Fundamentos de ciberseguridad

--

Glosario de Términos

Gonzalo Junquera Lorenzo

13 de noviembre de 2025

ÍNDICE

1. Amenazas y vulnerabilidades.

Amenazas

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Vulnerabilidades

Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit (fragmento de código, software o técnica que aprovecha una vulnerabilidad en un sistema, aplicación o dispositivo para lograr un objetivo no autorizado). Cuando se descubre, el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Confidencialidad

Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

Disponibilidad

Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

Malware

Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.

Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

https://www.microsoft.com/es-es/security/business/security-101/what-is-malware

Ingeniería social

Proceso mediante el cual se obtiene la información o el diseño de un producto con el propósito de determinar el proceso de fabricación o creación de sus componentes y de qué manera interactúan entre sí hasta lograr el producto final. Aplicado al software, la ingeniería inversa es la actividad que se ocupa de descubrir cómo funciona un programa, función o característica, de cuyo código fuente no se dispone, hasta generar código propio que cumpla las mismas funciones.

https://www.incibe.es/aprendeciberseguridad/ingenieria-social

Ataques a la red (DoS y DDoS)

Un **ataque de denegación de servicio (DoS)** es un tipo de ciberataque en el que un actor malicioso tiene como objetivo que una máquina u otro dispositivo no esté disponible para los usuarios a los que va dirigido, interrumpiendo el funcionamiento normal del mismo. Los ataques DoS suelen funcionar al sobrecargar o inundar una máquina objetivo con solicitudes hasta que el tráfico normal es incapaz de ser procesado, lo que provoca una denegación de servicio a los usuarios de la adición. Un ataque DoS se caracteriza por utilizar una única máquina para lanzar el ataque.

https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

Un **ataque de denegación de servicio distribuido (DDoS)** es un intento malintencionado de interrumpir el tráfico normal de un servidor, servicio o red determinada, sobrecargando el objetivo o su infraestructura asociada con una avalancha de tráfico de Internet.

La efectividad de los ataques DDoS reside en el uso de sistemas informáticos vulnerables desde los que se origina el ataque de tráfico. Entre los equipos afectados puede haber ordenadores y otros recursos de red, tales como dispositivos IoT.

https://www.cloudflare.com/es-es/learning/ddos/what-is-a-ddos-attack/

Man-in-the-Middle (MitM)

Se produce cuando una comunicación es espiada entre el emisor y el receptor del mensaje. En algunos casos la información se modifica mediante la inyección de paquetes con algún fin malicioso.

https://www.kaspersky.es/blog/que-es-un-ataque-man-in-the-middle/648/

Exploits

Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de exploit se suele perseguir:

- el acceso a un sistema de forma ilegítima
- obtención de permisos de administración en un sistema ya accedido
- un ataque de denegación de servicio a un sistema

https://www.redeszone.net/tutoriales/seguridad/tipos-exploit-amenaza-seguridad/

Inyección SQL

Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.

https://www.deltaprotect.com/blog/inyeccion-sql

Cross-Site Scripting (XSS)

Se trata de una vulnerabilidad existente en algunas páginas web generadas dinámicamente (en función de los datos de entrada). XSS viene del acrónimo en inglés de **Secuencias de comandos en sitios cruzados** (Cross-site Scripting).

Dado que los sitios web dinámicos dependen de la interacción del usuario, es posible insertar en un formulario un pequeño programa malicioso, ocultándolo entre solicitudes legítimas y hacer que éste se ejecute. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios alojados en una página web.

Una vez realizado el ataque XSS, el atacante puede cambiar la configuración del servidor, secuestrar cuentas, escuchar comunicaciones (incluso cifradas), instalar publicidad en el sitio víctima y en general cualquier acción que desee de forma inadvertida para el administrador.

https://www.arsys.es/blog/ataques-xss-que-son-y-como-evitarlos

Redes inalámbricas sin cifrar o con cifrados obsoletos

Se refiere a redes Wi-Fi que o bien no utilizan ningún tipo de cifrado (redes abiertas), dejando las comunicaciones totalmente expuestas, o utilizan protocolos de cifrado antiguos e inseguros (como WEP o versiones obsoletas de WPA), que pueden ser vulnerados o descifrados fácilmente por un atacante.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-en-redes-wifi.pdf

Ransomware

Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.

