personal, con el fin de que sea consciente de la seguridad y cuente con las habilidades necesarias para reducir los riesgos de ciberseguridad para la empresa.
15	Gestión de proveedores de servicios	Desarrollar un proceso para evaluar a los proveedores de servicios que poseen datos confidenciales o son responsables de las plataformas o procesos de TI críticos de una empresa, a fin de garantizar que estos proveedores protejan dichas plataformas y datos adecuadamente.

No.	Título	Descripción
16	Seguridad del software de aplicación	Gestionar el ciclo de vida de la seguridad del software desarrollado, alojado o adquirido internamente para prevenir, detectar y remediar las vulnerabilidades de seguridad antes de que afecten a la empresa.
17	Gestión de la respuesta a incidentes	Establecer un programa para desarrollar y mantener una capacidad de respuesta a incidentes (por ejemplo, políticas, planes, procedimientos, roles definidos, capacitación y comunicaciones) para prepararse, detectar y responder rápidamente a un ataque.
18	Pruebas de penetración	Poner a prueba la eficacia y la resiliencia de los activos empresariales mediante la identificación y explotación de debilidades en los controles (personas, procesos y tecnología) y simulando los objetivos y acciones de un atacante.

Fuente: elaboración propia con base en CIS (2026d).

Cada una de estas categorías contiene varios controles, lo que totaliza 153. Todos estos controles se dividen en seis funciones.

Tabla 8. Funciones de los controles CIS

Función	Cantidad
Detectar	24
Gobernar	25
Identificar	14
Proteger	78
Recuperar	6
Responder	6
TOTAL	153

Fuente: elaboración propia.

Cada uno de estos controles aplica a una tipo de activo en concreto (algunos controles pueden aplicar a más de un tipo, pero un activo es el principal y es en el que se clasifica).

Tabla 9. Tipos de Activos de los controles CIS

Tipo de Activo	Cantidad
Datos	32
Dispositivos	25
Documentación	20
Redes	23
Software	24
Usuarios	29
TOTAL	153

Fuente: elaboración propia.

NIST SP 800-53

El NIST SP 800-53 es un catálogo integral de controles de seguridad y privacidad diseñado para proteger sistemas de información y datos organizacionales (NIST, 2020), especialmente en entornos gubernamentales y empresariales con altos requisitos de seguridad. Sus controles se organizan en familias que cubren aspectos clave como control de acceso, auditoría y rendición de cuentas, gestión de configuración, identificación y autenticación, evaluación de riesgos, protección de sistemas y comunicaciones, y respuesta a incidentes. Este enfoque estructurado permite a las organizaciones seleccionar e implementar controles de manera coherente, alineándolos con su nivel de riesgo, criticidad de los activos y requisitos regulatorios.

En conjunto, los controles del NIST SP 800-53 proporcionan una base sólida para establecer una postura de ciberseguridad robusta y medible, promoviendo el principio de defensa en profundidad. El marco enfatiza no solo los controles técnicos, sino también los administrativos y operativos, reconociendo que la seguridad efectiva depende de procesos, personas y tecnología. Además, su flexibilidad permite que los controles se adapten a distintos contextos organizacionales y se integren con otros marcos de refe-

rencia, facilitando la gestión continua de riesgos y la protección de la confidencialidad, integridad y disponibilidad de la información.

ISO 27002

La ISO/IEC 27002:2022 es una norma de buenas prácticas que proporciona directrices para establecer, implementar y mejorar controles de seguridad de la información dentro de un sistema de gestión de seguridad de la información (SGSI). La versión actual organiza sus 93 controles en cuatro grandes temas: organizacionales, personas, físicos y tecnológicos. Esta nueva estructura simplifica la comprensión y aplicación de los controles, permitiendo a las organizaciones adoptar un enfoque más claro y alineado con la gestión de riesgos, independientemente de su tamaño o sector.

Los controles organizacionales abordan la gobernanza, la gestión de riesgos, las políticas, la seguridad en la cadena de suministro y la gestión de incidentes; los controles relacionados con las personas se centran en la concienciación, formación, responsabilidades y comportamientos seguros del personal; los controles físicos protegen instalaciones, equipos y activos frente a accesos no autorizados o daños; y los controles tecnológicos cubren aspectos técnicos como control de acceso, criptografía, seguridad de redes, protección contra *malware* y gestión de vulnerabilidades. En conjunto, los 93 controles de la ISO/IEC 27002 proporcionan un marco coherente y completo para proteger la confidencialidad, integridad y disponibilidad de la información, y sirven como referencia clave para el cumplimiento de la ISO/IEC 27001 (ISO–IEC, 2022a, 2022b).

Centro de operaciones de ciberseguridad (SOC)

Un centro de operaciones de ciberseguridad (SOC, por sus siglas en inglés de Security Operation Center) es un centro de seguridad, es decir, un equipo organizado –a veces interno, a veces externalizado– encargado de monitorizar, detectar, analizar y responder en tiempo real a incidentes de ciberseguridad dentro de una organización (Bidou, 2005).

Funciones de un SOC

Un SOC es un conjunto de personas, procesos y tecnologías dedicadas a:

- Vigilar continuamente la infraestructura digital.
- Analizar eventos y alertas generadas por sistemas de seguridad.
- Detectar amenazas o comportamientos anómalos.
- Responder e investigar incidentes.
- Minimizar daños y asegurar la continuidad del negocio.
- Normalmente opera 24/7 debido a que los ataques pueden ocurrir en cualquier momento.

Importancia de un SOC en los controles de ciberseguridad

El SOC es fundamental para la eficacia de los controles de seguridad, ya que permite visibilidad total. Los controles generan datos, como firewalls, antivirus, autenticación, etcétera, entonces el SOC centraliza esa información para detectar patrones y brechas en la herramienta conocida como SIEM.

Además, reduce el tiempo de detección (MTTD) y de respuesta (MTTR). Sin un SOC, un ataque puede pasar días o semanas sin ser descubierto. Con un SOC, se detecta en minutos u horas.

En este sentido, asegura el cumplimiento normativo, Muchas regulaciones exigen monitorización continua:

- ISO 27001.
- NIST.
- GDPR.
- PCI-DSS.

El SOC permite demostrar control y auditoría; previene daños mayores y puede evitar:

- Fugas de datos.
- Paradas operativas.
- Secuestro por *ransomware*.

» Pérdidas económicas o reputacionales.
» Mejora la madurez de seguridad.

Un SOC incrementa la capacidad de:

» Prevenir.
» Detectar.
» Responder.
» Recuperarse.

Respuesta a incidentes

La respuesta a incidentes requiere preparación previa. Esta metodología de respuesta a incidentes es una referencia dedicada a los encargados de investigar un problema de seguridad específico.

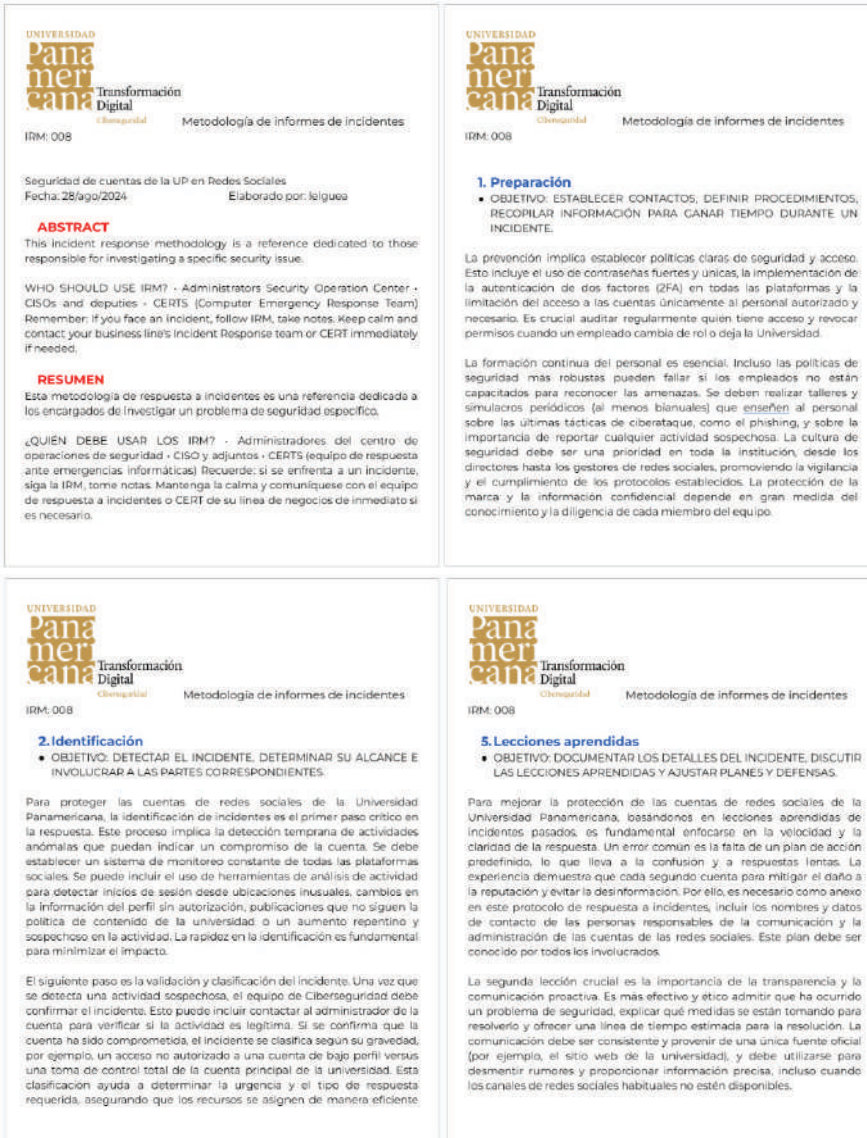
¿Quién debe usar los IRM?

» Administradores del centro de operaciones de seguridad.
» CISO y adjuntos.
» CERTS (equipo de respuesta ante emergencias informáticas).
» Usuarios que manejan información sensible.
» Equipos de TI/administradores de sistemas.
» Alta dirección y dueños de la información.
» Proveedores externos o socios que reciben información.

Se recomienda la creación de documentos diferentes para los posibles incidentes detectados o con probabilidad de incidencia. Para cada documento es importante incluir los siguientes puntos:

1. Resumen (*abstract*).
2. Preparación.
3. Identificación.
4. Contención.
5. Remediación.
6. Recuperación.
7. Lecciones aprendidas.

Figura 6. Ejemplo de contenido de un IRM común



UNIVERSIDAD Panamericana Transformación Digital Ciberseguridad

Metodología de informes de incidentes

IRM: 008

Seguridad de cuentas de la UP en Redes Sociales
Fecha: 28/ago/2024 Elaborado por: lalguea

ABSTRACT

This incident response methodology is a reference dedicated to those responsible for investigating a specific security issue.

WHO SHOULD USE IRM? - Administrators Security Operation Center - CISOs and deputies - CERTS (Computer Emergency Response Team) Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

RESUMEN

Esta metodología de respuesta a incidentes es una referencia dedicada a los encargados de investigar un problema de seguridad específico.

¿QUIÉN DEBE USAR LOS IRM? - Administradores del centro de operaciones de seguridad - CISO y adjuntos - CERTS (equipo de respuesta ante emergencias informáticas) Recuerde: si se enfrenta a un incidente, siga la IRM, tome notas. Mantenga la calma y comuníquese con el equipo de respuesta a incidentes o CERT de su línea de negocios de inmediato si es necesario.

UNIVERSIDAD Panamericana Transformación Digital Ciberseguridad

Metodología de informes de incidentes

IRM: 008

1. Preparación

- OBJETIVO: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, RECOPILAR INFORMACIÓN PARA GANAR TIEMPO DURANTE UN INCIDENTE.

La prevención implica establecer políticas claras de seguridad y acceso. Esto incluye el uso de contraseñas fuertes y únicas, la implementación de la autenticación de dos factores (2FA) en todas las plataformas y la limitación del acceso a las cuentas únicamente al personal autorizado y necesario. Es crucial auditar regularmente quién tiene acceso y revocar permisos cuando un empleado cambia de rol o deja la Universidad.

La formación continua del personal es esencial. Incluso las políticas de seguridad más robustas pueden fallar si los empleados no están capacitados para reconocer las amenazas. Se deben realizar talleres y simulacros periódicos (al menos bianuales) que enseñen al personal sobre las últimas tácticas de ciberataque, como el phishing, y sobre la importancia de reportar cualquier actividad sospechosa. La cultura de seguridad debe ser una prioridad en toda la institución, desde los directores hasta los gestores de redes sociales, promoviendo la vigilancia y el cumplimiento de los protocolos establecidos. La protección de la marca y la información confidencial depende en gran medida del conocimiento y la diligencia de cada miembro del equipo.

UNIVERSIDAD Panamericana Transformación Digital Ciberseguridad

Metodología de informes de incidentes

IRM: 008

2. Identificación

- OBJETIVO: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES CORRESPONDIENTES.

Para proteger las cuentas de redes sociales de la Universidad Panamericana, la identificación de incidentes es el primer paso crítico en la respuesta. Este proceso implica la detección temprana de actividades anómalas que puedan indicar un compromiso de la cuenta. Se debe establecer un sistema de monitoreo constante de todas las plataformas sociales. Se puede incluir el uso de herramientas de análisis de actividad para detectar inicios de sesión desde ubicaciones inusuales, cambios en la información del perfil sin autorización, publicaciones que no siguen la política de contenido de la universidad o un aumento repentino y sospechoso en la actividad. La rapidez en la identificación es fundamental para minimizar el impacto.

El siguiente paso es la validación y clasificación del incidente. Una vez que se detecta una actividad sospechosa, el equipo de Ciberseguridad debe confirmar el incidente. Esto puede incluir contactar al administrador de la cuenta para verificar si la actividad es legítima. Si se confirma que la cuenta ha sido comprometida, el incidente se clasifica según su gravedad, por ejemplo, un acceso no autorizado a una cuenta de bajo perfil versus una toma de control total de la cuenta principal de la universidad. Esta clasificación ayuda a determinar la urgencia y el tipo de respuesta requerida, asegurando que los recursos se asignen de manera eficiente.

UNIVERSIDAD Panamericana Transformación Digital Ciberseguridad

Metodología de informes de incidentes

IRM: 008

5. Lecciones aprendidas

- OBJETIVO: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR PLANES Y DEFENSAS.

Para mejorar la protección de las cuentas de redes sociales de la Universidad Panamericana, basándonos en lecciones aprendidas de incidentes pasados, es fundamental enfocarse en la velocidad y la claridad de la respuesta. Un error común es la falta de un plan de acción predefinido, lo que lleva a la confusión y a respuestas lentas. La experiencia demuestra que cada segundo cuenta para mitigar el daño a la reputación y evitar la desinformación. Por ello, es necesario como anexo en este protocolo de respuesta a incidentes, incluir los nombres y datos de contacto de las personas responsables de la comunicación y la administración de las cuentas de las redes sociales. Este plan debe ser conocido por todos los involucrados.

La segunda lección crucial es la importancia de la transparencia y la comunicación proactiva. Es más efectivo y ético admitir que ha ocurrido un problema de seguridad, explicar qué medidas se están tomando para resolverlo y ofrecer una línea de tiempo estimada para la resolución. La comunicación debe ser consistente y provenir de una única fuente oficial (por ejemplo, el sitio web de la universidad), y debe utilizarse para desmentir rumores y proporcionar información precisa, incluso cuando los canales de redes sociales habituales no estén disponibles.

Fuente: Universidad Panamericana.

Es muy común, por ejemplo, que el documento relacionado con respuesta a incidentes de redes sociales lo tengan y lo conozcan los responsables de esas actividades, sea personal interno o externo (como agencias de publicidad).

Directivas de grupo

Las directivas de grupo son un conjunto de reglas y configuraciones que un administrador puede aplicar de forma centralizada a usuarios y/o equipos dentro de un dominio de "Active Directory".

Implementación: se implementan a través de objetos de directiva de grupo (GPO), que contienen los ajustes específicos.

Alcance

Estos GPO se pueden vincular a diferentes niveles de la estructura de AD:

- *Dominio:* la configuración se aplica a todos los usuarios y equipos del dominio.
- *Sitios:* se aplica a los equipos en una ubicación geográfica o lógica específica.
- *Unidades organizativas (OU):* permite aplicar configuraciones solo a un subconjunto específico de usuarios o equipos (por ejemplo, solo a los usuarios del departamento de Contabilidad).

Configuraciones comunes

Permiten gestionar casi todos los aspectos de un sistema operativo Windows, incluyendo:

- Políticas de seguridad (por ejemplo, requisitos de contraseña, bloqueo de cuentas).
- Restricciones de software (por ejemplo, impedir la ejecución de ciertas aplicaciones).
- Configuración del escritorio/interfaz de usuario (por ejemplo, fondo de pantalla, menú de inicio).

- » Instalación de software (por ejemplo, desplegar una aplicación a todos los equipos).
- » Scripts (por ejemplo, ejecutar un script al inicio o cierre de sesión).

Importancia de las directivas para la implementación de controles

Las directivas de grupo son cruciales porque proporcionan un mecanismo de administración centralizada y coherente para implementar controles en toda la red.

Uniformidad y estandarización: aseguran que las configuraciones de seguridad y operativas sean idénticas y consistentes en todos los dispositivos de destino, eliminando la configuración manual y propensa a errores en cada equipo.

Escalabilidad: permiten gestionar cientos o miles de equipos y usuarios desde una única consola, lo que es inviable de forma individual.

Aplicación de la conformidad: hacen cumplir las políticas internas y los requisitos reglamentarios (como los de la industria o leyes de privacidad) automáticamente. Si un usuario o equipo intenta desviarse de la configuración, la directiva de grupo la restablece periódicamente.

Relevancia a la ciberseguridad

Las directivas de grupo son una de las herramientas más poderosas para fortalecer la postura de ciberseguridad de una organización:

Tabla 10. Ejemplo de directivas de grupo

Control de ciberseguridad	Ejemplo de directiva de grupo
Control de acceso	Forzar la complejidad de las contraseñas (longitud mínima, caducidad, uso de caracteres especiales) y configurar el bloqueo automático de cuentas después de un número de intentos fallidos.
Reducción de superficie de ataque	Deshabilitar puertos o servicios innecesarios, o restringir la ejecución de archivos desde medios extraíbles (USB).
Protección de *End-Points*	Configurar y habilitar el *firewall* de Windows, configurar automáticamente el antivirus//*antimalware* en todos los equipos, o habilitar BitLocker para el cifrado de disco.
Principio de mínimo privilegio	Restringir qué usuarios pueden instalar software o realizar cambios administrativos en sus equipos, limitándolos solo a tareas necesarias.
Auditoría y monitoreo	Habilitar el registro de eventos de seguridad para rastrear inicios de sesión fallidos, cambios en cuentas de usuario o acceso a archivos críticos.

Fuente: elaboración propia.

Otros controles

Las GPO y los marcos como NIST y CIS son solo una parte de un ecosistema más amplio de controles que incluyen organizativos, técnicos, físicos, operativos y legales. Un programa de seguridad maduro combina todos ellos, alineados con el riesgo del negocio. En esta sección se mencionan algunos de ellos.

Honeypots

Un *honeypot* (o "tarro de miel") es un señuelo diseñado para ser atacado. Es un recurso informático que no tiene valor operativo real; su único propósito es ser sondeado, atacado o comprometido para que puedas detectar intrusos y estudiar sus tácticas sin poner en riesgo tus sistemas reales.

La regla de oro de un *honeypot* es que cualquier tráfico que entre o salga de él es, por definición, sospechoso.

Para que tu *honeypot* sea realmente útil y no un dolor de cabeza, sigue estas reglas:

» *Aislamiento total:* el *honeypot* debe estar en una VLAN aislada o en una DMZ. No debe tener permisos para iniciar conexiones hacia tus servidores de producción.
» *Nombres creíbles:* no lo llames "Honeypot-01", ponle nombres que un atacante buscaría, como "SRV-SQL-DEV", "Caja-Pre-Producción" o "Backup-Finance".
» *Datos falsos:* si el *honeypot* simula un servidor de archivos, llénalo con PDFs o Excel que parezcan reales pero contengan datos basura.
» *Alertas críticas:* conecta los logs de tu *honeypot* a tu SIEM o envíalos a un canal de Slack/Teams. Como nadie debería entrar ahí, cada alerta es una prioridad 1.

Hay dos opciones muy recomendadas, que son:

1. *Canarytokens* (*la más sencilla y rápida):* ideal si quieres detección inmediata sin gestionar servidores. Los *canarytokens* son "migas de pan" que, al ser tocadas, te envían una alerta. Entra en canarytokens.org., genera un token de tipo "MS Word" o "Clave de API de AWS". Y, por último, coloca ese archivo de Word llamado "Sueldos2025.docx" en una carpeta compartida de tu red. El resultado sería que si un atacante entra en tu red y abre el archivo, recibirás un correo instantáneo con su dirección IP y el tipo de dispositivo que usó.
2. *T-Pot* (*La más robusta y visual):* si quieres una "estación de guerra" completa, T-Pot es un proyecto de Deutsche Telekom que corre en Docker y levanta más de 20 *honeypots* distintos a la vez (SSH, bases de datos, web, IoT). Para ello se requiere una máquina con Linux (Debian recomendado), 8 GB de RAM y 128 GB de disco. Para su implementación lo que necesitas es instalar Debian estable, clonas el repositorio: git clone (https: //github.com/telekom-security/tpotce) y ejecutas el instalador: ./install.sh. El resultado es que tendrás un panel en Kibana (visualización de datos) que te muestra mapas de calor de

ataques en tiempo real, qué nombres de usuario están probando y qué *malware* están intentando subir.

Logs de aplicaciones

Los *logs* de aplicaciones (o registros de eventos) son archivos cronológicos donde una aplicación escribe mensajes sobre lo que sucede mientras se está ejecutando. Piénsalos como la "caja negra" de un avión o el diario de vida de un software porque registran desde operaciones rutinarias hasta errores críticos, permitiendo a los desarrolladores entender qué pasó en el sistema sin tener que estar mirándolo en tiempo real.

Toda aplicación WEB debe tener, como mínimo, un registro de cada intento de validación –exitoso o no–. Se debe generar un evento, donde se registra la fecha, el nombre de la aplicación, el usuario, la dirección IPv4/IPv6 y si la autenticación fue exitosa o no en un archivo con formato json se facilita procesarla con el SIEM:

{"SyslogUP":{"aplicacion":"evaluaciones","usuario":"hperez", "evento":"login", "ip":"8.8.8.8","fecha":"2024-12-02 07:54", "status":"Success"}}
{"SyslogUP":{"aplicacion":"nomina","usuario":"auditor","evento": "login","ip":"2801:f0:f1:83:face:b00c:0:1","fecha":"2024-12-02 08:07","status":"Success"}}
{"SyslogUP":{"aplicacion":"proveedores","usuario":"hacker", "evento":"login", "ip":"127.0.0.1","fecha":"2024-12-02 09:11", "status":"Fail"}}

Microsegmentación

Basada en el "principio de confianza cero" (*Zero Trust*) a diferencia de la segmentación tradicional (VLANs), donde una vez que alguien entra a la red "Contabilidad" puede ver todas las computadoras de esa oficina, la microsegmentación pone una barrera a cada recurso individual.

Consiste en que se crean políticas donde el tráfico solo se permite si es estrictamente necesario para la aplicación. Se bloquea el movimiento lateral.

Para un ejemplo práctico, imagina que tienes tres servidores web. En una red normal, si el atacante hackea el servidor 1, puede saltar al servidor 2 por la red interna. Con microsegmentación, configuras una regla que dice: "el servidor 1 solo puede hablar con la base de datos por el puerto 3306; tiene prohibido hablar con cualquier otro servidor web". Esto "encierra" al atacante en una habitación sin puertas.

Pruebas de penetración (pentest)

Las pruebas de penetración son un componente fundamental para validar la eficacia de una estrategia de ciberseguridad y de los controles implementados, ya que permiten evaluar la capacidad real de la organización para resistir ataques similares a los que podrían ejecutar actores maliciosos. A diferencia de las auditorías teóricas, las pruebas de penetración ejecutan escenarios prácticos que exponen debilidades técnicas, errores de configuración o comportamientos no previstos en los sistemas, redes y aplicaciones. Esto ayuda a confirmar si los controles implementados –como *firewalls*, sistemas de detección de intrusiones o segmentación de red– están funcionando de manera adecuada frente a amenazas actuales (Bacudio et al., 2011; Vats et al., 2020).

Además, estas pruebas aportan una visión objetiva y basada en evidencia sobre la madurez de los controles de seguridad. Permiten identificar brechas que los equipos internos podrían pasar por alto, y muestran cómo un atacante podría encadenar vulnerabilidades menores para comprometer activos críticos. Esto resulta especialmente valioso para evaluar controles preventivos y detectivos, pues ponen a prueba su robustez en un entorno que simula condiciones de ataque reales.

Finalmente, los resultados de un *pentest* ayudan a priorizar mejoras y a justificar inversiones en seguridad con datos medibles. La organización no solo identifica qué controles fallan o necesitan fortalecerse, sino también qué prácticas están funcionando correctamente. De esta forma, las pruebas de penetración se convierten en una herramienta estratégica para ajustar, validar y acelerar la evolución del programa de ciberseguridad.

La frecuencia recomendada de un *pentest* y el tipo de prueba dependen del riesgo, la exposición y los cambios en tus sistemas.

No obstante, existen buenas prácticas generalmente aceptadas en seguridad de la información.

Recomendación general de frecuencia de pentest

La frecuencia base de pruebas de penetración es al menos una vez al año para cualquier organización con sistemas expuestos o datos sensibles. Existen casos en los que debe hacerse con mayor frecuencia.

Se recomienda realizar un *pentest* adicional cuando ocurre alguno de los siguientes eventos:

- Cambios importantes en la infraestructura (nuevos servidores, *cloud*, redes).
- Lanzamiento o rediseño de aplicaciones (web, mobile, APIs).
- Cambios relevantes en el código o arquitectura.
- Integración con terceros o proveedores críticos.
- Incidentes de seguridad previos.
- Requerimientos regulatorios o contractuales (PCI DSS, ISO 27001, SOC 2, etcétera).

Recomendación concreta de mayor frecuencia

En entornos dinámicos (DevOps, SaaS, *fintech*, *e-commerce*) cada seis meses es una práctica común y recomendada.

Entornos recomendados para *pentests* semestrales o más frecuentes:

1. Plataformas SaaS con despliegues continuos:
   - Cambios frecuentes en código y arquitectura.
   - Exposición directa a Internet (web y APIs).
   - Riesgo elevado de fallos de lógica de negocio.
   - La frecuencia recomendada es cada tres a seis meses.

2. Entornos *fintech* y servicios de pago:
   - Manejo de datos financieros y transacciones críticas.
   - Alto interés para atacantes.

   - » Requisitos regulatorios (PCI DSS, PSD2, reguladores locales).
   - » La frecuencia recomendada es semestral o trimestral.

