GLOSARIO DE CIBERSEGURIDAD

TÉRMINOS ESENCIALES

Primera Edición: Junio 2025

Por Jeremy José de la Cruz Pérez

Glosario de Ciberseguridad

Términos Esenciales

Primera Edición - Junio 2025

ISBN: En trámite

Sobre el Autor

Jeremy José de la Cruz Pérez
Estudiante de Licenciatura en Informática en la Universidad Nacional Pedro Henríquez Ureña (UNPHU), apasionado por la ciberseguridad, el desarrollo de software y la innovación tecnológica. Originario de La Vega, República Dominicana, se especializa en soporte técnico, redes, desarrollo front-end y automatización de procesos, utilizando herramientas como Python, C++, MySQL y principios de diseño UI/UX.

Actualmente, continúa su formación en áreas como hacking ético, administración de sistemas Linux y programación segura, con el objetivo de convertirse en un experto en ciberseguridad. Su enfoque es práctico, ético y orientado a soluciones reales que generen impacto positivo en la sociedad.

Contacto:

- je7remy@gmail.com
- Jeremy José de la Cruz Pérez
- github.com/Je7remy

Introducción

Bienvenido a esta guía práctica diseñada para ayudarte a dominar los **términos clave** en ciberseguridad. En este campo, conocer estos términos es fundamental para entender conceptos, tecnologías y protocolos que son esenciales para destacar profesionalmente en seguridad informática.

Este glosario, la primera de cuatro partes, te proporciona una lista completa de **términos** organizados alfabéticamente, cada uno acompañado por:

- **Una definición clara del término**: Para que comprendas exactamente qué significa.
- **Un ejemplo** (si aplica): Situaciones comunes que te ayudarán a conectar fácilmente con cada concepto.

Con un enfoque sencillo y directo, este glosario no solo te ayudará a memorizar términos, sino a entenderlos en profundidad, potenciando tu crecimiento en el ámbito de la seguridad informática.

Esta es la primera entrega de una serie de cuatro, cada una explorando diferentes aspectos de la ciberseguridad. ¡No te pierdas las próximas partes para seguir avanzando en este camino!

Prepárate para aprender de manera clara y descubre el significado real de cada **término** que puede impulsar tu trayectoria profesional.

> *"No se trata solo de tecnología, sino de lo que podemos construir con ella."*
> — Jeremy José de la Cruz Pérez

Glosario de Términos de Ciberseguridad

A

Access Control (Control de Acceso) Conjunto de mecanismos que restringen quién (o qué proceso) puede acceder a sistemas, aplicaciones o datos, y en qué condiciones. Incluye la autenticación (verificar identidad) y la autorización (determinar permisos), asegurando que solo usuarios legítimos con privilegios apropiados interactúen con los recursos protegidos.

Adversarial Artificial Intelligence (IA adversaria) Técnicas que explotan vulnerabilidades en sistemas de inteligencia artificial y aprendizaje automático para manipular su comportamiento y obtener resultados maliciosos. Un ejemplo es alimentar a un modelo de *machine learning* con datos falsificados para engañarlo y provocar decisiones erróneas en beneficio del atacante.

Adware Software publicitario no deseado que muestra anuncios en un dispositivo. Suele instalarse junto con aplicaciones gratuitas o mediante engaños, desplegando ventanas emergentes y contenido promocional. Aunque no siempre daña el sistema, resulta intrusivo y puede representar un riesgo a la privacidad al recopilar datos de usuario.

Antivirus Programa de seguridad diseñado para detectar, bloquear y eliminar **malware** (código malicioso) de un sistema informático. Utiliza bases de firmas conocidas y análisis heurístico para identificar virus, gusanos, troyanos y otras amenazas, protegiendo la integridad del sistema. Es fundamental mantener el antivirus actualizado para una protección efectiva contra las amenazas más recientes.

Asset (Activo) Recurso o elemento de valor para una organización, como datos, hardware, software o infraestructura. En ciberseguridad, los activos se protegen mediante controles y medidas de seguridad para evitar accesos no autorizados, daños, interrupciones o pérdidas de la información.

Attack Vector (Vector de Ataque) Ruta, medio o técnica que un atacante utiliza para explotar una vulnerabilidad y comprometer la seguridad de un sistema. Puede ser un canal técnico (como una conexión de red, correo electrónico infectado, dispositivo USB) o humano (ingeniería social) por el cual el agresor consigue acceder a un activo objetivo.

Authentication (Autenticación) Proceso de verificación de la identidad de un usuario o sistema antes de otorgar acceso a un recurso. Comúnmente se realiza mediante credenciales como usuario y contraseña, aunque también puede involucrar factores adicionales (ej. huella digital o token). La autenticación garantiza que quien intenta el acceso es quien dice ser; por ejemplo, solo si la contraseña introducida es correcta se permitirá el ingreso.

Authorization (Autorización) Proceso de otorgar permisos o acceso a recursos específicos una vez verificada la identidad mediante autenticación. Determina **qué** acciones o datos puede utilizar un usuario autenticado, según políticas de la organización. Por ejemplo, tras autenticarse, un empleado puede estar autorizado a ver ciertos archivos pero no a modificarlos si no tiene los privilegios adecuados.

Authorize (Autorizar) Sexto paso del marco NIST RMF que implica asumir la responsabilidad por los riesgos de seguridad y privacidad asociados a un sistema, autorizando su operación tras evaluar los

controles implementados y el riesgo residual.

Availability (Disponibilidad) Principio de seguridad que asegura que los datos, sistemas y servicios estén accesibles para los usuarios autorizados cuando los necesiten. Mantener la disponibilidad implica contar con infraestructura redundante, planes de continuidad de negocio y medidas contra ataques (como **DDoS**) o fallas, de modo que las operaciones esenciales no se vean interrumpidas.

AWS (Amazon Web Services) Plataforma líder de servicios de computación en la nube ofrecida por Amazon. Proporciona infraestructura y servicios escalables (cómputo, almacenamiento, bases de datos, etc.) bajo un modelo de responsabilidad compartida en seguridad, donde AWS asegura la **seguridad de la nube** (centros de datos, hardware subyacente) y el cliente es responsable de la **seguridad en la nube** (configuración segura de sus sistemas, protección de datos, control de acceso, etc.).

B

Backdoor (Puerta trasera) Funcionalidad oculta o software malicioso que brinda acceso remoto no autorizado a un sistema comprometido, eludiendo los mecanismos normales de autenticación. Un *backdoor* permite al atacante controlar el equipo (por ejemplo, ejecutar comandos, extraer archivos o espiar pulsaciones de teclas) sin conocimiento del usuario. Puede instalarse aprovechando vulnerabilidades o incluso ser dejado deliberadamente por desarrolladores maliciosos para acceder al sistema posteriormente.

Biometrics (Biometría) Características físicas o de comportamiento únicas de una persona (como huellas dactilares, patrones de iris, reconocimiento facial o incluso la forma de teclear) utilizadas para verificar su identidad. Los datos biométricos se emplean en sistemas de autenticación como métodos de factor adicional, dado que son difíciles de falsificar y vinculados intrínsecamente al individuo.

Blue Team (Equipo Azul) Equipo defensor en ciberseguridad encargado de la protección activa de las redes, sistemas e información de una organización frente a ataques. El equipo azul monitoriza continuamente la infraestructura, detecta y bloquea intrusiones, corrige vulnerabilidades descubiertas (por ejemplo, las reportadas por un **Red Team**) y refuerza las medidas de seguridad en tiempo real. Su labor es reaccionar eficazmente ante incidentes y mantener segura la organización.

Botnet Red de dispositivos (computadoras, IoT, etc.) infectados con malware — llamados *bots* o *zombis* — y controlados remotamente por un atacante (el *botmaster*). Las botnets se utilizan para llevar a cabo ataques coordinados a gran escala, como campañas de spam o ataques **DDoS**, enviando tráfico masivo desde los equipos comprometidos sin el conocimiento de sus propietarios. Cada equipo zombi recibe órdenes desde un servidor de comando y control, pudiendo robar datos, minar criptomonedas o participar en la distribución de malware.

Business Continuity (Continuidad del Negocio) Capacidad de una organización para mantener sus operaciones esenciales y seguir funcionando ante interrupciones significativas (fallos de TI, desastres naturales, ciberataques, etc.). Se basa en planes de recuperación y contingencia que garantizan que procesos críticos, sistemas y datos puedan restaurarse o seguir disponibles, minimizando el tiempo de inactividad y el impacto en la empresa.

Business Email Compromise (BEC) Tipo de ataque de *phishing* dirigido en el que el atacante se hace pasar por una fuente de alta confianza (por ejemplo, un ejecutivo de la compañía o un proveedor legítimo) mediante correo electrónico. El objetivo es engañar a la víctima para que realice transferencias financieras no autorizadas o revele información sensible. Estos ataques suelen ser muy personalizados, estudiando previamente la organización y sus empleados para aumentar la credibilidad del mensaje fraudulento.

C

Categorize (Categorizar) Segundo paso del marco NIST RMF (Risk Management Framework) que implica identificar y clasificar los sistemas y la información por niveles de riesgo. En esta fase se asigna una categorización de impacto (bajo, moderado, alto) a cada activo de información, lo cual ayuda a determinar la criticidad y los requisitos de seguridad necesarios. El resultado guía la selección de controles de seguridad proporcionales a la importancia de los activos categorizados.

Certificate Authority (Autoridad Certificadora) Entidad de confianza que emite certificados digitales para validar identidades en Internet. Una Autoridad Certificadora (o CA, por sus siglas en inglés) comprueba la identidad de personas o entidades y genera certificados electrónicos (por ejemplo, para sitios web HTTPS). Estos certificados vinculan una clave pública con la identidad verificada, permitiendo establecer comunicaciones seguras y garantizando al usuario que se está conectando con el servidor legítimo y no con un impostor.

