Fundamentos de la Ciberseguridad

CIB

ALBERTO MÉNDEZ NÚÑEZ

Contenido

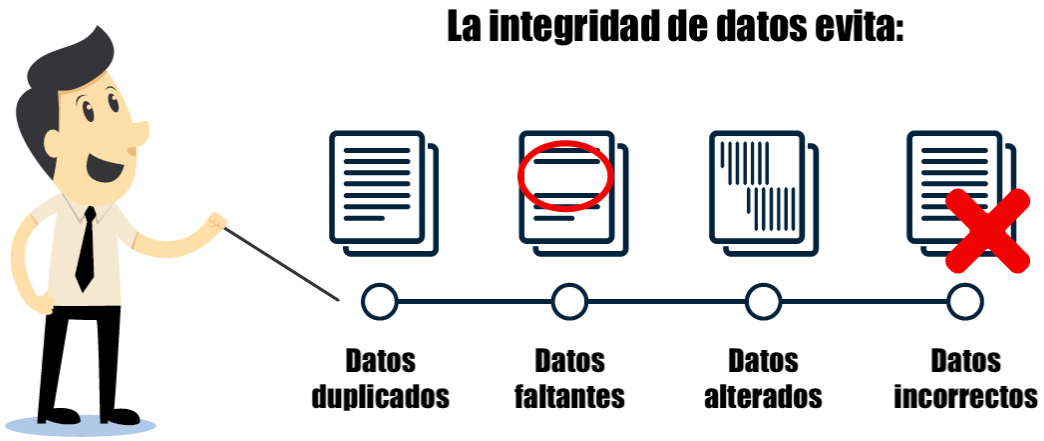
1. Conceptos básicos de seguridad

Amenaza: Una amenaza es cualquier circunstancia, evento, agente o acción potencial que puede causar daño a la información, a los sistemas o a los activos digitales de una organización o persona. Las amenazas pueden ser intencionadas, como un ciberataque realizado por un hacker, o no intencionadas, como errores humanos, fallos técnicos o desastres naturales. El impacto de una amenaza depende de su probabilidad de ocurrencia y del daño que podría causar.

Vulnerabilidad: Una vulnerabilidad es una debilidad, fallo o deficiencia en un sistema, aplicación, red o procedimiento que puede ser explotada por una amenaza para causar un incidente de seguridad. Estas debilidades pueden deberse a errores de configuración, software desactualizado, diseño inseguro o malas prácticas de los usuarios. La gestión de vulnerabilidades implica identificarlas, evaluarlas y corregirlas antes de que sean explotadas.

Confidencialidad: La confidencialidad se refiere a la protección de la información para que solo pueda ser accedida por personas, sistemas o procesos autorizados. Su objetivo es evitar accesos no autorizados, divulgaciones accidentales o robos de datos. Se logra mediante controles como el cifrado, la autenticación, el control de accesos y las políticas de seguridad.

Integridad: La integridad garantiza que la información se mantiene completa, exacta y sin modificaciones no autorizadas durante todo su ciclo de vida. Esto implica asegurar que los datos no sean alterados, eliminados o manipulados de forma indebida, ya sea por errores accidentales o por ataques maliciosos. Técnicas como hashes, firmas digitales y controles de acceso ayudan a preservar la integridad.



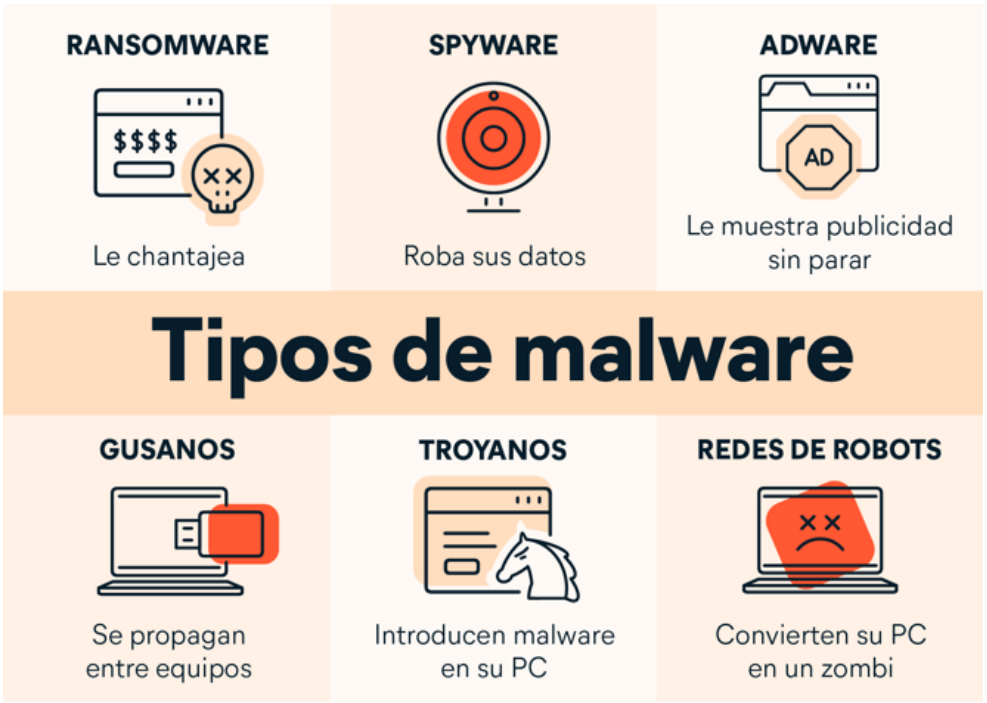
Disponibilidad: La disponibilidad asegura que los sistemas, servicios y la información estén accesibles y operativos cuando los usuarios autorizados los necesiten. Para mantenerla, se implementan medidas como redundancia, copias de seguridad, planes de contingencia y protección contra ataques de denegación de servicio.

Datos sensibles: Los datos sensibles son aquellos que, debido a su naturaleza personal, confidencial o estratégica, requieren un nivel de protección elevado. Incluyen datos personales, financieros, médicos, credenciales de acceso o información empresarial crítica. La exposición de estos datos puede causar graves consecuencias legales, económicas o reputacionales.

Ciclo de vida de la información: El ciclo de vida de la información describe las distintas etapas por las que pasan los datos desde su creación o recopilación hasta su eliminación final. Estas etapas suelen incluir creación, almacenamiento, uso, compartición, archivo y destrucción. En cada fase deben aplicarse medidas de seguridad adecuadas para proteger la información.

2. Tipos de ataques y malware

Malware: El malware es cualquier tipo de software malicioso diseñado para infiltrarse en un sistema sin el consentimiento del usuario con el objetivo de dañar, espiar, robar información o tomar control del sistema. Incluye virus, gusanos, troyanos, spyware y ransomware, entre otros.