3. Comercio electrónico de alto volumen:
   - » Procesamiento de pagos y datos personales.
   - » Integraciones con múltiples terceros (pasarelas, logística, marketing).
   - » Picos de tráfico y campañas temporales.
   - » La frecuencia recomendada es semestral y antes de campañas críticas.

4. Infraestructura *cloud* compleja (AWS, Azure, GCP):
   - » Uso intensivo de servicios gestionados, IAM y APIs.
   - » Cambios frecuentes en configuraciones.
   - » Riesgos de mala configuración (misconfigurations).
   - » La frecuencia recomendada es semestral, con revisiones focalizadas más frecuentes.

5. Aplicaciones con datos personales sensibles:
   - » Salud, educación, RRHH, identidad digital.
   - » Impacto legal y reputacional alto ante brechas.
   - » Obligaciones de protección de datos (GDPR, LOPDGDD).
   - » La frecuencia recomendada es cada seis meses.

6. Organizaciones con gran número de usuarios internos:
   - » Redes corporativas extensas.
   - » Acceso remoto, VPN, BYOD, múltiples roles.
   - » Riesgo de escalamiento de privilegios.
   - » La frecuencia recomendada es *pentest* interno semestral.

7. Entornos DevOps/CI-CD maduros:
   - » Automatización de *builds* y despliegues.
   - » Riesgos en pipelines, secretos y dependencias.
   - » Cambios constantes en infraestructura como código.
   - » La frecuencia recomendada es semestral o trimestral (focalizado).

8. Sistemas críticos para la operación del negocio:
   - » Caídas implican impacto económico inmediato.
   - » SLAs estrictos o servicios 24/7.
   - » Difícil tolerancia a interrupciones.
   - » La frecuencia recomendada es semestral, con pruebas específicas por componente.

Tipos de pentest

Existen diferentes tipos de *pentest* dependiendo de la información que se utiliza para la prueba y de accesibilidad a la información:

1. *Pentest* externo:
   ¿Qué evalúa? Sistemas expuestos a Internet (webs, APIs, VPN, firewalls, correo, *cloud*).
   ¿Cuándo hacerlo? Siempre, Idealmente una a dos veces por año.
   Objetivo: simular a un atacante externo sin acceso previo.

2. *Pentest* interno:
   ¿Qué evalúa? Qué puede hacer un atacante una vez dentro de la red y riesgos de escalamiento de privilegios y movimiento lateral.
   ¿Cuándo hacerlo? Al menos una vez al año. Muy recomendable si hay muchos usuarios, oficinas o accesos remotos.
   Objetivo: simular a un atacante interno con acceso previo.

3. *Pentest* según nivel de conocimiento:
   Black box: sin información previa (visión atacante real), *grey box*: con credenciales o información parcial (más eficiente), y *white box*: con código y arquitectura (más profundo).
   Buenas prácticas: *black/grey box* de forma regular y *white box* de manera puntual para aplicaciones críticas.

HERRAMIENTAS, PROTOCOLOS Y ESTÁNDARES

Se establece el marco técnico y metodológico que permite diseñar, operar y proteger sistemas de información de forma consistente y medible. Las herramientas proporcionan la capacidad operativa para detectar, analizar y responder a eventos; los protocolos aseguran la comunicación correcta y segura entre sistemas, y los estándares garantizan alineación con buenas prácticas reconocidas a nivel internacional. En conjunto, estos elementos reducen riesgos, facilitan la interoperabilidad entre tecnologías, fortalecen el cumplimiento normativo y permiten que las organizaciones adopten un enfoque sistemático y repetible frente a la ciberseguridad y la gestión de TI.

Resulta clave mencionar herramientas como analizadores de protocolos (por ejemplo, *Wireshark*) para la inspección y diagnóstico del tráfico de red; plataformas SIEM (por sus siglas en inglés, *Security Information and Event Management*) para la correlación de eventos y la detección de incidentes; y soluciones XDR (*Extended Detection and Response*) que integran visibilidad y respuesta a través de *endpoints*, redes y servicios en la nube.

Asimismo, es relevante abordar protocolos como TCP/IP, HTTPS, TLS, SSH, SNMP y DNS, que sustentan la comunicación segura y confiable, así como estándares ampliamente adoptados como ISO/IEC 27001, NIST, OWASP, ITIL y CIS Controls. La correcta comprensión y aplicación de estas herramientas, protocolos y estándares permite a las organizaciones mejorar su postura de seguridad, optimizar la respuesta ante incidentes y asegurar la continuidad y confiabilidad de sus operaciones tecnológicas.

Herramientas

Las herramientas de ciberseguridad son el conjunto de aplicaciones, software, dispositivos de hardware y servicios diseñados específicamente para proteger la integridad, confidencialidad y disponibilidad de la información en el entorno digital. En el contexto de tu libro, puedes definirlas como los instrumentos tácticos que permiten ejecutar las directrices de la política y el marco de gobernanza (como NIST o ISO).

Se dividen en:

- Herramientas de prevención.
- Herramientas de detección.
- Herramientas de respuesta y recuperación.

Las herramientas no sustituyen a la estrategia, los procesos ni las personas.

El éxito de los controles de seguridad, como los definidos por el CIS (Control 1 y 2) o el NIST CSF 2.0 (ID.AM), depende enteramente de la precisión del inventario de activos. Herramientas como OpenAudit resultan fundamentales en esta etapa, ya que permiten automatizar el descubrimiento de dispositivos y software dentro de la infraestructura, eliminando la dependencia de registros manuales que suelen quedar obsoletos rápidamente. Al realizar escaneos inteligentes, OpenAudit no solo identifica qué equipos están conectados, sino que extrae detalles técnicos profundos –como versiones de sistemas operativos, configuraciones de Hardware y parches instalados–, proporcionando la visibilidad necesaria para detectar activos no autorizados o vulnerables antes de que puedan ser explotados por un atacante.

Desde una perspectiva de gobernanza y gestión de riesgos, contar con una herramienta de auditoría de red robusta permite a la institución alinear sus recursos de protección con la realidad de su ecosistema. OpenAudit actúa como un sensor crítico que alimenta el análisis de impacto al negocio (BIA), permitiendo a los responsables de seguridad comprender las dependencias técnicas y asegurar que cada nodo de la red esté bajo el control de las políticas institucionales. Sin una capacidad de inventario automatizada, la

estrategia de ciberseguridad es ciega; con ella, la organización pasa de una postura reactiva a una defensa proactiva basada en datos exactos y verificables.

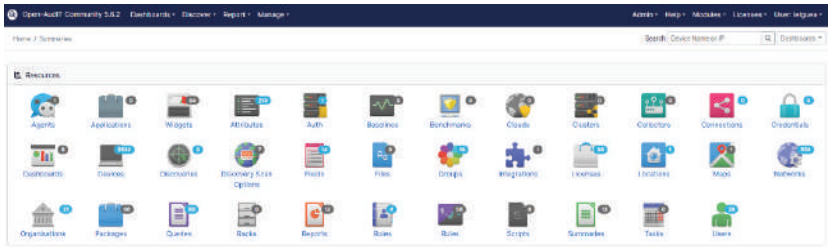
Inventario de hardware y software

Varias herramientas de ciberseguridad, como algunos SIEM, entre ellos Wazuh, tiene un módulo de inventario, principalmente de software y algo de hardware, pero si se busca una solución más completa y *open source*, está la solución de Open-AudIT.

Open-AudIT es una herramienta de descubrimiento y gestión de activos de TI que contribuye directamente al cumplimiento de controles fundamentales de ciberseguridad, especialmente aquellos relacionados con la visibilidad, inventario y control de los sistemas. Al identificar de forma automática dispositivos, sistemas operativos, software instalado, configuraciones y cambios en la infraestructura, Open-AudIT permite a las organizaciones mantener un inventario actualizado y verificable, requisito esencial en marcos como NIST CSF (función "Identify", categoría "Asset Management") y en los CIS Critical Security Controls, particularmente los controles de inventario y gestión de activos empresariales y de software.

Desde una perspectiva operativa, Open-AudIT apoya la detección temprana de desviaciones de configuración y activos no autorizados, lo que refuerza controles preventivos y de detección. Al facilitar auditorías periódicas, análisis de cambios y reportes de cumplimiento, la herramienta ayuda a demostrar conformidad con estándares como ISO/IEC 27001 (ISO–IEC, 2022a), al proporcionar evidencia objetiva para auditorías internas y externas. De este modo, Open-AudIT no actúa como un control de seguridad aislado, sino como un habilitador clave de Gobierno y gestión de riesgos, mejorando la capacidad de la organización para aplicar controles técnicos de forma coherente y basada en información confiable.

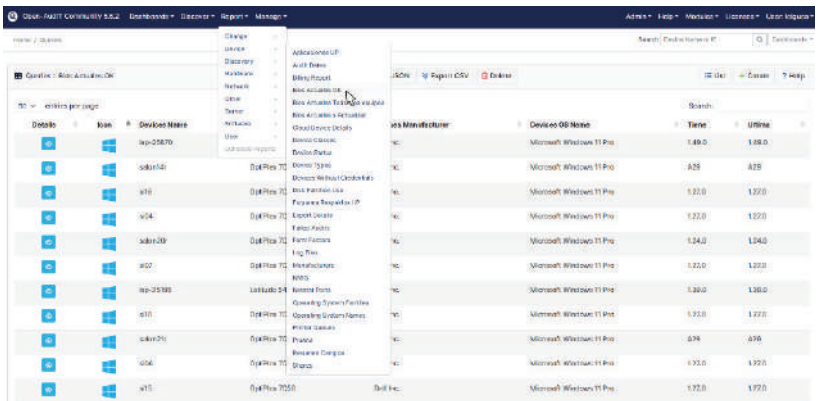
Figura 7. Ejemplo de recursos en Open-AudIT



Fuente: Open-AudIT (2026).

Personalmente lo uso, agregando una tabla más a la base de datos, lo que proporciona un indicador de los equipos que no tienen actualizado su BIOS/UEFI.

Figura 8. Ejemplo inventario de BIOS/UEFI



Fuente: captura de pantalla.

Gestión de información y eventos de seguridad (SIEM)

Una gestión de información y eventos de seguridad (SIEM, por sus siglas en inglés *Security Information and Event Management*) es una solución de seguridad que centraliza la recolección, el almacenamiento y el análisis de los eventos generados por toda la infraestructura tecnológica de una organización.

En un ecosistema donde la cantidad de datos generados supera la capacidad de análisis humano, el SIEM actúa como un motor de correlación inteligente que transforma el "ruido" de los *logs* en inteligencia accionable. Su implementación permite a las

organizaciones pasar de una postura reactiva a una capacidad de detección temprana, identificando ataques complejos y persistentes que intentan pasar desapercibidos mediante acciones fragmentadas en distintos puntos de la red.

Una de las herramientas más versátiles para implementar la estrategia definida en este libro es Wazuh. Al centralizar la recolección de eventos (SIEM) y permitir una respuesta extendida (XDR), Wazuh se convierte en el brazo ejecutor de las funciones de "detectar" y "responder" del NIST CSF 2.0, permitiendo que incluso instituciones pequeñas tengan visibilidad de nivel corporativo sobre sus activos críticos (Wazuh, 2026a, 2026b).

Desde una perspectiva funcional, con Wazuh se puede:

» Detectar intrusiones y comportamientos anómalos mediante análisis de logs y reglas de correlación.
» Monitorear la integridad de archivos (FIM) para identificar cambios no autorizados en sistemas críticos.
» Gestionar vulnerabilidades, integrándose con bases como CVE para detectar software desactualizado o vulnerable.
» Aplicar *hardening* y cumplimiento frente a estándares como CIS Benchmarks, ISO 27001, PCI DSS y NIST, generando reportes de auditoría.
» Centralizar eventos de seguridad y apoyar procesos de respuesta a incidentes, actuando como un habilitador de SOC básico o distribuido.

Detección y respuesta extendida (XDR)

La detección y respuesta extendida (XDR, conocido en inglés como *Extended Detection and Response*) es la evolución más reciente y avanzada de las herramientas de detección y respuesta. Mientras que el EDR se enfoca solo en los dispositivos finales (*endpoints)* y el NDR en la red, el XDR unifica y correlaciona automáticamente los datos de múltiples capas de seguridad: *endpoints*, red, nube, correo electrónico y gestión de identidades.

El XDR representa un cambio de paradigma en la defensa cibernética al sustituir la gestión fragmentada de herramientas por una arquitectura de detección y respuesta extendida y unificada. A diferencia de las soluciones tradicionales que operan de forma ais-

lada, el XDR utiliza la inteligencia artificial y la automatización para correlacionar eventos a través de todo el patrimonio digital de la organización, desde el perímetro hasta la nube.

En el ecosistema *open source* es una de las herramientas más relevantes para capacidades tipo XDR es YARA, la cual se utiliza principalmente para la detección y clasificación de *malware* mediante reglas basadas en patrones. YARA permite identificar comportamientos maliciosos en archivos, procesos y memoria, lo que la convierte en un componente clave para la detección extendida cuando se integra con otras fuentes de telemetría. Aunque por sí sola no es una plataforma XDR completa, YARA actúa como un motor de detección avanzado, ampliamente utilizado por equipos de respuesta a incidentes, laboratorios de *malware* y SOCs para detectar amenazas conocidas y personalizadas en múltiples entornos.

IPS e IDS

En el ámbito de la seguridad de red, el IDS y el IPS actúan como sistemas de vigilancia de la infraestructura. Aunque comparten la misma base tecnológica de inspección, su diferencia fundamental radica en su capacidad de acción: uno es un observador y el otro es un interventor.

La implementación de sistemas IDS e IPS constituye la base de la visibilidad y el control reactivo dentro de la arquitectura de red. Mientras que el IDS aporta una capacidad analítica indispensable para el diagnóstico y la auditoría de incidentes, el IPS eleva la postura de seguridad hacia la prevención automatizada, permitiendo neutralizar ataques a la velocidad del cable. Sin embargo, en un ecosistema organizacional moderno, la efectividad de estos sistemas depende de un ajuste fino (*tuning*) constante, evitando que la rigidez de un IPS genere falsos positivos que interrumpan la continuidad del negocio, o que la pasividad de un IDS resulte en una saturación de alertas que los analistas no puedan gestionar.

1. IDS (por sus siglas en inglés, *Intrusion Detection System)* es un sistema de monitoreo pasivo diseñado para detectar actividades sospechosas o violaciones de políticas en una red o un sistema.

- » *Función:* analiza el tráfico, lo compara con una base de datos de firmas (patrones de ataques conocidos) o anomalías de comportamiento, y genera una alerta para los administradores.
- » *Analogía:* como una alarma de seguridad que suena cuando alguien rompe una ventana, pero no puede evitar que el intruso entre; solo avisa para que alguien más intervenga.

2. IPS (por sus siglas en inglés, *Intrusion Prevention System*) es un sistema de control activo que no solo detecta la amenaza, sino que tiene la autoridad para bloquearla automáticamente en tiempo real.
   - » *Función:* se coloca "en línea" (*in-line*) con el tráfico de red, lo que significa que todo el flujo de datos pasa a través de él. Si identifica un paquete malicioso, puede descartarlo, cerrar la conexión o bloquear la dirección IP de origen.
   - » *Analogía:* como un guardia de seguridad en la puerta que, al ver que alguien intenta entrar con una identificación falsa, le impide el paso físicamente en ese mismo instante.

Una de las herramientas *open source* más utilizadas como IDS/IPS es Snort, desarrollada originalmente por Sourcefire. Snort funciona como un motor de detección y prevención de intrusiones basado en firmas, reglas y análisis de protocolos, capaz de inspeccionar el tráfico de red en tiempo real. En modo IDS, Snort analiza los paquetes y genera alertas cuando detecta patrones asociados a ataques conocidos, como escaneos de puertos, *exploits*, intentos de denegación de servicio o tráfico malicioso. En modo IPS, puede desplegarse en línea para bloquear o descartar paquetes que coincidan con reglas de ataque, actuando activamente para prevenir intrusiones antes de que impacten a los sistemas.

Desde el punto de vista operativo, Snort permite a las organizaciones implementar un control de seguridad de red robusto sin costos de licenciamiento, siendo especialmente útil en entornos pequeños y medianos o como complemento a *firewalls* tradicionales. Su comunidad mantiene un amplio conjunto de reglas actua-

lizadas, y además es posible crear reglas personalizadas para adaptarse a riesgos específicos del negocio. Integrado con herramientas como Wazuh o SIEMs, Snort contribuye a la detección temprana y respuesta a incidentes, reforzando la defensa perimetral y la visibilidad del tráfico de red dentro de una estrategia de ciberseguridad en capas.

La implementación de Snort dentro de un ecosistema organizacional aporta una capa de defensa proactiva que complementa otras herramientas de monitoreo como el SIEM o el XDR. Al ser una herramienta basada en firmas y anomalías, permite a los administradores de seguridad realizar un ajuste fino (*tuning*) de las alertas para evitar falsos positivos que interrumpan la continuidad del negocio, garantizando al mismo tiempo que la infraestructura cumpla con los estándares técnicos exigidos por marcos como el NIST SP 800-53 o ISO 27002. En resumen, Snort transforma la visibilidad de la red en una capacidad de respuesta inmediata, asegurando que el flujo de datos institucional se mantenga íntegro y protegido frente a las amenazas modernas.

Suricata es un motor de red de alto rendimiento que funciona como sistema de detección de intrusiones (IDS), prevención de intrusiones (IPS) y monitoreo de seguridad de red (NSM). A diferencia de otras herramientas, su arquitectura está diseñada para el procesamiento multihilo, lo que le permite analizar grandes volúmenes de tráfico en redes de alta velocidad (10 Gbps o superiores) utilizando de manera eficiente todos los núcleos del procesador. Además de basarse en firmas para detectar amenazas, Suricata destaca por su capacidad de realizar una inspección profunda de paquetes (DPI) y por su soporte nativo para la identificación de protocolos y la extracción de archivos, lo que facilita enormemente el análisis forense tras un incidente.

La importancia de Suricata en una estrategia de ciberseguridad madura radica en su versatilidad y en su capacidad para generar telemetría detallada. Al integrarse con herramientas de análisis de datos como el SIEM o el XDR, proporciona una visibilidad sin precedentes sobre lo que ocurre en el tráfico de red, permitiendo identificar patrones de ataque complejos que podrían pasar desapercibidos para controles más rígidos. Su compatibilidad con las reglas de Snort asegura una transición sencilla para las organizaciones, mientras que su enfoque moderno en el rendimiento y la

visibilidad la convierte en un componente indispensable para proteger infraestructuras críticas y entornos corporativos altamente exigentes.

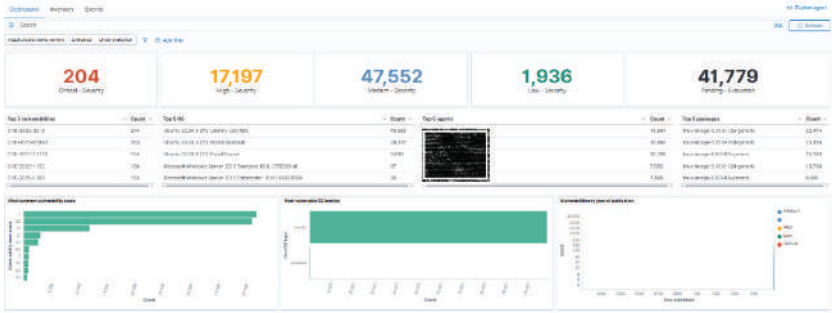
También, Suricata, sobresale en su capacidad para detectar amenazas avanzadas a alta velocidad, manteniendo visibilidad detallada del tráfico de red sin sacrificar desempeño. Además de generar alertas, Suricata produce registros enriquecidos que pueden integrarse con SIEMs y plataformas de monitoreo, permitiendo correlación, análisis forense y respuesta a incidentes. En una estrategia de ciberseguridad moderna, Suricata se posiciona como un componente clave para fortalecer la defensa perimetral y la detección interna, especialmente en organizaciones que requieren escalabilidad, automatización y compatibilidad con ecosistemas *open source*.

Escaneo de vulnerabilidades

Una herramienta destacada es OpenVAS (Greenbone Community Edition), orientada a la gestión y escaneo de vulnerabilidades. OpenVAS permite identificar debilidades en sistemas, servicios y aplicaciones mediante pruebas automatizadas, ayudando a priorizar la remediación de riesgos antes de que sean explotados. Junto con herramientas como TheHive (gestión de incidentes) y MISP (intercambio de inteligencia de amenazas), estas soluciones *open source* permiten construir una arquitectura de ciberseguridad robusta y escalable, alineada con buenas prácticas y marcos como NIST e ISO, sin depender exclusivamente de soluciones propietarias.

Wazuh tiene también un módulo de vulnerabilidades. La principal ventaja de este módulo es que esas vulnerabilidades se determinan con base al inventario de aplicaciones que el mismo agente detecta.

Figura 9. Ejemplo de vulnerabilidades Wazuh



Fuente: Wazuh (2026c).

Pruebas de penetración (pentest)

Dentro de esta categoría, destaca la distribución de Linux llamada Kali y un proyecto con fines educativos llamado Damn Vulnerable Web Application (DVWA, por sus siglas en inglés).

Kali

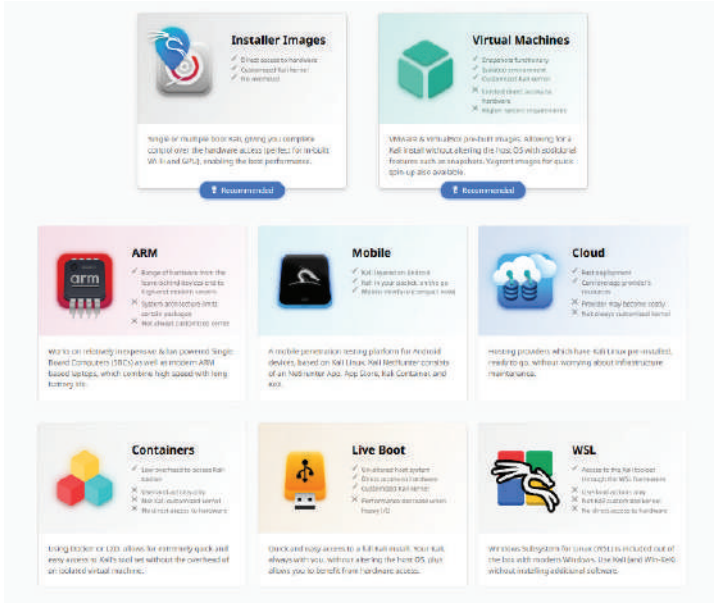
Kali Linux es una distribución basada en Debian creada específicamente para pruebas de penetración, auditorías de seguridad y análisis forense digital. Su historia comienza en 2013, cuando fue desarrollada por Offensive Security como sucesora de Back-Track Linux, una de las primeras distribuciones ampliamente utilizadas para *hacking* ético. Kali Linux fue diseñada desde cero con un enfoque profesional, incorporando un modelo de desarrollo más estable, repositorios firmados y una arquitectura preparada para entornos corporativos y académicos.

La finalidad principal de Kali Linux es servir como una plataforma integral para la evaluación de la seguridad de sistemas, redes y aplicaciones. Incluye cientos de herramientas especializadas para análisis de vulnerabilidades, explotación, pruebas de redes inalámbricas, ingeniería inversa y respuesta a incidentes. Su uso está orientado a profesionales de la ciberseguridad, investigadores y estudiantes, siempre dentro de marcos legales y éticos, contribuyendo a la identificación proactiva de fallos de seguridad antes de que puedan ser explotados por actores maliciosos.

Existen varios mecanismos para la instalación:

1. Instaladores.
2. Máquinas virtuales.
3. Dispositivos ARM.
4. Dispositivos móviles.
5. En la nube.
6. Contenedores.
7. USB (*live boot*).

Figura 10. Diferentes mecanismos para implementar Kali Linux



Fuente: Offensive Security (2026b).

Kali Linux contiene más de 600 herramientas de prueba de penetración incluidas clasificadas en las siguientes categorías (Offensive Security, 2026a):

1. Information Gathering.
2. Vulnerability Analysis.
3. Web Application Analysis.
4. Database Assessment.
5. Password Attacks.

6. Wireless Attacks.
7. Reverse Engineering.
8. Exploitation Tools.
9. Sniffing & Spoofing.
10. Post Exploitation.
11. Forensics.
12. Reporting Tools.
13. Social Engineering Tools.

Kali busca compatibilidad con una amplia variedad de dispositivos inalámbricos: un punto de conflicto habitual con las distribuciones de Linux ha sido la compatibilidad con las interfaces inalámbricas, lo que le permite ejecutarse correctamente en una amplia variedad de Hardware y hacerlo compatible con numerosos dispositivos USB y otros dispositivos inalámbricos.

Tiene Soporte multilingüe: aunque las herramientas de penetración tienden a estar escritas en inglés, nos hemos asegurado de que Kali incluya un verdadero soporte multilingüe.

Damn Vulnerable Web Application (DVWA)

Es un proyecto de software deliberadamente vulnerable diseñado para ayudar a estudiantes y profesionales de la ciberseguridad a comprender, identificar y explotar vulnerabilidades comunes en aplicaciones web dentro de un entorno controlado (Wood, 2026).

Es una aplicación web basada en PHP y MySQL diseñada deliberadamente con múltiples fallos de seguridad. Su propósito principal es servir como una herramienta educativa para profesionales de la ciberseguridad, permitiéndoles practicar técnicas de hacking ético y pruebas de penetración en un entorno controlado y legal. Al ser una plataforma vulnerable por diseño, ayuda a los desarrolladores a comprender las debilidades comunes en el código y a aprender cómo mitigarlas de manera efectiva.

El objetivo principal de DVWA es facilitar el aprendizaje práctico de vulnerabilidades web ampliamente documentadas, como inyección SQL, *cross-site scripting* (XSS), *cross-site request forgery* (CSRF), inclusión de archivos, subida insegura de ficheros y fallos de autenticación. DVWA permite configurar distintos niveles de seguridad, lo que ayuda a los usuarios a entender cómo pequeñas

variaciones en la implementación pueden convertir una aplicación segura en una vulnerable. Esta progresión resulta especialmente útil en entornos académicos y laboratorios de formación. Se pueden practicar los ataques más críticos del top 10 de OWASP.

Desde el punto de vista de la ciberseguridad, DVWA cumple una función clave como herramienta de concienciación y entrenamiento. Permite a desarrolladores, administradores de sistemas y analistas de seguridad experimentar con ataques reales y, posteriormente, aplicar medidas de mitigación y buenas prácticas. De este modo, el proyecto contribuye a fortalecer el enfoque defensivo al mejorar la comprensión de cómo y por qué se producen las vulnerabilidades, alineándose con principios de desarrollo seguro y pruebas de penetración.

Una de las características más destacadas de DVWA es su sistema de niveles de dificultad, que permite ajustar la complejidad de las vulnerabilidades entre bajo, medio, alto e "imposible". En el nivel bajo, la aplicación no tiene defensas, lo que facilita el aprendizaje de conceptos básicos; mientras que en el nivel imposible, el código está asegurado siguiendo las mejores prácticas para demostrar cómo debería ser una implementación robusta. Esta progresión la convierte en un recurso invaluable tanto para principiantes como para expertos que buscan poner a prueba sus habilidades de explotación.