Chronicle Herramienta nativa en la nube diseñada para retener, analizar y buscar datos de registro, permitiendo a las organizaciones monitorear eventos de seguridad y detectar amenazas en tiempo real mediante el análisis de grandes volúmenes de información (ver **SIEM**).

CIA Triad (Tríada CIA) Modelo fundamental de la seguridad de la información basado en tres principios: **Confidencialidad, Integridad y Disponibilidad**. Sirve para evaluar y mitigar riesgos asegurando que la información solo sea accesible por quienes deben (confidencialidad), que los datos sean precisos y no alterados indebidamente (integridad), y que los sistemas y datos estén accesibles cuando se necesitan (disponibilidad). La Tríada CIA guía el diseño de controles de seguridad equilibrados que protejan estos tres aspectos básicos.

Cloud Security (Seguridad en la Nube) Conjunto de prácticas y tecnologías destinadas a proteger datos, aplicaciones e infraestructuras alojadas en entornos de computación en la nube. Incluye configurar adecuadamente los recursos en la nube (por ejemplo, controlando el acceso a buckets de almacenamiento, cifrando datos sensibles, gestionando identidades y permisos) y cumplir con modelos de responsabilidad compartida provistos por el proveedor. El objetivo de la seguridad en la nube es prevenir accesos no autorizados, fugas de información y garantizar la continuidad de los servicios en entornos cloud.

Compliance (Cumplimiento) Adherencia a normas, leyes, estándares y regulaciones aplicables en materia de seguridad y privacidad, así como a políticas internas de la organización. En ciberseguridad, el cumplimiento puede involucrar requerimientos como GDPR (protección de datos personales en la UE), HIPAA (información médica en EE. UU.), PCI DSS (datos de tarjetas de pago), entre otros. Mantener el cumplimiento asegura que la empresa siga las mejores prácticas y evite sanciones legales, demostrando que se protegen adecuadamente los datos sensibles según las exigencias externas e internas.

Computer Virus (Virus Informático) Código malicioso diseñado para interferir con el funcionamiento normal de un sistema, que se adjunta a programas o archivos legítimos y se replica a sí mismo. Al ejecutarse el programa infectado, el virus puede propagarse a otros archivos o equipos, causando daños como la corrupción o eliminación de datos y afectando el rendimiento del sistema. Los virus clásicos requieren de la intervención del usuario (por ejemplo, abrir un archivo infectado) para activarse, a diferencia de los **gusanos** que se propagan automáticamente; no obstante, siguen siendo una amenaza vigente mitigada mediante el uso de antivirus actualizados y buenas prácticas de seguridad.

Confidentiality (Confidencialidad) Principio que garantiza que la información sensible solo sea accesible para las personas autorizadas. Mantener la confidencialidad implica implementar controles como cifrado de datos, mecanismos de autenticación estrictos y políticas de control de accesos, de modo que terceros no autorizados no puedan leer ni divulgar la información protegida. Junto con

la **integridad** y la **disponibilidad**, la confidencialidad forma parte de la Tríada CIA, constituyendo uno de los pilares básicos de la seguridad de la información.

Cryptographic Attack (Ataque Criptográfico) Intento malicioso de comprometer sistemas de comunicación seguros o datos cifrados, explotando debilidades en algoritmos criptográficos o en su implementación. Estos ataques buscan descifrar información sin autorización (por ejemplo, romper una clave de cifrado mediante fuerza bruta o criptoanálisis), suplantar firmas digitales o aprovechar errores de protocolo para interceptar y leer datos confidenciales. La resistencia frente a ataques criptográficos es un factor clave al diseñar y seleccionar esquemas y protocolos de cifrado seguros.

Cyberattack (Ciberataque) Intento deliberado de un actor malicioso de infiltrarse en sistemas, redes o dispositivos sin autorización, empleando diversas técnicas o vulnerabilidades, con fines dañinos como robo de información, extorsión o sabotaje. Un ciberataque puede manifestarse a través de malware (ej. ransomware, troyanos), **phishing**, ataques de fuerza bruta, **DDoS**, entre otros, y puede ocasionar daños significativos si tiene éxito. Para defenderse, las organizaciones implementan capas de seguridad y monitorización continua que permitan detectar y neutralizar estos intentos antes de que comprometan sus activos.

Cybercriminal (Ciberdelincuente) Persona que realiza actividades delictivas aprovechando medios digitales o cibernéticos. Un ciberdelincuente explota sistemas, redes y vulnerabilidades tecnológicas para beneficio propio o ajeno, incurriendo en delitos informáticos como robo o filtración de datos, fraude electrónico, espionaje, **hacktivismo** o ataques disruptivos. Sus motivaciones pueden ser económicas (las más comunes, como el ransomware para obtener rescate), ideológicas o simplemente el desafío técnico, y sus acciones representan amenazas constantes que evolucionan a medida que surgen nuevas tecnologías.

Cybersecurity (Ciberseguridad) Práctica y conjunto de medidas orientadas a proteger sistemas informáticos, redes, dispositivos y datos frente a ataques digitales, accesos no autorizados o daños. La ciberseguridad busca garantizar la **confidencialidad**, **integridad** y **disponibilidad** de la información, mediante controles técnicos (firewalls, cifrado, antivirus), procedimientos organizativos (políticas de seguridad, gestión de incidentes) y la concienciación de usuarios. Incluye actividades preventivas (gestión de vulnerabilidades, análisis de riesgos), de detección (monitorización, **IDS/IPS**) y respuesta (planes de respuesta a incidentes, recuperación) para reducir riesgos en el entorno digital.

D

Database (Base de Datos) Colección organizada de datos estructurados, típicamente almacenados electrónicamente en un sistema informático. Una base de datos permite el almacenamiento, consulta y actualización eficiente de grandes volúmenes de información mediante un software de gestión (DBMS). En ciberseguridad, se protegen las bases de datos con controles de acceso, cifrado y monitoreo para prevenir filtraciones o alteraciones de la información que contienen.

Data Point (Punto de Datos) Unidad específica de información dentro de un conjunto de datos o base de datos. Cada punto de datos representa un hecho o valor singular (por ejemplo, una entrada en una tabla, un valor medido por un sensor o un atributo de un registro). En análisis de seguridad, correlacionar múltiples puntos de datos (como eventos de registro) puede revelar patrones sobre incidentes o comportamientos anómalos.

DDoS (Distributed Denial of Service) Ataque de denegación de servicio distribuido, en el que múltiples sistemas (a menudo parte de una **botnet**) envían un aluvión de tráfico masivo a un servidor, servicio o red objetivo con la intención de sobrecargar sus recursos y dejarlo fuera de servicio. Al provenir de muchas fuentes simultáneas, un ataque DDoS es más difícil de filtrar o bloquear que un DoS simple (de una sola fuente). Su objetivo principal es interrumpir la **disponibilidad** del servicio víctima,

impidiendo que usuarios legítimos accedan a él hasta que cese el ataque o se tomen medidas de mitigación (como filtrado de tráfico o ampliación de capacidad).

Detect (Detectar) Función central del Marco de Ciberseguridad NIST (CSF) enfocada en la identificación oportuna de eventos e incidentes de seguridad. La función Detectar implica implementar capacidades de monitoreo continuo, sistemas de alerta temprana (como **SIEM**, **Intrusion Detection Systems**, etc.) y procesos de análisis que permitan descubrir actividades maliciosas o anomalías en la red. Fortalecer la fase de detección mejora la capacidad para responder rápidamente ante amenazas antes de que causen mayores impactos.

E

Encryption (Cifrado) Proceso de convertir datos en un formato ilegible (texto cifrado) para proteger su contenido frente a accesos no autorizados. El cifrado utiliza algoritmos matemáticos y claves criptográficas para codificar la información de modo que solo pueda ser leída por quien posea la clave de descifrado correcta. Esta técnica asegura la **confidencialidad** de los datos durante su almacenamiento o transmisión (por ejemplo, comunicaciones seguras mediante HTTPS). Existen métodos de cifrado simétrico (misma clave para cifrar/descifrar, e.g. AES) y asimétrico (par de claves pública/privada, e.g. RSA), ambos diseñados para ser resistentes a intentos de criptoanálisis.

Evaluate (Evaluar) Quinto paso del marco NIST RMF, enfocado en verificar si los controles de seguridad y privacidad seleccionados e implementados en un sistema funcionan correctamente y cumplen su propósito. En la etapa de evaluación se llevan a cabo pruebas, auditorías o revisiones de seguridad para determinar la efectividad de los controles, identificar deficiencias y garantizar que el riesgo residual se mantiene dentro de niveles aceptables antes de autorizar el sistema para su operación.

External Threat (Amenaza Externa) Cualquier entidad, actor o evento fuera del entorno organizacional que pueda causar daño a sus activos de información o sistemas. Las amenazas externas incluyen a **ciberdelincuentes**, hackers no autorizados, **malware** proveniente del exterior, así como factores no intencionales como desastres naturales que afecten infraestructuras. A diferencia de una **amenaza interna**, la externa se origina fuera del control directo de la organización, por lo que es importante establecer defensas perimetrales, monitoreo de fronteras de red y planes de contingencia para mitigar su impacto.

Exploit Código, secuencia de comandos o técnica que aprovecha una **vulnerabilidad** o fallo de seguridad en un sistema para lograr un comportamiento no deseado. Un exploit permite a un atacante tomar control, ejecutar código arbitrario, elevar privilegios o de otro modo comprometer el sistema afectado. Los exploits pueden ser desarrollados y compartidos por atacantes (incluso comercializados en mercados clandestinos) y suelen clasificarse según la vulnerabilidad que atacan (por ejemplo, exploit de día cero, exploit para desbordamiento de búfer). Mantener los sistemas parcheados y actualizados ayuda a prevenir la efectividad de exploits conocidos.