Acciones que NO debe realizar

No pague el rescate: Pagar no garantiza la recuperación de sus archivos y solo financia a los criminales para que sigan atacando a otros.

No haga clic en archivos adjuntos de correos electrónicos sospechosos: Este es un método común de infección. No abra archivos adjuntos, incluso si parecen ser de notificaciones de envío o protectores de pantalla atractivos, si no está seguro de la fuente.

Acciones que SÍ debe realizar

Mantenga el software actualizado: Las actualizaciones (parches) eliminan vulnerabilidades que los criminales aprovechan. Instale las actualizaciones tan pronto como estén disponibles.

Use software de seguridad: Instale y mantenga un software de seguridad (como un buen antivirus o una solución de protección más completa) para defender su equipo de las amenazas.

Haga una copia de seguridad (Backup): Esta es su mejor defensa. Tenga copias de todos sus archivos importantes guardadas en una ubicación segura (como un disco externo o la nube) para poder recuperar su información sin tener que pagar a los atacantes.

https://co.norton.com/blog/malware/ransomware-5-dos-and-donts

2. Medidas de protección básicas

Autenticación Multifactor (MFA)

Un método de autenticación de identidad que requiere que el usuario presente dos o más factores de verificación independientes para obtener acceso a un sistema o recurso. Estos factores suelen ser algo que el usuario sabe (contraseña), algo que el usuario posee (móvil, token) y/o algo que el usuario es (huella dactilar, biometría).

https://www.incibe.es/ciudadania/tematicas/contrasenas-seguras/autenticacion-de-dos-factores

Roles y permisos

- **Roles**: Conjunto de privilegios y responsabilidades predefinidos que se asignan a un usuario o grupo de usuarios dentro de un sistema (ejemplo: "Administrador", "Usuario Estándar", "Invitado").

- **Permisos**: Las capacidades específicas que un usuario, a través de su rol, tiene para interactuar con un recurso (ejemplo: leer, escribir, ejecutar, eliminar un archivo o registro).

https://blog.scalefusion.com/es/what-is-user-management/

Reglas de firewall

Directrices o políticas preconfiguradas que especifican qué tráfico de red se permite (aceptar) y qué tráfico se rechaza (denegar) en función de diversos criterios. Son esenciales para filtrar y controlar el flujo de datos entre redes (o dentro de ellas).

https://www.pandasecurity.com/es/features/firewall/

Filtro de puertos y protocolos

Una función de las firewalls que inspecciona el tráfico de red:

Puertos: Se utiliza para permitir o denegar la comunicación basándose en el número de puerto de red (ejemplo: puerto 80 para HTTP, 443 para HTTPS).

Protocolos: Se utiliza para permitir o denegar basándose en el protocolo de comunicación utilizado (ejemplo: TCP, UDP, ICMP).

https://www.incibe.es/ciudadania/blog/puertos-router-que-son-como-afectan-nuestra-seguridad

Routers

Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es).

En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS.

El router comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación.

https://www.incibe.es/node/506664

Monitoreo y auditoría

- **Monitoreo:** Proceso continuo de vigilancia de un sistema, una red o una aplicación para recopilar, analizar y evaluar datos de actividad en tiempo real. Su objetivo es detectar incidentes de seguridad, anomalías o cambios operativos.

- **Auditoría**: Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

https://secureframe.com/es-es/blog/cybersecurity-audit

3. Análisis de los incidentes de seguridad

Ciclo de vida de un incidente

La respuesta ante incidentes es el proceso mediante el cual una organización reacciona ante amenazas de TI, como es el caso de los ciberataques, las vulneraciones de seguridad y el tiempo de inactividad de los servidores.

El ciclo de vida de la respuesta ante incidentes es el marco de trabajo pormenorizado de tu organización para identificar y reaccionar ante una interrupción del servicio o ante una amenaza de seguridad.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_gestion_ciberincidentes_sector_privado.pdf

https://www.piranirisk.com/es/blog/guia-para-la-gestion-de-incidentes-de-seguridad

Detección

Sistema que analiza determinados parámetros y elementos que sirven para monitorizar, detectar y verificar indicios de posibles incidentes de seguridad, que pueden registrarse en el sistema objeto de estudio y evaluación.

https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad
https://www.cisco.com/c/es_mx/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html