Certificados digitales

Es un mecanismo que sirve para poder verificar tu identidad real de forma inequívoca. La encriptación o cifrado es un mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario. De modo inverso, la desencriptación o descifrado[10] permitirá hacer legible un mensaje que estaba cifrado. Hay mecanismos de cifrado simétrico y asimétrico. En el anexo A.3.1 está un ejemplo de certificado digital.

[10] La RAE aceptó el verbo encriptar en 2014 como sinónimo de cifrar. Por reglas de formación de palabras; desencriptar y desencriptación serían derivados válidos. Sin embargo, la academia y los expertos prefieren fuertemente cifrar, descifrar y descifrado.

Cifrado simétrico

Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. Hay varios estándares modernos para eso.

- AES.
- DES.
- 3DES / TDEA.
- Blowfish.
- RC4 / RC5 / RC6.

En el anexo A.4.1 está un ejemplo de AES.

Cifrado asimétrico

Un sistema de cifrado asimétrico es un tipo de cifrado que usa una clave para cifrar y otra diferente para descifrar.

- Diffie-Hellman.
- RSA.
- DSA.
- Cifrado ElGamal.
- Criptografía de curva elíptica.
- Criptosistema de Merkle-Hellman.
- Goldwasser-Micali.
- Goldwasser-Micali-Rivest.

Cifrado, certificados y firmas

Si se cifra el mensaje utilizando la llave privada, cualquiera puede descifrarlo utilizando su llave pública correspondiente. De esta forma se logra la identificación y autenticación del remitente, ya que solo él pudo haber utilizado su llave privada.

La firma digital se basa en el hecho de que un documento cifrado utilizando la llave privada de una persona solo puede ser descifrado utilizando la llave pública asociada a esa misma persona.

La firma digital es un digesto o huella del documento, el cual se cifra utilizando la llave privada del firmante.

Integridad de los datos: algoritmos hash

El verificar la no alteración de los datos es crítico en las transacciones electrónicas. Los sistemas criptográficos utilizan funciones *hash* para realizar el chequeo de integridad, mediante la generación de una "huella digital" o digesto (*digest*). Ejemplos comunes son:

- MD2 / MD5.
- SHA-1, SHA-256 / SHA-384 / SHA-512.
- CRC32.

Se usan para descargar archivos, en comunicaciones de redes, etcétera. Por ejemplo, archivos ZIP y RAR: cuando intentas abrirlo y te dice "Error de CRC", significa que el archivo está dañado. El programa calculó el *hash* del archivo y no coincide con el *hash* que el creador puso en el archivo original.

Un ejemplo de redes ethernet y wifi: cada paquete de datos que llega a tu ordenador tiene un código CRC al final. Si tu tarjeta de red calcula el CRC y no coincide, sabe que hubo interferencia eléctrica en el cable o en el aire y pide que le reenvíen el dato automáticamente.

En el anexo A.5.1 está un ejemplo de codificación usando Base64.

Respaldos

Los respaldos o copias de seguridad son el último baluarte de la resiliencia organizacional, consistiendo en duplicados de datos críticos que permiten la recuperación ante desastres, fallos de hardware o ataques de *ransomware*. En la gestión moderna, el estándar de oro es la regla 3-2-1: mantener al menos tres copias de los datos, almacenadas en dos soportes diferentes (como un disco local y una cinta o NAS), con una de esas copias ubicada fuera del sitio (*off-site*), preferiblemente en la nube o en una ubicación geográfica distinta. Este esquema garantiza que, incluso ante un incendio físico o un

compromiso total de la red local, siempre exista una vía de recuperación íntegra y disponible.

Para optimizar el almacenamiento y el tiempo de ejecución, existen tres estrategias fundamentales. El respaldo completo copia la totalidad de los datos, siendo la base necesaria pero la que más recursos consume. El respaldo diferencial copia únicamente los archivos que han cambiado desde el último respaldo completo, facilitando una restauración rápida ya que solo requiere dos piezas: el último completo y el diferencial más reciente. Por su parte, el respaldo incremental solo guarda los cambios realizados desde el último respaldo de cualquier tipo (ya sea completo o incremental); es el más rápido de ejecutar y el que menos espacio ocupa, aunque su restauración es más compleja al depender de toda la cadena de incrementos anteriores.

Los tipos más comunes de respaldos son:

» Un **respaldo completo** es una copia íntegra de todos los datos seleccionados, que permite restaurar la información de forma directa y sencilla a partir de un único respaldo.
» Un **respaldo diferencial** es una copia de seguridad que guarda todos los cambios realizados **desde el último respaldo completo**. A diferencia del incremental, cada respaldo diferencial crece con el tiempo hasta que se realiza un nuevo respaldo completo.
» Un **respaldo incremental** es aquel que solo copia los datos que han sido modificados o creados desde la última copia de seguridad realizada (ya sea un respaldo completo u otro respaldo incremental).

La utilidad de un respaldo es nula si no se puede garantizar su integridad; por ello, la verificación periódica es un proceso crítico que separa a las organizaciones resilientes de las vulnerables. No basta con recibir una notificación de "tarea completada"; es indispensable realizar pruebas de restauración consistentes para asegurar que los datos no solo existan, sino que sean legibles y funcionales. Un respaldo que no se ha probado es simplemente una esperanza de recuperación que puede fallar en el momento más inoportuno debido a corrupción de datos o errores en la cadena de escritura.

La verificación periódica de los respaldos es crítica, ya que un respaldo que no puede restaurarse es inútil. Es indispensable probar restauraciones de forma regular para confirmar la integridad, disponibilidad y tiempos de recuperación. Como recomendaciones clave para hacer buenos respaldos es necesario automatizar el proceso para evitar errores humanos y proteger los respaldos mediante cifrado y controles de acceso, garantizando que no puedan ser alterados o eliminados por atacantes o usuarios no autorizados.

Finalmente, para implementar una estrategia de respaldo de alta calidad, se recomienda aplicar el principio de inmutabilidad, asegurando que al menos una copia de seguridad no pueda ser modificada ni borrada por ningún usuario o proceso durante un tiempo determinado, lo cual es vital para sobrevivir a un ataque de *ransomware*. Además, es fundamental automatizar y monitorear el proceso para eliminar el error humano y garantizar que la frecuencia de los respaldos esté alineada con el objetivo de punto de recuperación (RPO) definido por el negocio, asegurando que la pérdida de datos sea mínima y aceptable ante cualquier contingencia.

Tres herramientas muy recomendables para respaldos son:

» *Bacula:* sistema de respaldo *open source* de nivel empresarial, diseñado para automatizar copias de seguridad, restauración y verificación de datos en redes heterogéneas (incluyendo Windows). Ofrece una arquitectura modular cliente/servidor con soporte avanzado de programación de *jobs*, catálogos, dispositivos de almacenamiento y verificación *post-backup*. Puntos clave:

    1. Arquitectura cliente-servidor escalable para centros de *backups* corporativos.
    2. Soporta Windows como cliente y puede integrarse con Linux/UNIX/macOS.
    3. Gestión de *backups* completos, incrementales y diferenciales con catálogo central.
    4. Integración con bases de datos como MySQL/PostgreSQL/SQLite para registrar catálogos.
    5. Interfaces de configuración CLI, GUI y web (por ejemplo Bacula-Web).

Uso típico en organizaciones medianas y grandes con muchos equipos y servidores, donde se requiere gestión centralizada y automatización completa de respaldos.

» *Duplicati*: cliente de copias de seguridad *open source* que funciona bien en Windows y permite enviar respaldos cifrados y comprimidos a una amplia variedad de destinos, incluidos almacenamientos en la nube y servidores remotos. Puntos clave:

1. Compatible con Windows, Linux y macOS.
2. Soporta respaldos incrementales, cifrado fuerte (AES-256), y compresión automática.
3. Puede almacenar copias en múltiples destinos: OneDrive, Google Drive, Amazon S3, FTP, WebDAV, SFTP, etcétera.
4. Interfaz de usuario basada en navegador web para gestión y programación.

Uso típico en entornos personales, PYMES o equipos individuales donde se requiere copia de archivos cifrada y flexible hacia almacenamiento local o en la nube, con mínima infraestructura.

» *Veeam Backup & Replication:* plataforma de respaldo y recuperación de nivel empresarial, ampliamente utilizada en entornos Windows y virtualizados. Está diseñada para garantizar alta disponibilidad, recuperación rápida y continuidad del negocio, con especial foco en infraestructuras VMware, Hyper-V, cloud híbrido y cargas críticas. A diferencia de Bacula y Duplicati, Veeam es software propietario, pero es considerado un estándar de facto en muchas organizaciones. Puntos clave:

1. Respaldos basados en imagen (*image-level*) con recuperación bare-metal.
2. Integración profunda con entornos virtualizados (VMware vSphere, Hyper-V).

3. Soporte avanzado para Windows Servers, Active Directory, SQL Server, Exchange y NAS.
4. Recuperación granular (archivos, objetos de AD, correos, bases de datos).
5. Replicación de máquinas virtuales para *failover* rápido.
6. Cifrado de datos en tránsito y en reposo.
7. Orquestación de recuperación y pruebas automáticas de *backups* (SureBackup).
8. Amplio ecosistema de soporte comercial y certificaciones.

Uso típico en empresas medianas y grandes con infraestructura crítica, Centros de datos con virtualización intensiva. y organizaciones que requieren recuperación ante desastres (DR) con tiempos mínimos. Entornos donde la disponibilidad del servicio es prioritaria frente al coste de licencias. Infraestructuras híbridas (*on-prem* + *cloud*).

Tabla 11. Comparativa de herramientas de respaldo: Bacula, Duplicati y Veeam

Característica	Bacula	Duplicati	Veeam
Licencia	*Open source* (AGPL)	*Open source* (LGPL)	Propietaria
Soporte para Windows	Sí (cliente)	Sí (nativo)	Sí (nativo)
Arquitectura	Cliente/servidor	Cliente individual	Centralizada
Escalabilidad	Alta (empresarial)	Media/Baja	Muy alta
Respaldos incrementales	Sí	Sí	Sí
Respaldos diferenciales	Sí	No	Sí
Cifrado de respaldos	Sí	Sí (AES-256)	Sí

Característica	Bacula	Duplicati	Veeam
Backups de imagen (*bare metal*)	Limitado	No	Sí
Soporte para virtualización	Básico	No	Avanzado (VMware/ Hyper-V)
Destinos de respaldo	Disco, NAS, cinta, *cloud*	Disco, FTP, SFTP, *cloud*	Disco, NAS, *cloud*, tape
Interfaz gráfica	Opcional (Web/GUI)	Web (integrada)	GUI completa
Automatización y políticas	Avanzada	Básica	Muy avanzada
Soporte comercial	Opcional	No oficial	Sí
Caso de uso ideal	Empresa/ datacenter	Usuario/PYME	Empresa crítica

Fuente: elaboración propia.

Plan de recuperación ante desastres (DRP)

El Plan de recuperación ante desastres (DRP, por sus siglas en inglés) es un documento estratégico y operativo que detalla los procedimientos técnicos específicos para restaurar los servicios críticos de TI tras un evento catastrófico, ya sea natural, humano o tecnológico. Mientras que el Plan de continuidad del negocio (BCP) se enfoca en mantener la operación global de la empresa, el DRP es su brazo técnico, centrándose exclusivamente en la infraestructura digital, los datos y los sistemas. Su objetivo primordial es minimizar el tiempo de inactividad y garantizar que la organización pueda recuperar su capacidad tecnológica en un periodo predefinido.

La importancia de un DRP radica en su capacidad para proteger la supervivencia de la organización frente a escenarios de pérdida total o parcial de datos. En un ecosistema digital interconectado, cada minuto de indisponibilidad se traduce en pérdidas financieras directas, daños reputacionales y posibles sanciones legales. Un DRP bien estructurado permite que el equipo de res-

puesta actúe con precisión y sin dudas bajo presión, reduciendo el caos durante una crisis y asegurando que los objetivos de tiempo de recuperación (RTO) y los puntos de recuperación de datos (RPO) se cumplan según las necesidades del negocio.

Para una implementación exitosa, la recomendación fundamental es realizar un análisis de impacto al negocio (BIA) previo, el cual permite identificar qué sistemas son vitales y en qué orden deben recuperarse. Es un error común intentar recuperar todo al mismo tiempo; la priorización es la clave de la eficiencia. Además, el DRP debe ser un documento dinámico, pues de nada sirve un plan estático que no se actualice tras cambios en la infraestructura de red o la migración a la nube. La documentación debe ser clara, estar disponible fuera del sitio (*off-site*) y ser conocida por los responsables de su ejecución.

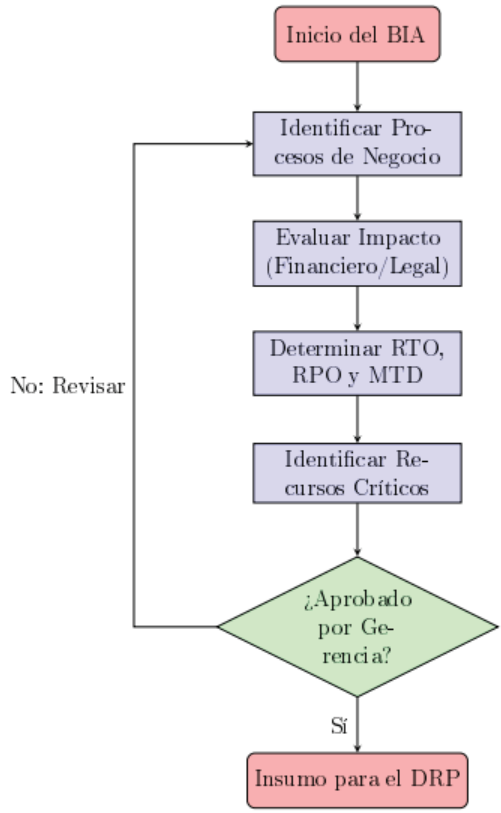
El MTD es el periodo máximo de tiempo que un proceso, servicio o sistema puede permanecer inactivo antes de que la interrupción cause daños inaceptables para la organización, como pérdidas financieras graves, incumplimiento legal, daño reputacional o riesgos operativos críticos.

Dentro del BIA, el MTD actúa como un límite absoluto: una vez superado, la continuidad del negocio ya no es viable en condiciones aceptables. A partir del MTD se definen otros objetivos clave, como el RTO (*Recovery Time Objective*), que siempre debe ser menor al MTD, y el RPO (*Recovery Point Objective*), que establece cuánta información se puede perder sin afectar de forma crítica al negocio.

Finalmente, la recomendación más crítica es la prueba y validación periódica. Un DRP que no se prueba es simplemente una teoría. Se deben realizar simulacros frecuentes, desde revisiones de escritorio hasta pruebas de conmutación (*failover*) reales, para identificar cuellos de botella y errores en los procedimientos. Estas pruebas no solo validan la tecnología, sino que también entrenan al personal en sus roles de emergencia, asegurando que la cultura organizacional esté alineada con la resiliencia tecnológica y que el plan sea verdaderamente ejecutable en el momento de mayor necesidad.

El costo de recuperación aumenta a medida que el RTO y el RPO se acercan a cero. Lograr un RPO de "cero" requiere inversiones masivas en infraestructura de replicación síncrona.

Figura 11. Diagrama de flujo metodológico para el BIA



Fuente: elaboración propia.

Prevención de pérdida de datos (DLP)

Una prevención de pérdida de datos (DLP, por sus siglas en inglés *Data Loss Prevention*) es un conjunto de herramientas y estrategias diseñadas para garantizar que la información sensible de una organización no se pierda, se utilice de manera indebida o se acceda a ella por parte de usuarios no autorizados. Su funcionamiento se basa en la inspección profunda de contenidos y el análisis contextual de los datos en tres estados críticos: en reposo (almacenados en servidores o nubes), en uso (siendo manipulados por una aplicación o usuario) y en tránsito (moviéndose a través de la red). Al identificar datos protegidos, como números de tarjetas, secretos industriales o datos

de salud, el DLP aplica políticas automáticas que pueden ir desde el simple registro del evento hasta el bloqueo total de la acción.

Tabla 12. Métricas de recuperación (RTO y RPO) por niveles de criticidad

Criticidad	RTO (tiempo)	RPO (datos)	Estrategia sugerida
Misión crítica	< 1 hora	Cero (tiempo real)	Espejo/alta disponibilidad
Alta prioridad	1-4 horas	< 1 hora	Respaldos continuos/ replicación
Media	4-24 horas	24 horas (diario)	Respaldo incremental/ diferencial
Baja	> 24 horas	>24 horas	Respaldos semanales/ archivo

Fuente: elaboración propia.

La importancia de implementar un sistema DLP radica en la protección del activo más valioso del ecosistema organizacional moderno: la información. En un entorno donde el teletrabajo y el uso de servicios en la nube han difuminado el perímetro de seguridad tradicional, el DLP actúa como una salvaguarda contra la fuga de datos tanto accidental (un empleado enviando un archivo por error) como maliciosa (un ataque de exfiltración por parte de un hacker o un empleado deshonesto). Además, es un componente indispensable para el cumplimiento normativo, ya que permite a la institución demostrar ante auditores que mantiene controles técnicos rigurosos sobre la privacidad y la propiedad intelectual.

Para una implementación exitosa, la recomendación fundamental es iniciar con una clasificación de datos exhaustiva. No se puede proteger lo que no se conoce; por lo tanto, la organización debe categorizar su información según su nivel de sensibilidad antes de activar reglas de bloqueo. Intentar proteger *"todo"* desde el primer día suele generar una gran cantidad de falsos positivos que interrumpen los procesos de negocio y frustran a los usuarios. Es vital que el despliegue sea gradual, comenzando en un modo de *"solo monitoreo"* para entender los flujos de trabajo reales y ajustar las políticas antes de pasar al modo de prevención activa.

Finalmente, se recomienda involucrar activamente a la cultura organizacional en el proceso. El DLP no debe verse como un sistema de vigilancia "espía", sino como una herramienta de apoyo que educa al usuario. Una buena implementación incluye notificaciones en tiempo real que informan al colaborador por qué una acción ha sido bloqueada, fomentando la conciencia sobre el manejo seguro de la información. Al combinar tecnología avanzada con una estrategia de comunicación clara, el DLP se convierte en un habilitador que permite la colaboración digital sin comprometer la seguridad ni el cumplimiento de la institución.

Otras herramientas

Have I Been Pwned (HIBP)

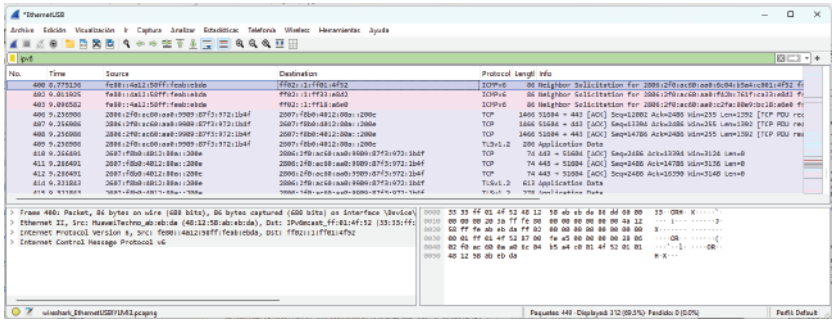
Es una plataforma gratuita de referencia mundial en ciberseguridad, creada por el experto Troy Hunt, que permite a los usuarios verificar si sus correos electrónicos o contraseñas han sido expuestos en filtraciones de datos masivas. Su importancia radica en que actúa como un sistema de alerta temprana y concienciación, permitiendo que las personas y empresas identifiquen vulnerabilidades antes de que sus cuentas sean secuestradas mediante ataques de "relleno de credenciales". Al centralizar miles de millones de registros de brechas de seguridad en una base de datos consultable y segura (que protege la privacidad mediante técnicas de anonimato), HIBP se ha convertido en una herramienta esencial para la higiene digital, impulsando acciones correctivas inmediatas como el cambio de contraseñas comprometidas y la adopción de la autenticación de dos factores (2FA) (Have I Been Pwned, 2026).

Wireshark

Es considerada la herramienta de análisis de protocolos de red más importante y utilizada en el mundo de la ciberseguridad, actuando esencialmente como un "microscopio" para el tráfico digital. Su importancia radica en su capacidad para capturar e inspeccionar paquetes de datos en tiempo real, lo que permite a los analistas desglosar cada capa de una comunicación para identificar compor-

tamientos anómalos, intentos de intrusión o exfiltración de información (Wireshark, 2026).

Figura 12. Ejemplo de captura de paquetes con Wireshark



Fuente: Wireshark (2026).

VeraCrypt

Se ha consolidado como una herramienta fundamental en la ciberseguridad moderna debido a su capacidad para implementar un cifrado de disco completo (FDE) y de archivos de código abierto, lo que garantiza la transparencia y la ausencia de "puertas traseras". Su importancia radica en la protección de la confidencialidad de los datos en reposo, mitigando los riesgos derivados del robo físico de dispositivos o el acceso no autorizado a particiones sensibles.

Al utilizar algoritmos de cifrado robustos como AES, Serpent y Twofish, junto con técnicas de derivación de claves que ralentizan los ataques de fuerza bruta, VeraCrypt ofrece una capa de defensa crítica tanto para usuarios individuales como para organizaciones que manejan información clasificada. Además, su función de negación plausible, que permite crear volúmenes ocultos, es vital en escenarios de alta seguridad donde el usuario podría verse coaccionado a revelar sus contraseñas. Adicionalmente están las herramientas propietarias de Microsoft Windows: BitLocker, y de Apple MacOS: FileVault (VeraCrypt, 2025).

Network Mapper (Nmap)

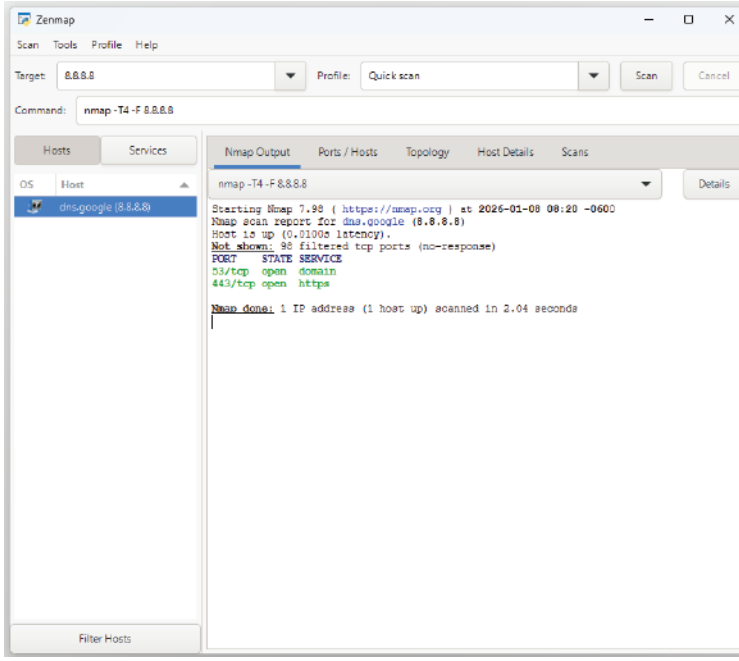
Es una herramienta de código abierto y gratuita que se utiliza para la exploración de redes, la auditoría de seguridad y el escaneo de puertos. Es el estándar para descubrimiento tanto para administradores de sistemas como para profesionales de la ciberseguridad.

Envía paquetes diseñados específicamente a una red o un equipo objetivo y luego analiza las respuestas para determinar qué está sucediendo en esa red. Nmap es extremadamente versátil y se utiliza para resolver cuatro preguntas fundamentales sobre una red:

1. *Descubrimiento de hosts:* ¿qué dispositivos (computadoras, servidores, teléfonos, routers) están encendidos y conectados a la red?
2. *Escaneo de puertos:* ¿qué "puertas" (puertos lógicos) están abiertas en esos dispositivos? (por ejemplo: el puerto 80 para web o el 22 para SSH).
3. *Detección de servicios:* ¿qué aplicaciones específicas y qué versiones están corriendo en esos puertos abiertos?
4. *Detección de sistema operativo:* ¿el objetivo está usando Windows, Linux, macOS o algún sistema especializado?

Zenmap es la interfaz gráfica oficial del escáner de seguridad de Nmap. Es una aplicación multiplataforma (Linux, Windows, Mac OS X, BSD, entre otras) gratuita y de código abierto que facilita su uso a principiantes, a la vez que ofrece funciones avanzadas para usuarios experimentados. Los análisis frecuentes se pueden guardar como perfiles para facilitar su ejecución repetida. Un creador de comandos permite la creación interactiva de líneas de comando de Nmap. Los resultados de los análisis se pueden guardar y consultar posteriormente (Nmap, 2026).

Figura 13. Ejemplo escaneo de servicios
con NMAP modo gráfico (Zenmap)



Fuente: Nmap (2026).

VirusTotal

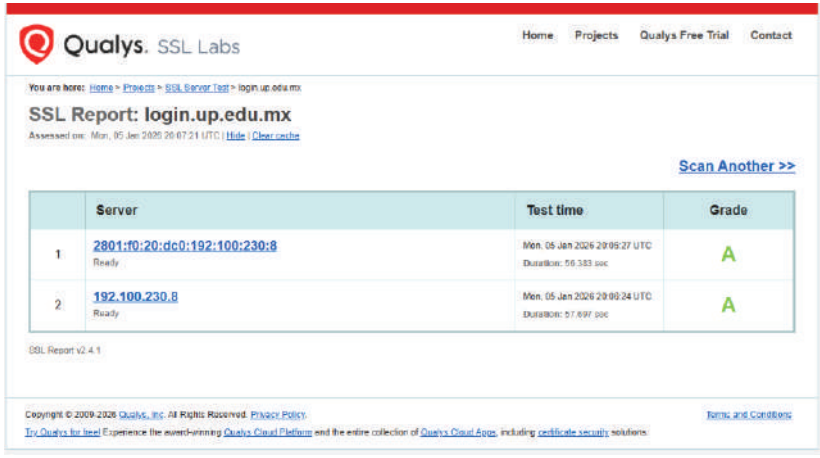
Es una herramienta fundamental en el ecosistema de la ciberseguridad, ya que actúa como un agregador masivo de inteligencia colectiva que permite analizar archivos y URLs sospechosas en tiempo real. Su importancia radica en su capacidad para contrastar una amenaza potencial contra más de 70 motores de antivirus y diversas herramientas de inspección técnica, lo que reduce drásticamente los falsos negativos y permite una detección temprana de *malware*. Al centralizar datos de múltiples proveedores y ofrecer información detallada sobre el comportamiento de las muestras, VirusTotal no solo ayuda a los usuarios individuales, sino que también facilita a los analistas de seguridad la identificación de infraestructuras maliciosas y la comprensión de nuevas tendencias de ataque a nivel global (VirusTotal, 2026).