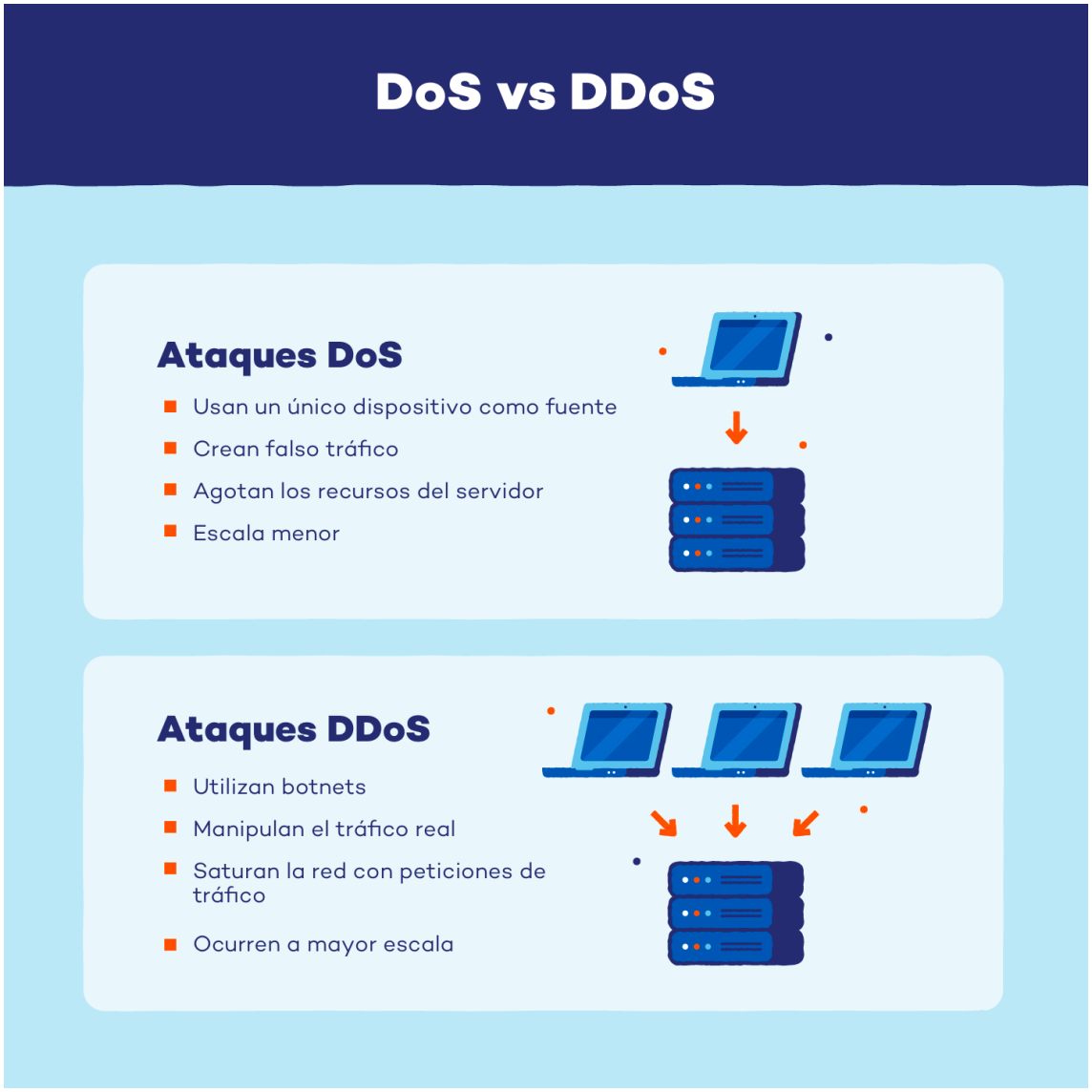


Ransomware: El ransomware es un tipo específico de malware que cifra los archivos o bloquea el acceso a un sistema y exige un rescate económico, normalmente en criptomonedas, para restaurar el acceso. Puede causar grandes pérdidas económicas y operativas, especialmente si no existen copias de seguridad.

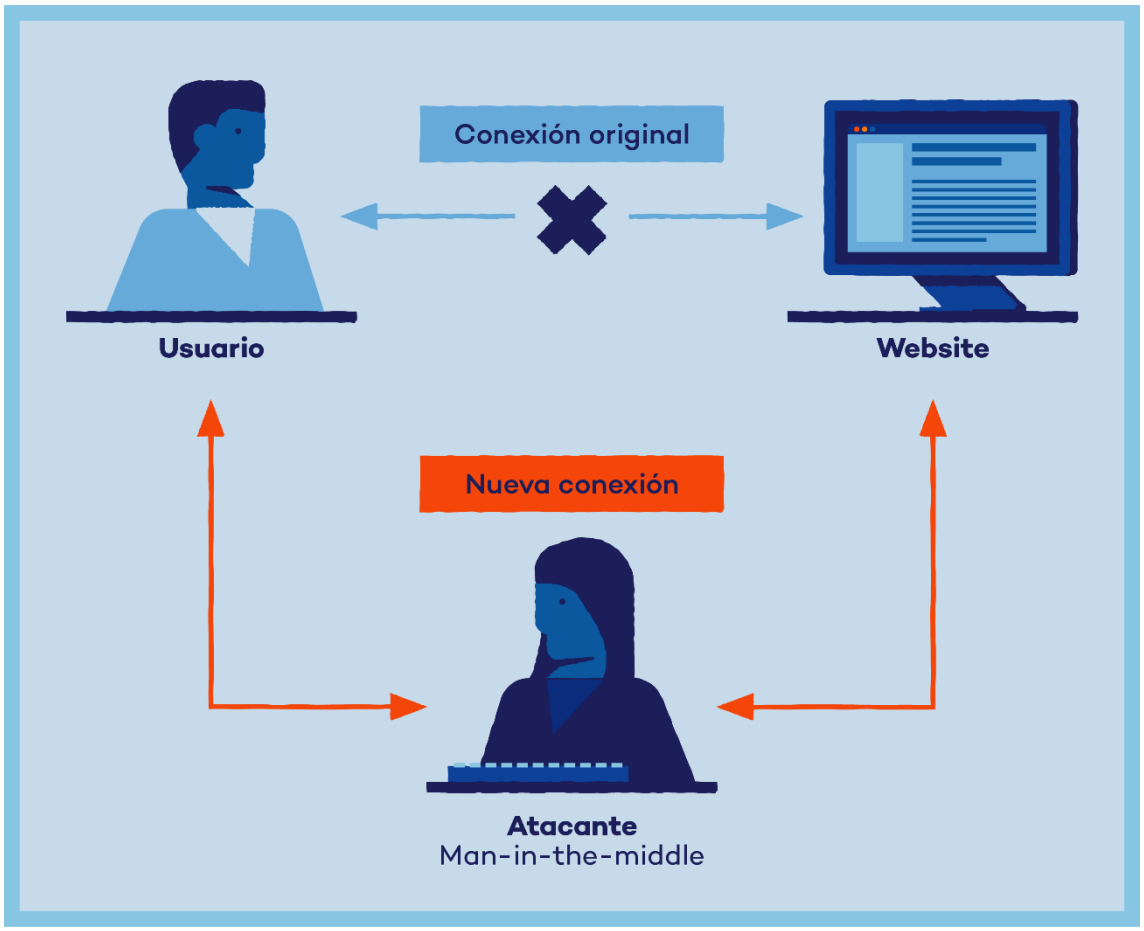
Ingeniería social: La ingeniería social es una técnica de ataque que se basa en la manipulación psicológica de las personas para que revelen información confidencial o realicen acciones que comprometan la seguridad. Aprovecha la confianza, el miedo o la urgencia, y suele manifestarse en forma de phishing, llamadas fraudulentas o suplantación de identidad.