Análisis

La etapa donde se examinan los datos recopilados (registros, tráfico, logs) para comprender la naturaleza, el alcance y la causa raíz del incidente, donde se detecta el incidente, se determina el alcance y se conforma una solución. Esta fase engloba a los responsables del negocio, operaciones y comunicación (contactos con soportes técnicos, CERT, peritos forenses, policía o asesores legales si fueran necesarios, etc.).

https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

Contención

La acción de tomar medidas inmediatas para detener la propagación del incidente y limitar el daño, aislando los sistemas afectados sin apagarlos necesariamente (ejemplo: desconectar un servidor de la red) impidiendo que el incidente se extienda a otros recursos. Como consecuencia, se minimizará su impacto (separando equipos de la red afectada, deshabilitando cuentas comprometidas, cambiando contraseñas, etc.).

https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

Erradicación

La fase en la que se eliminan completamente la causa raíz del incidente, los elementos maliciosos (como el malware) y las vulnerabilidades que fueron explotadas por el atacante.

Mitigación: donde se procede a la eliminación de los elementos comprometidos, en caso de ser necesario y posible, y reinstalación de sistemas afectados o backups. En cualquier caso, Las medidas de mitigación dependerán del tipo de incidente.

https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

Recuperación

El proceso de restaurar los sistemas y servicios afectados a su estado normal de funcionamiento, asegurando que estén limpios, parcheados y listos para volver a la producción.

https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

Aprendizaje

La etapa final, y crucial, donde se documenta todo el proceso, se realiza una revisión post-incidente y se identifican las lecciones aprendidas para mejorar las políticas, procedimientos y defensas de seguridad futuras.

Recapitulación: donde se documentan los detalles del incidente. Para ello, se archivarán los datos recogidos y se debatirán las lecciones aprendidas. Se informará a los empleados y se les enseñarán las recomendaciones dirigidas a prevenir situaciones de riesgo futuras.

https://www.incibe.es/empresas/tematicas/gestion-incidentes-seguridad

Indicadores de compromiso (IoC)

Los indicadores de compromiso o Indicators of Compromise (IOCs) hacen referencia a una tecnología estandarizada que consiste en definir las características técnicas de una amenaza por medio de las evidencias existentes en un equipo comprometido; es decir, se identifican diferentes acciones como ficheros creados, entradas de registro modificadas, procesos o servicios nuevos, etc.; de manera que puedan servir para identificar otros ordenadores afectados por la misma amenaza o prevenirlos de la misma.

https://support.kaspersky.com/KEDR_Optimum/2.0/es-ES/220373.htm

Estrategias proactivas

Una estrategia de ciberseguridad proactiva **se basa en la prevención, monitorización constante y capacidad de reacción frente a ciberataques.** Para llevar a cabo este tipo de estrategia es imprescindible la adopción de herramientas específicas que ayuden a la prevención de ciberataques 24/7 y de manera gestionada.

https://www.esedsl.com/blog/ciberseguridad-proactiva-vs-reactiva

Análisis forense

Seguridad pasiva que sirve para **analizar** que ha ocurrido ante un ataque o un accidente sufrido en un servidor. Es importante para saber **qué ha ocurrido** y **cómo evitar que vuelva a pasar**.

Peritaje (otra forma de llamar a análisis forense), archivos log (lo que apunta el servidor) (apache de inicio de sesión y de uso los más importantes), trazabilidad (es lo que escribe la aplicación web).

https://onretrieval.com/que-es-el-analisis-forense-informatico/

4. Herramientas y tecnologías de aplicación.

Router

Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es).

https://www.incibe.es/sites/default/files/docs/guia_router/osi-guia-tu-router-tu-castillo.pdf

Cortafuegos (Firewall)

Sistema de seguridad compuesto o bien de programas (software) o de dispositivos hardware situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación.