SSL Labs

Desarrollado por Qualys, es una herramienta fundamental en la ciberseguridad moderna porque proporciona una auditoría profunda y gratuita de la configuración de SSL/TLS de un servidor web. Su importancia radica en que permite a los administradores identificar vulnerabilidades críticas, como versiones de protocolos obsoletas o cifrados débiles, antes de que puedan ser explotados por atacantes.

Al asignar una calificación de la "A" a la "F", ofrece una métrica clara sobre la salud del cifrado de un sitio, ayudando a las organizaciones a cumplir con estándares de cumplimiento (como PCI DSS) y a garantizar la integridad y confidencialidad de los datos de los usuarios. En un panorama donde los ataques de interceptación son constantes, SSL Labs se convierte en el estándar de oro para validar que la comunicación entre el cliente y el servidor es realmente segura (SSL Labs, 2026a, 2026b).

Figura 14. Ejemplo evaluación con SSL Labs



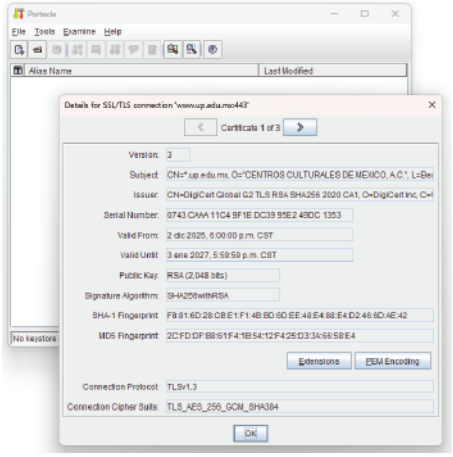
Fuente: SSL Labs (2026b).

Portecle

Es una herramienta en Java muy útil para el manejo de:

- Administrar y consultar almacenes de llaves.
- Generar par de llaves (pública y privada).
- Importar certificados.
- Examinar conexiones SSL\TLS.
- Examinar solicitudes de certificados (SourceForge, 2026).

Figura 15. Ejemplo de certificado con Portecle



Fuente: SourceForge (2026).

Protocolos

La comprensión profunda de los protocolos de comunicación constituye el pilar fundamental sobre el cual se erige cualquier arquitectura de defensa resiliente. Debido a que estos estándares definen las reglas de interacción y el intercambio de datos entre entidades de red, su conocimiento técnico permite a los especialistas en ciberseguridad identificar vectores de ataque específicos y vulnerabilidades de diseño, tales como la exposición de credenciales en texto plano o la susceptibilidad a la interceptación de tráfico. Sin este dominio, la implementación de controles de seguridad resultaría superficial, dejando brechas críticas en la superficie de exposición que podrían

ser aprovechadas para comprometer la integridad y la disponibilidad de los activos digitales.

Asimismo, el dominio de los protocolos es indispensable para la ejecución de estrategias de endurecimiento (*hardening*) y la configuración precisa de sistemas de detección de intrusiones. Al comprender la estructura y el comportamiento esperado de protocolos como TLS, IPsec o DNS, los administradores pueden diferenciar el tráfico legítimo de actividades anómalas, como el tunelizado malicioso o el escaneo de puertos. En última instancia, la correcta alineación entre las políticas de seguridad y la configuración técnica de los protocolos garantiza el cumplimiento de los estándares internacionales y fortalece la postura de seguridad frente a amenazas persistentes avanzadas que operan en las capas más profundas de la red.

Lightweight Directory Access Protocol (*LDAP*)

Es un protocolo de red estándar que permite a las aplicaciones y servicios consultar y gestionar información sobre usuarios, dispositivos y recursos dentro de un directorio jerárquico. Es como una base de datos especializada y altamente organizada, donde en lugar de solo nombres y números, se almacenan credenciales de acceso, permisos de grupo, direcciones de correo y otros atributos de identidad. Al ser "ligero", está optimizado para realizar búsquedas rápidas y eficientes en grandes volúmenes de datos, facilitando que diversos sistemas se comuniquen con un servidor central –como Microsoft Active Directory– para verificar quién es un usuario y qué puede hacer.

En el ámbito de la seguridad, LDAP es fundamental porque establece un punto único de verdad para la autenticación. En lugar de que cada aplicación gestione su propia base de datos de usuarios (lo que crearía silos de información vulnerables), las organizaciones utilizan LDAP para centralizar el control. Esto mejora la seguridad al permitir la implementación de políticas de contraseñas consistentes y el uso de LDAPS (LDAP sobre SSL/TLS), que cifra la comunicación entre el cliente y el servidor para evitar que atacantes intercepten credenciales en tránsito. Además, facilita la revocación inmediata de accesos: si un empleado deja la empresa, desactivar su

cuenta en el directorio LDAP corta automáticamente su acceso a todos los sistemas conectados.

Dentro de una estrategia de IAM (por sus siglas en inglés, *Identity and Access Management*), LDAP actúa como la infraestructura base o el "almacén de identidades" que alimenta el ciclo de vida del usuario. Su función principal es dar soporte al inicio de sesión único sesión único (SSO, por sus siglas en inglés, *Single Sign-On*), permitiendo que un usuario acceda a múltiples recursos con una sola identidad. Mientras que el IAM se encarga de la gobernanza, las políticas y los flujos de trabajo (quién debe tener acceso y por qué), LDAP es el protocolo que ejecuta la verificación técnica de esas identidades y distribuye los atributos necesarios para que las herramientas de IAM tomen decisiones de autorización precisas en tiempo real.

En el Anexo C.1.1, C.1.2 y C.1.3, se encuentra un ejemplo de conexión al LDAP con Java. La primera clase es la clase principal, que requiere a las otras 2 para permitir certificados autofirmados. En el Anexo C.2.1 está el código en PHP que también permite certificados autofirmados.

Protocolos seguros

Los protocolos seguros son los siguientes:

TLS 1.3 (*Transport Layer Security):* el sucesor de SSL, cifra la comunicación web (el candado o llave en el navegador).

Secure Shell (*SSH):* para administrar servidores de forma remota y segura (reemplazo de Telnet).

Internet Protocol Security (*IPsec):* conjunto de protocolos para asegurar comunicaciones IP autenticando y cifrando cada paquete (base de muchas VPNs).

Hypertext Transfer Protocol Secure (*HTTPS):* HTTP sobre TLS, es el estándar de navegación web segura.

SSH File Transfer Protocol (*SFTP):* transferencia de archivos segura utilizando el canal cifrado de SSH.

Wi-fi Protected Access 3 (WPA3): el protocolo de seguridad más actual para redes inalámbricas, con mejor cifrado que WPA2.

Domain Name System Security Extensions (DNSSEC): protege contra ataques de suplantación de identidad en el sistema de nombres de dominio (evita que te redirijan a webs falsas).

Kerberos: protocolo de autenticación de redes que permite a nodos comunicarse sobre una red insegura para probar su identidad de manera segura (muy usado en Windows/Active Directory).

Protocolos monitoreo

Los protocolos de monitoreo:

Simple Network Management Protocol v3 (SNMPv3): a diferencia de las versiones 1 y 2, esta versión incluye autenticación y cifrado para gestionar dispositivos de red.

Secure/Multipurpose Internet Mail Extensions (S/MIME): estándar para cifrado de clave pública y firma de correo electrónico.

Domain-based Message Authentication, Reporting, and Conformance (DMARC): protocolo de autenticación de correo para prevenir *spoofing* (suplantación) y *phishing*.

WireGuard: un protocolo de VPN moderno, más rápido y fácil de configurar que IPsec o OpenVPN.

OAuth 2.0: estándar abierto para autorización (no autenticación) de acceso, usado para iniciar sesión con Google o Facebook en otras webs.

Extensible Authentication Protocol-Transport Layer Security (EAP-TLS): uno de los estándares más seguros para autenticación en redes wi-fi empresariales usando certificados.

Security Assertion Markup Language (*SAML):* estándar abierto basado en el lenguaje XML que permite el intercambio de datos de autenticación y autorización entre dos partes: un Proveedor de identidad (IdP) y un proveedor de servicios (SP). En ciberseguridad, SAML es el estándar de predeterminado para implementar el inicio de sesión único (SSO) o, permitiendo que un usuario acceda a múltiples aplicaciones con una sola credencial, eliminando la necesidad de recordar decenas de contraseñas (personalmente solo le veo un inconveniente, pero está fuera del alcance de este libro).

Estándares

En ciberseguridad son marcos de trabajo, normas y directrices técnicas que establecen un "lenguaje común" para proteger la información. Sin ellos, cada empresa u organización intentaría protegerse de forma improvisada, lo que dejaría enormes huecos de seguridad.

En un mundo donde las empresas usan software de diferentes proveedores (Microsoft, Google, Cisco, etcétera), los estándares aseguran que todos los sistemas puedan comunicarse de forma segura. Por ejemplo, gracias a los estándares de cifrado, tu navegador web puede conectarse de forma segura a cualquier servidor del mundo sin necesidad de una configuración especial.

Algunos estándares importantes son:

IEC 62443

IEC 62443 es el estándar internacional para la ciberseguridad en sistemas de control industrial (OT) y automatización (fábricas, plantas eléctricas) (IEC, 2026). Es el marco de referencia internacional más crítico para la seguridad de los sistemas de automatización y control industrial (IACS).

A diferencia de los estándares de TI tradicionales que priorizan la confidencialidad de los datos, esta norma se centra en la disponibilidad, integridad y seguridad física de los procesos industriales, protegiendo infraestructuras vitales como plantas de energía, redes de agua y sistemas de manufactura. Su enfoque integral abarca no solo los componentes tecnológicos, sino también las políticas, los procedimientos y las capacidades del personal, estableciendo un

ecosistema de seguridad que mitiga riesgos ante ataques cibernéticos que podrían tener consecuencias físicas reales.

Una de las innovaciones más importantes de este estándar es su metodología de "zonas y conductos" y la definición de niveles de seguridad (*Security Levels*). La norma propone segmentar la red industrial en zonas lógicas basadas en su función y criticidad, controlando estrictamente las comunicaciones entre ellas a través de conductos protegidos. Además, permite a las organizaciones escalar sus defensas del nivel 1 al 4, donde el nivel más alto está diseñado para resistir ataques sofisticados de actores estatales. Este enfoque de "defensa en profundidad" asegura que, incluso si una zona se ve comprometida, el impacto se mantenga contenido, garantizando la continuidad operativa de la infraestructura crítica.

Reglamento General de Protección de Datos (RGPD o GDPR)

El Reglamento General de Protección de Datos (RGPD), también conocido como GDPR (por sus siglas en inglés, General Data Protection Regulation), aunque es una ley europea, se ha convertido en un estándar de facto mundial para la privacidad y protección de datos personales.

El GDPR es el marco jurídico más estricto del mundo en materia de privacidad y seguridad de la información personal, entrando en vigor en la Unión Europea en mayo de 2018. Su objetivo principal es devolver a los ciudadanos el control sobre sus datos personales y unificar las normativas de privacidad en todo el mercado común. Este reglamento no solo afecta a las empresas con sede en Europa, sino a cualquier organización a nivel global que ofrezca bienes o servicios a residentes de la UE o que monitoree su comportamiento, estableciendo multas severas que pueden alcanzar los 20 millones de euros o el 4 % de la facturación anual global de la empresa infractora.

La importancia del GDPR en la ciberseguridad radica en que obliga a las organizaciones a implementar la "privacidad desde el diseño y por defecto". Esto significa que la seguridad no puede ser una capa añadida al final, sino un componente fundamental del desarrollo de cualquier sistema. Entre sus exigencias clave se encuentra el derecho al olvido, la portabilidad de los datos y la obli-

gación de notificar cualquier brecha de seguridad a las autoridades competentes en un plazo máximo de 72 horas.

Al estandarizar estos procesos, el GDPR ha elevado el listón de la protección de datos a nivel internacional, convirtiéndose en el modelo a seguir para legislaciones similares en otros países, como la LGPD en Brasil. La Ley sobre Protección de la Vida Privada (LPVP) en Chile, la Ley de Protección de Datos Personales - Ley 25.326 (LPDP) en Argentina, mientras que la Personal Information Protection and Electronic Documents Act (PIPEDA) en Canadá.

En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) es la norma que rige a las empresas y negocios privados, mientras que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) es la ley que rige a todas las instituciones del Estado y organismos públicos.

Federal Information Processing Standards (FIPS)

FIPS 140-2/140-3 es el estándar del gobierno de EE.UU. que especifica los requisitos de seguridad para módulos criptográficos (hardware y software). Estos estándares y directrices son desarrollados por el gobierno de los Estados Unidos, específicamente por el NIST, para ser utilizados en sistemas informáticos por agencias gubernamentales no militares y contratistas del gobierno.

Su objetivo es establecer requisitos mínimos de seguridad y operatividad, asegurando que todas las instituciones federales utilicen tecnologías compatibles y de alta calidad. Aunque son obligatorios solo para el sector público estadounidense, se han convertido en una referencia de oro a nivel mundial en la industria privada, donde las empresas buscan la "certificación FIPS" para demostrar que sus productos cumplen con niveles de cifrado y protección de datos extremadamente rigurosos.

El estándar más reconocido dentro de esta familia es el FIPS 140-2 (y su sucesor 140-3), que se centra específicamente en los módulos criptográficos. Este estándar evalúa tanto el hardware como el software para garantizar que el cifrado de la información sea resistente a ataques físicos y lógicos. Cuando una aplicación o dispositivo cumple con FIPS, garantiza que los algoritmos utilizados (como AES para cifrado o SHA para firmas digitales) han sido imple-

mentados correctamente y no contienen debilidades conocidas, lo que proporciona una capa de confianza esencial para la protección de infraestructuras críticas y datos sensibles en todo el mundo (NIST, 2001b, 2019).

Service Organization Control 2 (SOC 2)

El Service Organization Control 2 (SOC 2) es un estándar de auditoría desarrollado por el American Institute of Certified Public Accountants (AICPA) que evalúa cómo una organización gestiona y protege la información de sus clientes. Está diseñado especialmente para empresas de servicios tecnológicos y proveedores de servicios en la nube, y se basa en cinco criterios de confianza: seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad. El objetivo principal del SOC 2 es demostrar que la organización cuenta con controles internos adecuados para salvaguardar los datos y reducir riesgos operativos y de seguridad (AICPA, 2017).

Existen dos tipos de informes SOC 2: tipo I, que evalúa el diseño de los controles en un momento específico en el tiempo, y tipo II, que analiza tanto el diseño como la efectividad operativa de dichos controles durante un período determinado. Obtener un informe SOC 2 no es una certificación, sino una evaluación independiente que brinda confianza a clientes, socios y reguladores sobre la madurez de los procesos de control interno de la organización, siendo especialmente relevante en entornos B2B y en sectores donde la protección de la información es crítica.

Common Criteria (ISO/IEC 15408)

El Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) es un estándar internacional que proporciona un marco formal para la especificación, implementación y evaluación de la seguridad de productos y sistemas de tecnologías de la información para certificar que un producto de software o hardware de seguridad cumple con lo que promete.

Su objetivo principal es establecer un lenguaje común y criterios técnicos que permitan evaluar de manera consistente las propiedades de seguridad, asegurando que los productos cumplan con requisitos de confidencialidad, integridad y disponibilidad. El

estándar es ampliamente utilizado para la certificación de componentes como sistemas operativos, dispositivos de red, tarjetas inteligentes y soluciones criptográficas (ISO–IEC, 2009).

El estándar ISO/IEC 15408 se estructura en tres partes: conceptos y modelos de seguridad, requisitos funcionales de seguridad (SFR) y requisitos de aseguramiento de seguridad (SAR). A partir de estos elementos, se definen los Evaluation Assurance Levels (EAL), que van del EAL1 al EAL7 y reflejan distintos niveles de rigor en el proceso de evaluación. La certificación bajo Common Criteria permite a organizaciones y gobiernos confiar en que un producto ha sido evaluado de forma independiente bajo un esquema reconocido internacionalmente, facilitando la aceptación de soluciones de seguridad en mercados regulados y de alta criticidad.

Otros marcos de referencia

- *NIST CSF:* marco de trabajo del gobierno de EE.UU. (pero usado mundialmente) basado en cinco pilares: identificar, proteger, detectar, responder y recuperar.[11]
- *CIS Controls:* una lista priorizada de acciones defensivas (anteriormente conocidos como los SANS Top 20).[12]
- *ISO/IEC 27001:* el estándar internacional más famoso para la gestión de la seguridad de la información (SGSI). Define cómo gestionar el riesgo.[13]
- *PCI-DSS:* estándar obligatorio para cualquier empresa que procese, almacene o transmita datos de tarjetas de crédito/débito.[14]
- *OWASP ASVS:* un estándar para probar y verificar la seguridad técnica de aplicaciones web.[15]

---

[11] Más información en Marco de referencia/NIST CSF 2.0 de la presente obra.

[12] Más información en Marco de referencia/Center for Internet Security/CIS Critical Security Controls de la presente obra.

[13] Más información en Marco de referencia/Familia ISO/IEC 27001/ISO/IEC 27001 y 27002 de la presente obra.

[14] Más información en Marco de referencia/Payment Card Industry Data Security Estándar (PCI DSS) de la presente obra.

[15] Más información en Marco de referencia/OWASP SAMM y OWASP ASVS/Application Security Verification Standard (OWASP ASVS) de la presente obra.

GESTIÓN DE RIESGOS Y VULNERABILIDADES

La seguridad del software es el concepto de implementar mecanismos en la construcción de la seguridad para ayudarla a permanecer funcional (o resistente) a los ataques. Esto significa que una pieza de software se somete a pruebas de seguridad antes de salir al mercado para comprobar su capacidad para resistir ataques maliciosos. Un fallo en software, o bug, puede o no poner en riesgo la seguridad. Si pone el riesgo, se conoce como vulnerabilidad, esto se corrige con un parche o una actualización (ver versiones) Si la vulnerabilidad se aprovecha antes de que el desarrollador tenga un parche, se conoce como Día Cero.

Pueden existir vulnerabilidades en el hardware, algunos ejemplos son:

1. *Fallos en chips de TPM:* permiten extraer claves encriptadas.

2. *Meltdown y Spectre (2018):* son vulnerabilidades encontradas en muchos procesadores (CPU) modernos de Intel, AMD y ARM. No eran fallas de software, sino de diseño del hardware del procesador.

3. *Rowhammer (el martillo de filas):* vulnerabilidad puramente física. No es un error de código, es un problema de "vecindad ruidosa" en los componentes eléctricos microscópicos de tu memoria RAM.

4. *Hertzbleed (el sangrado de hertzios):* vulnerabilidad que permite robar claves criptográficas que se creían seguras

> porque usa una característica que supuestamente es buena, el ahorro de energía y el "Turbo Boost".

El hardware se compone principalmente de componentes mecánicos, eléctricos y/o electrónicos. Los componentes mecánicos, sufren desgaste por la fricción, por ejemplo un disco duro o un ventilador. Los componentes eléctricos son sensibles a variaciones de voltaje o fuera de especificaciones (por ejemplo, temperatura en los sites). Este tipo de fallas también se pueden convertir en vulnerabilidad.

Gestión de riesgos

La gestión de riesgos implica identificar de forma sistemática las amenazas y vulnerabilidades que pueden afectar a una organización, sus procesos, activos e información. Incluye reconocer eventos potenciales, estimar su probabilidad y evaluar el impacto que tendrían si llegaran a materializarse.

También implica analizar y priorizar esos riesgos para decidir qué controles o medidas deben aplicarse. Esto puede incluir aceptar, mitigar, transferir o evitar los riesgos, dependiendo del nivel de tolerancia definido por la organización y de los recursos disponibles para tratarlos.

Finalmente, la gestión de riesgos requiere un seguimiento continuo y la actualización de las evaluaciones conforme cambian las amenazas, tecnologías y condiciones de negocio. No es un proceso puntual, sino un ciclo constante que busca asegurar que los riesgos se mantengan dentro de niveles aceptables y alineados con los objetivos estratégicos (ISO, 2018; NIST, 2012).

Componentes de los riesgos

Los componentes principales de todo riesgo suelen resumirse en tres elementos fundamentales que permiten evaluarlo y gestionarlo adecuadamente:

Amenaza

Es el agente, evento o circunstancia que puede causar daño. Puede ser intencional (como un ciberataque), accidental (un error humano) o natural (un terremoto). La amenaza es lo que podría ocurrir.

Vulnerabilidad

Es la debilidad o falta de control que permite que la amenaza tenga efecto. Puede ser técnica (un sistema sin parches), organizacional (falta de políticas), física (acceso no controlado) o humana (falta de capacitación).

Impacto

Es la consecuencia o daño resultante si la amenaza explota la vulnerabilidad. Puede afectar la operación, reputación, finanzas, cumplimiento regulatorio, disponibilidad de servicios o la confidencialidad de la información.

Con estos componentes se puede definir:

Riesgo = amenaza + vulnerabilidad + impacto.
(Fórmula del riesgo)

Sin la presencia de estos tres componentes simultáneamente no existe un riesgo real.

Categorías

Existen categorías de riesgos ampliamente aceptadas y usadas como estándares en gestión de riesgos (ISO 31000, COSO ERM, NIST, etcétera).

1. *Riesgos estratégicos:* relacionados con decisiones de negocio, mercados, competencia, reputación o estrategias fallidas.

2. *Riesgos operacionales:* provienen de fallas en procesos internos, personas, sistemas o factores externos. Incluye

errores humanos, fallos de procedimientos, interrupciones operativas.

3. *Riesgos financieros:* asociados a liquidez, crédito, tasas de interés, mercado, inversión o pérdidas económicas.

4. *Riesgos de cumplimiento/regulatorios:* derivados de incumplir leyes, normas, contratos, políticas internas o estándares requeridos.

5. *Riesgos tecnológicos/de TI:* fallas de sistemas, indisponibilidad, obsolescencia, problemas de infraestructura, mal uso de tecnología.

6. *Riesgos de ciberseguridad:* ataques, brechas de datos, *malware*, *ransomware*, intrusiones, accesos no autorizados.

7. *Riesgos humanos:* rotación de personal, falta de capacitación, negligencia, conflictos laborales, capacidades insuficientes.

8. *Riesgos de seguridad física:* accesos no autorizados, robo, vandalismo, incendios, desastres físicos o fallas en controles ambientales.

9. *Riesgos ambientales/naturales:* fenómenos naturales (terremotos, inundaciones, huracanes), impactos ecológicos o medioambientales.

10. *Riesgos de proveedores/terceros:* dependencia excesiva, fallas en la cadena de suministro, incumplimientos o baja calidad del servicio.

11. *Riesgos reputacionales:* pérdida de confianza del público, crisis mediáticas, quejas masivas, impacto negativo en la marca.

12. *Riesgos legales:* demandas, litigios, sanciones, disputas contractuales o responsabilidad civil.

Activos relacionados

La gestión de riesgos no comienza con la tecnología, sino con el inventario de activos. Un activo no es solo un servidor en el rack, es el flujo de datos que permite la facturación o la confianza que el cliente deposita en la institución. Al categorizar los activos en información, software, hardware y servicios, la organización puede aplicar de manera estratégica las funciones de PROTECT e IDENTIFY del NIST CSF 2.0, asegurando que los recursos de mitigación se asignen proporcionalmente al valor real que cada elemento aporta al negocio.

Los activos relacionados son todos aquellos elementos que aportan valor al negocio y cuya confidencialidad, integridad o disponibilidad puede verse afectada por una amenaza. Identificarlos correctamente es un paso fundamental para evaluar riesgos de forma consistente.

Algoritmo de evaluación del riesgo

Se recomienda tener un catálogo de riesgos, en este se puede definir el algoritmo de evaluación del riesgo para cada uno de los diferentes tipos.

Tabla 13. Ejemplo de catálogo de riesgos

Id	Nombre	Descripción
R-AC-1	Incapacidad para mantener la responsabilidad individual	No se mantiene la propiedad de los activos y no es posible que no se repudie ninguna acción o inacción.
R-AC-2	Asignación inadecuada de funciones privilegiadas	No se implementan los privilegios mínimos.
R-AC-3	Escalada de privilegios	El acceso a funciones privilegiadas es inadecuado o no se puede controlar.
R-AC-4	Acceso no autorizado	Se concede acceso a personas, grupos o servicios no autorizados.
R-AM-1	Activos perdidos, dañados o robados	Se pierden, dañan o roban activos.
R-AM-2	Pérdida de integridad a través de cambios no autorizados	Los cambios no autorizados corrompen la integridad del sistema, la aplicación o el servicio.
R-BC-1	interrupción comercial	Hay una mayor latencia o una interrupción del servicio que afecta negativamente las operaciones comerciales.
R-BC-2	Pérdida/corrupción de datos	No se mantiene la confidencialidad de los datos (compromiso) o los datos se corrompen (pérdida).
R-BC-3	Reducción de la productividad	La productividad del usuario se ve afectada negativamente por el incidente.
R-EX-1	Pérdida de ingresos	Se produce una pérdida financiera debido a la pérdida de clientes o la incapacidad de generar ingresos futuros.
R-EX-2	Contrato cancelado	Se cancela un contrato debido a la violación de una cláusula contractual.
R-EX-3	Disminución de la ventaja competitiva	Se pone en peligro la ventaja competitiva de la organización.
R-EX-4	Disminución de la reputación	La publicidad negativa empaña la reputación de la organización.

Id	Nombre	Descripción
R-EX-5	Multas y sentencias	El incumplimiento de las normas legales, reglamentarias o contractuales da lugar a daños legales o financieros. Existen vulnerabilidades técnicas mitigadas sin controles compensatorios u otras acciones de mitigación.
R-EX-6	Vulnerabilidades no mitigadas	El sistema/aplicación /servicio se ve comprometido y afecta su confidencialidad, integridad, disponibilidad y/o seguridad.
R-EX-7	Compromiso del sistema	El *malware*, el *phishing*, la piratería u otros ataques técnicos comprometen datos, sistemas, aplicaciones o servicios.
R-BC-4	Pérdida/corrupción de información o compromiso del sistema debido a un ataque técnico	La ingeniería social, el sabotaje u otros ataques no técnicos comprometen datos, sistemas, aplicaciones o servicios.
R-BC-5	Pérdida/corrupción de información o compromiso del sistema debido a un ataque no técnico	Las prácticas de seguridad/privacidad implementadas son insuficientes para respaldar los requisitos de tecnologías y procesos seguros de la organización.
R-GV-1	Incapacidad para respaldar los procesos comerciales	No existen prácticas internas o son inadecuadas. Los procedimientos no cumplen con las "prácticas razonables" esperadas por los estándares de la industria.
R-GV-4	Prácticas internas inadecuadas	No existen prácticas de terceros o son inadecuadas. Los procedimientos no cumplen con las prácticas razonables esperadas por los estándares de la industria.
R-GV-5	Prácticas de terceros inadecuadas	No existen funciones y responsabilidades documentadas de seguridad/privacidad o son inadecuadas.
R-GV-3	Falta de roles y responsabilidades	El alcance de los controles es incorrecto o inadecuado, lo que conduce a una posible brecha o falla en la cobertura de los controles de seguridad/privacidad.