DoS (Denegación de Servicio): Un ataque DoS busca impedir que un sistema, servicio o red esté disponible para los usuarios legítimos, saturándolo con un gran número de solicitudes desde una única fuente. El resultado es la interrupción del servicio o una degradación grave del rendimiento.

DDoS (Denegación de Servicio Distribuida): El ataque DDoS es similar al DoS, pero se realiza de forma distribuida desde múltiples dispositivos, normalmente infectados y controlados remotamente (botnets). Esto lo hace más difícil de detectar y mitigar.



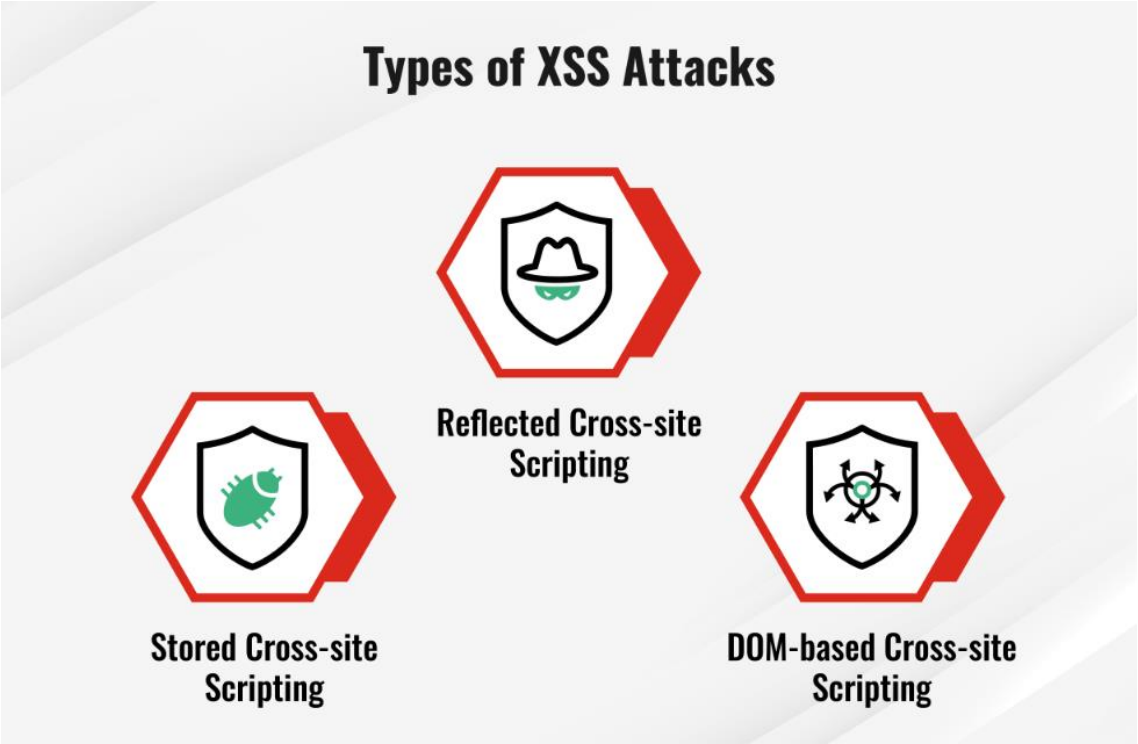
Man-in-the-Middle: Este ataque ocurre cuando un intruso intercepta y, en algunos casos, modifica la comunicación entre dos partes que creen estar comunicándose directamente. El atacante puede robar información sensible como contraseñas o datos financieros sin que las víctimas lo detecten.



Exploit: Un exploit es un código, técnica o método que aprovecha una vulnerabilidad específica en un sistema o aplicación para provocar un comportamiento no deseado, como la ejecución de código malicioso o el acceso no autorizado.

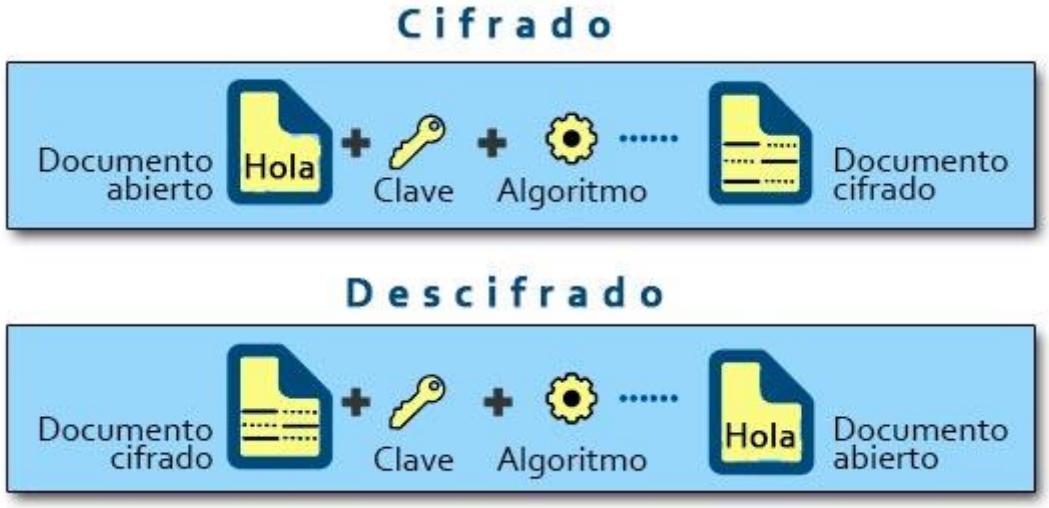
Inyección SQL: La inyección SQL es un ataque que consiste en insertar comandos SQL maliciosos en campos de entrada de una aplicación para acceder, modificar o eliminar información de una base de datos. Suele ocurrir cuando no se validan correctamente las entradas del usuario.

Cross-Site-Scripting (XSS): El XSS es un ataque que inyecta scripts maliciosos en páginas web legítimas que luego son ejecutados en el navegador de otros usuarios. Puede utilizarse para robar sesiones, credenciales o redirigir a sitios maliciosos.