F

Firewall (Cortafuegos) Dispositivo o software de seguridad de red que monitoriza y filtra el tráfico entrante y saliente entre redes (por ejemplo, entre Internet y la red interna de una empresa). Un firewall aplica un conjunto de reglas predefinidas para permitir o bloquear paquetes de datos según criterios como direcciones IP, puertos o contenido, actuando como una barrera protectora que impide accesos no autorizados. Existen firewalls a nivel de red (filtrado básico de paquetes) y de aplicación (analizan protocolos específicos, e.g. un WAF para aplicaciones web). En esencia, su función es

mitigar ataques al perímetro de la red y reforzar la postura de seguridad controlando el flujo de comunicaciones.

Forensic Analysis (Análisis Forense) Proceso de investigar y analizar evidencia digital tras un incidente de seguridad para identificar cómo ocurrió, qué impacto tuvo y quién fue el responsable. El análisis forense incluye la recolección protegida de datos (registros de sistemas, imágenes de discos, memoria, etc.), su examen detallado y la documentación de hallazgos, manteniendo la integridad de las evidencias para su posible uso legal. Esta disciplina permite reconstruir la secuencia de eventos de un ataque, entender las **vulnerabilidades** explotadas y obtener información clave que ayude a fortalecer la seguridad y, si aplica, respaldar acciones legales contra los atacantes.

G

Governance (Gobernanza) En el contexto del NIST CSF, función transversal que asegura que la organización establezca, supervise y mejore continuamente sus estrategias, políticas y procedimientos de ciberseguridad alineados con los objetivos del negocio. La gobernanza de seguridad involucra la definición de roles y responsabilidades claras, el apoyo de la alta dirección, la asignación de recursos adecuados y la medición del desempeño en seguridad. Un buen gobierno de ciberseguridad garantiza que las decisiones de seguridad se integren con la dirección estratégica de la empresa y cumplan con requerimientos legales o regulatorios.

H

Hacker Individuo experto en tecnología y sistemas informáticos que utiliza sus conocimientos técnicos para acceder a sistemas, redes o datos. Originalmente, el término "hacker" no implicaba una intención maliciosa, sino la habilidad de solucionar problemas complejos o mejorar sistemas; sin embargo, en el uso común se asocia a veces con actividades ilegales. En seguridad se distingue entre *black hats* (hackers maliciosos o criminales), *white hats* (expertos éticos que ayudan a mejorar la seguridad) y *gray hats* (acciones ambiguas), dependiendo de la motivación y permiso con que realicen sus intrusiones.

Hacktivist (Hacktivista) Tipo de hacker que lleva a cabo ataques informáticos motivados por razones políticas o sociales, buscando promover una causa o expresar una protesta. Un hacktivista puede, por ejemplo, filtrar información confidencial para denunciar actividades indebidas, desfigurar sitios web de entidades que desaprueba o realizar ataques de **denegación de servicio** contra organizaciones a las que considera opositoras a su causa. Aunque emplean técnicas de hacking similares a las de otros atacantes, los hacktivistas se distinguen por su agenda ideológica o activista más que por beneficio personal.

Hardening (Bastionado) Proceso de fortalecimiento de la seguridad de un sistema mediante la correcta configuración y refuerzo de sus componentes para reducir **vulnerabilidades**. El hardening incluye medidas como deshabilitar servicios innecesarios, aplicar todos los parches y actualizaciones disponibles, usar contraseñas robustas, eliminar cuentas o accesos predeterminados, y aplicar el principio de mínimo privilegio. Al bastionar servidores, aplicaciones o dispositivos de red, se minimiza la superficie de ataque y se dificulta la explotación de fallos de configuración o debilidades presentes por omisión.

HIPAA (Ley de Portabilidad y Responsabilidad del Seguro Médico) Ley federal de EE. UU. que establece estándares para la protección de la información médica de los pacientes. HIPAA (Health Insurance Portability and Accountability Act) obliga a las entidades de salud y sus asociados a resguardar la **confidencialidad** e **integridad** de la información de salud identificable (PHI), implemen-

tando medidas de seguridad administrativas, físicas y técnicas. Asimismo, exige notificar brechas de seguridad que involucren datos médicos y promueve principios de privacidad para garantizar que los datos sanitarios de las personas se utilicen adecuadamente.

I

Identify (Identificar) Función central del Marco de Ciberseguridad NIST (CSF) que se enfoca en entender el contexto de la organización para gestionar proactivamente el riesgo de ciberseguridad. La fase de Identificar incluye el inventario de **activos** (hardware, software, datos), la evaluación de **vulnerabilidades** y el análisis de **riesgos** potenciales que podrían afectar al negocio. Al conocer qué recursos se deben proteger y cuáles son las **amenazas** y consecuencias posibles, la organización puede priorizar esfuerzos y planificar controles de seguridad adecuados.

Implement (Implementar) Cuarto paso del NIST RMF que consiste en llevar a cabo la implantación de los controles de seguridad y privacidad seleccionados en la fase de planeación. En esta etapa, la organización ejecuta las soluciones técnicas y operativas (configuraciones, herramientas, procedimientos, capacitación) diseñadas para mitigar los **riesgos** identificados. Una vez implementados los controles, el sistema es configurado conforme a las políticas de seguridad establecidas, preparando el entorno para posteriormente ser evaluado y autorizado antes de entrar en operación.

Incident Response (Respuesta a Incidentes) Proceso estructurado y rápido mediante el cual una organización identifica, contiene, erradica y se recupera de un incidente de ciberseguridad, corrigiendo los efectos de una violación de seguridad. Incluye etapas como la detección y análisis del incidente, la contención del daño (por ejemplo, aislando sistemas afectados), la eliminación de la amenaza (borrado de **malware**, cierre de brechas explotadas), la recuperación de sistemas y datos a condiciones normales, y la documentación de lecciones aprendidas. El objetivo es minimizar el impacto y restablecer la operatividad, fortaleciendo la seguridad para prevenir futuros incidentes.

Integrity (Integridad) Principio que asegura que los datos se mantengan exactos, completos y confiables, sin haber sido alterados o destruidos de forma indebida. Mantener la integridad implica prevenir modificaciones no autorizadas, errores no detectados o alteraciones maliciosas de la información. Esto se logra mediante controles como sumas de verificación, firmas digitales, permisos de escritura restringidos y copias de seguridad regulares. La integridad, junto a la **confidencialidad** y la **disponibilidad**, constituye uno de los pilares de la seguridad de la información (ver **Tríada CIA**).

Internal Threat (Amenaza Interna) Riesgo de seguridad originado desde dentro de la propia organización, ya sea por empleados actuales, exempleados, contratistas, proveedores de confianza u otras personas con acceso interno a sistemas y datos. Las amenazas internas pueden ser intencionales (un empleado descontento que filtra datos, por ejemplo) o accidentales (un usuario con privilegios que por error provoca una brecha). Dado que los insiders poseen cierto nivel de confianza y acceso legítimo, este tipo de amenaza es difícil de detectar y gestionar. Mitigarla requiere controles como la segregación de funciones, monitoreo de actividades privilegiadas, políticas estrictas de gestión de cuentas y concienciación para evitar negligencias.

Intrusion Detection System (IDS) Sistema o aplicación que monitorea el tráfico de red o la actividad en equipos para identificar comportamientos sospechosos o conocidos como maliciosos, generando alertas cuando detecta posibles intrusiones. Un IDS puede basarse en firmas (comparando eventos con patrones de ataques conocidos) o en anomalías (detectando desviaciones respecto al comportamiento normal). Al activarse una alerta, los analistas de seguridad pueden investigar el incidente y tomar acciones de respuesta. A diferencia de un IPS (Sistema de Prevención de Intrusiones), que puede bloquear activamente las conexiones maliciosas, un IDS típicamente opera en modo monitoreo y notificación.

L

Linux Sistema operativo de código abierto muy utilizado en servidores, dispositivos de red y entornos de seguridad informática. Linux se destaca por su estabilidad, flexibilidad y la fuerte comunidad que lo respalda, ofreciendo distribuciones enfocadas en ciberseguridad (como Kali Linux para pruebas de penetración). En seguridad, Linux es valorado por las herramientas de administración y monitoreo que integra (firewall iptables/nftables, sistemas de registros detallados, etc.), aunque requiere de configuración experta para mantenerlo robusto frente a amenazas.

Log (Registro) Archivo o bitácora que documenta cronológicamente eventos, actividades y transacciones que ocurren en un sistema informático o red. Los registros pueden incluir accesos de usuarios, cambios en configuraciones, comunicaciones de red, eventos de seguridad, entre otros. En ciberseguridad, los logs son esenciales para auditoría y **análisis forense**, ya que permiten reconstruir incidentes y detectar comportamientos anómalos. Una buena práctica es centralizar y proteger los registros (por ejemplo, mediante un **SIEM**) para facilitar su revisión y prevenir manipulaciones por parte de atacantes que intenten borrar sus huellas.

M

Malware (Software malicioso) Término genérico para cualquier programa o código informático diseñado con propósitos dañinos. Incluye diversas categorías como **virus**, **gusanos**, **troyanos**, **ransomware**, **spyware**, **adware** malicioso, **rootkits**, entre otros. El malware puede destruir o cifrar datos, robar información confidencial, otorgar control remoto del sistema al atacante o desplegar publicidad no deseada, entre muchas otras actividades perjudiciales. Para combatirlo, se emplean herramientas antivirus/antimalware actualizadas, junto con prácticas seguras (no descargar software de fuentes no confiables, parchar **vulnerabilidades**) a fin de reducir el riesgo de infección.