Id	Nombre	Descripción
R-GV-2	Alcance incorrecto de los controles	Hay contenido abusivo/discurso dañino/ amenazas de violencia/contenido ilegal que afecta negativamente las operaciones comerciales.
R-GV-8	Contenido ilegal o acción abusiva	No se pueden detectar incidentes.
R-SA-1	Incapacidad para mantener la conciencia situacional	El personal carece de conocimientos a nivel de usuario sobre los principios de seguridad y privacidad.
R-SA-2	Falta de una fuerza laboral preocupada por la seguridad	No se ejerce la debida diligencia o el debido cuidado en la supervisión de los controles internos de seguridad y privacidad de la organización.
R-GV-6	Falta de supervisión de los controles internos	No se ejerce la debida diligencia o el debido cuidado en la supervisión de los controles de seguridad y privacidad operados por proveedores de servicios externos.
R-GV-7	Falta de supervisión de los controles de terceros	Las acciones de respuesta corrompen las pruebas o impiden la capacidad de procesar los incidentes.
R-IR-1	Incapacidad para investigar/procesar incidentes	Las acciones de respuesta no actúan de manera adecuada y oportuna para abordar el incidente de manera adecuada.
R-IR-2	Respuesta inadecuada a los incidentes	No hay supervisión para garantizar que las acciones de remediación sean correctas o efectivas.
R-IR-3	Ineficacia acciones de remediación	Existen repercusiones financieras por responder a un incidente o una pérdida.
R-IR-4	Gastos asociados con la gestión de un evento de pérdida	Existen repercusiones financieras por responder a un incidente o pérdida.

Fuente: elaboración propia con datos de Simplerisk.com

Mitigación de riesgos

La mitigación de riesgos consiste en el conjunto de acciones planificadas y sistemáticas destinadas a reducir la probabilidad de ocurrencia de un riesgo y/o el impacto de sus consecuencias, hasta un nivel aceptable para la organización. En el contexto de tecnologías de la información y ciberseguridad, implica identificar amenazas y vulnerabilidades, evaluarlas, y aplicar controles técnicos, administrativos y operativos que permitan prevenir incidentes, detectarlos oportunamente y responder de forma efectiva. La mitigación no siempre elimina el riesgo por completo, pero busca gestionarlo de manera consciente y controlada, alineándolo con los objetivos del negocio y el apetito de riesgo definido (ISO, 2018).

Entre las principales recomendaciones para una adecuada mitigación de riesgos se encuentran: realizar evaluaciones de riesgo periódicas y actualizadas; aplicar estándares y marcos reconocidos como ISO/IEC 27001, NIST o CIS Controls; implementar controles de seguridad como autenticación fuerte, cifrado de datos, segmentación de redes y gestión de parches, y adoptar el principio de mínimo privilegio.

Asimismo, es clave contar con herramientas de monitoreo y respuesta como SIEM y XDR, establecer planes de respuesta a incidentes y continuidad del negocio, y fomentar la concienciación y capacitación del personal, ya que el factor humano sigue siendo uno de los principales vectores de riesgo.

Dentro del ciclo de gestión de riesgos, la mitigación es la fase de acción técnica y administrativa que responde a los hallazgos del BIA y el análisis de vulnerabilidades que mencionamos anteriormente.

Estrategias de mitigación en enfoques principales:

- *Reducción (mitigación propiamente dicha):* implementar controles para bajar el riesgo (por ejemplo, instalar un *firewall* o usar DLP).
- *Transferencia:* pasar el impacto financiero a un tercero (por ejemplo, contratar un ciberseguro).
- *Eliminación:* cambiar el proceso para evitar la exposición (por ejemplo, dejar de recolectar ciertos datos sensibles que no son vitales).

» *Aceptación:* decidir conscientemente que el costo de mitigar es mayor que el daño potencial, manteniendo el riesgo bajo monitoreo.

Para que la mitigación no sea solo un gasto, sino una inversión estratégica, te recomendamos:

1. *Priorización basada en el riesgo:* no todos los riesgos merecen la misma inversión. Utiliza la matriz de impacto vs. probabilidad para mitigar primero aquello que sea "muy probable" y de "alto impacto".

2. *Defensa en profundidad:* no confíes en un solo control. Si un control de red falla, debe haber uno de *endpoint* (EDR) o de identidad (SAML/SSO) que contenga la amenaza.

3. *Costo-beneficio:* la medida de mitigación no debe ser más cara que el activo que protege. Es fundamental alinear esto con los presupuestos de la gobernanza de TI.

4. *Monitoreo continuo:* el entorno de amenazas cambia diariamente. Una medida de mitigación que fue efectiva el año pasado (como un antivirus tradicional) puede ser obsoleta hoy frente a un *ransomware* moderno.

5. *Automatización:* siempre que sea posible, utiliza herramientas que mitiguen en tiempo real, como reglas de bloqueo automático en el WAF o revocación de accesos mediante SCIM cuando se detecta un comportamiento anómalo.

La mitigación de riesgos no es un evento único, sino un proceso dinámico de ajuste constante entre la operatividad del negocio y la seguridad. Una mitigación exitosa es aquella que logra un equilibrio donde los controles técnicos, como el cifrado y la segmentación, se fusionan con políticas administrativas claras, creando una arquitectura resiliente capaz de absorber impactos sin interrumpir las funciones críticas identificadas en el BIA.

Vulnerabilidades

Una vulnerabilidad es una debilidad, falla o condición en un sistema, proceso, aplicación, dispositivo o comportamiento humano que puede ser explotada por una amenaza para causar un daño o impacto negativo. En otras palabras, es un punto débil que facilita que un atacante consiga acceso no autorizado, altere información, interrumpa servicios o comprometa la seguridad de la organización.

Las vulnerabilidades pueden aparecer por errores de configuración, fallas de diseño, software desactualizado, malas prácticas, falta de controles, o incluso comportamientos humanos inseguros. Por sí sola, una vulnerabilidad no causa daño. El riesgo surge cuando una amenaza la aprovecha. Por eso, identificarlas, evaluarlas y corregirlas es esencial para reducir el riesgo de incidentes de ciberseguridad.

Las vulnerabilidades se pueden clasificar de acuerdo con diferentes criterios, incluyendo su impacto, su gravedad y su tipo.

Clasificación de las vulnerabilidades

Las vulnerabilidades se pueden clasificar de acuerdo con diferentes criterios, incluyendo su impacto, su gravedad y su tipo.

1. *Impacto:* el impacto de una vulnerabilidad se refiere a los daños que puede causar a un sistema informático. Las vulnerabilidades se pueden clasificar en tres categorías de impacto:
    - *Alta:* las vulnerabilidades de alta impactan significativamente en la seguridad de un sistema informático. Pueden permitir que un atacante obtenga acceso no autorizado a los datos, modifique o elimine datos, o interrumpa el funcionamiento del sistema.
    - *Media:* las vulnerabilidades de media impactan moderadamente en la seguridad de un sistema informático. Pueden permitir que un atacante obtenga acceso limitado a los datos o interrumpa el funcionamiento del sistema de forma temporal.
    - *Baja:* las vulnerabilidades de baja impactan mínimamente en la seguridad de un sistema informático.

Pueden permitir que un atacante obtenga información confidencial, pero no pueden causar daños significativos.

2. *Gravedad:* la gravedad de una vulnerabilidad se refiere a la facilidad con la que puede ser explotada por un atacante. Las vulnerabilidades se pueden clasificar en tres categorías de gravedad:
    - *Alta:* las vulnerabilidades de alta son fáciles de explotar por un atacante con conocimientos básicos.
    - *Media:* las vulnerabilidades de media son más difíciles de explotar, pero pueden ser explotadas por un atacante con conocimientos avanzados.
    - *Baja:* las vulnerabilidades de baja son difíciles de explotar y requieren conocimientos especializados.

3. *Tipo:* las vulnerabilidades se pueden clasificar según su tipo, las más comunes incluyen:
    - *Errores de programación:* los errores de programación son errores en el código fuente de un software que pueden ser explotados por un atacante.
    - *Errores de configuración:* los errores de configuración son configuraciones incorrectas de un sistema que pueden ser explotadas por un atacante.
    - *Exposición de datos:* las exposiciones de datos son la divulgación de datos confidenciales a personas no autorizadas.
    - *Ingeniería social:* la ingeniería social es una técnica que utiliza la manipulación psicológica para engañar a las personas para que revelen información confidencial o realicen acciones que les perjudiquen.

Análisis de vulnerabilidades

Existe una base de datos pública para registrar, identificar y clasificar cada vulnerabilidad. Dicho sistema se conoce como Common Vulnerabilities and Exposures (CVE) y es una lista donde se especifican las versiones y la criticidad de las vulnerabilidades (CVE Program, 2025).

MITRE Corporation se encarga de supervisar los CVE con la financiación de la Agencia de Ciberseguridad y Seguridad de la Infraestructura, que forma parte del Departamento de Seguridad Nacional de Estados Unidos.

El formato es CVE es CVE-YYYY-#####. Algunos ejemplos de CVE famosos son:

» CVE-2021-44228 (NIST–NVD, 2021c).
» CVE-2021-40539 (NIST–NVD, 2021b).
» CVE-2017-11882 (NIST–NVD, 2017).
» CVE-2021-26084 (NIST–NVD, 2021a).

Los CVE se componen de cuatro partes:

» *Prefijo:* el prefijo indica el tipo de vulnerabilidad. Por ejemplo, "CWE-" indica una vulnerabilidad de diseño, "CAN-" indica una vulnerabilidad de configuración y "NVD-" indica una vulnerabilidad de producto.
» *Número:* este es un identificador único para la vulnerabilidad.
» *Descripción:* la descripción proporciona información sobre la vulnerabilidad, incluyendo su impacto, cómo puede ser explotada y cómo puede ser mitigada.
» *Fecha:* la fecha indica la fecha en que se publicó la vulnerabilidad.

Hay muchas formas de evaluar la gravedad de un punto vulnerable, Una de ellas es el sistema común de calificación de los puntos vulnerables (CVSS).

El Common Vulnerability Scoring System (CVSS) es el estándar industrial global para evaluar la severidad de una vulnerabilidad de seguridad informática (NIST, 2024a). El sistema asigna un puntaje del 0.0 al 10.0; mientras más alto el número más grave es el problema.

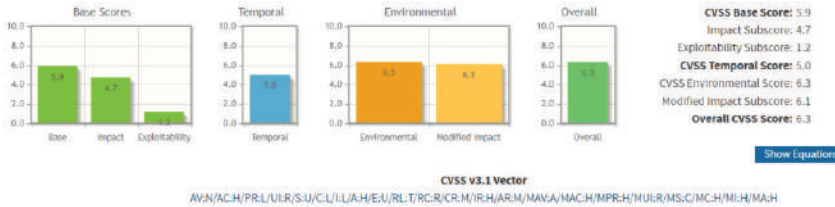
Se divide en los siguientes niveles de severidad (según la versión v3.1 y v4.0) (NIST, 2024b, 2026).

Tabla 14. Escala de severidad de puntuación

Puntuación (Score)	Severidad	¿Qué significa?
0	Ninguna	No hay riesgo.
0.1-3.9	Baja	Difícil de explotar o impacto mínimo.
4.0-6.9	Media	Requiere ciertas condiciones para ser explotada.
7.0-8.9	Alta	Fácil de explotar o gran impacto (por ejemplo, robo de datos).
9.0-10.0	Crítica	Requiere respuesta inmediata. Generalmente permite control total del sistema de forma remota y sin contraseña.

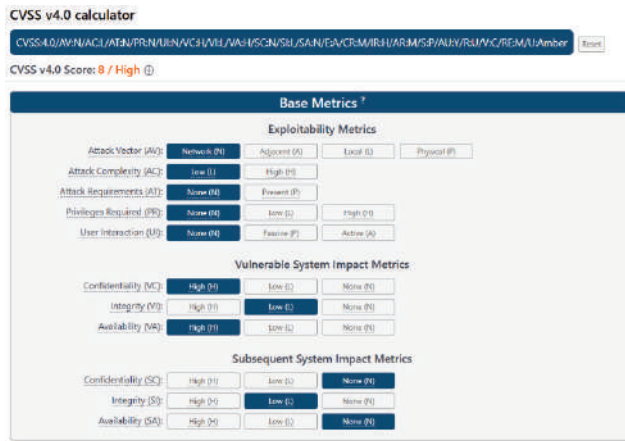
Fuente: elaboración propia.

Figura 16. Common Vulnerability Scoring System v3.1



Fuente: Olaes (2025).

Figura 17. Common Vulnerability Scoring System v4.0



Fuente: Gavois (2025).

Vulnerabilidades de factor humano

Las vulnerabilidades que son explotadas mediante la ingeniería social, como el *phishing*, y que tienen su origen en las personas, se denominan vulnerabilidades humanas o vulnerabilidad de factor humano.

Este tipo de vulnerabilidades se centran en el eslabón más débil de la cadena de seguridad: el usuario final. No son fallos en el código de un software o en la configuración de un sistema (que serían vulnerabilidades técnicas), sino en los aspectos psicológicos y de comportamiento de las personas.

Se explotan a través de técnicas de ingeniería social, que manipulan a las personas para que realicen acciones o revelen información confidencial.

Tabla 15

Tipo de vulnerabilidad	Explicación
Descuido/negligencia	Dejar contraseñas escritas, no bloquear la pantalla, o no seguir políticas de seguridad.
Confianza excesiva	Confiar en una fuente (por ejemplo, un email) sin verificar su legitimidad.
Falta de conocimiento	Desconocimiento sobre cómo funciona un ataque de *phishing* o *malware*.
Curiosidad/miedo	Abrir un archivo adjunto prometedor o hacer clic en un enlace que genera alarma.

Fuente: elaboración propia.

Vulnerabilidades humanas también conocidas como:

» Vulnerabilidades de factor humano.
» Vulnerabilidades organizacionales.
» Vulnerabilidades no técnicas.
» Vulnerabilidades de procedimiento o de personas.

¿Por qué se consideran vulnerabilidades humanas? Debido a que no dependen de una falla técnica en un sistema, sino de errores,

desconocimiento, confianza excesiva o manipulación psicológica de las personas. El atacante no necesita vulnerar una computadora, vulnera al usuario.

Ejemplos típicos:

» *Phishing* (correos falsos para robar credenciales).
» *Vishing* (llamadas telefónicas fraudulentas).
» *Pretexting* (usar un pretexto convincente para obtener información).
» *Baiting* (dejar un USB infectado para que alguien lo conecte).
» Robos de información por engaño o suplantación.

Las vulnerabilidades también se clasifican estándares, según marcos como ISO 27001, NIST o OWASP, y entran dentro de:

» Vulnerabilidades de tipo administrativo o de procesos.
» Vulnerabilidades de concientización y capacitación.
» Vulnerabilidades de control interno.

En el caso específico de OWASP, se consideran parte de:

» Conciencia y capacitación débil (*Weak Security Awareness and Training*).
» Insufficient Identity and Access Management Controls cuando el usuario es engañado para revelar credenciales.

Open Worldwide Application Security Project (OWASP)

El OWASP Top 10 es una lista de las diez categorías de riesgos de seguridad más críticos en aplicaciones web, publicada y mantenida por el Open Worldwide Application Security Project (OWASP). Su objetivo es concienciar y guiar a desarrolladores, arquitectos, equipos de seguridad y responsables de TI sobre las vulnerabilidades más comunes y de mayor impacto, para que puedan prevenirlas, detectarlas y mitigarlas de manera sistemática. No es un estándar obligatorio, sino una referencia ampliamente aceptada a nivel internacional para evaluación y mejora de la seguridad de aplicaciones.

El OWASP Top 10 se utiliza como base para auditorías, pruebas de penetración, desarrollo seguro y cumplimiento normativo, ya que resume riesgos reales observados en miles de aplicaciones. Cada categoría describe el tipo de falla, su impacto potencial y buenas prácticas de mitigación. Además, el listado se actualiza periódicamente para reflejar la evolución de las amenazas, incorporando aspectos como fallos de diseño, errores de configuración y problemas en la cadena de suministro de software, lo que lo convierte en un recurso clave para fortalecer la postura de seguridad de aplicaciones web y APIs.

OWASP 2021

Los riesgos actuales que se publicaron en 2021 (OWASP Foundation, 2021b), son:

- A01 Control de acceso defectuoso (*Broken Access Control*).
- A02 Fallos criptográficos (*Cryptographic Failures*).
- A03 Inyección (*Injection*).
- A04 Diseño inseguro (*Insecure Design*).
- A05 Configuración incorrecta de seguridad (*Security Misconfiguration*).
- A06 Componentes vulnerables y obsoletos (*Vulnerable and Outdated Components*).
- A07 Fallos de identificación y autenticación (*Identification and Authentication Failures*).
- A08 Fallos de integridad de software y datos (*Software and Data Integrity Failures*).
- A09 Fallos de registro y monitorización de seguridad (*Security Logging and Monitoring Failures*).
- A10 Falsificación de solicitud del lado del servidor (*Server Side Request Forgery* [SSRF]).

OWASP 2025 RC

El OWASP Top 10 2025 –actualmente en fase de Release Candidate– marca una evolución significativa respecto a la versión de 2021 (OWASP Foundation, 2025). El cambio principal es un giro

estratégico: se deja de poner el foco solo en síntomas o bugs de código aislados para centrarse en causas raíz y riesgos sistémicos.

Los riesgos propuestos para el 2025 son:

» A01:2025: control de acceso defectuoso (*Broken Access Control*).
» A02:2025: configuración incorrecta de seguridad (*Security Misconfiguration*).
» A03:2025: fallos en la cadena de suministro de software (*Software Supply Chain Failures*).
» A04:2025: fallos criptográficos (*Cryptographic Failures*).
» A05:2025: inyección (*Injection*).
» A06:2025: diseño inseguro (*Insecure Design*).
» A07:2025: fallos de autenticación (*Authentication Failures*).
» A08:2025: fallos de integridad de software o datos (*Software or Data Integrity Failures*).
» A09:2025: fallos de registro y alertas de seguridad (*Security Logging and Alerting Failures*).
» A10:2025: manejo inadecuado de condiciones excepcionales (*Mishandling of Exceptional Conditions*).

Tabla 16. OWASP Top 10: comparativa 2021 vs. 2025 (Propuesto)

Ranking	OWASP Top 10: 2021	OWASP Top 10: 2025 (Propuesto)	Cambio principal
A01	*Broken Access Control*	*Broken Access Control*	Se mantiene en #1. Absorbe a SSRF (A 10:20 21).
A02	*Cryptographic Failures*	*Security Misconfiguration*	Sube del #5 al #2 por la complejidad de la nube.
A03	*Injection*	*Software Supply Chain Failures*	NUEVA/EXPANDIDA. Antes eran solo componentes obsoletos.
A04	*Insecure Design*	*Cryptographic Failures*	Baja posiciones, pero sigue siendo crítico.
A05	*Security Misconfiguration*	*Injection*	Las defensas modernas han hecho que baje de prioridad.

Ranking	OWASP Top 10: 2021	OWASP Top 10: 2025 (Propuesto)	Cambio principal
A06	*Vuln. & Outdated Components*	*Insecure Design*	El enfoque en "Seguridad por Diseño" sigue vigente.
A07	*Identification & Auth. Failures*	*Authentication Failures*	Cambio de nombre para mayor claridad.
A08	*Software & Data Integrity Failures*	*Software or Data Integrity Failures*	Amplía su alcance a pipelines de CI/CD.
A09	*Security Logging & Monitoring*	*Logging & Alerting Failures*	Enfoque en la respuesta y detección temprana
A10	*Server-Side Request Forgery (SSRF)*	*Mishandling of Exceptional Conditions*	NUEVA. Falla en manejo de errores y resiliencia

Fuente: elaboración propia con base en OWASP Foundation 2021b, 2025.

MITRE ATT&CK

MITRE ATT&CK es una base de conocimientos global y accesible que cataloga las tácticas, técnicas y procedimientos (TTPs) utilizados por los ciberdelincuentes en ataques reales. A diferencia de otros marcos que se centran en el cumplimiento normativo, ATT&CK ofrece una matriz de comportamiento que permite a los equipos de seguridad visualizar cómo actúa un adversario después de comprometer un sistema, facilitando la detección de brechas, la caza de amenazas (*threat hunting*) y la emulación de ataques para validar qué tan efectivas son realmente las defensas técnicas de la organización (MITRE, 2024).

La base de conocimientos de ATT&CK (MITRE, 2024) se utiliza como base para el desarrollo de metodologías y modelos de amenazas específicos en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad. El marco es una base de conocimiento accesible a nivel mundial de tácticas y técnicas de los adversarios que pueden describirse como un inventario de indicadores de compromiso (IOC, por sus siglas en inglés, *Indicators of Compromise*) estáticos basados en la reputación que cambian con el tiempo, expiran y solo tienen un valor en un punto en el tiempo.

El Mitre ATT&CK se divide en tres niveles:

- *Tácticas:* son los grandes objetivos que los adversarios intentan lograr en sus ataques. Por ejemplo, "obtener acceso a los datos", "obtener privilegios elevados" o "ejecutar código malicioso".
- *Técnicas:* son los métodos específicos que los adversarios utilizan para lograr sus tácticas. Por ejemplo, "utilizar un *exploit* de Día Cero", "engañar a un usuario para que abra un archivo adjunto malicioso" o "utilizar un troyano para cargar *malware*".
- *Conocimientos comunes:* son los conocimientos que los adversarios necesitan para utilizar las técnicas. Por ejemplo, "conocer las vulnerabilidades de un sistema", "conocer los comportamientos de los usuarios" o "conocer las herramientas y técnicas de seguridad".

MITRE tiene ATT&CK distribuido en algunas matrices diferentes: Enterprise, Mobile y PRE-ATT&CK. Cada una de estas matrices contiene diversas tácticas y técnicas asociadas con el contenido de la matriz.

La matriz Enterprise se compone de técnicas y tácticas que se aplican a los sistemas Windows, Linux o MacOS; Mobile contiene tácticas y técnicas que se aplican a los dispositivos móviles, y PRE-ATT&CK contiene tácticas y técnicas relacionadas con lo que los atacantes hacen antes de intentar vulnerar una red o un sistema en particular.

TECNOLOGÍAS RELACIONADAS

El contenido está organizado desde lo más profundo (la protección del dato) hasta el perímetro (la red y el usuario).

Criptografía

La criptografía y el cifrado son los pilares fundamentales que sostienen la confianza en el mundo digital. En esencia, la criptografía es la disciplina científica que utiliza técnicas matemáticas para proteger la información, garantizando cuatro principios clave: confidencialidad, integridad, disponibilidad y autenticidad. El cifrado, por su parte, es la aplicación práctica de estas técnicas para transformar un mensaje legible (texto plano) en un código ininteligible (texto cifrado), el cual solo puede ser revertido por alguien que posea la clave adecuada.

Históricamente, la criptografía se dividía principalmente en algoritmos de clave simétrica, donde una misma clave se utiliza tanto para cifrar como para descifrar la información. Aunque este método es extremadamente rápido y eficiente para procesar grandes volúmenes de datos (como en el estándar AES), presenta el desafío logístico de cómo compartir la clave de forma segura entre las partes sin que sea interceptada.

Para resolver este problema, surgió la criptografía asimétrica o de clave pública, que utiliza un par de llaves matemáticamente relacionadas: una pública, que se puede compartir con cualquier persona o de forma pública, y una privada, que debe permanecer en secreto. Si alguien quiere enviarte un mensaje, lo cifra con tu clave pública, y solo tú, con tu clave privada, puedes abrirlo. Este sistema, ejemplificado por algoritmos como RSA o curva elíptica (ECC), es lo que permite que realicemos compras seguras en internet o usemos firmas digitales hoy en día.

En la actualidad, la protección de los datos se analiza bajo tres estados distintos: 1) en tránsito (cuando viajan por la red mediante protocolos como TLS/HTTPS); 2) en reposo (cuando están almacenados en discos duros o bases de datos), y, más recientemente, 3) en uso. Para este último estado, están emergiendo tecnologías como el cifrado homomórfico, que permite realizar cálculos sobre datos cifrados sin necesidad de revelarlos, abriendo la puerta a un procesamiento de datos masivo y privado en la nube.

Figura 18. Estados de los datos: reposo, tránsito y uso

Fuente: elaboración propia.

Finalmente, el campo se enfrenta a un cambio de paradigma con la llegada de la computación cuántica. Los ordenadores cuánticos tienen el potencial teórico de romper muchos de los algoritmos asimétricos que usamos hoy en cuestión de segundos. Esto ha dado lugar a la criptografía post-cuántica (PQC), una nueva generación de algoritmos diseñados para resistir ataques de computadoras cuánticas, asegurando que nuestras comunicaciones sigan siendo privadas en las décadas venideras.

Seguridad en la nube

La seguridad en la nube ha dejado de ser un complemento para convertirse en el núcleo de la infraestructura digital moderna. Se define como un conjunto de políticas, tecnologías y controles diseñados para proteger los datos, las aplicaciones y la infraestructura virtualizada. A diferencia de la seguridad tradicional basada en perímetros físicos, la seguridad *cloud* opera bajo un modelo de responsabilidad compartida, donde el proveedor (como AWS, Azure o Google Cloud) asegura la infraestructura global, mientras que el cliente es responsable de configurar adecuadamente sus datos, identidades y cargas de trabajo.

En la actualidad, la mayoría de las organizaciones han evolucionado hacia arquitecturas multinube, utilizando servicios de múltiples proveedores simultáneamente. Esta estrategia no es solo

una cuestión de preferencia técnica, sino una medida crítica de resiliencia y continuidad de negocio. Al distribuir los servicios en diferentes nubes, las empresas evitan el "bloqueo del proveedor" (*vendor lock-in*) y mitigan el riesgo de que una caída masiva en un solo proveedor paralice toda su operación, permitiendo además elegir la nube que mejor cumpla con normativas locales de soberanía de datos.

Sin embargo, la gestión multinube introduce una complejidad operativa sin precedentes. Cada proveedor tiene su propio modelo de identidad, consola de gestión y protocolos de red, lo que crea silos de información y aumenta el riesgo de errores de configuración, que son la causa principal de las brechas de datos en la nube. Para solucionar esto, han surgido tecnologías unificadas como el CSPM (por sus siglas en inglés, Cloud Security Posture Management), que monitoriza continuamente errores de configuración en todas las nubes desde un solo panel, y el CIEM (por sus siglas en inglés, Cloud Infrastructure Entitlement Management), que gestiona los permisos excesivos de usuarios y máquinas para aplicar el principio de privilegio mínimo.

Finalmente, la importancia de la seguridad multinube radica en su capacidad para ofrecer una visibilidad centralizada en un entorno fragmentado. En un mundo donde el trabajo es remoto y las aplicaciones son microservicios dispersos, contar con una estrategia de seguridad que sea "agnóstica" al proveedor permite aplicar políticas de cumplimiento y detección de amenazas de forma consistente. Esto garantiza que, sin importar dónde resida el dato, la postura de seguridad de la organización sea sólida, automatizada y capaz de responder a ataques en tiempo real.

