11-11-2025

Cyberseguridad

Ejercicio 1 - Vocabulario

VERONIQUE GRUÉ

1. Amenazas y vulnerabilidades

➢ Amenazas:

Cualquier tipo de **actividad maliciosa** o **potencialmente dañina** dirigida a sistemas informáticos, redes o datos. Estas amenazas pueden provenir de diversas fuentes, como hackers, empleados descontentos o incluso errores accidentales.

Fuente: https://www.godaddy.com/resources/es/seguridad/7-tipos-de-amenazas-informaticas-que-toda-pyme-debe-saber

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

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

➢ Integridad:

Es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.
Fuente: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

➢ Disponibilidad:

La disponibilidad informática es la característica o capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados, es decir, que lo necesitan para desenvolver sus actividades.

Fuente : https://www.bancosantander.es/glosario/disponibilidad-informatica

➢ Amenazas activas:

Buscan modificar, dañar o robar información (ransomware, troyanos, inyección SQL).

➢ Amenazas pasivas:

Se limitan a espiar o recopilar información sin alterar nada (sniffing de red, espionaje industrial).

El sniffing es una técnica que consiste en interceptar y analizar el tráfico de datos que circula por una red informática, utilizando un software o hardware especializado llamado sniffer o "ladrón de paquetes".

➢ Malware:

Es software malintencionado diseñado para interrumpir, dañar u obtener acceso no autorizado a los sistemas informáticos. Los ciberdelincuentes usan malware para infectar dispositivos con el fin de robar datos, obtener credenciales bancarias, vender acceso a recursos informáticos o información personal, o extorsionar pagos de las víctimas.

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

➢ **Ingeniería social:** manipulación psicológica para engañar a las personas (phishing, vishing, smishing).

- **El phishing**: ataque cibernético donde los estafadores se hacen pasar por una entidad de confianza para obtener información personal y financiera de la víctima, como contraseñas, datos bancarios o de tarjetas.
- **El vishing** es una estafa telefónica (una combinación de "voice" y "phishing") donde los ciberdelincuentes, haciéndose pasar por entidades legítimas, engañan a la víctima para que revele información confidencial o bancaria.
- **El smishing** es un tipo de ciberataque de ingeniería social que emplea mensajes de texto (SMS) fraudulentos para engañar a las víctimas y obtener su información confidencial, como datos bancarios o credenciales de acceso, o para que instalen software malicioso.

➢ Ataques a redes:

- **DoS** (Denial of Service: Denegación de Servicio): Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones. (Defensa: firewall de red(servidor), en la capa de aplicación (reverse proxy))
- **DDoS** (Distributed DoS): Es un DoS pero las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo, y más complicado de detener y determinar su origen.
- **Man-in-the-Middle**: 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 (ej.: robo de credenciales en una red WiFi pública).

Ataques a aplicaciones web:

- **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.
- **XSS** (Cross-Site Scripting: Secuencias de comandos en sitios cruzados): Se conoce como XSS a un tipo de ataque en el cual actores maliciosos logran inyectar un script malicioso en un sitio web para luego ser procesado y ejecutado. Comúnmente, este proceso que se basa en la confianza que tiene el sitio sobre la entrada de los datos, consiste en enviar la URL con el payload(carga útil es la porción de los datos transmitidos que tiene un propósito útil y directo,) precargado al usuario víctima con un objetivo determinado: robar datos personales del usuario, cookies de sesión, implementar técnicas de ingeniería social, entre otras.

Fuente: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
Fuente: https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/

➢ Cifrar:

El cifrado es el proceso de transformar un texto plano legible en un texto cifrado ilegible para ocultar información sensible a usuarios no autorizados. Las organizaciones suelen utilizar el cifrado en la seguridad de los datos para proteger los datos confidenciales del acceso no autorizado y las vulneraciones de datos.

➢ Ransomware:

Es un tipo de malware (es un tipo de software diseñado para dañar, espiar, robar información o tomar el control de sistemas informáticos sin el consentimiento del usuario.) que retiene como rehenes los datos confidenciales o el dispositivo de una víctima, amenazando con mantenerlos bloqueados, o algo peor, a menos que la víctima pague un rescate al atacante.

Fuente: https://www.ibm.com/es-es/think/topics/ransomware

2. Medidas de protección básicas.

- **Autenticación multifactor (MFA):** combina algo que sabes (contraseña), algo que tienes (móvil, token) y algo que eres (huella, reconocimiento facial).

Ejemplo: acceder al banco online con contraseña + SMS, o entrar en Educa con la contraseña y un código (que dura poco tiempo activo) del Authenticator, que genera una app en el móvil.