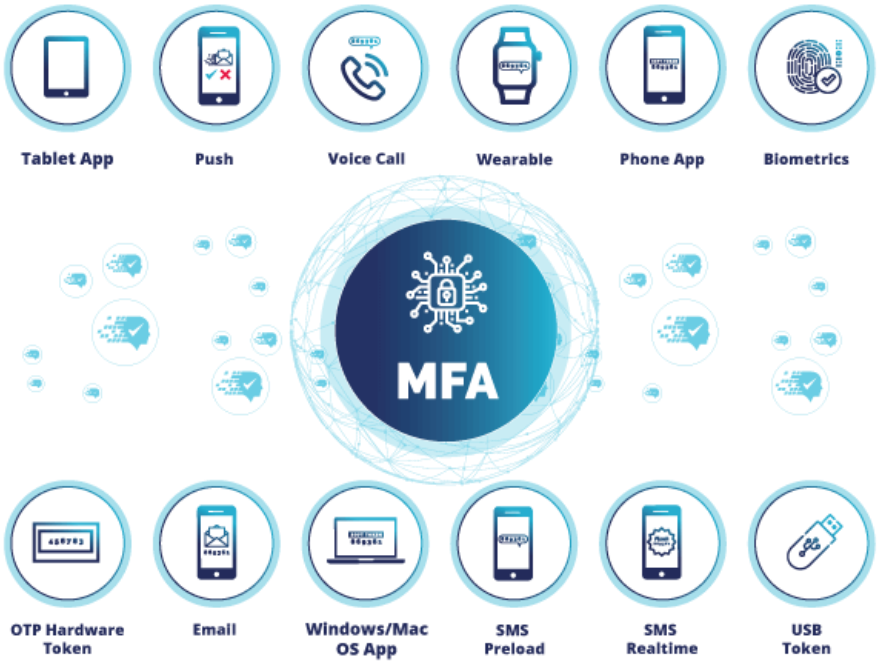


3. Protección de la información y acceso

Cifrar: Cifrar consiste en transformar la información original en un formato ilegible mediante algoritmos criptográficos, de forma que solo pueda ser interpretada por quienes posean la clave adecuada. Es una medida fundamental para proteger datos almacenados o transmitidos.



Autenticación Multifactor (MFA): La autenticación multifactor es un método de verificación que requiere al menos dos factores distintos: algo que el usuario sabe (contraseña), algo que tiene (token, móvil) o algo que es (biometría). Aumenta significativamente la seguridad frente a accesos no autorizados.



Roles: Los roles definen las funciones y responsabilidades asignadas a un usuario dentro de un sistema. Permiten gestionar el acceso de forma estructurada, asignando permisos según el puesto o función del usuario.

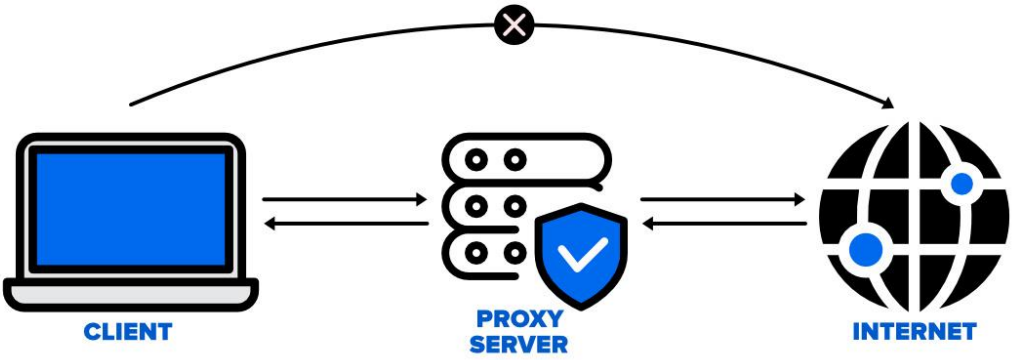
Permisos: Los permisos son las autorizaciones específicas que determinan qué acciones puede realizar un usuario sobre recursos concretos, como leer, modificar o eliminar información. Ayudan a aplicar el principio de mínimo privilegio.

Políticas de acceso: Las políticas de acceso son normas y directrices que regulan quién puede acceder a determinados recursos, bajo qué condiciones y con qué nivel de privilegios, garantizando un uso seguro y controlado de los sistemas.

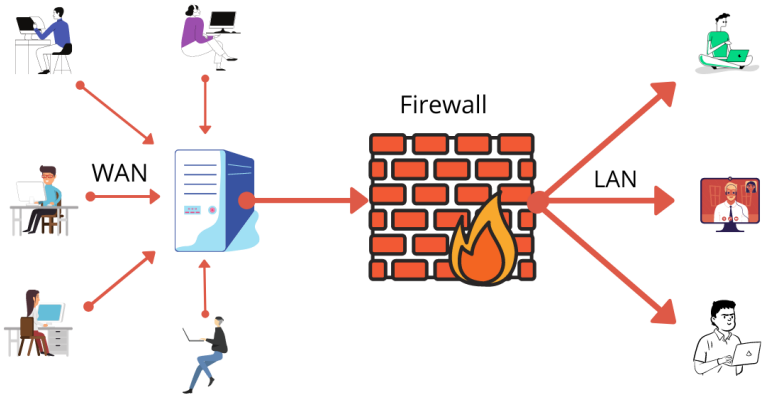
4. Dispositivos y control de red

Router: Un router es un dispositivo de red que conecta diferentes redes entre sí y dirige el tráfico de datos, aplicando reglas básicas de seguridad como filtrado y traducción de direcciones.

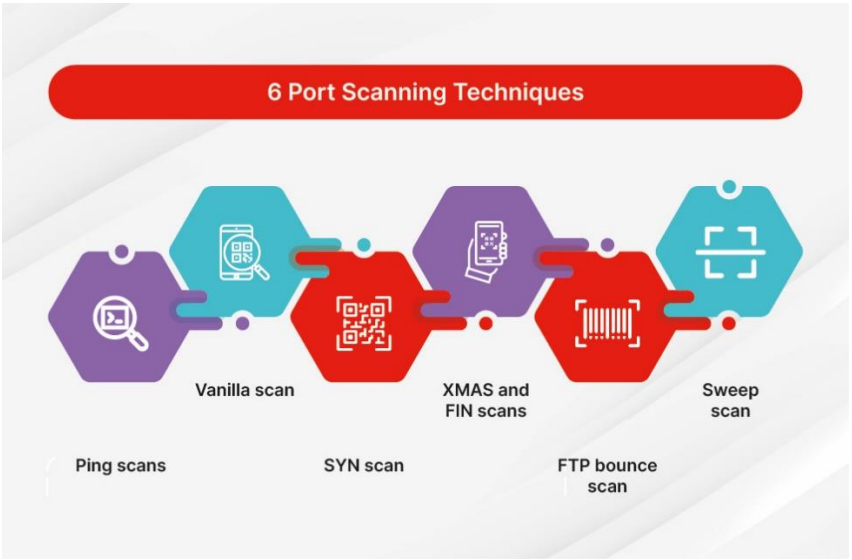
Proxy: Un proxy actúa como intermediario entre el usuario e internet, permitiendo controlar, filtrar y registrar el tráfico, además de mejorar la seguridad y, en algunos casos, el rendimiento.



Regla de firewall: Una regla de firewall es una instrucción que define qué tipo de tráfico está permitido o bloqueado en una red, basándose en criterios como dirección IP, puerto o protocolo.