Validación multifactor

La validación tradicional usuario/contraseña se basa únicamente en un factor de conocimiento, es decir, algo que el usuario sabe. Este modelo ha sido históricamente el más utilizado, pero presenta debilidades estructurales: las contraseñas pueden ser robadas, reutilizadas, adivinadas o expuestas mediante phishing, *malware* o brechas de datos. En contraste, la autenticación multifactor (MFA, por sus siglas en inglés, Multi-Factor Authentication) combina dos o más factores independientes –algo que el usuario sabe (contraseña),

algo que tiene (token, móvil, tarjeta) y/o algo que es (biometría)–, reduciendo drásticamente la probabilidad de acceso no autorizado incluso cuando una credencial es comprometida.

La importancia de implementar MFA radica en que ataca directamente el vector de ataque más explotado hoy en día: el robo de credenciales. Diversos incidentes de seguridad demuestran que una gran mayoría de accesos no autorizados se producen con credenciales válidas, no mediante *exploits* sofisticados. MFA introduce una barrera adicional de verificación, dificultando ataques como *phishing*, fuerza bruta, *credential stuffing* y uso de contraseñas filtradas.

Desde una perspectiva de gestión de riesgos, MFA reduce tanto la probabilidad como el impacto de incidentes relacionados con identidad y acceso. En los marcos de referencia de ciberseguridad, la MFA es un control explícitamente recomendado y, en muchos casos, obligatorio. El NIST Cybersecurity Framework (CSF, por sus siglas en inglés) (NIST, 2024b) la incluye dentro de la función "Protect", específicamente en la categoría "Identity Management, Authentication and Access Control (PR.AA)".

El estándar NIST SP 800-63 (NIST, 2023) define niveles de aseguramiento de identidad basados en autenticación multifactor, mientras que los CIS Critical Security Controls (Control 6: Access Control Management) establecen el uso de MFA como una salvaguarda esencial. Asimismo, normas como ISO/IEC 27001 (ISO–IEC, 2022a) y enfoques como Zero Trust, NIST SP 800-207, consideran la MFA un pilar fundamental para garantizar accesos seguros en entornos modernos, locales y en la nube (NIST, 2020b).

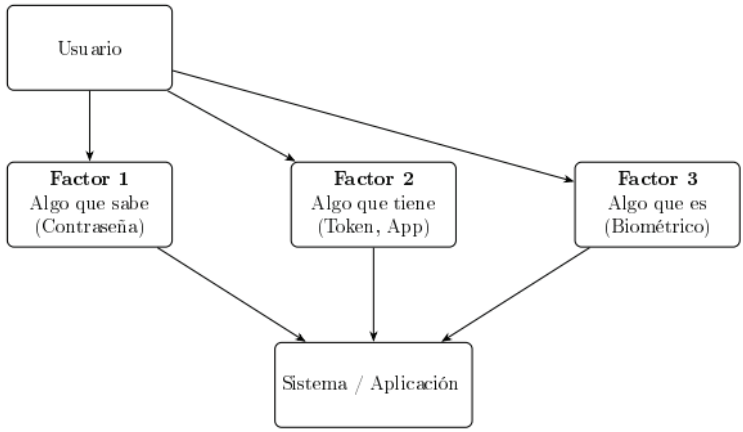
En el Anexo A.2.1 y A.2.2 está un ejemplo de MFA usando Google Authenticator. Con base en el estándar rfc6238 (M'Raihi et al., 2011).

Internet de las cosas

La ciberseguridad en el internet de las cosas (IoT) representa uno de los mayores desafíos técnicos de la actualidad debido a la naturaleza heterogénea y masiva de estos dispositivos. A diferencia de un ordenador convencional, muchos dispositivos IoT (sensores, cámaras, electrodomésticos inteligentes) cuentan con recursos de hardware limitados, lo que impide la ejecución de software de

seguridad robusto o cifrado complejo. Esta debilidad estructural, sumada a la frecuencia con la que los fabricantes omiten mecanismos de actualización de software, convierte a estos dispositivos en puntos de entrada ideales para atacantes que buscan crear redes *botnet* (como la famosa Mirai) para lanzar ataques de denegación de servicio (DDoS) a escala global.

Figura 19. Validación de autenticación multifactor (MFA)



Fuente: elaboración propia.

El riesgo se magnifica cuando el IoT se traslada a infraestructuras críticas o entornos industriales (IIoT), donde un sensor comprometido puede alterar procesos de fabricación o redes de suministro eléctrico. En estos escenarios, la seguridad no solo se centra en proteger los datos, sino en garantizar la seguridad física y operativa. Para combatir esto, las estrategias modernas de defensa ya no confían en el dispositivo *per se*, sino en la red que los aloja, implementando tecnologías de segmentación dinámica y microsegmentación. Esto asegura que, si una cámara inteligente es vulnerada, el atacante quede aislado en una burbuja de red y no pueda saltar hacia los servidores centrales o las bases de datos de la organización.

En la actualidad, el enfoque está cambiando hacia la seguridad por diseño y la implementación de marcos de confianza cero (*Zero Trust*). Esto implica que cada dispositivo debe identificarse de forma única y segura mediante certificados digitales, y sus privilegios de comunicación deben estar estrictamente limitados a su función específica. Además, la integración de inteligencia artificial y

machine learning en las puertas de enlace (*gateways*) de IoT permite analizar patrones de tráfico en tiempo real, detectando comportamientos anómalos –como un termostato intentando enviar datos a un servidor desconocido– para bloquear la amenaza antes de que se convierta en una brecha de seguridad mayor.

Inteligencia artificial

La ciberseguridad de la inteligencia artificial (IA) es un campo de doble vertiente: por un lado, se enfoca en proteger los propios modelos de IA contra ataques diseñados para engañarlos y, por otro, en cómo la IA se utiliza para potenciar las capacidades defensivas y ofensivas. En el primer caso, nos enfrentamos a amenazas como el envenenamiento de datos (*data poisoning*), donde un atacante manipula los datos de entrenamiento para que el modelo aprenda sesgos o "puertas traseras", y los ataques adversarios, que consisten en introducir pequeñas perturbaciones en los datos de entrada para que una IA cometa errores de clasificación, como hacer que un coche autónomo ignore una señal de stop.

Un pilar fundamental en esta disciplina es el concepto de IA explicable (XAI). Dado que muchos modelos de aprendizaje profundo funcionan como una "caja negra", es difícil detectar si una decisión ha sido manipulada. La XAI permite a los analistas de seguridad comprender la lógica detrás de una predicción, facilitando la identificación de anomalías que podrían indicar un ataque. Además, la protección de la privacidad en la IA ha dado lugar a técnicas como el aprendizaje federado, que permite entrenar modelos de forma colaborativa sin que los datos originales salgan de los dispositivos de los usuarios, reduciendo drásticamente la superficie de exposición de información sensible.

En el ámbito operativo, la IA está revolucionando los centros de operaciones de seguridad (SOC) mediante la automatización de la detección de amenazas. Mientras que un analista humano puede verse desbordado por miles de alertas diarias, los algoritmos de *machine learning* pueden identificar patrones sutiles de ataques de día cero o movimientos laterales que pasarían desapercibidos. Sin embargo, esto ha dado pie a una "carrera armamentista" tecnológica, ya que los cibercriminales también emplean IA para crear *malware* polimórfico (que cambia su código para evadir antivirus) y ataques

de phishing altamente personalizados y convincentes mediante el uso de modelos de lenguaje avanzados.

Finalmente, la seguridad de la IA también debe abordar la exfiltración de modelos. El desarrollo de una IA potente requiere una inversión masiva en datos y cómputo, lo que convierte al modelo en una propiedad intelectual valiosísima. Los ataques de inversión de modelo buscan "extraer" la lógica o incluso los datos confidenciales utilizados para el entrenamiento a través de consultas repetitivas a la API del servicio. Por ello, las organizaciones están implementando capas de seguridad que limitan la información revelada en las respuestas de la IA y monitorizan intentos de ingeniería inversa para proteger su ventaja competitiva y la privacidad de sus usuarios.

Cadena de bloques (*blockchain*)

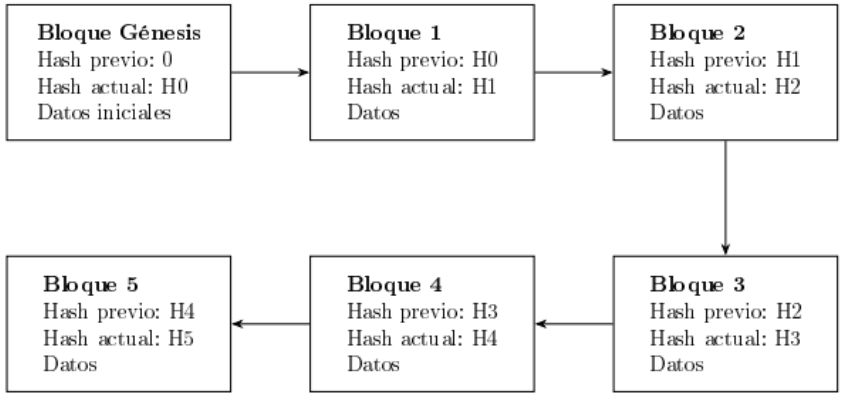
Son una tecnología de registro distribuido que permite almacenar información de forma descentralizada, inmutable y verificable. En lugar de depender de una base de datos central, los datos se agrupan en bloques que se enlazan criptográficamente entre sí mediante funciones hash, formando una cadena cronológica. Cada bloque contiene información, un hash propio y el hash del bloque anterior, lo que impide la modificación de datos sin que el cambio sea detectado por la red.

Desde la perspectiva de la ciberseguridad, la principal aportación de las cadenas de bloques es la integridad de la información. Al estar los registros replicados en múltiples nodos y protegidos mediante criptografía, resulta extremadamente difícil alterar datos sin consenso. Esto reduce riesgos como la manipulación de registros, el fraude o los ataques internos. Además, los mecanismos de consenso y la firma digital permiten verificar la autenticidad de las transacciones sin necesidad de una autoridad central confiable.

La importancia de *blockchain* en ciberseguridad radica en su aplicación práctica en áreas como la gestión de identidades, el registro seguro de eventos, la trazabilidad de transacciones y la protección de cadenas de suministro digitales. También se utiliza para reforzar modelos de confianza cero (*Zero Trust*) y auditorías inmutables. Si bien, no elimina todos los riesgos –ya que sigue dependiendo de la seguridad de los *endpoints* y de los contratos inteligentes–,

aporta una capa sólida de confianza criptográfica que complementa los controles tradicionales de seguridad.

Figura 20. Cadena de bloques mostrando génesis, *hash* previo y hash actual



Fuente: elaboración propia.

En el Anexo B se encuentra el código de una pequeña aplicación que implementa cadena de bloques.

El código principal es *blockchain* (B.1.2). Cada vez que se ejecuta produce:

1. Si el archivo "Cadena.txt" no existe, genera el primer bloque, el génesis, y lo almacena en "Cadena.txt".
2. Si "Cadena.txt" existe y no hay "Nuevo.txt", se genera un mensaje indicando que "No se pudo agregar nuevo bloque".
3. Si "Cadena.txt" existe y también hay "Nuevo.txt" y el "previousHash" coincide con el último de "Cadena.txt" se agrega ese bloque al final de la cadena.
4. Si "Cadena.txt" existe y también hay "Nuevo.txt" y el "previousHash" no coincide con el último de "Cadena.txt", muestra que "No se pudo agregar nuevo bloque".

El código del Anexo B.2.1, cada vez que se ejecuta, produce un nuevo bloque se guarda en "Nuevo.txt".

EQUILIBRIO TRABAJO Y VIDA

La búsqueda de la felicidad a menudo se siente como una carrera agotadora. Nos han enseñado a escalar, a producir, a estar siempre disponibles, y en ese ascenso frenético, corremos el riesgo de perder el rastro de aquello que realmente nutre nuestra alma: la quietud, la risa fácil, el tiempo no medido con quienes amamos. El éxito, cuando se paga con la pérdida de nuestra paz mental y nuestras relaciones más valiosas, es un logro vacío. Si te encuentras constantemente agotado, sintiendo que tu vida personal es solo un hueco que intentas llenar después de la jornada laboral, es hora de hacer una pausa.

Este capítulo no es una receta mágica, sino una invitación a la revolución personal. Requiere valentía para declarar que tu bienestar no es negociable. A continuación, exploraremos dos pilares esenciales de un plan de vida intencional. El primero se centra en cómo blindar tu mente contra la marea del estrés crónico en el trabajo, mientras que el segundo te enseña a construir un calendario donde el amor, la amistad y el tiempo libre sean citas sagradas, inamovibles. Por último, recomendaciones para un plan de vida y mantener la felicidad no es un destino, sino una disciplina diaria de elección consciente.

Gestionando el estrés y redefiniendo el éxito

Desactivando la bomba de tiempo: estrategias contra el estrés crónico en la cultura actual, el estrés no es un defecto, sino a menudo visto, erróneamente, como una insignia de honor. Para construir un plan de vida feliz, el primer paso es desmontar esta creencia. No se trata de eliminar el trabajo, sino de redefinir el éxito. El éxito verdadero no solo se mide en logros profesionales o saldo bancario,

sino en el tiempo de calidad que dedicas a tu bienestar y a tus seres queridos (Huffington, 2015).

Bloques de trabajo profundo (*Deep Work Blocks*), bloques de enfoque/concentración (*Focus Blocks*) o bloques de tiempo (*Time Blocks*): en lugar de jornadas largas y dispersas, implementa bloques de 60-90 minutos de trabajo ininterrumpido en tus tareas más importantes. Al terminar un bloque, haz una pausa activa de 10-15 minutos (estiramientos, caminar, etcétera). Esto incrementa la productividad y reduce la sensación de "estar ocupado, pero no ser efectivo". En ciberseguridad, son muy importantes estos bloques para no saturarse.

La regla de las "3 R" al salir del trabajo:

- *Reconocimiento:* reconoce un logro o tarea importante del día. Cierra el ciclo mentalmente.
- *Rito de transición*: crea una actividad corta y significativa al llegar a casa (escuchar una canción, cambiarte de ropa, cinco minutos de respiración).
- *Restricción tecnológica:* designa al menos dos horas al día donde el teléfono de trabajo y el correo electrónico estén prohibidos. Este es un regalo que le haces a tu mente y a tu familia.

Blindando el tiempo para la familia y los amigos

El calendario sagrado: diseñando intencionalmente tus conexiones la felicidad a largo plazo está profundamente ligada a la calidad de nuestras relaciones. Sin un esfuerzo consciente, el trabajo siempre devorará el tiempo personal. Para ser feliz, debemos dejar de esperar a que "sobre" tiempo y, en su lugar, protegerlo y priorizar como cualquier otra reunión crucial.

Agenda familiar no negociable: introduce en tu calendario personal semanal "citas" inamovibles, tan importantes como las laborales. Puede ser una cena familiar sin dispositivos, una "noche de juegos" con los hijos, o una llamada semanal con un amigo importante. Estas no son opcionales; son inversiones en tu felicidad.

Micromomentos de conexión: entiende que no necesitas grandes vacaciones para conectar. Aprovecha los pequeños momentos. Por ejemplo, haz del trayecto de vuelta del colegio o de la preparación de la cena un tiempo para conversar realmente, no solo para hacer tareas. Pregunta: "¿cuál fue el momento más interesante/divertido de tu día?", en lugar del rutinario: "¿qué tal te fue?".

El poder del no: aprende a decir "no" a compromisos laborales o sociales que no están alineados con tus valores o que sacrificarán repetidamente tu tiempo familiar. Cada "no" a lo superficial es un "sí" a tu paz mental y a tu vida plena. Este es el cimiento de un plan de vida que prioriza lo que verdaderamente importa.

Recomendaciones para diseñar un plan de vida en entornos laborales exigentes

En un mundo profesional que avanza a un ritmo cada vez más acelerado, la sensación de estar desbordado se ha convertido en una experiencia común. Las jornadas extensas, la presión por cumplir objetivos y la constante hiperconexión suelen desplazar aquello que realmente sostiene nuestra calidad de vida: el bienestar emocional, la presencia en nuestras relaciones y la claridad sobre hacia dónde queremos dirigir nuestra existencia. Un plan de vida no es un lujo ni una teoría abstracta; es una herramienta práctica para recuperar el control, ordenar prioridades y recordar que la productividad no tiene valor si se construye a costa de la salud o de los vínculos más importantes.

Sin embargo, alcanzar este equilibrio no ocurre de manera espontánea. Requiere reflexión, estructura y la valentía de cuestionar hábitos que hemos normalizado por años. Diseñar un plan consciente permite alinear el trabajo con el propósito personal, incorporar prácticas de autocuidado y asegurar espacios genuinos para la familia, los amigos y la propia realización. Las siguientes planillas ofrecen un marco sencillo pero profundo para iniciar este proceso: son guías pensadas para transformar la presión cotidiana en decisiones más equilibradas, sostenibles y, sobre todo, humanas.

Define tu propósito personal y profesional: escribe en una frase qué te motiva profundamente. Identifica qué tipo de trabajo, relaciones y actividades te acercan a ese propósito.

Establece límites laborales saludables: determina horarios de desconexión digital. Define cuáles tareas son críticas y cuáles pueden delegarse. Comprométete a no sacrificar descanso por productividad.

Diseña rituales diarios de bienestar: diez minutos de respiración, estiramiento o meditación. Una caminata breve después del almuerzo. Lectura o actividad relajante antes de dormir.

Reserva tiempo obligatorio para tu vida personal: asigna días fijos para la familia o amigos. Programa actividades significativas (no solo "cuando sobre tiempo"). Incluye celebraciones, hobbies y pausas anuales de descanso.

Evalúa tu nivel de satisfacción cada mes: ¿qué te dio energía?, ¿qué te frenó?, ¿qué necesitas ajustar para el mes siguiente?

Bienestar en entornos de alta exigencia

Manejo del estrés laboral: identifica los principales detonantes (carga, tiempos, dinámicas). Implementa micropausas durante tu jornada. Utiliza técnicas de respiración o mindfulness para regular la tensión.

Relaciones saludables dentro y fuera del trabajo: establece comunicación clara con colegas y líderes. Agenda encuentros periódicos con amigos. Cultiva vínculos familiares mediante rutinas compartidas (cenas, llamadas, actividades).

Gestión inteligente del tiempo: prioriza tareas por impacto, no por urgencia aparente. Agrupa actividades similares para optimizar energía. Dedica espacios fijos semanales a objetivos personales.

Autocuidado integral: mantén un patrón de sueño estable. Integra actividad física moderada al menos tres veces por semana. Adopta hábitos nutricionales que favorezcan la energía sostenida.

Reconexión con lo que te hace feliz: lista cinco actividades que disfrutas y asegúrate de realizarlas cada semana. Reflexiona sobre tus logros y escribe gratitudes diarias. Permítete descansar sin culpa.

CONCLUSIONES

Es importante reconocer que cualquier tamaño de empresa debe tener una estrategia de ciberseguridad, una política básica y, claramente, cumplir con algunos controles, como un buen inventario de software y hardware y hacer respaldos periódicamente.

También es fundamental recordar que la ciberseguridad no es un destino, sino un proceso continuo de adaptación. Podemos resumir el aprendizaje en tres pilares esenciales:

a) *La ciberseguridad no tiene escalas:* existe el mito peligroso de que los ciberataques solo buscan grandes corporativos o gobiernos. La realidad es que ninguna institución es demasiado pequeña para ser ignorada. Para un atacante, una pequeña organización puede ser el blanco perfecto: un punto de entrada a una cadena de suministro más grande o simplemente un objetivo con defensas más bajas. La seguridad debe ser una prioridad desde el día uno, escalando según los recursos, pero nunca ignorándose.

b) *El poder de la solución integral:* implementar herramientas aisladas es como poner una puerta blindada en una casa con ventanas de papel. Una verdadera postura de seguridad requiere una visión 360º:

- Marcos de referencia para dar orden y cumplir con estándares.
- Políticas para dar dirección.
- Tecnología para dar protección.
- Controles para mitigar riesgos.
- Para todo lo demás, factor humano.

Sin la integración de estos elementos, solo estamos creando una falsa sensación de seguridad. La protección real nace de la cohesión entre los procesos y la estrategia.

c) *El factor humano: la primera y última línea de defensa:* podemos tener los *firewalls* más avanzados del mercado, pero la ciberseguridad sigue siendo una disciplina humana.

Cultura sobre herramientas: una institución es tan segura como el empleado menos capacitado.

Bienestar y desempeño: como exploramos en este libro, un equipo agotado o bajo estrés extremo es más propenso a cometer errores críticos. El equilibrio entre trabajo y vida no es solo una prestación laboral, es una estrategia de mitigación de riesgos. Cuidar a las personas es, intrínsecamente, cuidar la red.

Resumen

La ciberseguridad dejó de ser un tema "de IT" para convertirse en un tema de gestión del riesgo del negocio.

Para diferenciar, el riesgo es la posibilidad de que una institución sufra un daño o impacto negativo , y se define mediante una fórmula donde deben converger tres componentes fundamentales: la amenaza, que es el agente o evento externo (como un ciberataque o desastre natural) capaz de causar el perjuicio; la vulnerabilidad, que representa la debilidad técnica, humana y organizacional que permite que dicha amenaza tenga éxito; y el impacto, que mide las consecuencias resultantes para la operación o reputación de la organización.

Marcos de referencia y estrategia: el mapa y la brújula

La ciberseguridad no puede ser reactiva ni improvisada. Los marcos de referencia (como NIST o ISO 27001) proporcionan el lenguaje común y las mejores prácticas globales, mientras que la estrategia alinea la seguridad con los objetivos del negocio. Sin estos, la institución gasta recursos sin un norte claro.

Política y controles: la regla y la acción

La política de ciberseguridad es la declaración de intenciones de la dirección; es el "qué" se debe proteger. Por su parte, los controles son el "cómo": las medidas técnicas y administrativas que hacen que la política se cumpla. Juntos, transforman las palabras en muros reales de protección.

Gestión de riesgos y vulnerabilidades: el escudo proactivo

Esta es la inteligencia del sistema. No se puede proteger todo por igual; la gestión de riesgos permite identificar qué es lo más valioso y qué amenazas son más probables. Al gestionar las vulnerabilidades, cerramos las brechas antes de que el atacante las encuentre, pasando de la defensa pasiva a la prevención activa.

Equilibrio trabajo-vida: el motor humano

Este es, quizás, el componente más crítico y menos discutido en la literatura técnica. La ciberseguridad es una disciplina de alta presión donde el agotamiento (*burnout*) conduce inevitablemente a errores humanos. Un analista fatigado ignora alertas críticas. Un líder estresado toma decisiones erráticas. El equilibrio no es un lujo, es una medida de seguridad. Cuidar la salud mental del equipo garantiza que el "*firewall* humano" esté siempre alerta y operativo.

Recomendaciones

Si eres una PYME o estás iniciando en ciberseguridad, iniciar con los marcos de referencia del CIS es la mejor idea, pues son fáciles de entender, concretos y detallados (CIS, 2025a). Luego el NIST CSF 2.0 es el camino natural (NIST, 2024b).

En paralelo, define tu estrategia, tu política y comunica estos documentos a toda tu institución.

> *Controles:* asignarles una importancia relativa a los controles, con relación a tu institución, su visión, sus metas, y sus objetivos te ayuda a definir en qué orden se implementan. Hay controles que no son bien recibidos, pero muchas veces son

necesarios. Por ejemplo, si todos tus vendedores usan laptops, ¿qué puede ser más importante que encriptar sus discos duros?

Herramientas: el SIEM es lo primero, pues te dará visibilidad de lo que pasa y muchas veces, detectar incidentes en curso.

Gestión: para gestionar eficazmente la seguridad institucional es fundamental comprender que el riesgo no es un evento aislado, sino la convergencia de una amenaza (el agente externo o interno capaz de causar daño), una vulnerabilidad (la debilidad técnica, humana u organizacional) y el impacto resultante para la operación o reputación. Implementar una estrategia proactiva implica que la organización debe dejar de reaccionar de forma fragmentada para centrarse en identificar qué activos son los más valiosos y cuáles son las brechas que un atacante podría encontrar primero. Al gestionar las vulnerabilidades de manera sistemática, se cierran las ventanas de oportunidad antes de que sean explotadas, transformando la defensa pasiva en un escudo resiliente alineado con los objetivos del negocio.

Consejo final

La ciberseguridad efectiva no se mide por la complejidad de sus algoritmos, sino por la solidez de su cultura y la integridad de su estrategia. Protegemos bits para salvaguardar el esfuerzo, el tiempo y el bienestar de las personas.

ANEXOS

Anexo A
Código en Java

Las aplicaciones listadas en este anexo no contienen la declaración de *package* para facilitar su uso en otros proyectos. En Java se recomienda que se utilice *package* por razones técnicas y de buenas prácticas de ingeniería de software. Los *packages* no son solo una convención estética. Este código es para Java ver. 25.