Metrics (Métricas) Atributos técnicos clave, como el tiempo de respuesta, la **disponibilidad** y la tasa de fallos, que se utilizan para evaluar el rendimiento de una aplicación de software o sistema. En ciberseguridad, las métricas también miden la efectividad de los controles de seguridad (por ejemplo, tiempo de detección de incidentes, tasa de éxito en bloqueo de amenazas) y ayudan a las organizaciones a monitorear y mejorar su postura de seguridad de manera cuantificable.

Monitor (Monitorear) Séptimo paso del NIST RMF que implica supervisar continuamente el funcionamiento de los sistemas y la efectividad de los controles de seguridad implementados. La fase de monitoreo abarca la recolección periódica de información (eventos de registro, alertas de seguridad, estado de parches), el análisis de dicha información para detectar cambios o incidentes, y la ejecución de acciones de mejora cuando sea necesario. Al monitorear de forma continua, la organización puede identificar rápidamente nuevas **amenazas**, comprobar el **cumplimiento** continuo de las políticas de seguridad y ajustar sus controles para responder a la evolución del **riesgo** en el tiempo.

Multi-Factor Authentication (MFA, Autenticación Multifactor) Método de **autenticación** que requiere dos o más evidencias (factores) independientes para verificar la identidad de un usuario antes de concederle acceso. Combina típicamente algo que el usuario sabe (una contraseña o PIN), algo que tiene (por ejemplo, un código de un token o enviado al teléfono móvil) y/o algo que es (una característica biométrica como huella digital o reconocimiento facial). Al añadir factores adicionales más allá de la sola contraseña, se refuerza significativamente la seguridad del proceso de autenticación, dificultando que un atacante suplante la identidad aunque haya comprometido uno de los factores (por ejemplo, la contraseña). Un ejemplo común de MFA es ingresar la contraseña correcta y luego proporcionar un código de un solo uso recibido en el teléfono.

N

Network Protocol Analyzer (Packet Sniffer) Herramienta que captura y analiza el tráfico de datos que circula por una red, permitiendo inspeccionar en detalle los paquetes enviados y recibidos. También conocido como sniffer o analizador de protocolos, permite al usuario ver las cabeceras e incluso el contenido (si no está cifrado) de las comunicaciones en la red local. Administradores de red utilizan estas herramientas (como Wireshark o tcpdump) para diagnosticar problemas de conectividad, verificar configuraciones y monitorear el uso de la red. En manos de un atacante, un sniffer puede emplearse para interceptar información sensible transmitida sin cifrar, por lo que es importante usar protocolos seguros (ej. TLS) en redes potencialmente expuestas.

Network Security (Seguridad de Red) Práctica de proteger la infraestructura de redes de comunicación contra accesos no autorizados, mal uso o ataques maliciosos. La seguridad de red implica una combinación de hardware, software y políticas para controlar el tráfico que entra y sale de la red, asegurando la **confidencialidad** e **integridad** de los datos en tránsito. Entre las medidas comunes de seguridad de red se incluyen la segmentación de la red, el uso de **firewalls** y sistemas de detección/prevención de intrusos (**IDS/IPS**), redes privadas virtuales (VPN) para conexiones seguras, protocolos seguros (SSH, HTTPS) y la gestión adecuada de dispositivos y parches en todos los puntos de la red.

NIST Cybersecurity Framework (CSF) Marco voluntario desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., que proporciona estándares, directrices y mejores prácticas para gestionar el **riesgo** de ciberseguridad. El NIST CSF se compone de cinco funciones centrales — **Identify, Protect, Detect, Respond, Recover** — que ayudan a las organizaciones a estructurar sus programas de seguridad. Aunque nació para proteger infraestructuras críticas, ha sido ampliamente adoptado en diversos sectores como una referencia para evaluar madurez en ciberseguridad y alinear las estrategias de seguridad con objetivos de negocio y **cumplimiento** normativo.

NIST Special Publication 800-53 Conjunto de estándares y controles de seguridad publicado por NIST que ofrece un marco unificado para proteger sistemas de información del gobierno federal de EE. UU. (y organizaciones que operan con este). La SP 800-53 lista controles técnicos, operativos y administrativos divididos en familias (como control de accesos, **autenticación**, auditoría, etc.) y en niveles de garantía, permitiendo seleccionar controles adecuados según la categorización de impacto del sistema (bajo, moderado, alto). Aunque diseñado para entornos gubernamentales, este marco de control es también una referencia útil para organizaciones que buscan implementar prácticas de seguridad integrales y reconocidas.

O

Order of Volatility (Orden de Volatilidad) Secuencia establecida que determina el orden en que deben recolectarse o preservarse los distintos tipos de datos durante una investigación forense, priorizando aquellos que desaparecerán con mayor facilidad. La regla general es capturar primero la información más volátil (que se esfuma rápidamente, típicamente la RAM o procesos en ejecución) y luego proceder hacia datos menos volátiles (como el contenido de discos o almacenamiento persistente). Siguiendo el orden de volatilidad — por ejemplo: registros en memoria, tablas de red, procesos activos, datos temporales, luego discos duros, medios extraíbles, etc. — se evita perder evidencias críticas que podrían sobrescribirse o perderse ante un apagado del sistema o transcurso del tiempo.

OS (Sistema Operativo) Interfaz entre el hardware de una computadora y el usuario, que gestiona recursos del sistema como memoria, procesadores y dispositivos de entrada/salida. En ciberseguridad, el sistema operativo es clave para la seguridad del entorno, ya que debe configurarse adecuadamente

(por ejemplo, deshabilitando servicios innecesarios, aplicando parches) y monitorearse para detectar actividades maliciosas. Ejemplos comunes incluyen Windows, **Linux** y macOS, cada uno con implicaciones específicas para la protección y gestión de **amenazas**.

OWASP (Open Web Application Security Project) Organización sin fines de lucro dedicada a mejorar la seguridad del software, en especial de las aplicaciones web, a través de iniciativas comunitarias, documentación y herramientas gratuitas. OWASP es reconocida por proyectos emblemáticos como el OWASP Top 10, que lista periódicamente las diez **vulnerabilidades** más críticas en aplicaciones web, sirviendo de guía para desarrolladores y evaluadores de seguridad. También ofrece numerosas guías de buenas prácticas de desarrollo seguro, herramientas como OWASP ZAP (proxy para pruebas de penetración web) y proyectos educativos. En esencia, OWASP proporciona a profesionales y empresas recursos actualizados para construir, probar y mantener aplicaciones más seguras desde su concepción hasta su despliegue.

P

Password Attack (Ataque de Contraseña) Intento de obtener acceso no autorizado a un sistema protegido por contraseña, mediante el descifrado o adivinanza de la misma. Este tipo de ataque puede llevarse a cabo con técnicas de fuerza bruta (probando sistemáticamente todas las combinaciones posibles), ataques de diccionario (probando contraseñas comunes o derivadas de palabras conocidas), credential stuffing (usando credenciales filtradas de otros servicios) o mediante **phishing** para engañar al usuario y que revele su clave. La defensa contra ataques de contraseña incluye usar contraseñas robustas y únicas, limitar intentos fallidos, emplear **autenticación multifactor** y monitorear accesos sospechosos.

Penetration Testing (Pruebas de Penetración) Simulación controlada de ataques contra sistemas, redes o aplicaciones de una organización con el fin de identificar **vulnerabilidades** explotables. Estas pruebas las realizan profesionales llamados pentesters (a veces organizados como **Red Team**), quienes, con autorización, emplean herramientas y técnicas similares a las de atacantes reales para descubrir fallos de seguridad, configuraciones débiles o errores humanos. Tras la prueba, se elabora un informe detallando las vulnerabilidades encontradas y recomendaciones para corregirlas. Las pruebas de penetración ayudan a las organizaciones a fortalecer sus defensas antes de que atacantes genuinos aprovechen esas brechas.

Personally Identifiable Information (PII, Información de Identificación Personal) Datos que permiten identificar de manera única a una persona, ya sea directa o indirectamente. La PII incluye elementos como el nombre completo, número de identificación (como DNI o número de seguro social), dirección, número de teléfono, correo electrónico personal, fecha de nacimiento, información biométrica, entre otros. Debido a su naturaleza sensible, la PII está protegida por diversas leyes y regulaciones de privacidad (por ejemplo, GDPR en Europa exige su correcto manejo). La exposición no autorizada de PII puede derivar en robo de identidad, fraude u otros perjuicios, por lo que las organizaciones deben salvaguardarla mediante controles estrictos de seguridad y políticas de privacidad.

Phishing Técnica de **ingeniería social** que utiliza comunicaciones digitales fraudulentas (habitualmente correos electrónicos, pero también mensajes de texto o sitios web falsos) para engañar a usuarios y lograr que revelen información confidencial (credenciales, datos bancarios) o instalen **malware**. Un atacante de phishing se hace pasar por una entidad confiable — como un banco, una red social o el departamento de TI de la empresa — y suele incluir en el mensaje un enlace o archivo adjunto malicioso. Al clicar o proporcionar los datos solicitados, la víctima sin saberlo entrega sus datos al atacante o compromete su dispositivo. Para prevenirlo, se recomienda verificar la legitimidad de los remitentes, no seguir enlaces sospechosos y usar factores de **autenticación** adicionales.

Physical Attack (Ataque Físico) Incidente de seguridad que afecta al entorno físico de los sistemas y,

por ende, a sus componentes digitales. Incluye acciones como el robo de hardware (por ejemplo, un atacante sustrae un portátil o servidor con información sensible), el sabotaje de equipos o instalaciones (desconectar cables, dañar dispositivos deliberadamente) o cualquier agresión tangible que derive en un compromiso de la seguridad lógica. Los ataques físicos pueden provocar pérdida de **disponibilidad** (si se destruye o secuestra un equipo), de **confidencialidad** (si se accede al disco duro robado) e **integridad** (si se manipulan dispositivos). Las contramedidas incluyen control de acceso físico estricto, vigilancia, cerraduras de seguridad en racks y **cifrado** de discos para proteger datos en caso de extravío de dispositivos.