Estos sistemas suelen poseer características de privacidad y autentificación.

https://www.pandasecurity.com/es/mediacenter/que-es-un-firewall/

Cortafuegos basados en red

Un cortafuegos de red se sitúa en el punto de unión entre las redes de confianza y las que no lo son, como los sistemas internos e internet. Su principal función es supervisar, controlar y determinar la validez del tráfico entrante y saliente a partir de un conjunto de reglas predefinido, diseñado para evitar el acceso no autorizado y preservar la integridad de la red.

https://www.paloaltonetworks.es/cyberpedia/types-of-firewalls

Cortafuegos basados en host

Un cortafuegos basado en el host es un software que funciona en un solo dispositivo dentro de una red. Se instala directamente en ordenadores o dispositivos concretos para protegerlos de posibles amenazas mediante una capa de seguridad específica. Examinando el tráfico entrante y saliente del dispositivo en cuestión, filtra con eficacia el contenido dañino para evitar que accedan al sistema elementos maliciosos como malware o virus.

https://www.paloaltonetworks.es/cyberpedia/types-of-firewalls

Proxy

El proxy es tanto el equipo, como el software encargado de dar el servicio, que hacen de intermediario en las peticiones de los equipos de la redes LAN hacia Internet.

Su cometido es de centralizar el tráfico entre Internet y una red privada, de forma que se evita que cada una de las máquinas de la red privada tenga que disponer necesariamente de una conexión directa a Internet y una dirección IP pública.

Al mismo tiempo un proxy puede proporcionar algunos mecanismos de seguridad (firewall o cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

IDS (Sistema de Detección de Intrusos)

Un sistema de detección de intrusiones (IDS) es una herramienta de seguridad de red que monitoriza el tráfico y los dispositivos de la red en busca de actividades maliciosas conocidas, actividades sospechosas o infracciones de las políticas de seguridad.

https://www.ibm.com/es-es/think/topics/intrusion-detection-system

IPS (Sistema de Prevención de Intrusos)

Un sistema de prevención de intrusiones (IPS), también conocido como sistema de prevención de detección de intrusiones (IDPS), es una tecnología que vigila una red para detectar cualquier actividad maliciosa que intente aprovechar la vulnerabilidad conocida.

La función principal de un sistema de prevención de intrusiones es identificar cualquier actividad sospechosa y detectar y permitir (IDS) o prevenir (IPS) la amenaza. El intento se registra y se informa a los administradores de red.

https://www.checkpoint.com/es/cyber-hub/network-security/what-is-ips/

Control de acceso

Sistema de verificación que permite o deniega el acceso a un recurso tecnológico según los derechos concedidos a cada usuario dependiendo de la clase o grupo a la que esté adscrito. Se pueden establecer roles, por ejemplo, por áreas de la empresa (ventas, operaciones…) o por la posición jerárquica dentro de la estructura; cada rol con los permisos necesarios para realizar su trabajo. Al dar de alta a un usuario en el sistema, el admistrador le asignará un rol dependiendo de las tareas que deba realizar y que tendrá asociados los permisos de acceso necesarios.

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Software Antivirus

El antivirus es un software de ciberseguridad que detecta y elimina el software malicioso (malware) de un ordenador, dispositivo o red. Si la red tiene usuarios finales, el software antivirus es fundamental para prevenir las filtraciones de datos. Siga leyendo para saber más sobre el funcionamiento de los antivirus, los riesgos del malware y el ransomware, etc.

https://www.sophos.com/es-es/cybersecurity-explained/antivirus

Antimalware

El malware es un término general que se refiere a software malicioso diseñado para dañar, alterar, robar información o tomar el control de un sistema informático sin el consentimiento del usuario. El término "malware" es una abreviatura de "software malicioso".

Hay muchos tipos diferentes de malware, incluyendo virus, gusanos, troyanos, spyware, adware y ransomware. Cada tipo de malware tiene su propia forma de operar y objetivo, pero todos están diseñados para causar daño o interrupción en un sistema informático.

El virus

Un virus informático es un tipo de malware que se propaga a través de la inserción de su código en archivos o programas legítimos en un sistema informático, con el fin de dañar o alterar el funcionamiento del sistema.

Los virus informáticos tienen la capacidad de replicarse y propagarse a través de la descarga y ejecución de programas infectados, la apertura de archivos adjuntos de correo electrónico infectados, y la descarga de software malicioso a través de sitios web no seguros.

Una vez que un virus infecta un sistema, puede realizar diversas acciones maliciosas, como eliminar archivos, alterar el funcionamiento del sistema, robar información personal o confidencial, o incluso dañar hardware. Los virus pueden también enviar correos electrónicos no deseados o mensajes a otros usuarios en la red, propagando así el virus.