A.1. Ejemplo de almacén de Contraseñas con SALT moderno

A.1.1. Algoritmo PBKDF2WithHmacSHA512

```
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.PBEKeySpec;

import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;
import java.security.spec.InvalidKeySpecException;
import java.security.spec.KeySpec;
import java.util.Base64;

public class PasswordManager {

  // Configuraciones de seguridad
  private static final int ITERATIONS = 1_420_000; // Número de
     veces que se repite el hash (cuanto más alto, más seguro pero
     más lento)
  private static final int KEY_LENGTH = 512; // Longitud del hash
     resultante en bits
  private static final String ALGORITHM = "PBKDF2WithHmacSHA512";
  private static final int SALT_LENGTH = 16; // Longitud del Salt
     en bytes
```

```
17
18    /**
19    * Método 1: Genera el hash de la contraseña con un Salt aleatorio
          .
20    * Retorna un String con el formato: "salt:hash" codificado en
          Base64.
21    * @param password
22    * @return
23    */
24    public static String hashPassword(String password) {
25      // 1. Generar un Salt aleatorio criptográficamente seguro
26      SecureRandom random = new SecureRandom();
27      byte[] salt = new byte[SALT_LENGTH];
28      random.nextBytes(salt);
29
30      // 2. Crear el Hash
31      byte[] hash = createHash(password, salt);
32
33      // 3. Codificar ambos a Base64 para almacenarlos como texto
34      String saltBase64 = Base64.getEncoder().encodeToString(salt);
35      String hashBase64 = Base64.getEncoder().encodeToString(hash);
36
37      // 4. Retornar concatenado (El salt es necesario para validar
            después)
38      return saltBase64 + ":" + hashBase64;
39    }
40
41    /**
42    * Método 2: Valida si la contraseña proporcionada coincide con el
          hash almacenado.
43    * @param passwordToCheck
44    * @param storedPassword
45    * @return
46    */
47    public static boolean verifyPassword(String passwordToCheck,
          String storedPassword) {
48      // 1. Separar el Salt y el Hash almacenados
49      String[] parts = storedPassword.split(":");
50      if (parts.length != 2) return false; // Formato inválido
51
52      String saltBase64 = parts[0];
53      String storedHashBase64 = parts[1];
54
55      // 2. Decodificar el Salt original
56      byte[] salt = Base64.getDecoder().decode(saltBase64);
57
58      // 3. Calcular el hash de la contraseña entrante usando el
            MISMO Salt
59      byte[] newHash = createHash(passwordToCheck, salt);
60
61      // 4. Decodificar el hash almacenado para comparar bytes
62      byte[] storedHash = Base64.getDecoder().decode(storedHashBase64
            );
63
64      // 5. Comparar los hashes de manera segura (evita ataques de
            tiempo)
```

```
65      return slowEquals(storedHash, newHash);
66    }
67
68    // --- Métodos Auxiliares Privados ---
69
70    // Lógica central del hashing
71    private static byte[] createHash(String password, byte[] salt) {
72      KeySpec spec = new PBEKeySpec(password.toCharArray(), salt,
          ITERATIONS, KEY_LENGTH);
73      try {
74        SecretKeyFactory factory = SecretKeyFactory.getInstance(
            ALGORITHM);
75        return factory.generateSecret(spec).getEncoded();
76      } catch (NoSuchAlgorithmException | InvalidKeySpecException e)
          {
77        throw new RuntimeException("Error al hashear la contraseña",
            e);
78      }
79    }
80
81    // Comparación segura (Constant-time comparison)
82    private static boolean slowEquals(byte[] a, byte[] b) {
83      int diff = a.length ^ b.length;
84      for (int i = 0; i < a.length && i < b.length; i++) {
85        diff |= a[i] ^ b[i];
86      }
87      return diff == 0;
88    }
89
90    // --- Main para probarlo ---
91    public static void main(String[] args) {
92      String miPassword = "MiSecretoSuperSeguroParaEl2026!";
93
94      // 1. Almacenar (Simulación)
95      String hashGuardado = hashPassword(miPassword);
96      System.out.println("Guardar en BD: " + hashGuardado);
97
98      // 2. Validar (Login correcto)
99      boolean esCorrecta = verifyPassword("
          MiSecretoSuperSeguroParaEl2026!", hashGuardado);
100     System.out.println("¿Contraseña correcta?: " + esCorrecta); //
          true
101
102     // 3. Validar (Login incorrecto)
103     boolean esIncorrecta = verifyPassword("OtraCosa", hashGuardado)
          ;
104     System.out.println("¿Contraseña correcta?: " + esIncorrecta);
          // false
105   }
106 }
```

Anexo A.1.1: Almacén de Contraseñas PBKDF

A.1.2. Algoritmo Argon2

```java
import org.bouncycastle.crypto.generators.Argon2BytesGenerator;
import org.bouncycastle.crypto.params.Argon2Parameters;
import java.security.SecureRandom;
import java.util.Base64;

public class Argon2Hasher {

  // Parámetros recomendados (pueden ajustarse según el hardware)
  private static final int SALT_LENGTH = 16; // 128 bits
  private static final int HASH_LENGTH = 64; // 512 bits
  private static final int PARALLELISM = 1;  // Hilos
  private static final int MEMORY = 65536;   // 64 MB
  private static final int ITERATIONS = 3;   // Pasadas

  public static String hashPassword(String password) {
    byte[] salt = new byte[SALT_LENGTH];
    new SecureRandom().nextBytes(salt);

    byte[] hash = new byte[HASH_LENGTH];

    Argon2Parameters params = new Argon2Parameters.Builder(
       Argon2Parameters.ARGON2_id)
    .withSalt(salt)
    .withParallelism(PARALLELISM)
    .withMemoryAsKB(MEMORY)
    .withIterations(ITERATIONS)
    .build();

    Argon2BytesGenerator generator = new Argon2BytesGenerator();
    generator.init(params);
    generator.generateBytes(password.toCharArray(), hash);

    // Retornamos salt + hash en Base64 para guardarlo en la BD
    return Base64.getEncoder().encodeToString(salt) + ":" +
    Base64.getEncoder().encodeToString(hash);
  }

  public static boolean verify(String password, String storedHash)
     {
    String[] parts = storedHash.split(":");
    byte[] salt = Base64.getDecoder().decode(parts[0]);
    byte[] expectedHash = Base64.getDecoder().decode(parts[1]);

    byte[] actualHash = new byte[HASH_LENGTH];

    Argon2Parameters params = new Argon2Parameters.Builder(
       Argon2Parameters.ARGON2_id)
    .withSalt(salt)
    .withParallelism(PARALLELISM)
    .withMemoryAsKB(MEMORY)
    .withIterations(ITERATIONS)
    .build();
```

```
50
51      Argon2BytesGenerator generator = new Argon2BytesGenerator();
52      generator.init(params);
53      generator.generateBytes(password.toCharArray(), actualHash);
54
55      // Comparación en tiempo constante para evitar ataques de
            tiempo
56      return java.util.Arrays.equals(actualHash, expectedHash);
57    }
58
59    public static void main(String[] args) {
60      String passwordUsuario = "MiSecretoSuperSeguroParaEl2026!";
61
62      // 1. Registro: Hashear y guardar
63      String hashParaBD = Argon2Hasher.hashPassword(passwordUsuario);
64      System.out.println("Hash generado para la BD:\n" + hashParaBD);
65
66      // 2. Login: Verificar contraseña
67      boolean esValida = Argon2Hasher.verify("
            MiSecretoSuperSeguroParaEl2026!", hashParaBD);
68      boolean esInvalida = Argon2Hasher.verify("password_incorrecto",
             hashParaBD);
69
70      System.out.println("\n--- Resultados de verificación ---");
71      System.out.println("¿Contraseña correcta?: " + esValida);   //
            true
72      System.out.println("¿Contraseña incorrecta?: " + esInvalida);
            // false
73    }
74  }
```

Anexo A.1.2: Almacén de Contraseñas Argon2

A.2. Ejemplo de Google Authenticator

Para el siguiente código se debe de utilizar las librerías de:

```
<dependencies>
  <dependency>
    <groupId>com.warrenstrange</groupId>
    <artifactId>googleauth</artifactId>
    <version>1.5.0</version>
  </dependency>
  <dependency>
    <groupId>com.google.zxing</groupId>
    <artifactId>javase</artifactId>
    <version>3.5.3</version>
  </dependency>
</dependencies>
```

A.2.1. Generador de QR para GAuth

```
import com.warrenstrange.googleauth.*;
import com.google.zxing.BarcodeFormat;
import com.google.zxing.client.j2se.MatrixToImageWriter;
import com.google.zxing.common.BitMatrix;
import com.google.zxing.qrcode.QRCodeWriter;
import java.io.IOException;

import java.nio.file.*;

/**
*
* @author lelguea
*/
public class GAuthenticator {

  public static void main(String[] args) {
    GoogleAuthenticator gAuth = new GoogleAuthenticator();
    // 1. Generar una clave secreta aleatoria para el usuario
    final GoogleAuthenticatorKey key = gAuth.createCredentials();
    String secretKey = key.getKey();
    System.out.println("Esta es tu Llave de la aplicación: " +
       secretKey);
    guardarLlave(secretKey);
    // 2. Crear la URL para el código QR
    // "MiApp" es el nombre que aparecerá en tu celular
    // "usuario@correo.com" es el identificador del usuario
    String issuer = "MiAppSegura";
    String user = "lelguea@up.edu.mx";
    String qrData = GoogleAuthenticatorQRGenerator.
       getOtpAuthTotpURL(issuer, user, key);
    // 3. Generar la imagen del QR
    try {
      generarImagenQR(qrData, "codigo_qr.png");
      System.out.println("QR generado con éxito: codigo_qr.png");
    } catch (Exception e) {
      System.err.println(e.toString());
    }
  }

  public static void generarImagenQR(String data, String filePath)
     throws Exception {
    QRCodeWriter qrCodeWriter = new QRCodeWriter();
    BitMatrix bitMatrix = qrCodeWriter.encode(data, BarcodeFormat.
       QR_CODE, 300, 300);
    Path path = FileSystems.getDefault().getPath(filePath);
    MatrixToImageWriter.writeToPath(bitMatrix, "PNG", path);
  }

```

```
44
45    public static void guardarLlave(String contenido) {
46      try {
47        Files.write(Paths.get("llave.txt"), contenido.getBytes());
48        System.out.println("Archivo guardado exitosamente.");
49      } catch (IOException e) {
50        System.err.println("Error al manejar el archivo: " + e.
              getMessage());
51      }
52    }
```

Anexo A.2.1: Generador de QR para GAuth

A.2.2. Validador de GAuth

```
1  import com.warrenstrange.googleauth.GoogleAuthenticator;
2  import java.io.*;
3  import java.nio.file.*;
4  /**
5  *
6  * @author lelguea
7  */
8  public class ValidaCodigo {
9
10   public static void main(String[] adadad) {
11
12     GoogleAuthenticator gAuth = new GoogleAuthenticator();
13     String secreto=leerLlave();
14     int codigoIngresado = 884954; // Lo que el usuario escribió
15     boolean esValido = gAuth.authorize(secreto, codigoIngresado);
16
17     if (esValido) {
18       System.out.println("Acceso concedido!");
19     } else {
20       System.out.println("Código incorrecto.");
21     }
22   }
23
24   public static String leerLlave() {
25     try {
26       // Lee todos los bytes del archivo y los convierte a una
             cadena de texto
27       byte[] bytes = Files.readAllBytes(Paths.get("llave.txt"));
28       return new String(bytes).trim(); // .trim() elimina espacios
             o saltos de línea accidentales
29     } catch (IOException e) {
30       System.err.println("No se pudo leer la llave: " + e.
             getMessage());
31       return null; // O puedes lanzar una excepción personalizada
32     }
33   }
34
35 }
```

Anexo A.2.2: Validador de GAuth

A.3. Ejemplo de certificado en hexadecimal

```
import java.io.ByteArrayInputStream;
import java.math.BigInteger;
import java.security.cert.CertificateFactory;
import java.security.cert.X509Certificate;
import java.util.Base64;
/**
*
* @author lelguea
*/
public class Certificado {

  /**
  * @param args the command line arguments
  * @throws java.lang.Exception
  */
  public static void main(String[] args) throws Exception {

    String cert1="""
    308203d5308202bda003020102020043f955225300d06092a864886f7
    0d01010b050030819a310b3009060355040613024d58310d300b0603
    550408130443444d583116301406035504071307d42656e69746f204a
    756172657a3121301f060355040a1318556e697665727369646164420
    50616e616d65726963616e6131173015060355040b130e4369626572
    736567757269646164312830260603550403131f4c6f72656e7a6f20
    4d696775656c20456c6775656120466572 6e616e64657a301e170d32
    333032303832333336323435a170d333330323038323333363234 5a30
    819a310b3009060355040613024d58310d300b060355040813044344
    4d583116301406035504071307d42656e69746f204a756172657a3121
    301f060355040a1318556e697665727369646164205061 6e616d6572
    6963616e6131173015060355040b130e436962657273656775726964
    6164312830260603550403131f4c6f72656e7a6f204d696775656c20
    456c67756561204665726e616e64657a30820122300d06092a864886
    f70d01010105000382010f003082010a0282010100998e26ca535a57
    508e948f33949d3b1aebb01930c618bed1a5d52683209bd4da0ea119
    134bba90a8ad9ff7c162def5444f3e203a51a680766ebf1b0c8b4dcd
    43995d0e4449665983b86ea02db45d8974563ebdeef891c1c222ec67
    c8d3acd4327a6698aed475676ba7b56435bd56dc92d3690386f687d2
    b206fddcf90ce73a9f12f892043ae5ce1b9a0bd2896c8c2b3388abb3
    763db284505d7d8e9a3ba4abf923f1ea6300fe943635a00a493c3f2e
    2de0ca8d3fdf7e35aef79150718c007429e7f67b93f47bf4efa9531b
    c2f53323aa2422708e84d5e7f4e5443362683165a8848d1611b2619e
    ce81efd391d2cd57450941587be6af7e69b4bf6c3b302655d1020301
    0001a321301f301d0603551d0e04160414256ca5d5c36c570367655f
```

```
        5bd344f5e483cb6a13300d06092a864886f70d01010b050003820101
        004541227de5f2563f97249d241056b60297f59ef575b3c570d44fb4
        3d7b6b9b6d4fc743dfb888bfcbec412f2dea8d359ee74bad936e8dbd
        07951194902e2e4e23c2b13ec7eab8c5bf6ccc2043b826909c71f3df
        0a437ce3e836cf4d91e42f9ba723de4bbfcafcdddb8b90758f3e332e
        d60f6e047ae36f0aea39eb4a81023251b7294be7ea079ac4b28b11cc
        7b5a31e4587f3e00a6646f560ac994b32b9338bdbec3201f43ea866c
        35c728a991a903b1cbf00b0d7d888b84ca6c73602f0e492347d20cec
        ea863ee37bbd282ad6be6a444003bf43c85cf76a6e13e51edc58c10f
        0a46932cc9f5013a04386a197f873f1147626bff7e87f8456a0fed57
        6d6d7777da
        """;

        cert1=cert1.replaceAll("\n","");
        byte[] certBytes=new BigInteger(cert1, 16).toByteArray();
        String Codifica=Base64.getEncoder().encodeToString(certBytes);
        System.out.println(Codifica);

        //X509Certificate cert = loadCertificateFromString(Codifica);
        X509Certificate cert = loadCertificateFromString(certBytes);
        // Mostrar información del certificado
        System.out.println("=== Información del Certificado ===");
        System.out.println("Sujeto: " + cert.getSubjectX500Principal())
            ;
        System.out.println("Emisor: " + cert.getIssuerX500Principal());
        System.out.println("Número de serie: " + cert.getSerialNumber()
            );
        System.out.println("Válido desde: " + cert.getNotBefore());
        System.out.println("Válido hasta: " + cert.getNotAfter());
        System.out.println("Algoritmo de firma: " + cert.getSigAlgName
            ());
        System.out.println("Versión: " + cert.getVersion());
    }

    public static X509Certificate loadCertificateFromString(String
        clean) throws Exception {
        // Decodificar Base64
        byte[] certBytes = Base64.getDecoder().decode(clean);
        // Crear certificado X.509
        CertificateFactory cf = CertificateFactory.getInstance("X.509")
            ;
        return (X509Certificate) cf.generateCertificate(
        new ByteArrayInputStream(certBytes));
    }

    public static X509Certificate loadCertificateFromString(byte[]
        certBytes) throws Exception {
        // Crear certificado X.509
        CertificateFactory cf = CertificateFactory.getInstance("X.509")
            ;
        return (X509Certificate) cf.generateCertificate(
        new ByteArrayInputStream(certBytes));
    }
}
```

Anexo A.3.1: Ejemplo de certificado en hexadecimal (Base16) a Base64

A.4. Ejemplo cifrado simétrico con AES

```java
import javax.crypto.*;
import javax.crypto.spec.IvParameterSpec;
import java.security.SecureRandom;
import java.util.Base64;

public class CifradoSimetrico {

  // Genera una clave AES de 128 bits
  public static SecretKey generateKey() throws Exception {
    KeyGenerator keyGen = KeyGenerator.getInstance("AES");
    keyGen.init(128);
    return keyGen.generateKey();
  }

  // Genera un IV aleatorio de 16 bytes
  public static IvParameterSpec generateIv() {
    byte[] iv = new byte[16];
    new SecureRandom().nextBytes(iv);
    return new IvParameterSpec(iv);
  }

  // Cifra texto plano
  public static String encrypt(
  String input,
  SecretKey key,
  IvParameterSpec iv) throws Exception {

    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    cipher.init(Cipher.ENCRYPT_MODE, key, iv);
    byte[] cipherText = cipher.doFinal(input.getBytes("UTF-8"));

    return Base64.getEncoder().encodeToString(cipherText);
  }

  // Descifra texto cifrado
  public static String decrypt(
  String cipherText,
  SecretKey key,
  IvParameterSpec iv) throws Exception {

    Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
    cipher.init(Cipher.DECRYPT_MODE, key, iv);
    byte[] plainText = cipher.doFinal(
    Base64.getDecoder().decode(cipherText));
    return new String(plainText, "UTF-8");
  }

  public static void main(String[] args) throws Exception {

    String originalText = "Mensaje super secreto \nY muy secreto";
```

```
50
51      // Generar clave e IV
52      SecretKey key = generateKey();
53      System.out.println("Llave : " + Base64.getEncoder().
           encodeToString(key.getEncoded())+" ("+key.getFormat()+")");
54      IvParameterSpec iv = generateIv();
55      System.out.println("Vector de inicialización: "+Base64.
           getEncoder().encodeToString(iv.getIV()));
56
57      // Cifrado
58      String encryptedText = encrypt(originalText, key, iv);
59      System.out.println("Texto cifrado: " + encryptedText);
60
61      // Descifrado
62      String decryptedText = decrypt(encryptedText, key, iv);
63      System.out.println("Texto descifrado: " + decryptedText);
64    }
65  }
```

Anexo A.4.1: Ejemplo cifrado simétrico con AES

A.5. Ejemplo de codificación en Base64

```
1  import java.util.Base64;
2  /**
3  *
4  * @author lelguea
5  */
6  public class CodificaBase64 {
7
8    /**
9    * @param args the command line arguments
10   */
11   public static void main(String[] args) {
12     String TextoPlano="Gracias profesor por sus "+
13     "enseñanzas\n" +
14     " en todo";
15     String Codifica=Base64.getEncoder().encodeToString(TextoPlano.
          getBytes());
16     byte[] decode=Base64.getDecoder().decode(Codifica);
17     System.out.println(Codifica);
18     System.out.println(new String(decode));
19
20     Codifica="SG9sYSBNdW5kbyB4MiA=";
21     decode=Base64.getDecoder().decode(Codifica);
22     System.out.println(new String(decode));
23   }
24 }
```

Anexo A.5.1: Ejemplo de codificación en Base64

Anexo B
Cadena de Bloques

B.1. Package blockchain

```
1  package blockchain;
2
3  // Java implementation for creating
4  // a block in a Blockchain
5
6  import java.text.SimpleDateFormat;
7  import java.util.Date;
8
9  public final class Block {
10
11   // Every block contains
12   // a hash, previous hash and
13   // data of the transaction made
14   public String hash;
15   public String previousHash;
16   private String data;
17   private long timeStamp;
18
19   // Constructor for the block
20   public Block(String data, String previousHash) {
21     this.data = data;
22     this.previousHash = previousHash;
23     this.timeStamp = new Date().getTime();
24     this.hash = calculateHash();
25   }
26
27   // Constructor for the block
28   public Block(String data, String previousHash, String HashAct,
        long tiempo) {
29     this.data = data;
30     this.previousHash = previousHash;
31     this.timeStamp = tiempo;
32     this.hash = HashAct;
33   }
34
35
36
37   // Function to calculate the hash
38   public String calculateHash() {
39
40     // Calling the "crypt" class
41     // to calculate the hash
42     // by using the previous hash,
43     // timestamp and the data
44     String calculatedhash = crypt.sha256(previousHash + Long.
          toString(timeStamp)+ data);
```

```
45
46        return calculatedhash;
47      }
48
49      @Override
50      public String toString() {
51        return "Block{" + "hash=" + hash + ", previousHash=" +
              previousHash + ", data=" + data + ", timeStamp=" +
              timeStamp + '}';
52      }
53
54      public void modifica(String nuevodato) {
55        this.data=nuevodato;
56        this.timeStamp = new Date().getTime();
57        this.hash = calculateHash();
58
59      }
60
61      public String Muestra() {
62        return "data=" + data + ", hash=" + hash + ", previousHash="
              + previousHash + ", time=" + new SimpleDateFormat("dd/MM/
              yyyy HH:mm:ss").format(timeStamp);
63      }
64
65
66
67    }
```

Anexo B.1.1: Block

```
1   package blockchain;
2
3
4   import java.util.ArrayList;
5
6
7   /**
8   *
9   * @author lelguea
10  */
11  public class BlockChain {
12
13    // Java implementation to store
14    // blocks in an ArrayList
15
16    // ArrayList to store the blocks
17    public static ArrayList<Block> blockchain = new ArrayList<>();
18
19    // Driver code
20    public static void main(String[] args) {
21      // Adding the data to the ArrayList
22      blockchain= utilerias.Almacen.Leer();
23      if (blockchain.isEmpty()) {
24        blockchain.add(new Block("Genesis", "0"));
25      }
26
27
```

```
28        Block nuevo=utilerias.Almacen.LeerUno();
29        if (!utilerias.Almacen.UltimoHash().equals(nuevo.previousHash
              )) {
30          System.err.println("No se pudo agregar nuevo bloque");
31          //System.exit(0);
32        } else {
33          blockchain.add(nuevo);
34          System.out.println("Se agrego nuevo bloque ("+nuevo.
                toString()+")");
35        }
36
37
38        utilerias.Almacen.Guarda(blockchain);
39        MuestraTodo();
40        System.out.println("Valido: "+isChainValid());
41      }
42
43
44      // Java implementation to check
45      // validity of the blockchain
46
47      // Function to check
48      // validity of the blockchain
49      public static Boolean isChainValid() {
50        Block currentBlock;
51        Block previousBlock;
52
53        // Iterating through
54        // all the blocks
55        for (int i = 1; i < blockchain.size();i++) {
56
57          // Storing the current block
58          // and the previous block
59          currentBlock = blockchain.get(i);
60          previousBlock = blockchain.get(i - 1);
61
62          // Checking if the current hash
63          // is equal to the
64          // calculated hash or not
65          if (!currentBlock.hash.equals(currentBlock.calculateHash())
                ) {
66            System.out.println("Hashes are not equal");
67            return false;
68          }
69
70          // Checking of the previous hash
71          // is equal to the calculated
72          // previous hash or not
73          if (!previousBlock.hash.equals(currentBlock.previousHash))
                {
74            System.out.println("Previous Hashes are not equal ("+i+"
                  & "+(i+1)+")");
75            return false;
76          }
77        }
78
```

```
79        // If all the hashes are equal
80        // to the calculated hashes,
81        // then the blockchain is valid
82        return true;
83      }
84
85
86      public static void MuestraTodo() {
87        for (int i=0;i<blockchain.size();i++) {
88          System.out.println(blockchain.get(i).Muestra());
89        }
90      }
91    }
```

Anexo B.1.2: blockchain

```
1   package blockchain;
2
3   // Java program for Generating Hashes
4
5   import java.io.UnsupportedEncodingException;
6   import java.security.MessageDigest;
7   import java.security.NoSuchAlgorithmException;
8
9   public class crypt {
10
11    // Function that takes the string input
12    // and returns the hashed string.
13    public static String sha256(String input) {
14
15      try {
16        MessageDigest sha = MessageDigest.getInstance("SHA-256");
17        int i = 0;
18
19        byte[] hash = sha.digest(input.getBytes("UTF-8"));
20
21        // hexHash will contain
22        // the Hexadecimal hash
23        StringBuilder hexHash = new StringBuilder();
24
25        while (i < hash.length) {
26          String hex = Integer.toHexString(0xff & hash[i]);
27          if (hex.length() == 1) {
28            System.out.println("Entre");
29            hexHash.append('0');
30          }
31          hexHash.append(hex);
32          i++;
33        }
34
35        return hexHash.toString();
36      } catch (UnsupportedEncodingException |
             NoSuchAlgorithmException e) {
37        System.err.println(e.toString());
```

```
38        }
39        return "";
40      }
41    }
```

Anexo B.1.3: crypt

B.2. Package utilerías

```
1  package utilerias;
2
3  import blockchain.Block;
4  import java.io.*;
5  import java.util.ArrayList;
6
7  /**
8  *
9  * @author lelguea
10 */
11 public class Almacen {
12
13   public static void Guarda(ArrayList<Block> datos) {
14     String Nombre="Cadena.txt";
15     File fout = new File(Nombre);
16     try {
17       FileOutputStream fos = new FileOutputStream(fout);
18
19       BufferedWriter bw = new BufferedWriter(new OutputStreamWriter
           (fos));
20
21       for (int i=0;i<datos.size();i++) {
22         Block b=datos.get(i);
23         bw.write(b.toString());
24         bw.newLine();
25
26       }
27       bw.close();
28     } catch (IOException e) {
29       System.err.println(e.toString());
30     }
31
32   }
33
34   public static void Guarda(Block datos) {
35     String Nombre="Nuevo.txt";
36     File fout = new File(Nombre);
37     try {
38       FileOutputStream fos = new FileOutputStream(fout);
39
40       BufferedWriter bw = new BufferedWriter(new OutputStreamWriter
           (fos));
41
42       bw.write(datos.toString());
43       bw.newLine();
```

```
44
45        bw.close();
46      } catch (IOException e) {
47        System.err.println(e.toString());
48      }
49
50    }
51
52
53    public static ArrayList<Block> Leer() {
54      ArrayList<Block> salida=new ArrayList<>();
55      String Nombre="Cadena.txt";
56      BufferedReader reader;
57
58      try {
59        reader = new BufferedReader(new FileReader(Nombre));
60        String line = "";
61
62        while (line != null) {
63          //System.out.println(line);
64          // read next line
65          line = reader.readLine();
66          if (line !=null && line.length()>64) {
67            line=line.replace("Block{", "");
68            line=line.substring(0,line.length()-1);
69            //System.out.println(line);
70            String[] datos=line.split(",");
71            //System.out.println("Hay "+datos.length+" datos");
72            if (datos.length==4) {
73              String hash=datos[0];
74              hash=hash.replace("hash=","").trim();
75              String previo=datos[1];
76              previo=previo.replace("previousHash=","").trim();
77              String info=datos[2];
78              info=info.replace("data=","").trim();
79              String tiempo=datos[3];
80               tiempo=tiempo.replace("timeStamp=","").trim();
81               //System.out.println(info+", "+tiempo);
82               Block b = new Block(info, previo,hash,Long.parseLong(
                     tiempo));
83               salida.add(b);
84             }
85          }
86        }
87
88        reader.close();
89      } catch (IOException e) {
90        System.err.println(e.toString());
91      }
92
93      return salida;
94
95    }
96
97    public static Block LeerUno() {
98      Block salida=new Block("", "0");
99      String Nombre="Nuevo.txt";
100     BufferedReader reader;
```

```
101
102       try {
103         reader = new BufferedReader(new FileReader(Nombre));
104         String line = "";
105
106         while (line != null) {
107           //System.out.println(line);
108           // read next line
109           line = reader.readLine();
110           if (line !=null && line.length()>64) {
111             line=line.replace("Block{", "");
112             line=line.substring(0,line.length()-1);
113             //System.out.println(line);
114             String[] datos=line.split(",");
115             //System.out.println("Hay "+datos.length+" datos");
116             if (datos.length==4) {
117               String hash=datos[0];
118               hash=hash.replace("hash=","").trim();
119               String previo=datos[1];
120               previo=previo.replace("previousHash=","").trim();
121               String info=datos[2];
122               info=info.replace("data=","").trim();
123               String tiempo=datos[3];
124               tiempo=tiempo.replace("timeStamp=","").trim();
125               //System.out.println(info+", "+tiempo);
126               Block b = new Block(info, previo,hash,Long.parseLong(
                    tiempo));
127               //System.out.println("Revisa ************** "+b.
                    toString());
128               return b;
129             } else {
130               System.err.println("Datos erroneos.");
131               System.exit(0);
132             }
133           }
134         }
135
136         reader.close();
137       } catch (IOException e) {
138         System.err.println(e.toString());
139       }
140
141       return salida;
142     }
143
144       public static String UltimoHash() {
145     String salida="";
146     String Nombre="Cadena.txt";
147     BufferedReader reader;
148
149     try {
150       reader = new BufferedReader(new FileReader(Nombre));
151       String line = "";
152
153       while (line != null) {
154         //System.out.println(line);
155         // read next line
```

```
156         line = reader.readLine();
157         if (line !=null && line.length()>64) {
158           line=line.replace("Block{", "");
159             line=line.substring(0,line.length()-1);
160             //System.out.println(line);
161             String[] datos=line.split(",");
162             //System.out.println("Hay "+datos.length+" datos");
163             if (datos.length==4) {
164               String hash=datos[0];
165               hash=hash.replace("hash=","").trim();
166               String previo=datos[1];
167               previo=previo.replace("previousHash=","").trim();
168               String info=datos[2];
169               info=info.replace("data=","").trim();
170               String tiempo=datos[3];
171               tiempo=tiempo.replace("timeStamp=","").trim();
172               //System.out.println(info+", "+tiempo);
173               //Block b = new Block(info, previo,hash,Long.parseLong(
                      tiempo));
174               salida=hash;
175             }
176           }
177         }
178 
179         reader.close();
180       } catch (IOException e) {
181         System.err.println(e.toString());
182       }
183 
184       return salida;
185 
186     }
```