Physical Social Engineering (Ingeniería Social Física) Variante de la **ingeniería social** donde el atacante se vale de engaños cara a cara o interacción personal para obtener acceso físico a instalaciones o activos restringidos. El atacante se hace pasar por alguien con autorización (por ejemplo, un técnico de soporte, un empleado, personal de limpieza o un visitante legítimo) y aprovecha la confianza o cortesía del personal para entrar en áreas seguras. Técnicas comunes incluyen el tailgating (colarse detrás de alguien en una puerta de acceso controlado) o pretextos convincentes para que seguridad le deje pasar. Una vez dentro, el atacante podría conectar un USB malicioso a la red interna, robar documentos confidenciales impresos o instalar dispositivos de espionaje. La defensa implica entrenar al personal para verificar identidades, usar credenciales visibles y mantener políticas estrictas de acceso físico.

Playbook Manual o guía que proporciona detalles específicos sobre acciones operativas, como procedimientos estandarizados para responder a incidentes de seguridad. En ciberseguridad, un playbook describe pasos claros y predefinidos (por ejemplo, cómo aislar un sistema comprometido o notificar a las partes interesadas) para garantizar una respuesta rápida, consistente y efectiva ante eventos específicos.

Port Scanning (Escaneo de Puertos) Técnica utilizada (tanto por administradores de sistemas como por atacantes) para descubrir qué puertos y servicios están abiertos o activos en un sistema o red. Consiste en enviar solicitudes a una serie de puertos en un host y analizar las respuestas para determinar si esos puertos están abiertos, cerrados o filtrados. Un escaneo de puertos ayuda a identificar servicios en ejecución (HTTP, FTP, SSH, etc.) y posibles puntos vulnerables que podrían ser explotados. Herramientas como Nmap automatizan este proceso. En un contexto de ataque, el escaneo de puertos suele ser una fase de reconocimiento previa, para mapear la superficie de ataque de un objetivo; por ello, muchos sistemas de seguridad monitorean y limitan estas actividades para detectar intrusos tempranamente.

Prepare (Preparación) Primer paso del NIST RMF, enfocado en establecer un fundamento sólido para la gestión de **riesgos** de seguridad antes de que ocurran incidentes. La fase de Preparación incluye actividades como la definición del contexto organizacional (misión, procesos, regulaciones aplicables), la identificación de partes interesadas, el establecimiento de un programa de seguridad y la asignación de roles y recursos. También abarca la concienciación y capacitación en ciberseguridad. En resumen, es la etapa previa donde la organización se alista proactivamente para enfrentar **amenazas**, de modo que los pasos posteriores del RMF (**Categorizar**, **Seleccionar** controles, etc.) se realicen de manera informada y efectiva.

Privacy Protection (Protección de la Privacidad) Conjunto de medidas y prácticas destinadas a salvaguardar la información personal de individuos frente a accesos o usos no autorizados. Implica recolectar y procesar únicamente los datos personales necesarios, almacenarlos de forma segura (p. ej., cifrados), limitar quién puede acceder a ellos, y cumplir con los principios y regulaciones de privacidad aplicables (como el derecho al consentimiento, a la rectificación y al olvido bajo GDPR). La protección de la privacidad busca asegurar que los datos personales se utilicen de manera transparente y legítima, evitando filtraciones o abusos que puedan afectar los derechos y libertades de las personas dueñas de esos datos.

Programming (Programación) Proceso de crear instrucciones y escribir código fuente para que una computadora ejecute tareas específicas. En el ámbito de la ciberseguridad, la programación es esencial para desarrollar herramientas de seguridad (por ejemplo, scripts de automatización, exploits de prueba, software de **cifrado**), así como para entender y auditar el comportamiento de aplicaciones desde la perspectiva de seguridad. Los profesionales de seguridad con habilidades de programación pueden analizar código malicioso, crear sus propios métodos de detección o personalizar soluciones de protección, lo que resulta valioso en la identificación de **vulnerabilidades** y la implementación de defensas a medida.

Protected Health Information (PHI, Información de Salud Protegida) Subconjunto de datos personales referente a la salud de un individuo, cuya divulgación no autorizada puede comprometer su privacidad. Incluye información médica identificable, como historiales clínicos, diagnósticos, resultados de pruebas, datos de pago de servicios de salud y cualquier otro dato que vincule la identidad de una persona con detalles sobre su estado de salud pasado, presente o futuro. La PHI está fuertemente regulada (por leyes como **HIPAA** en EE. UU.), exigiendo salvaguardas adicionales debido a su sensibilidad. Las organizaciones sanitarias deben implementar medidas técnicas y administrativas estrictas para garantizar que la información de salud protegida se mantenga **confidencial** y solo sea accesible para quienes estén autorizados.

Protect (Proteger) Función del NIST CSF dedicada a desarrollar e implementar salvaguardas apropiadas para asegurar la prestación de servicios críticos tras una potencial incidencia de seguridad. La fase de Proteger engloba la implementación de políticas, procedimientos y controles que mitiguen **amenazas** o limiten su impacto. Ejemplos de actividades en esta función son el control de accesos (asegurar que solo personal autorizado ingrese a sistemas), la concienciación y capacitación en seguridad, el mantenimiento de protecciones de datos (**cifrado**, respaldos), y la aplicación de configuraciones seguras en sistemas. En esencia, Protect busca prevenir incidentes o dificultar su ejecución, reduciendo la probabilidad de brechas de seguridad exitosas.

Protecting and Preserving Evidence (Protección y Preservación de Evidencias) Conjunto de prácticas para manejar la evidencia digital de forma que conserve su **integridad** y valor probatorio durante una investigación de seguridad. Esto implica aislar y resguardar dispositivos o registros inmediatamente tras un incidente, realizar copias forenses (imágenes) de discos o memoria en lugar de trabajar sobre los originales, documentar la cadena de custodia (quién accede a las evidencias y cuándo) y almacenar los datos en entornos seguros. El objetivo es evitar la alteración, corrupción o pérdida de la evidencia (por la volatilidad de ciertos datos o por acciones inadvertidas), de modo que los analistas forenses puedan analizarla y, si es necesario, sea admisible en procesos legales o disciplinarios.

R

Ransomware Tipo de ataque o **malware** que cifra los archivos o sistemas de una víctima y exige el pago de un rescate (usualmente en criptomonedas) a cambio de proporcionar la clave para restaurar el acceso a los datos secuestrados. El ransomware suele propagarse a través de correos maliciosos, descargas fraudulentas o explotando **vulnerabilidades**, y una vez activado, muestra un mensaje informando del cifrado y la demanda de pago bajo amenaza de borrar datos o publicarlos. Este ataque causa un grave impacto en la **disponibilidad** de la información. Para mitigar el riesgo, se recomienda mantener copias de seguridad offline actualizadas, contar con soluciones de seguridad que detecten comportamientos de cifrado anómalos y capacitar a los usuarios para evitar caer en engaños iniciales.

Recover (Recuperación) Función del NIST CSF enfocada en restaurar y volver a la operación normal después de un incidente de ciberseguridad. La fase de Recuperación incluye actividades como la ejecución de planes de recuperación de desastres o **continuidad de negocio**, restauración de datos

desde respaldos, reparación de sistemas afectados, y comunicación a las partes interesadas sobre la situación resuelta. El objetivo es minimizar el tiempo de inactividad y las pérdidas tras un incidente, asegurando que los sistemas críticos vuelvan a estar disponibles y confiables. Además, la recuperación suele involucrar una revisión post-incidente para aprender de lo ocurrido y mejorar la preparación ante eventos futuros.

Red Team (Equipo Rojo) Equipo ofensivo en ciberseguridad encargado de simular ataques reales y controlados contra la organización para probar la eficacia de sus defensas. El equipo rojo utiliza técnicas de hacking ético, **pruebas de penetración** y tácticas de adversarios reales (pero con autorización) para intentar vulnerar los sistemas, redes y aplicaciones corporativas. Su objetivo es identificar **vulnerabilidades** y debilidades de seguridad que el equipo defensor (**Blue Team**) pueda haber pasado por alto. Tras sus ejercicios, el Red Team reporta sus hallazgos detalladamente al Blue Team y a la dirección, de modo que se puedan corregir las fallas antes de que un atacante genuino las explote. Esta dinámica de prueba continua ayuda a la organización a mejorar su postura de seguridad de manera proactiva.

Respond (Responder) Función del NIST CSF destinada a asegurar que, una vez detectado un evento de ciberseguridad, se realicen acciones efectivas para contenerlo, mitigarlo y analizarlo. La fase de Responder abarca la ejecución de procedimientos de **respuesta a incidentes**: contención inmediata (aislar sistemas comprometidos para que el incidente no se propague), neutralización de la **amenaza** (eliminar **malware**, cerrar brechas explotadas), comunicación interna y externa según el plan (por ejemplo, notificación a reguladores o clientes si corresponde), y recolección de información sobre el evento. Un proceso de respuesta bien gestionado reduce el impacto de los incidentes y aporta información valiosa para ajustar estrategias defensivas, enlazando luego con la fase de **Recuperación** para restaurar la normalidad.

Risk (Riesgo) Cualquier circunstancia o factor que pueda comprometer la **confidencialidad**, **integridad** o **disponibilidad** de un **activo**, causando un impacto negativo a la organización. El riesgo en ciberseguridad se evalúa típicamente como la combinación de la probabilidad de que ocurra un evento de **amenaza** y la gravedad de sus consecuencias. Por ejemplo, la posibilidad de que un atacante explote una **vulnerabilidad** crítica (alta probabilidad si no está parchada) y filtre datos sensibles (alto impacto) constituye un riesgo significativo. La gestión de riesgos implica identificar los riesgos, analizarlos, priorizarlos y tratarlos (mediante mitigación, transferencia, aceptación o evitación) para mantenerlos dentro de niveles tolerables.