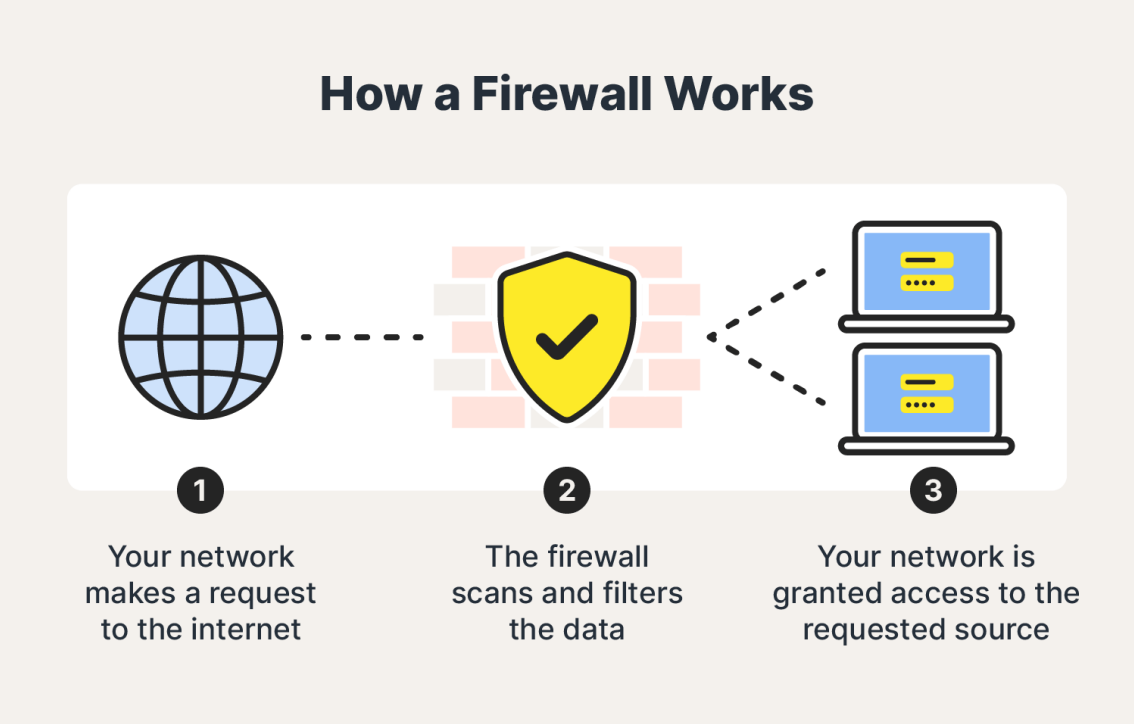


Filtrado de puertos: El filtrado de puertos controla el tráfico de red permitiendo o bloqueando comunicaciones según los puertos utilizados, reduciendo la superficie de ataque.



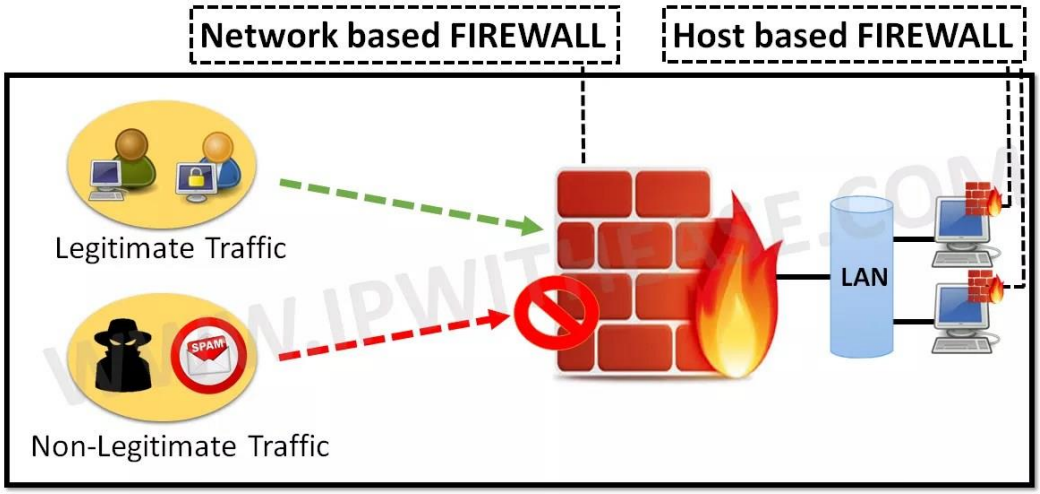
Filtrado de protocolos: El filtrado de protocolos limita el tráfico según el tipo de protocolo de red, permitiendo solo aquellos necesarios para el funcionamiento del sistema.

Cortafuegos: Un cortafuegos es un sistema de seguridad, hardware o software, que monitorea y controla el tráfico de red según reglas predefinidas, actuando como barrera entre redes seguras y no seguras.



Cortafuegos basado en red: Un cortafuegos basado en red es un sistema de seguridad, generalmente implementado como un dispositivo dedicado o como un servicio integrado en infraestructuras de red, cuya función principal es proteger a múltiples equipos y sistemas dentro de una red.