Anexo B.2.1: Almacén

B.3. Package pruebas

```
1  package Pruebas;
2  
3  import blockchain.Block;
4  /**
5  *
6  * @author lelguea
7  */
8  public class UnBloque {
9  
10   public static void main(String[] asdasd) {
11     String UltimoHash=utilerias.Almacen.UltimoHash();
12     System.out.println(UltimoHash);
13 
14     Block bloqueUnico = new Block("Soy el Principal",UltimoHash);
15     System.out.println(bloqueUnico.toString());
16     utilerias.Almacen.Guarda(bloqueUnico);
17   }
18 
19 }
```

Anexo B.3.1: UnBloque

Anexo C
Conexión LDAP seguro (LDAPS)

C.1. Conexión a LDAPs usando Java

```
1  package conexionldap;
2
3  import java.util.Properties;
4  import javax.naming.Context;
5  import javax.naming.NamingEnumeration;
6  import javax.naming.NamingException;
7  import javax.naming.directory.Attribute;
8  import javax.naming.directory.Attributes;
9  import javax.naming.directory.InitialDirContext;
10 import javax.naming.directory.SearchControls;
11 import javax.naming.directory.SearchResult;
12
13 /**
14 *
15 * @author lelguea
16 */
17 public class ConexionLDAP {
18
19   InitialDirContext idc;
20
21   public ConexionLDAP(String LDAPS) {
22     Properties ldapEnv = new Properties();
23     ldapEnv.put("java.naming.ldap.factory.socket", "conexionldap.
          SSLSocketFactoryUP");
24     ldapEnv.put(Context.INITIAL_CONTEXT_FACTORY, "com.sun.jndi.ldap
          .LdapCtxFactory");
25     ldapEnv.put(Context.PROVIDER_URL, LDAPS);
26     ldapEnv.put(Context.SECURITY_AUTHENTICATION, "simple");
27     ldapEnv.put(Context.SECURITY_PROTOCOL, "ssl");

28     ldapEnv.put(Context.SECURITY_PRINCIPAL, "[dominio]\[usuario]");
29     ldapEnv.put(Context.SECURITY_CREDENTIALS, "Contraseñ
          aSuperSecreta$");
30
31     ldapEnv.put("com.sun.jndi.ldap.connect.pool", "true");
32     //ldapEnv.put("com.sun.jndi.ldap.connect.timeout", "2000");
33     ldapEnv.put("com.sun.jndi.ldap.connect.pool.debug","all");
34     ldapEnv.put("com.sun.jndi.ldap.connect.pool.timeout","10000");
35
36     try {
37       // Create initial context
38       idc = new InitialDirContext(ldapEnv);
39     } catch (NamingException ex) {
40       System.err.println(ex.toString());
41     }
42   }
43
44   public  String buscaNombre(String usuario) {
45     try {
```

```
46        String[] attrIDs = {"displayName"};
47        SearchControls ctls = new SearchControls();
48        ctls.setReturningAttributes(attrIDs);
49        ctls.setSearchScope(SearchControls.SUBTREE_SCOPE);
50
51        NamingEnumeration<SearchResult> answer = idc.search("dc=
              dominio,dc=up,dc=edu,dc=mx", "(sAMAccountName="+usuario+")
              ",ctls);
52
53        while (answer.hasMore()) {
54          SearchResult sr = answer.next();
55          Attributes result = sr.getAttributes();
56
57          Attribute attr = result.get("displayName");
58          String Nombre;
59          if (attr != null) {
60            NamingEnumeration<?> vals = attr.getAll();
61            if (vals.hasMoreElements()) {
62              Nombre= vals.nextElement().toString();
63              return Nombre;
64            }
65          }
66          System.out.println();
67        }
68      } catch (NamingException e) {
69        // e.printStackTrace();
70      }
71      return null;
72    }
73
74    /**
75    * @param args the command line arguments
76    */
77    public static void main(String[] args) {
78      Properties defaultProps = System.getProperties(); //obtiene las
            "properties" del sistema
79      defaultProps.put("java.net.preferIPv6Addresses", "true");//
            mapea el valor true en la variable java.net.
            preferIPv6Addresses
80
81      ConexionLDAP conectaLDAPS= new ConexionLDAP("ldaps://dcpublico.
            up.edu.mx:636");
82      String Nombre1=conectaLDAPS.buscaNombre("iis");
83      System.out.println("Nombre en LDAPs: "+Nombre1+"\n");
84
85      // Conexion al GC
86      ConexionLDAP conectaLDAPSGC= new ConexionLDAP("ldaps://
            dcpublico.up.edu.mx:3269");
87      String Nombre2=conectaLDAPSGC.buscaNombre("iis");
88      System.out.println("Nombre en GCs  : "+Nombre2+"\n");
89
90    }
91  }
```

Anexo C.1.1: Conexión LDAPs Java

```
package conexionldap;

import java.security.cert.CertificateException;
import java.security.cert.X509Certificate;
import javax.net.ssl.X509TrustManager;

public class ConfiaRutaCertificacion implements X509TrustManager {
  @Override
  public void checkClientTrusted(X509Certificate[] cert, String
     string) throws CertificateException {
    System.out.println("checkClientTrusted");
  }

  @Override
  public void checkServerTrusted(X509Certificate[] cert, String
     string) throws CertificateException {
    System.out.println("checkServerTrusted: "+cert.length);
    //System.out.println("checkServerTrusted: "+cert[0].toString())
       ;
  }

  @Override
  public X509Certificate[] getAcceptedIssuers() {
    System.out.println("getAcceptedIssuers");
    return new java.security.cert.X509Certificate[0];
  }
}
```

Anexo C.1.2: ConfiaRutaCertificacion

```
package conexionldap;

import java.io.IOException;
import java.net.InetAddress;
import java.net.Socket;
import java.net.UnknownHostException;
import java.security.KeyManagementException;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;

import javax.net.SocketFactory;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSocketFactory;
import javax.net.ssl.TrustManager;

public class SSLSocketFactoryUP extends SSLSocketFactory {

  private SSLSocketFactory socketFactory;

  public SSLSocketFactoryUP() {
    try {
      SSLContext ctx = SSLContext.getInstance("TLS");
      ctx.init(null, new TrustManager[]{ new
         ConfiaRutaCertificacion()}, new SecureRandom());
      socketFactory = ctx.getSocketFactory();
    } catch ( KeyManagementException | NoSuchAlgorithmException ex
```

```
        ) {
26        System.err.println(ex.toString());
27      }
28    }
29
30    public static SocketFactory getDefault() {
31      return new SSLSocketFactoryUP();
32    }
33
34    @Override
35    public String[] getDefaultCipherSuites() {
36      return socketFactory.getDefaultCipherSuites();
37    }
38
39    @Override
40    public String[] getSupportedCipherSuites() {
41      return socketFactory.getSupportedCipherSuites();
42    }
43
44    @Override
45    public Socket createSocket(Socket socket, String string, int num,
          boolean bool) throws IOException {
46      return socketFactory.createSocket(socket, string, num, bool);
47    }
48
49    @Override
50    public Socket createSocket(String string, int num) throws
         IOException, UnknownHostException {
51      return socketFactory.createSocket(string, num);
52    }
53
54    @Override
55    public Socket createSocket(String string, int num, InetAddress
         netAdd, int i) throws IOException, UnknownHostException {
56      return socketFactory.createSocket(string, num, netAdd, i);
57    }
58
59    @Override
60    public Socket createSocket(InetAddress netAdd, int num) throws
         IOException {
61      return socketFactory.createSocket(netAdd, num);
62    }
63
64    @Override
65    public Socket createSocket(InetAddress netAdd1, int num,
         InetAddress netAdd2, int i) throws IOException  {
66      return socketFactory.createSocket(netAdd1, num, netAdd2, i);
67    }
68  }
```

Anexo C.1.3: SSLSocketFactoryUP

C.2. Conexion a LDAPs usando PHP

```php
<?php
// --- Configuración LDAP ---
$ldap_server = "ldaps://dcpublico.up.edu.mx:636"; // Por ejemplo: "ldap.ejemplo.com"
$ldap_rdn = "[dominio]\\[usuario]"; // RDN del usuario para "bind" (conexión inicial)
$ldap_password = "ContraseñaSuperSecreta$";   // Contraseña del usuario para "bind"
ldap_set_option(null, LDAP_OPT_X_TLS_REQUIRE_CERT, LDAP_OPT_X_TLS_NEVER);

$user_to_find = "iis"; // El usuario cuyo nombre deseas obtener

// --- Conexión a LDAP ---
$ds = ldap_connect($ldap_server);

if ($ds) {
  echo "Conexión a LDAPs exitosa a " . $ldap_server . "<br>";
  //ldap_set_option($ds, LDAP_OPT_X_TLS_REQUIRE_CERT, LDAP_OPT_X_TLS_NEVER);


  // Configurar protocolo LDAP (opcional, pero recomendado para versiones recientes)
  ldap_set_option($ds, LDAP_OPT_PROTOCOL_VERSION, 3);
  ldap_set_option($ds, LDAP_OPT_REFERRALS, 0); // Importante para evitar problemas de referencia

  // --- Autenticación (Bind) ---
  $r = ldap_bind($ds, $ldap_rdn, $ldap_password);


  if ($r) {
    echo "Autenticación LDAPs exitosa.<br>";

    // --- Búsqueda del usuario ---
    // Aquí ajusta el filtro de búsqueda según la estructura de tu LDAP.
    // Common filters:
    // - (sAMAccountName=$user_to_find) for Active Directory
    // - (uid=$user_to_find) for OpenLDAP
    $ldap_base_dn = "dc=dominio,dc=up,dc=edu,dc=mx"; // Base DN de tu directorio LDAP

    $filter = "mail=".$user_to_find."*"; // Escapar para seguridad

    $sr = ldap_search($ds, $ldap_base_dn, $filter);

    if ($sr) {
      $info = ldap_get_entries($ds, $sr);

      if ($info["count"] > 0) {
        echo "Usuario encontrado seguro: " . $info[0]["cn"][0] . "<br>"; // "cn" suele ser el nombre común
      } else {
        echo "El usuario '$user_to_find' no fue encontrado.<br>";
      }
```

```
47      } else {
48        echo "Error␣en␣la␣búsqueda␣LDAP:␣" . ldap_error($ds) . "<br>"
              ;
49      }
50
51    } else {
52      echo "Error␣de␣autenticación␣LDAP:␣" . ldap_error($ds) . "<br>"
          ;
53    }
54
55    // --- Cerrar conexión LDAP ---
56    ldap_close($ds);
57  } else {
58    echo "No␣se␣pudo␣conectar␣al␣servidor␣LDAP␣'$ldap_server'.␣Asegú
        rate␣de␣que␣el␣servidor␣esté␣accesible␣y␣el␣puerto␣sea␣
        correcto.<br>";
59  }
60
61  ?>
```

Anexo C.2.1: Ejemplo LDAPs PHP

REFERENCIAS

American Institute of Certified Public Accountants (AICPA) (2017). SOC 2®: Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. AICPA.

AXELOS (2019). ITIL Foundation, ITIL 4 Edition. TSO.

Bacudio, A. G., Yuan, X., Chu, B. T. B., and Jones, M. (2011). An overview of penetration testing. International Journal of Network Security & Its Applications, 3(6), 19.

Bidou, R. (2005). Security Operation Center Concepts & Implementation. http://www. iv2-technologies.com.

Center for Internet Security (CIS) (2024, noviembre 25). A Roadmap to the CIS Critical Security Controls. https://www.cisecurity.org/insights/white-papers/roadmap-cis-critical-security-controls

Center for Internet Security (CIS) (2025a). CIS Controls. https://www.dnsfilter.com/glossary/cis-controls

Center for Internet Security (CIS) (2025b). CIS Critical Security Controls®. https://www.cisecurity.org/controls

Center for Internet Security (CIS) (2025c). CIS SecureSuite® Membership. https://www.cisecurity.org/cis-securesuite

Center for Internet Security (CIS) (2026a). CIS Critical Security Controls Version 8. https://www.cisecurity.org/controls/v8

Center for Internet Security (CIS) (2026b). Microsoft Windows Desktop [CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0]. https://www.cisecurity.org/benchmark/microsoft_windows_desktop

Center for Internet Security (CIS) (2026c). Página web oficial. https://www.cisecurity.org/

Center for Internet Security (CIS) (2026d). The 18 CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list

CMMI Institute (2018, marzo 28). CMMI V2.0: Model Definition. https://cmmiinstitute.com/news/press-releases/march-2018/annoucingv2

CVE Program (2025). Common vulnerabilities and exposures (CVE). https://www.cve.org/

European Union Agency for Cybersecurity (ENISA). (2009). Cloud Computing Risk Assessment. ENISA. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

European Union Agency for Cybersecurity (2024). ENISA Threat Landscape 2024. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

European Union Agency for Cybersecurity (ENISA). (2026). Topics. https://www.enisa.europa.eu/topics

Federal Risk and Authorization Management Program (FedRAMP) (2023). Fedramp Security Assessment Framework (saf). Technical guidance. U.S. General Services Administration. https://www.fedramp.gov/documents/

Federal Risk and Authorization Management Program (FedRAMP) (2024). Fedramp Program Overview. https://www.fedramp.gov/

Gavois, S. (2025, septiembre 26). Faille OnePlus : n'importe quelle application peut lire vos SMS, le correctif en octubre. Next. https://next.ink/201754/faille-oneplus-nimporte-quelle-application-peut-lire-vos-sms-le-correctif-en-octobre/

Google (s.f.). Google Authenticator [Open Source software]. https://github.com/google/google-authenticator

Have I Been Pwned (2026). Página web oficial. https://haveibeenpwned.com/

HITRUST Alliance (2023). HITRUST CSF — Our Cybersecurity Framework, Version 11.2.0. https://hitrustalliance.net/hitrust-csf

Huffington, A. (2015). La vida plena: Bienestar, sabiduría, asombro y compasión: los pilares del éxito. Aguilar.

Information Systems Audit and Control Association (ISACA) (2018a). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

Information Systems Audit and Control Association (ISACA) (2018b). COBIT 2019 Framework: Introduction and Methodology. ISACA https://www.isaca.org/resources/cobit

Information Systems Audit and Control Association (ISACA) (2019). COBIT 2019 Focus Area: Information and Technology Risk. ISACA.

International Electrotechnical Commission (IEC) (2026). IEC 62443: Industrial Communication Networks - Network and System Security. Standard. https://www.iec.ch/home

International Organization for Standardization (ISO) (2018). ISO 31000:2018 Risk Management — Guidelines. ISO. https://www.iso.org/standard/65694.html

International Organization for Standardization (ISO)–International Electrotechnical Commission (IEC) (2009). ISO/IEC 15408-1:2009 Information technology —Security techniques— Evaluation criteria for it security (common criteria). ISO–IEC. https://www.iso.org/standard/72891.html

International Organization for Standardization (ISO)–International Electrotechnical Commission (IEC) (2020). ISO/IEC 27014:2020 information security, cybersecurity and privacy protection — governance of information security. ISO–IEC.

International Organization for Standardization (ISO)–International Electrotechnical Commission (IEC) (2022a). ISO/IEC 27001:2022. information security, cybersecurity and privacy protection — information security management systems — requirements. ISO–IEC. https://www.iso.org/standard/27001

International Organization for Standardization (ISO)–International Electrotechnical Commission (IEC) (2022b). ISO/IEC 27002:2022 information security, cybersecurity and privacy protection — information security controls. ISO–IEC. Número de referencia ISO/IEC 27002:2022(E).

International Organization for Standardization (ISO)–International Electrotechnical Commission (IEC) (2022c). ISO/IEC 27005:2022

information security, cybersecurity and privacy protection — guidance on managing information security risks.

International Organization for Standardization (ISO)–International Electrotechnical Commission (IEC) (2024). ISO/IEC 27000 family - Information technology Security techniques Information security management systems. ISO–IEC. https://www.iso.org/iso-iec-27001-information-security.html

Katai, N. (2025, marzo 25). NIST CSF 2.0 Tools Guide (2026): The Best Software for Compliance & Security. iFeeltech. https://ifeeltech.com/nist-csf-2-0-cybersecurity-tools/

MITRE (2024). ATT&CK. https://attack.mitre.org/

M'Raihi, D., Rydell, J., Pei, M. y Machani, S. (2011). TOTP: Time-Based One-Time Password Algorithm. RFC 6238. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc6238

Mutune, G. (2019). 23 Top Cybersecurity Frameworks. CyberExperts.com. https://cyberexperts.com/cybersecurity-frameworks/

Nacimba, M. (2024). Diseño de políticas de Ciberseguridad enfocadas a una institución de nivel superior caso Instituto Rumiñahui. [Tesis de Maestría, Universidad Tecnológica Israel, Quito, Ecuador].

National Institute of Standards and Technology (NIST) (2001a). Advanced Encryption Standard (AES). FIPS Pub (197). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

National Institute of Standards and Technology (NIST) (2001b). Security Requirements for Cryptographic Modules. FIPS Pub, 140(2). https://csrc.nist.gov/publications/detail/fips/140/2/final

National Institute of Standards and Technology (NIST) (2008). Performance Measurement Guide for Information Security. NIST Special Publication, 800(55). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-55r1.pdf

National Institute of Standards and Technology (NIST) (2012). Guide for Conducting Risk Assessments. NIST SP, 800(30), Rev. 1. https://csrc.nist.gov/pubs/sp/800/30/r1/final

National Institute of Standards and Technology (NIST) (2017). An Introduction to Information Security. NIST SP, 800(12) Rev. 1. https://csrc.nist.gov/pubs/sp/800/12/r1/final.

National Institute of Standards and Technology (NIST) (2019). Security Requirements for Cryptographic Modules. FIPS Pub, 140(3). https://csrc.nist.gov/publications/detail/fips/140/3/final

National Institute of Standards and Technology (NIST) (2020). Security and Privacy Controls for Information Systems and Organizations NIST SP, 800(53), Rev. 5. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

National Institute of Standards and Technology (NIST) (2020b). Zero Trust Architecture. NIST SP, 800(207). https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

National Institute of Standards and Technology (NIST) (2023). Digital Identity Guidelines. NIST SP, 800(63) [incluye SP 800-63A, 800-63B y 800-63C].

National Institute of Standards and Technology (NIST) (2024a). CVSS v3 Calculator. https: //nvd.nist.gov/vuln-metrics/cvss/v3-calculator

National Institute of Standards and Technology (NIST) (2024b). The NIST Cybersecurity Framework (CSF) 2.0. NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

National Institute of Standards and Technology (NIST) (2025a). Cybersecurity Framework. https://www.nist.gov/cyberframework

National Institute of Standards and Technology (NIST) (2025b). CSF 2.0 Informative References. https://www.nist.gov/cyberframework/informative-references

National Institute of Standards and Technology (NIST) (2026). NVD CVSS v4.0 Calculator. https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator.

National Institute of Standards and Technology (NIST)–National Vulnerability Database (NVD) (2017). CVE-2017-11882 Detail: Microsoft Oce Equation Editor Stack-based Buffer Overflow. https://nvd.nist.gov/vuln/detail/CVE-2017-11882

National Institute of Standards and Technology (NIST)–National Vulnerability Database (NVD) (2021a). CVE-2021-26084 Detail: Atlassian Confluence Server OGNL Injection. https://nvd.nist.gov/vuln/detail/CVE-2021-26084

National Institute of Standards and Technology (NIST)–National Vulnerability Database (NVD) (2021b). CVE-2021-40539 Detail: Zoho ManageEngine ADSelfService Plus Authentication Bypass. https://nvd.nist.gov/vuln/detail/CVE-2021-40539

National Institute of Standards and Technology (NIST)–National Vulnerability Database (NVD) (2021c). CVE-2021-44228 Detail: Apache Log4j2 Remote Code Execution. https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Nmap (2026). Página web oficial. https://nmap.org/

Offensive Security (2026a). Kali Tools. https://www.kali.org/tools/

Offensive Security (2026b). Installer Images. https://www.kali.org/get-kali/#kali-installer-images

Olaes, T. (2025, febrero 26). Understanding Environmental CVSS Scores. Balbix. https://www.balbix.com/insights/environmental-cvss-scores/

Open-AudiIT (2026). Página web oficial. https://www.open-audit.org/

OWASP Foundation (2020). OWASP Software Assurance Maturity Model (SAMM) v2.0. https://owaspsamm.org/

OWASP Foundation (2021a). OWASP Application Security Verication Standard (ASV) 4.0.3. https://owasp.org/www-project-application-security-verification-standard/

OWASP Foundation (2021b). OWASP Top 10:2021. https://owasp.org/Top10/2021/

OWASP Foundation (2025). OWASP Top 10:2025. https://owasp.org/Top10/2025/

PCI Security Standards Council (2022). Payment Card Industry (PCI) Data Security Standard, Requirements and Testing Procedures, Version 4.0. https://www.pcisecuritystandards.org/document_library

Stallings, W. (2017). Computer Security: Principles and Practice, 4.ª Ed. Pearson.

SSL Labs (2026a). Página web oficial. https://www.ssllabs.com/ y

SSL Labs (2026b). SSL Server Test. https://www.ssllabs.com/ssltest/

SourceForge (2026). Portecle. https://portecle.sourceforge.net/

The Legion of the Bouncy Castle (s.f.). bcprov-jdk18on [Librería de software]. Maven Central Repository. https://repo1.maven.org/maven2/org/bouncycastle/bcprov-jdk18on/

The Open Group (2020). The Open FAIR™ Body of Knowledge. https://www.opengroup.org/open-fair

The Open Group (2022). The TOGAF Standard, 10.ª Ed. Reading. https://www.opengroup.org/togaf

Vats, P., Mandot, M., and Gosain, A. (2020). A comprehensive literature review of penetration testing & its applications. En 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), (pp. 674-680). IEEE.

VeraCrypt (2025). Página web oficial. https://veracrypt.io/en/Home.html

VirusTotal (2026). Página web oficial. https://www.virustotal.com/gui/home/upload

Wazuh (2026a). Documentation Index. https://documentation.wazuh.com/current/index.html

Wazuh (2026b). Página web oficial. https://wazuh.com/

Wazuh (2026c). Vulnerability detection. https://documentation.wazuh.com/current/proof-of-concept-guide/poc-vulnerability-detection.html

Wetzel, K. A., Petersen, R., Santos, D., Witte, G. y Runi, B. L. (2020). Workforce framework for cybersecurity (nice framework). NIST SP, 800(181), Rev. 1.

Wireshark (2026). Página web oficial. https://www.wireshark.org/

Wood, R. (2026). Damn Vulnerable Web Application (DVWA). https://github.com/digininja/DVWA

¿QUÉ TE PARECE ESTE LIBRO?

¡CUÉNTAMELO EN 5 MINUTOS!

FORMA PARTE DE LA CREACIÓN:
OPINA SOBRE

CIBERSEGURIDAD INTEGRAL

ESTRATEGIA, RIESGO, TECNOLOGÍA Y CULTURA ORGANIZACIONAL

LORENZO ELGUEA FERNÁNDEZ

UNIVERSIDAD
Panamericana

CIBERSEGURIDAD INTEGRAL

ESTRATEGIA, RIESGO, TECNOLOGÍA Y CULTURA ORGANIZACIONAL

LORENZO ELGUEA FERNÁNDEZ

Se terminó de editar en febrero de 2026

por Santi Ediciones (Rosario Ivonne Lara Alba)
Nance 1370, Colonia Del Fresno, Guadalajara, Jalisco.
www.santiediciones.com

UNIVERSIDAD
Panamericana

Lorenzo Miguel Elguea Fernández

lelguea@up.edu.mx

Cuenta con más de 35 años de trayectoria en tecnología y ciberseguridad. Es Doctor en Ingeniería por la Universidad Panamericana, Maestro en Tecnologías de Información y Administración por el ITAM, y cuenta con estudios de alta dirección en el IPADE. Su investigación se ha enfocado en redes definidas por software (SDN) y optimización de protocolos de red, con publicaciones en revistas internacionales como *Procedia Computer Science* y *Wireless Networks*. Actualmente lidera el área de Ciberseguridad y Transformación Digital en la Universidad Panamericana, donde es responsable de la protección de infraestructura, operación del SOC y pruebas de penetración. Ha sido reconocido como CEO del mes por una revista nacional de tecnología por su capacidad innovadora. Casado con Rosa Elena, pedagoga de profesión, y padre de un futuro ingeniero, Lorenzo es también un curioso por naturaleza: disfruta la astronomía y desarmar cosas para entender cómo funcionan.

CIBERSEGURIDAD
INTEGRAL

Estrategia, riesgo, tecnología y cultura organizacional

UNIVERSIDAD Panamericana

UNIVERSIDAD Panamericana Facultad de Ingeniería

A menudo caemos en el error de pensar que la ciberseguridad es una preocupación exclusiva de grandes bancos, gobiernos o infraestructuras críticas, pero la realidad digital actual nos demuestra que nadie está exento del riesgo. En un mundo donde cada negocio, escuela y hogar opera en la nube, la seguridad de la información ha dejado de ser un lujo técnico para convertirse en un pilar fundamental de la supervivencia operativa y la confianza social. ***Ciberseguridad Integral*** rompe con el mito de que esto "no va con nosotros" y expone con claridad por qué proteger nuestros activos digitales es tan vital como cerrar la puerta de nuestra casa.

Más allá de los *firewalls* y los algoritmos, este libro pone el foco en el eslabón más importante y frecuentemente olvidado: el capital humano. A través de un enfoque que une estrategia, tecnología y cultura, esta obra no solo te enseña a gestionar riesgos, sino que te invita a construir un escudo organizacional donde cada persona es consciente de su rol en la defensa. Es una lectura obligada para entender que la verdadera resiliencia no se compra con software, sino que se construye integrando la seguridad en el ADN de nuestra cultura diaria sin olvidar la capacitación de todos.

UNIVERSIDAD Panamericana

UNIVERSIDAD Panamericana Facultad de Ingeniería

ISBN: 978-607-8826-95-7