Risk Mitigation (Mitigación de Riesgos) Proceso de implementar medidas y controles para reducir la probabilidad de ocurrencia o el impacto de **riesgos** de seguridad identificados. La mitigación de riesgos busca disminuir las **amenazas** o **vulnerabilidades** a un nivel aceptable para la organización. Ejemplos de estrategias de mitigación incluyen corregir vulnerabilidades técnicas (aplicando parches de software), fortalecer políticas y procedimientos (formando a empleados contra **phishing**), agregar controles preventivos adicionales (instalando sistemas de detección de intrusos, segmentando la red), o preparar medidas reactivas (mantener respaldos para contrarrestar **ransomware**). En resumen, es actuar sobre los riesgos priorizados para minimizar la posibilidad de incidentes y su daño potencial.

Rootkit Tipo de **malware** o conjunto de técnicas cuyo objetivo es ocultar la presencia de un atacante o software malicioso en un sistema comprometido, obteniendo persistencia con privilegios elevados sin ser detectado. Un rootkit típico se integra profundamente en el sistema (a nivel de kernel o de firmware, por ejemplo) para manipular funciones del sistema operativo, de modo que archivos, procesos o comunicaciones del atacante queden camuflados de las herramientas de monitoreo y antivirus. Al mantener ese acceso oculto, el atacante puede controlar el sistema durante largos períodos. La detección de rootkits es compleja y a menudo requiere herramientas especializadas o análisis fuera de línea, y en muchos casos la forma más segura de erradicarlos es reinstalando por completo el sistema afectado.

S

Security Architecture (Arquitectura de Seguridad) Diseño global de los componentes de seguridad (herramientas, controles, procesos y políticas) integrados en la infraestructura de TI de una organización. La arquitectura de seguridad define cómo se disponen y relacionan las distintas capas defensivas (perímetro, red interna, host, aplicación, datos) para proteger los **activos** frente a **amenazas**. Una buena arquitectura de seguridad asegura que los controles estén alineados y sean complementarios entre sí (defensa en profundidad), cubriendo brechas y minimizando puntos únicos de fallo. Por ejemplo, puede incluir **firewalls** perimetrales, segmentación de redes, **autenticación** robusta, **cifrado** de datos sensibles y monitoreo centralizado, todos orquestados bajo principios y estándares coherentes.

Security Audit (Auditoría de Seguridad) Examen sistemático de los controles, políticas y procedimientos de seguridad de una organización para evaluar su efectividad y **cumplimiento**. En una auditoría de seguridad se revisan configuraciones de sistemas, registros de actividad, esquemas de acceso, prácticas operativas y documentación para identificar desviaciones respecto a normativas o mejores prácticas. El auditor suele generar un informe con hallazgos, que pueden incluir **vulnerabilidades** técnicas, configuraciones débiles o incumplimientos regulatorios, junto con recomendaciones de remediación. Las auditorías (internas o externas) ayudan a la organización a detectar puntos de mejora y demostrar diligencia debida en la protección de la información.

Security Controls (Controles de Seguridad) Medidas específicas diseñadas para reducir la exposición a **riesgos** o prevenir, detectar y responder a **amenazas** contra **activos** de información. Los controles de seguridad pueden ser de naturaleza técnica (ejemplo: **cifrar** datos, usar **firewalls**, implementar **MFA** en accesos), administrativa (políticas de seguridad, procedimientos, capacitación del personal) o física (guardias de seguridad, cerraduras, videovigilancia en centros de datos). Cada control apunta a mitigar una **vulnerabilidad** o bloquear un **vector de ataque** concreto. Un buen programa de seguridad selecciona controles adecuados según el análisis de riesgo y verifica regularmente su eficacia, ajustándolos conforme evolucionan las amenazas.

Security Ethics (Ética de Seguridad) Conjunto de principios y directrices que orientan a los profesionales de ciberseguridad para actuar de forma responsable, legal y respetuosa de los valores durante el desempeño de sus funciones. La ética de seguridad aborda situaciones como el respeto a la privacidad al monitorear sistemas, la necesidad de **confidencialidad** en el manejo de información sensible, la obtención de consentimiento adecuado antes de **pruebas de penetración**, y en general, la toma de decisiones que equilibren la protección del conjunto con los derechos individuales. Un profesional ético de seguridad se adhiere a códigos de conducta (por ejemplo, no explotar conocimientos para beneficio propio ilícito) y prioriza hacer el bien, incluso cuando posee habilidades que podrían emplearse maliciosamente.

Security Frameworks (Marcos de Seguridad) Conjuntos estructurados de estándares, lineamientos y mejores prácticas que sirven como guía para establecer y administrar un programa integral de ciberseguridad. Ejemplos de marcos reconocidos incluyen el **NIST CSF**, ISO/IEC 27001 (sistema de gestión de seguridad de la información), CIS Controls (controles críticos recomendados), entre otros. Un marco de seguridad proporciona un lenguaje común y una hoja de ruta para implementar controles, evaluar **riesgos** y madurar la postura de seguridad de manera consistente. Las organizaciones adoptan marcos de seguridad para asegurarse de no pasar por alto aspectos clave de protección, facilitar el **cumplimiento** regulatorio y evaluar su progreso en comparación con estándares internacionales.

Security Governance (Gobernanza de Seguridad) Conjunto de prácticas y procesos mediante los cuales la alta dirección de una organización dirige, gestiona y respalda sus esfuerzos de seguridad de la información. La gobernanza de seguridad se manifiesta en la definición de una estrategia clara de ciberseguridad alineada al negocio, la asignación de responsabilidades (por ejemplo, comité de se-

guridad, CISO), la integración de la seguridad en la gestión de **riesgos** corporativos y la supervisión del **cumplimiento** de políticas y objetivos de seguridad. A través de la gobernanza, la seguridad deja de ser solo un asunto técnico y se incorpora en la cultura y toma de decisiones organizacionales, asegurando continuidad y mejoras continuas en la protección de los **activos** críticos.

Security Posture (Postura de Seguridad) Estado general de la capacidad de una organización para protegerse contra las **amenazas** cibernéticas y responder a los incidentes de seguridad. La postura de seguridad refleja la fortaleza de todos los controles y procesos de seguridad implementados, así como el nivel de preparación ante posibles ataques. Una postura sólida implica no solo tener múltiples defensas (tecnológicas y administrativas) en funcionamiento, sino también adaptabilidad para ajustar dichas defensas frente a nuevos **riesgos**. Evaluar la postura de seguridad suele implicar revisar **métricas** de desempeño (como tiempos de respuesta a incidentes, resultados de auditorías, penetración lograda por **Red Teams**, etc.) y comparar el estado actual contra un marco deseado, con el fin de identificar áreas de mejora.

Select (Seleccionar) Tercer paso del NIST RMF que consiste en elegir y documentar los controles de seguridad y privacidad necesarios para proteger un sistema, basándose en la categorización de **riesgos** realizada previamente. En esta etapa, se determinan las medidas específicas que se implementarán para mitigar las **amenazas** identificadas.

Sensitive Personally Identifiable Information (SPII) Subtipo de información personal identificable (**PII**) que, por su naturaleza sensible, requiere un manejo más estricto y protecciones adicionales. La SPII incluye datos personales que podrían causar un mayor perjuicio al individuo si se divulgan sin autorización, tales como números de identificación gubernamental (ej. número de seguridad social), información financiera (cuentas bancarias, números de tarjeta de crédito), datos de salud, credenciales de **autenticación**, información biométrica, entre otros. Debido al posible impacto en la privacidad y seguridad individual, muchos marcos legales imponen obligaciones más rigurosas cuando se trata de SPII, por lo que las organizaciones deben clasificar los datos personales y aplicar medidas de seguridad proporcionadas al nivel de sensibilidad.

Shared Responsibility (Responsabilidad Compartida) Concepto que establece que la seguridad es un deber de todos los miembros de una organización, no solo del equipo de TI o seguridad. Bajo este enfoque, cada área y persona – desde ejecutivos hasta usuarios finales – tiene un rol en la protección de los **activos**: por ejemplo, los desarrolladores deben escribir código seguro, el personal debe seguir políticas (como no compartir contraseñas), Recursos Humanos debe incorporar controles en los procesos de contratación y desvinculación, etc. En entornos de computación en la nube, la "responsabilidad compartida" también se refiere al modelo en el que el proveedor cloud asegura la infraestructura subyacente, mientras que el cliente es responsable de proteger lo que despliega en la nube. En resumen, solo mediante la colaboración y conciencia de todos los involucrados se logra una defensa efectiva y capas de seguridad robustas.

SIEM (Security Information and Event Management) Sistema de Gestión de Información y Eventos de Seguridad que recopila y analiza datos de registro de múltiples fuentes (**firewalls**, sistemas operativos, aplicaciones, bases de datos, etc.) para monitorear actividades críticas y detectar **amenazas** en tiempo real. Un SIEM correlaciona eventos para identificar patrones sospechosos, genera alertas cuando detecta posibles incidentes y almacena registros de forma organizada para facilitar auditorías o **análisis forense**. Al proveer una vista unificada de la actividad de seguridad, es una herramienta clave para la detección proactiva y la respuesta rápida a incidentes.

SOAR (Orquestación, Automatización y Respuesta de Seguridad) Colección de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a eventos de seguridad de manera eficiente. SOAR integra sistemas como **SIEM** con procesos automatizados para priorizar alertas, ejecutar respuestas predefinidas (como bloquear una IP maliciosa) y coordinar acciones entre equipos, reduciendo el tiempo de reacción ante incidentes y el esfuerzo manual requerido.