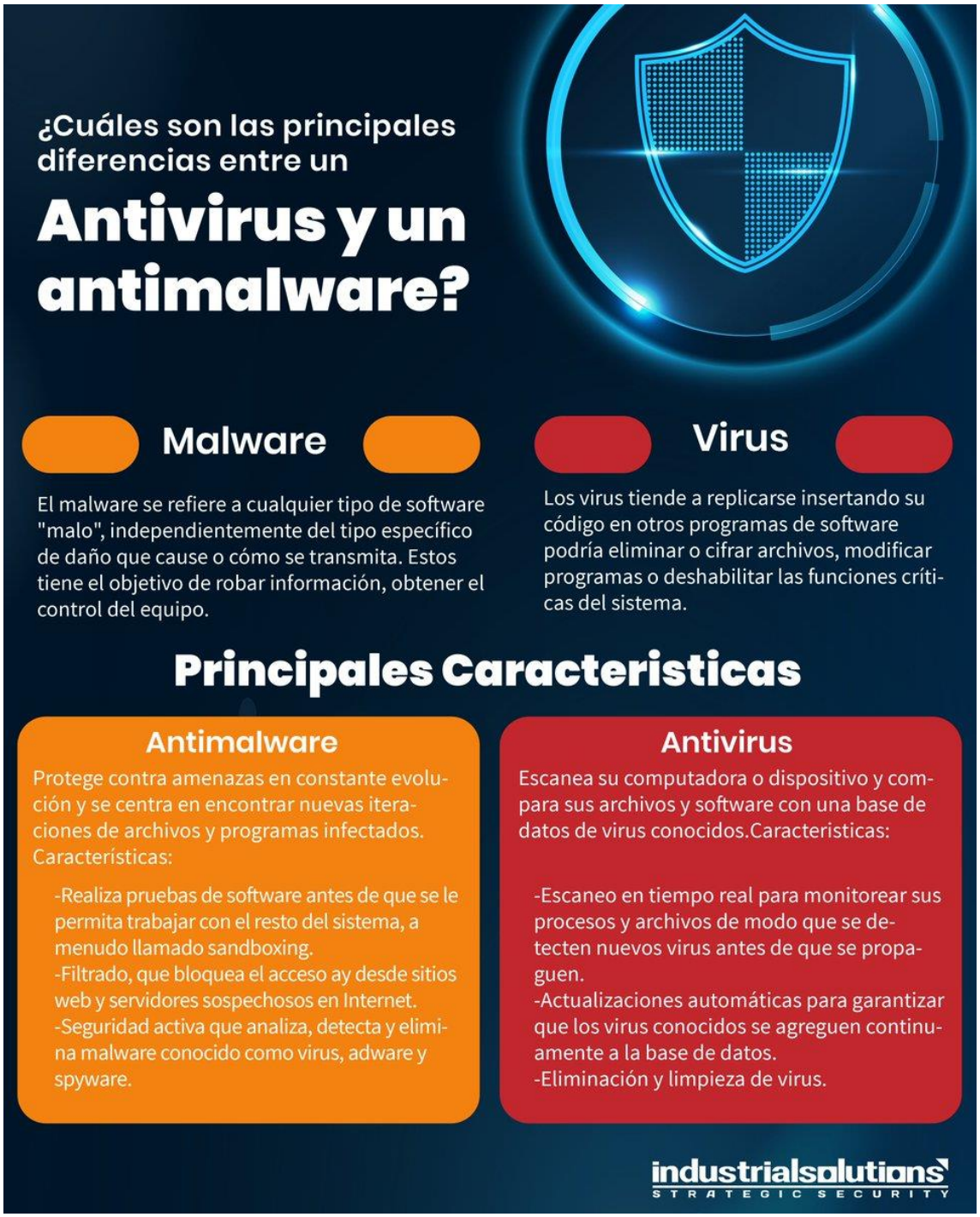
Cortafuegos basado en host: Un cortafuegos basado en host es un sistema de seguridad que se instala y ejecuta directamente en un dispositivo individual, como un ordenador personal, un servidor o un equipo portátil. Su función principal es proteger ese sistema concreto controlando el tráfico de red que entra y sale del dispositivo, evitando accesos no autorizados y posibles ataques externos o internos.



5. Sistemas de seguridad y software

Antivirus: Un antivirus es un software de seguridad diseñado para proteger sistemas informáticos y dispositivos frente a virus y otros tipos de software malicioso. Su función principal es detectar, prevenir y eliminar amenazas que puedan dañar el sistema, comprometer la información o afectar al funcionamiento normal del equipo.

Antimalware: Un antimalware es un software de seguridad diseñado para detectar, prevenir y eliminar una amplia variedad de amenazas informáticas, englobando no solo virus tradicionales, sino también otros tipos de malware como troyanos, spyware, ransomware, gusanos, rootkits y software potencialmente no deseado. Su objetivo principal es proteger los sistemas y la información frente a ataques que puedan comprometer la seguridad y la privacidad.



IDS: Un IDS es un sistema de seguridad que se encarga de monitorear de manera continua la red y los sistemas para identificar actividades sospechosas, accesos no autorizados o ataques informáticos. Utiliza técnicas basadas en firmas de amenazas conocidas o en el análisis de anomalías respecto al comportamiento habitual del sistema. Su propósito principal es detectar intrusiones a tiempo, generar alertas y registrar evidencia de los eventos para que los equipos de seguridad puedan responder adecuadamente, contribuyendo a la protección de la confidencialidad, integridad y disponibilidad de la información.

IPS: Un IPS es un sistema de seguridad que, además de detectar actividades maliciosas en la red o sistemas, tiene la capacidad de bloquearlas automáticamente en tiempo real, previniendo que los ataques lleguen a comprometer los recursos de la organización. Opera interceptando tráfico sospechoso, eliminando amenazas y reforzando políticas de acceso, lo que permite reducir riesgos, minimizar impactos y mantener la continuidad operativa frente a incidentes de seguridad.

Herramientas de monitoreo: Las herramientas de monitoreo son sistemas o software que supervisan de manera continua redes, servidores, aplicaciones y dispositivos, con el fin de detectar problemas de rendimiento, fallos, caídas o actividades sospechosas. Estas herramientas permiten anticiparse a posibles incidentes, alertar sobre anomalías y garantizar la disponibilidad y estabilidad de los sistemas, contribuyendo a una gestión proactiva de la seguridad informática.

Herramientas de auditoría: Las herramientas de auditoría son sistemas diseñados para revisar, evaluar y documentar la seguridad, configuraciones y cumplimiento de políticas de los sistemas de información. Su objetivo principal es identificar vulnerabilidades, debilidades o incumplimientos normativos, ofreciendo información detallada que permite a las organizaciones implementar mejoras en sus controles de seguridad y cumplir con estándares y regulaciones aplicables.

Comparación de herramientas para auditoría de ciberseguridad

The following slide showcases key points including software, description, features, ease of use, and pricing for a tool comparison in cybersecurity audits. This aids in evaluating and selecting the most suitable tools for effective security assessments.

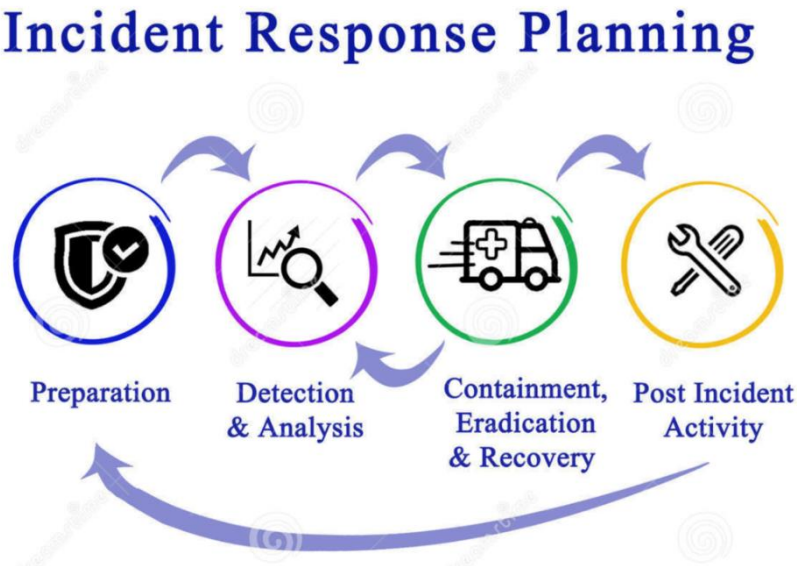
Tool/Software	Description	Key Features	Ease of Use	Pricing
SolarWinds Network Configuration Manager	Configuration management with vulnerability scanning	○ Network security audit	User-friendly	30-day free trial
Intruder	Cloud-based vulnerability scanner	○ Monthly scans ○ On-demand scanning ○ Pen-testing services	User-friendly	Free trial available
ManageEngine Vulnerability Manager Plus	System security checks	○ Network security sweeps for vulnerabilities	User-friendly	Free trial available
Atera	SaaS platform for managed service providers	○ Remote monitor and management systems	User-friendly	Free trial available
ManageEngine Log360	SIEM package for log collection and compliance auditing	○ Collects logs from network endpoints and cloud platforms	User-friendly	Free trial available
Add text here	Add text here	Add text here	Add text here	Add text here