Diferencia entre antivirus y antimalware

5. Normativa y buenas prácticas de uso.

Reglamento General de Protección de Datos (RGPD)

Acrónimo de Reglamento General de Protección de Datos, regulación de la Unión Europea introducida en 2016 orientada a la protección de los datos personales de las personas físicas por parte de organizaciones e instituciones que operan en la Unión Europea, así como de los procesos que estas realizan de dicha información personal (procesamiento, almacenamiento o destrucción) y las consecuencias y multas en caso de sufrir una filtración o pérdida de información personal por parte de las organizaciones.

https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf

ISO/IEC 27 001

La ISO/IEC 27 001 es una norma de seguridad de la información reconocida internacionalmente, desarrollada por el organismo de certificación Organización Internacional de Normalización (ISO) y la CEI (Comisión Electrotécnica Internacional). La norma ISO 27 001 ha pasado por varias versiones, incluida la norma ISO 27 001:2013; la última versión es la norma ISO/IEC 27 001:2022.

La norma ISO 27 001 proporciona directrices y un marco, con requisitos para "establecer, implementar, mantener y mejorar continuamente" un sistema de gestión de la seguridad de la información (ISMS). La norma ISO 27 001 comprende 93 controles de gestión de riesgos, pero no todos son necesarios para cumplir con la norma ISO 27 001; en su lugar, el cumplimiento de la norma ISO 27 001 consiste en comprender el nivel de riesgo de su organización y decidir cuáles de los 93 controles son los más adecuados para mitigar ese riesgo para los activos de información.

https://www.akamai.com/es/glossary/what-is-iso-27 001
https://www.industriaconectada40.gob.es/difusion/Documents/Documento_Norma_UNE-EN_ISO-IEC_27 001%20MINTUR.pdf

Esquema Nacional de Seguridad (ENS)

Marco normativo español que establece la política de seguridad en la utilización de medios electrónicos para el sector público (administraciones) y para los proveedores que colaboren con ellas. Su objetivo es garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

https://portal.mineco.gob.es/es-es/ministerio/estrategias/Paginas/Esquema_Nacional_de_Seguridad.aspx

Datos sensibles

Son datos personales que, por su naturaleza, su tratamiento tiene un especial impacto en los derechos y las libertades fundamentales de su titular. En el RGPD aparecen como categorías especiales de datos y son los siguientes: datos genéticos, datos biométricos, datos relativos a la salud, datos relativos a la vida sexual o la orientación sexual, el origen étnico o racial, y también los datos personales que revelen las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical.

https://www.pridatect.es/diferencias-entre-datos-personales-y-datos-sensibles-a-efectos-del-rgpd/

Políticas de acceso

Normas y procedimientos que definen quién (usuarios o sistemas) puede acceder a qué recursos (datos, aplicaciones, sistemas) y bajo qué condiciones. Son un pilar fundamental del control de acceso en cualquier entorno profesional.

https://www.adaptacion-rgpd.eu/por-que-es-importante-implementar-una-politica-de-control-de-acceso-en-nuestra-empresa-i/

Diagnóstico de fallos

La detección de fallos de seguridad, también conocida como pentesting, es una práctica común en la industria de la ciberseguridad. Esta técnica se utiliza para identificar las vulnerabilidades y debilidades en la seguridad de un sistema informático, aplicaciones o redes.

El pentesting implica la simulación de un ataque cibernético, en el que el pentester (persona que realiza el pentesting) intenta encontrar vulnerabilidades y brechas de seguridad en el sistema en cuestión. Este tipo de prueba es una excelente manera de evaluar el nivel de seguridad del sistema y determinar si es vulnerable a los ataques de los hackers.

https://www.fide.edu.pe/blog/detalle/deteccion-de-fallas-de-seguridad-pentesting/

Propuestas de mejora

Acciones o recomendaciones específicas, derivadas del diagnóstico de fallos o de la gestión de riesgos, destinadas a corregir deficiencias de seguridad, optimizar procesos, reducir vulnerabilidades e incrementar la eficacia del SGSI de la organización.

Registro de incidencias

Documento o base de datos que registra de manera formal y detallada todos los eventos de seguridad o incidentes ocurridos (desde la detección hasta el cierre). Es fundamental para la trazabilidad, el análisis forense, el aprendizaje y el cumplimiento normativo.

https://www.metacompliance.com/es/blog/cyber-security-awareness/dominar-la-gestion-de-incidentes-pasos-clave-para-una-respuesta-eficaz-de-ciberseguridad