Social Engineering (Ingeniería Social) Conjunto de técnicas de manipulación psicológica utilizadas por atacantes para engañar a personas y hacer que revelen información confidencial o realicen acciones que comprometan la seguridad. En lugar de atacar directamente sistemas tecnológicos, la ingeniería social explota la confianza, la curiosidad, el temor o la ignorancia de los usuarios. Ejemplos comunes son llamadas telefónicas haciéndose pasar por soporte técnico para obtener contraseñas, correos de **phishing** simulando ser de una entidad legítima, o incluso interacciones en persona (**ingeniería social física**) para sortear controles de acceso. La mejor defensa contra estas tácticas es la educación y concienciación de los usuarios, junto con procesos de verificación (por ejemplo, nunca proporcionar credenciales por email o confirmar identidades en solicitudes inusuales).

Social Media Phishing (Phishing en Redes Sociales) Variante de **phishing** que se apoya en la información recopilada de redes sociales para personalizar el engaño y hacerlo más verosímil. El atacante investiga el perfil público de la víctima (por ejemplo, sus amigos, lugar de trabajo, intereses publicados) y luego le envía un mensaje malicioso a través de la propia red social o por correo, haciendo referencia a datos reconocibles (un amigo en común, un evento reciente, algo que la víctima haya publicado) para ganarse su confianza. Al creer que el mensaje proviene de alguien conocido o que está relacionado con su vida, la víctima es más propensa a caer en la trampa y hacer clic en enlaces fraudulentos o proporcionar la información solicitada. Este tipo de ataque demuestra la importancia de configurar adecuadamente la privacidad en redes sociales y ser cauteloso incluso con mensajes que contengan detalles personales.

Spam (Correo no deseado) Mensajes electrónicos no solicitados, usualmente de tipo publicitario o engañoso, enviados de forma masiva. El spam llega típicamente por correo electrónico, pero también puede presentarse vía SMS, mensajería instantánea o publicaciones automatizadas en redes sociales. Además de la molestia que genera al saturar bandejas de entrada con contenido irrelevante, el spam puede servir como vehículo para **amenazas**: muchos mensajes de spam contienen enlaces a sitios maliciosos, adjuntos con **malware** o forman parte de estafas (como correos de **phishing** o esquemas de fraude). Para combatir el spam, los proveedores de correo y soluciones antispam utilizan filtros que identifican estos mensajes en base a patrones, remitentes conocidos y contenido sospechoso, reduciendo la cantidad que llega al usuario final.

Spear Phishing Ataque de **phishing** altamente dirigido a una persona o grupo específico dentro de una organización, en el cual el atacante adapta el mensaje para que parezca provenir de una fuente confiable que el objetivo conoce. A diferencia del phishing genérico (que es masivo y no personalizado), el spear phishing emplea información detallada sobre la víctima — obtenida de redes sociales, brechas previas u otras fuentes — para aumentar la probabilidad de engaño. Por ejemplo, un atacante podría enviarte un correo aparentando ser tu jefe, mencionando un proyecto real en el que trabajas, y solicitando urgentemente que descargues un archivo (infectado) o que ingreses tus credenciales en un sitio clonado. Dada su sofisticación, incluso personas precavidas pueden ser engañadas, por lo que es crucial verificar solicitudes inusuales por otro canal y contar con filtros de seguridad avanzados en la organización.

Splunk Cloud Herramienta alojada en la nube que se utiliza para recopilar, buscar y supervisar datos de registro en tiempo real. Diseñada para ayudar a las organizaciones a analizar grandes volúmenes de datos generados por sistemas y aplicaciones, Splunk Cloud proporciona información de seguridad y alertas que facilitan la detección de **amenazas** y la **respuesta a incidentes** (ver **SIEM**).

Splunk Enterprise Herramienta autoalojada que permite a las organizaciones retener, analizar y buscar datos de registro para obtener información de seguridad y generar alertas en tiempo real. Similar a Splunk Cloud, pero instalada localmente, ofrece flexibilidad para entornos que requieren control interno sobre la infraestructura de monitoreo de seguridad (ver **SIEM**).

Spyware (Software espía) Programa maligno diseñado para infiltrarse en un sistema y espiar la actividad del usuario, recopilando información sensible sin su consentimiento. El spyware puede registrar

pulsaciones de teclas (keyloggers para capturar contraseñas), tomar capturas de pantalla, monitorear el historial de navegación o acceder a la cámara y micrófono, todo de forma sigilosa para permanecer activo el mayor tiempo posible sin ser descubierto. A veces el spyware viene oculto dentro de aplicaciones aparentemente legítimas o se instala junto con otros **troyanos**. Su objetivo final es obtener datos privados (credenciales, información financiera, hábitos del usuario) y enviarlos al atacante. Incluso algunas aplicaciones comerciales recopilatorias de datos pueden considerarse spyware si recolectan información del usuario de manera excesiva y la transmiten para publicidad dirigida. Para combatirlo, se utilizan antispyware y las mismas prácticas que contra cualquier **malware**: mantener sistemas actualizados, evitar software de dudosa procedencia y contar con soluciones de seguridad que detecten comportamientos anómalos.

SQL (Structured Query Language) Lenguaje de consulta estructurado utilizado para gestionar y manipular bases de datos relacionales. El SQL permite realizar operaciones como insertar, modificar, eliminar y consultar datos almacenados en tablas mediante sentencias legibles (SELECT, INSERT, UPDATE, DELETE, etc.). En ciberseguridad, el conocimiento de SQL es importante por dos razones principales: primero, para la administración segura de **bases de datos** (gestionando permisos, implementando consultas preparadas para evitar inyecciones, etc.), y segundo, para comprender y prevenir ataques de SQL Injection, donde un atacante inserta código SQL malicioso en entradas de una aplicación web con el fin de extraer datos confidenciales o alterar la base de datos de forma no autorizada.

Supply Chain Attack (Ataque a la Cadena de Suministro) Tipo de ataque que compromete la seguridad a través de terceros o proveedores en la cadena de suministro de software o hardware de una organización. En lugar de atacar directamente a la víctima final, el adversario identifica componentes confiables que esta utiliza — por ejemplo, librerías de software de terceros, actualizaciones de software legítimo, servicios de proveedores externos o dispositivos de hardware en la infraestructura — e introduce código malicioso o **backdoors** en ellos antes de que lleguen a la organización objetivo. Cuando la víctima integra la pieza comprometida (por confiar en su origen), sin saberlo permite al atacante infiltrarse. Casos notables incluyen la inserción de **malware** en actualizaciones de software legítimo o en aplicaciones ampliamente distribuidas. La mitigación implica realizar evaluaciones de seguridad a proveedores críticos, verificar firmas o hashes de software, limitar la confianza ciega en componentes externos y mantener un monitoreo por si aparecen comportamientos sospechosos en productos de terceros.

T

Technical Skills (Habilidades Técnicas) Conocimientos especializados y capacidades prácticas en el uso de herramientas, tecnologías, metodologías y procedimientos relacionados con la ciberseguridad. Estas habilidades incluyen, por ejemplo, comprensión de redes y sistemas operativos, programación, análisis de vulnerabilidades, administración de dispositivos de seguridad (firewalls, IDS/IPS), criptografía básica aplicada, realización de análisis forense y manejo de incidentes. Las habilidades técnicas permiten a los profesionales de seguridad implementar y mantener defensas, así como detectar y responder eficazmente a amenazas. La disciplina de ciberseguridad evoluciona rápidamente, por lo que requiere actualización continua de estas competencias técnicas.

Threat (Amenaza) Cualquier circunstancia, evento o agente con potencial para explotar una vulnerabilidad y afectar negativamente los activos o la información de una organización. Las amenazas pueden ser intencionales (un atacante externo, malware diseñado para robar datos), accidentales (un fallo de energía que cause caída de sistemas, errores humanos que expongan información) o naturales (inundaciones, incendios que dañen centros de datos). Si una amenaza llega a materializarse, puede provocar un incidente de seguridad o brecha, impactando la confidencialidad, integridad o disponibilidad de la información. La gestión de la seguridad implica identificar amenazas relevantes y

tomar medidas preventivas para reducir la probabilidad de que se concreten o mitigar su impacto.

Threat Actor (Actor de Amenazas) Individuo, grupo organizado o entidad que representa una amenaza para la seguridad de sistemas e información. Puede tratarse de hackers delincuentes, grupos patrocinados por estados nación, terroristas cibernéticos, insiders maliciosos (empleados o ex-empleados con intenciones dañinas) e incluso hacktivistas. Cada tipo de actor de amenazas tiene motivaciones (económicas, políticas, personales), recursos y tácticas diferentes. Por ejemplo, un actor estatal puede llevar a cabo espionaje cibernético con herramientas avanzadas, mientras que un cibercriminal puede lanzar campañas masivas de ransomware por lucro. Comprender quiénes son los potenciales actores de amenaza y sus métodos forma parte del análisis de riesgo, ayudando a ajustar las defensas de acuerdo con los adversarios más probables que enfrentaría la organización.

Transferable Skills (Habilidades Transferibles) Competencias y aptitudes desarrolladas en otros ámbitos o profesiones que resultan aplicables a roles de ciberseguridad. Estas habilidades no técnicas complementan el perfil del profesional de seguridad y pueden incluir la resolución de problemas (pensamiento analítico y creativo para enfrentar desafíos nuevos), capacidad de comunicación (explicar riesgos y políticas de manera clara a distintos públicos), gestión del tiempo y proyectos, trabajo en equipo, adaptabilidad al cambio, y ética profesional. Por ejemplo, alguien con experiencia en atención al cliente puede aportar empatía y claridad al educar en seguridad a usuarios finales; o un profesional de gestión de proyectos puede mejorar la implementación de iniciativas de seguridad. En un campo tan multidisciplinario como la ciberseguridad, las habilidades transferibles ayudan a coordinar esfuerzos, integrar la seguridad con objetivos empresariales y fomentar una cultura de seguridad en toda la organización.