This slide is 100% editable. Adapt it to your needs and capture your audience's attention. 4

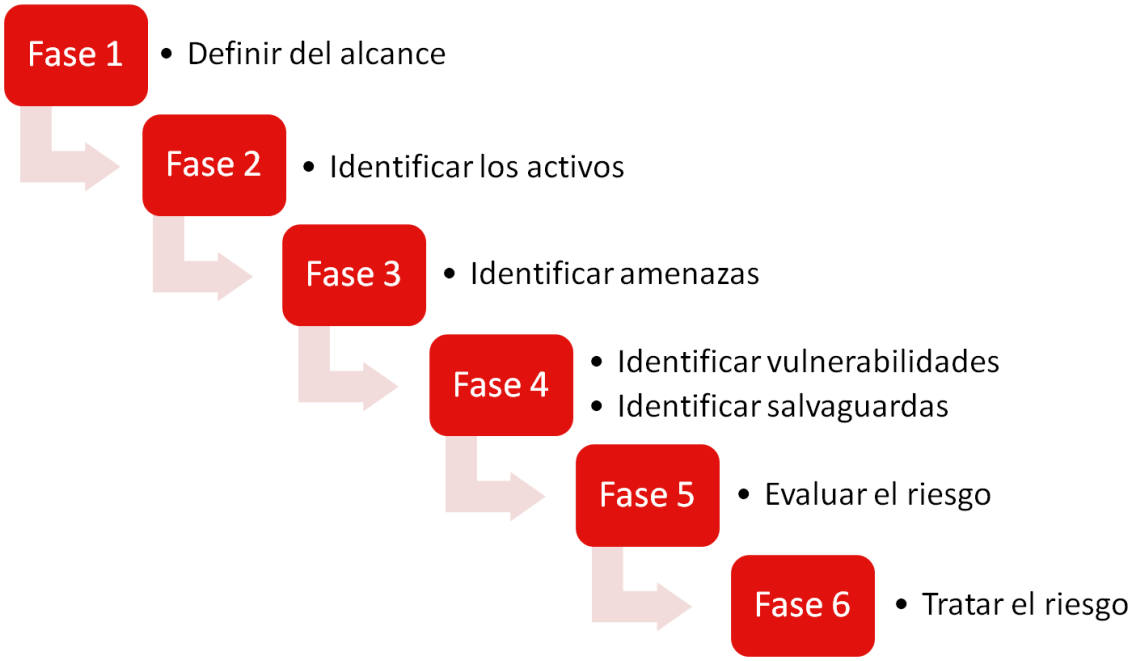
6. Gestión de incidentes y respuesta

Incidentes de seguridad: Un incidente de seguridad es cualquier evento o serie de eventos que comprometen la confidencialidad, integridad o disponibilidad de la información o los sistemas de una organización. Incluye ataques de malware, accesos no autorizados, fugas de información y otros eventos que puedan afectar la operación normal. La gestión adecuada de los incidentes permite minimizar daños, proteger los activos de información y garantizar la continuidad de los servicios.

Detección: La detección es el proceso mediante el cual se identifican actividades sospechosas o incidentes de seguridad dentro de una red o sistema. Involucra la recopilación de registros, el análisis de alertas de sistemas como IDS/IPS y la supervisión del comportamiento de los usuarios y sistemas, con el objetivo de reconocer amenazas a tiempo y activar las medidas de respuesta necesarias.



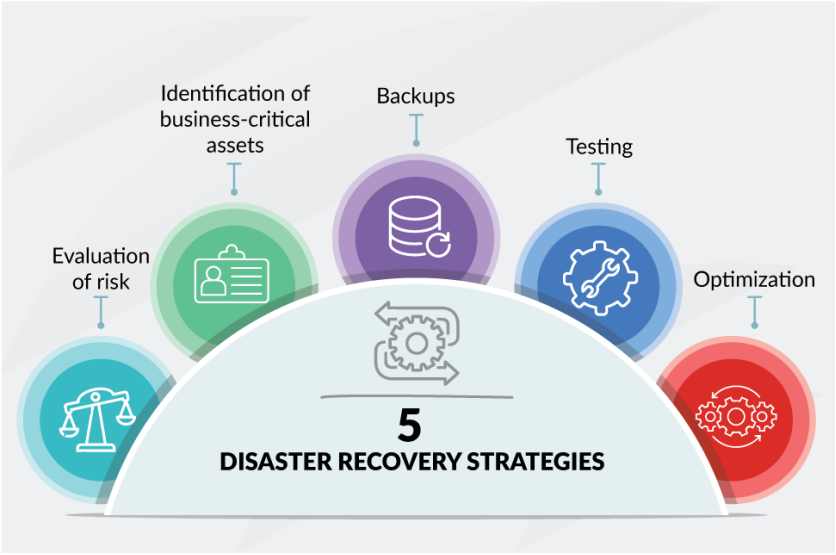
Análisis: El análisis de seguridad consiste en investigar un incidente detectado para determinar su causa, alcance, sistemas afectados y el impacto que puede generar sobre la organización. Esta etapa permite priorizar la respuesta, definir medidas de contención adecuadas y planificar acciones de erradicación y recuperación, contribuyendo a una gestión efectiva de incidentes.



Contención: La contención es el conjunto de acciones orientadas a limitar la propagación o el impacto de un incidente de seguridad mientras se desarrollan medidas de respuesta más profundas. Esto puede incluir aislar equipos comprometidos, bloquear accesos no autorizados o suspender servicios afectados, con el objetivo de proteger los sistemas y la información crítica.

Erradicación: La erradicación es el proceso de eliminar completamente la causa raíz de un incidente de seguridad, asegurando que no queden amenazas residuales en los sistemas. Esto incluye la eliminación de malware, corrección de vulnerabilidades, cierre de accesos no autorizados y restauración de configuraciones seguras, garantizando que el incidente no se repita.

Recuperación: La recuperación es la fase en la que los sistemas afectados por un incidente de seguridad son restaurados a su estado normal de funcionamiento, asegurando que los datos, aplicaciones y servicios operen de manera segura y confiable. Esto puede implicar restauración desde copias de seguridad, reinstalación de sistemas y pruebas de funcionamiento, buscando retomar la operativa habitual con mínima interrupción.