Trojan (Troyano) Programa malicioso que se presenta ante el usuario como un software legítimo o inofensivo, pero que al ejecutarlo realiza acciones ocultas y dañinas en el sistema. El nombre alude al Caballo de Troya de la mitología: el usuario "invita" el software creyendo que es benigno (por ejemplo, una aplicación gratuita atractiva, un adjunto aparentemente seguro), sin saber que contiene código malicioso. A diferencia de un virus o gusano, los troyanos no se replican por sí mismos, sino que dependen de la instalación voluntaria o engañosa. Una vez activo, el troyano puede abrir backdoors, robar información, descargar más malware o permitir el control remoto del equipo por parte del atacante. Para protegerse, se recomienda descargar software solo de fuentes oficiales, mantener actualizado el antivirus y estar alerta a comportamientos extraños de programas recién instalados.

U

USB Baiting Técnica de ataque perteneciente a la ingeniería social donde un atacante deja intencionalmente un dispositivo USB infectado (por ejemplo, en el estacionamiento o recepción de una empresa) con la esperanza de que alguien lo encuentre y lo conecte a un equipo por curiosidad o buena voluntad de devolverlo. Al insertar el USB "cebo" en un ordenador, se ejecuta malware almacenado en el dispositivo, comprometiendo esa máquina y potencialmente la red entera. Los ataques por USB baiting explotan la curiosidad humana y la falta de políticas de restricción de dispositivos extraíbles. Para prevenirlos, las organizaciones deben concientizar a su personal de no conectar medios desconocidos, deshabilitar la ejecución automática de USBs y utilizar soluciones de seguridad que analicen o bloqueen dispositivos extraíbles no autorizados.

V

Vishing Forma de engaño similar al phishing pero realizada a través de comunicaciones de voz (teléfono o mensajes de voz). En un ataque de vishing, el estafador llama a la víctima haciéndose pasar por una entidad confiable — como un banco, un servicio técnico o un organismo público — y mediante

tácticas de ingeniería social intenta obtener información confidencial (contraseñas, números de tarjeta de crédito, códigos OTP) o persuadirla para que realice alguna acción (por ejemplo, transferir dinero a una cuenta "segura"). Los ataques vishing suelen aprovechar la urgencia o temor (avisando de supuestos cargos fraudulentos o problemas legales) para que la persona actúe sin verificar la autenticidad de la llamada. Para protegerse, se recomienda desconfiar de llamadas inesperadas que soliciten datos sensibles y, ante cualquier duda, colgar y contactar uno mismo al organismo en cuestión mediante los canales oficiales conocidos.

Vulnerability (Vulnerabilidad) Debilidad o falla en un sistema de información que puede ser explotada por una amenaza para comprometer la seguridad. Las vulnerabilidades pueden ser de distinta naturaleza: errores de software (bugs en código que permiten ejecución de comandos no autorizados), configuraciones incorrectas (un servidor abierto a Internet sin protección, contraseñas por defecto sin cambiar), debilidades en protocolos o incluso procesos operativos deficientes. Cuando una vulnerabilidad es descubierta por atacantes, puede dar lugar a incidentes que afecten la confidencialidad (exfiltración de datos), integridad (modificación no autorizada) o disponibilidad (interrupciones). La gestión de vulnerabilidades comprende la identificación (mediante scanners o auditorías), la evaluación de su criticidad, y su remediación oportuna (aplicando parches, cambios de configuración o medidas compensatorias) para reducir la ventana de exposición.

W

Watering Hole Attack (Ataque de Abrevadero) Ataque en el que los ciberdelincuentes comprometen un sitio web frecuentemente visitado por un grupo específico de objetivos, con el fin de infectar a los miembros de ese grupo. La estrategia se asemeja a cazar en el "abrevadero" donde bebe la presa: en lugar de atacar directamente a la víctima deseada, el atacante infecta páginas web legítimas (por ejemplo, un foro profesional, una web de proveedores o un medio de noticias) que sabe que la víctima consulta. Cuando la víctima accede al sitio comprometido, sin sospechar porque es un lugar confiable, se descarga o ejecuta malware en su dispositivo mediante exploit. Este tipo de ataque es especialmente utilizado contra organizaciones o sectores particulares, ya que explota hábitos comunes de navegación. Para mitigarlo, además de mantener navegadores y plugins actualizados para no caer en exploits, las empresas pueden controlar y limitar las categorías de sitios accesibles desde su red y utilizar herramientas de detección de intrusiones web.

Worm (Gusano) Malware autorreplicable que se propaga automáticamente a través de redes explotando vulnerabilidades o debilidades de configuración, sin necesidad de intervención humana una vez iniciado. A diferencia de un virus, un gusano no requiere infectar un archivo ejecutable existente para reproducirse; suele ser un programa independiente que busca otros sistemas vulnerables en la red y se copia a sí mismo en ellos. Los gusanos pueden causar estragos en poco tiempo, generando enormes volúmenes de tráfico que congestionan redes (causando denegaciones de servicio) y a menudo llevan cargas maliciosas adicionales que dañan los sistemas infectados (por ejemplo, el gusano WannaCry se propagó globalmente en 2017 cifrando archivos de sus víctimas como ransomware). La rápida propagación de los gusanos hace crucial la instalación ágil de parches de seguridad en los sistemas y el uso de cortafuegos para restringir el tráfico entrante no esencial.

Z

Zero-Day Vulnerability Vulnerabilidad desconocida para el fabricante o el público en general, de la cual no existe aún un parche o solución disponible al momento de ser descubierta (es decir, el desarrollador ha tenido "cero días" para arreglarla). Cuando un atacante encuentra una vulnerabilidad zero-day y la explota antes de que sea corregida, puede comprometer sistemas con gran eficacia, ya

que incluso las herramientas de defensa no tienen firmas o actualizaciones para ese exploit nuevo. Una vez que la brecha de seguridad se hace pública, comienza la carrera tanto de los proveedores por desarrollar un parche como de los atacantes por aprovecharla rápidamente en víctimas no parcheadas. Mitigar el riesgo de los zero-days es complejo; se confía en estrategias como la seguridad en profundidad (múltiples capas de control pueden dificultar la explotación), la aplicación de políticas de privilegio mínimo y el uso de sistemas de detección basados en comportamiento anómalo para intentar identificar ataques inéditos.

Zero Trust (Confianza Cero) Modelo moderno de seguridad de la información que establece el principio de "nunca confiar, verificar siempre" para cualquier acceso a los recursos, independientemente de su procedencia. A diferencia del enfoque tradicional que solía asumir confianza implícita para quienes estaban dentro de la red corporativa, Zero Trust parte de la premisa de que una brecha puede ocurrir en cualquier momento y que cada usuario o dispositivo puede estar comprometido. Por ello, en un entorno de Confianza Cero, a cada solicitud de acceso se le exige autenticación y autorización continuas y contextuales (evaluando la identidad del usuario, el dispositivo, su ubicación, la sensibilidad del recurso al que accede, etc.), estableciendo además una segmentación estricta de la red. Implementar Zero Trust implica usar tecnologías como gestión robusta de identidades y accesos (IAM), autenticación multifactor, microsegmentación de redes, monitoreo constante y cifrado de comunicaciones internas. El resultado es que ningún elemento tiene acceso libre por el mero hecho de estar "dentro" de la infraestructura: todo debe probar que es confiable en cada interacción, reduciendo drásticamente la superficie de ataque y movimiento lateral de posibles intrusos.

Referencias y Créditos

Este glosario ha sido elaborado como una herramienta educativa independiente que compila, interpreta y organiza términos fundamentales en el ámbito de la ciberseguridad, con fines de aprendizaje autodidacta y profesional.

Los conceptos presentados han sido inspirados y estructurados a partir de la experiencia de aprendizaje obtenida en el programa profesional **Google Cybersecurity**, ofrecido por **Google** a través de la plataforma **Coursera**. En particular, se ha tomado referencia de los siguientes cursos completados por el autor:

- **Foundations of Cybersecurity** — Curso 1 de 8
- **Play It Safe: Manage Security Risks** — Curso 2 de 8

Este libro no reproduce materiales oficiales ni transcripciones de dichos cursos, sino que representa una reinterpretación y reescritura basada en la comprensión personal del autor, orientada a compartir el conocimiento de forma accesible y transformada.

Descargo de responsabilidad legal: Este glosario no está afiliado, respaldado, patrocinado ni autorizado por Google ni por Coursera. El contenido presentado ha sido elaborado de forma original por el autor y tiene propósitos únicamente formativos. Todos los nombres de marcas y plataformas mencionados pertenecen a sus respectivos propietarios.

ISBN: En trámite

Agradecimientos y Próximos Pasos

Gracias por haber llegado hasta aquí y por dedicar tu tiempo a aprender sobre el apasionante mundo de la ciberseguridad. Este glosario es solo el **inicio** de una serie que busca acompañarte en tu formación profesional con lenguaje claro, útil y ejemplos que conectan con la realidad de quienes hablamos español.

¡No te pierdas las próximas partes del glosario!
Exploraremos temas más avanzados, frameworks clave y herramientas prácticas que todo profesional de seguridad debería dominar.

Te invito a seguirme en redes, compartir este recurso con colegas y formar parte de una comunidad de latinos que impulsa el conocimiento y la tecnología con propósito.

> *"Construir tecnología segura es una forma de cuidar a los demás.*
> *Sigamos aprendiendo para proteger lo que importa."*
> — Jeremy José de la Cruz Pérez