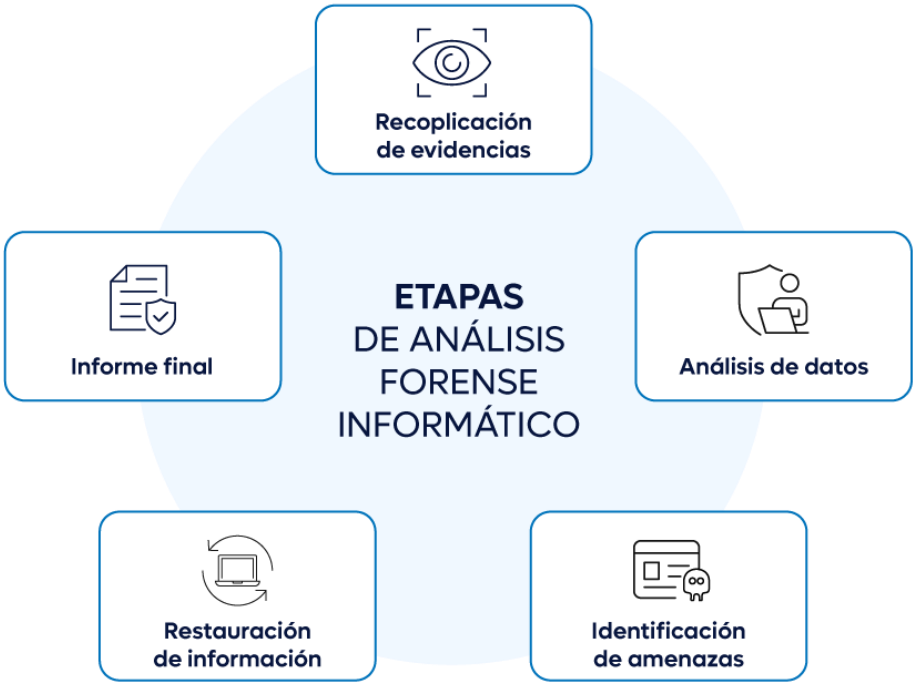


Aprendizaje: El aprendizaje posterior a un incidente de seguridad consiste en la revisión detallada de los eventos y de la respuesta implementada, con el objetivo de identificar mejoras en procesos, políticas, herramientas y capacitación del personal. Esta fase permite fortalecer la postura de seguridad de la organización y reducir la probabilidad de futuros incidentes.

Indicadores de compromiso: Los indicadores de compromiso son evidencias o señales que sugieren que un sistema ha sido comprometido o atacado, incluyendo archivos sospechosos, conexiones a direcciones maliciosas, cambios anómalos en configuraciones o registros de actividad inusual. Su identificación permite a los equipos de seguridad detectar ataques tempranos y tomar medidas correctivas de manera oportuna.

Estrategias proactivas: Las estrategias proactivas en ciberseguridad son medidas preventivas implementadas para reducir la probabilidad de incidentes, incluyendo parches de seguridad, segmentación de redes, configuraciones robustas, formación del personal y análisis de riesgos. Su objetivo es anticiparse a las amenazas y minimizar vulnerabilidades antes de que se materialicen en ataques efectivos.

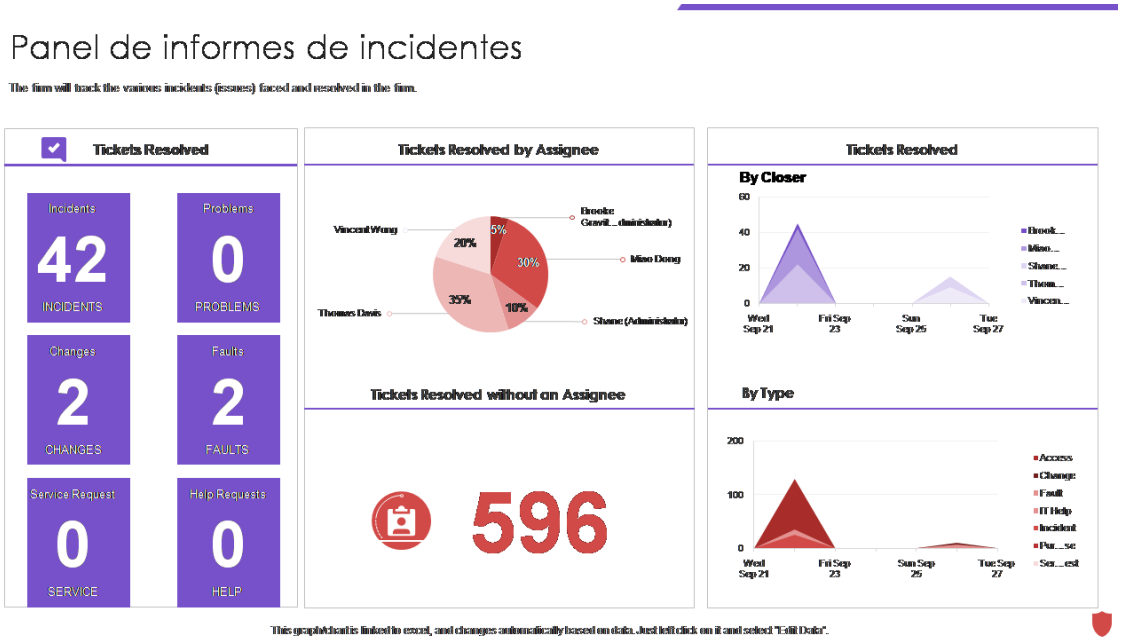
Análisis forense: El análisis forense en ciberseguridad es una investigación exhaustiva de incidentes para determinar cómo ocurrieron, quién los causó y qué sistemas o datos fueron afectados. Implica la revisión de registros, discos duros, memoria y comunicaciones, proporcionando evidencia que puede ser utilizada tanto para mejorar la seguridad como en procedimientos legales o judiciales.



Diagnóstico de fallos: El diagnóstico de fallos es el proceso de identificación, análisis y localización de problemas o errores en sistemas, redes o aplicaciones. Su objetivo es comprender la causa raíz de los fallos, proponer soluciones efectivas y prevenir que se repitan, asegurando la continuidad y seguridad de los servicios tecnológicos.

Propuesta de mejora: Una propuesta de mejora es un conjunto de sugerencias o un plan estratégico para optimizar procesos, sistemas o controles de seguridad, basado en auditorías, diagnósticos o incidentes previos. Busca fortalecer la postura de seguridad, incrementar la eficiencia operativa y reducir riesgos frente a posibles amenazas.

Registro de incidencias: El registro de incidencias es un documento o sistema en el que se documentan de manera detallada todos los incidentes de seguridad ocurridos, incluyendo fechas, responsables, descripción de los eventos, acciones tomadas y resultados. Este registro permite análisis históricos, seguimiento de patrones y cumplimiento de normativas de seguridad.



7. Normativas y cumplimiento

RGPD: El RGPD es la normativa europea que regula la protección de los datos personales de los ciudadanos de la Unión Europea, obligando a las organizaciones a implementar medidas de seguridad, obtener consentimiento para el tratamiento de información y notificar brechas de seguridad. Su objetivo es proteger la privacidad de los usuarios y garantizar el cumplimiento legal en la gestión de datos.

ENS: El ENS es un marco normativo español que establece medidas de seguridad obligatorias para los sistemas de información del sector público, definiendo niveles de seguridad, controles técnicos y procedimientos de gestión de riesgos. Su finalidad es garantizar la confidencialidad, integridad y disponibilidad de la información en las administraciones públicas.

Fuente: Portal de la Administración Electrónica del Gobierno de España