➢ Roles:

Son grupos de usuarios que comparten permisos específicos, estableciendo jerarquías que van desde los lectores registrados hasta los super administradores. Estos permisos son acciones o privilegios que regulan el acceso y las capacidades de los usuarios, desde la simple lectura hasta la gestión completa del sistema.

➢ Permisos:

Permiten a los usuarios o roles realizar acciones como crear, editar, publicar y eliminar contenido, así como controlar aspectos no relacionados directamente con el contenido, como menús y categorías, por ejemplo.

Estos roles y permisos no solo afectan a los creadores de contenido y administradores, sino que se extienden a todos los que interactúan con el CMS(Sistemas de gestión de contenido), incluyendo departamentos como SEO(optimización para los motores de búsqueda), marketing y ventas.

Fuente: https://www.mejorcms.com/wordpress/roles-permisos-cms/

➢ Firewall (cortafuegos):

Sistema de seguridad compuesto o bien de programas 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.

Tipos de firewalls:

- Filtrado de paquetes, o sin estado: inspeccionan uno a uno cada paquete. Estos no son conscientes del estado de conexión y solo pueden permitir o denegar paquetes que se basan en los encabezados de los paquetes individuales. Se trata de la primera generación de firewalls.

- Con estado: son mucho más flexibles que los anteriores ya que pueden determinar el estado de conexión de los paquetes. Esta segunda generación funciona recopilando paquetes relacionados hasta poder determinar el estado de conexión antes de aplicar las reglas de firewall al tráfico.
- De aplicaciones: analizan los datos que se están transmitiendo, permitiendo así que el tráfico de red coincida con las reglas de firewall que son específicas de servicios o aplicaciones individuales. Estos últimos son la tercera generación, pese a que se califican como de "última generación" ya que combinan todos los enfoques.

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

https://www.iukanet.com/es/blog/que-son-los-firewall

➢ Reglas de Firewall:

son directivas de seguridad que **controlan el tráfico de red**, especificando qué se permite o se deniega basándose en parámetros como direcciones IP de origen/destino, puertos y protocolos

Ejemplos de reglas de Firewall:

Diremos que tenemos un servidor con una serie de reglas firewall aplicadas al tráfico que entra:

1. Aceptar tráfico entrante nuevo y establecido a la interfaz de red pública en los puertos 80 y 443 (tráfico web HTTP y HTTPS)
2. Coloquar el tráfico entrante de las direcciones IP de los empleados no técnicos de su oficina al puerto 22 (SSH)
3. Aceptar tráfico entrante nuevo y establecido desde el intervalo IP de la oficina a la interfaz de red privada en el puerto 22 (SSH)

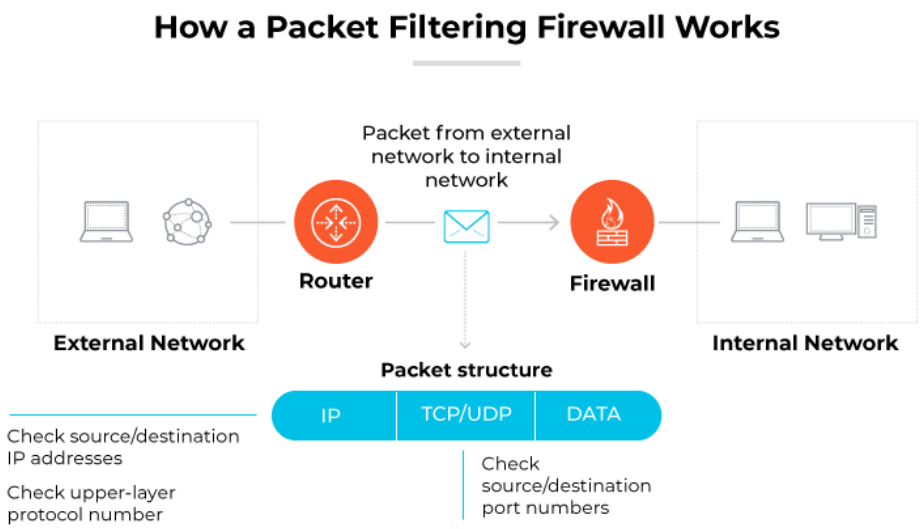
Las primeras palabras en estos ejemplos son o bien 'accept' (aceptar), 'reject' (rechazar) o 'drop' (descartar). Lo que especifica que acción tiene que hacer el firewall.

Partiendo de nuestro ejemplo de servidor, si un empleado intentara establecer conexión SSH con el servidor, en función de la regla 2 se rechazaría, antes de comprobar la regla 3. En cambio, se aceptaría un administrador del sistema porque coincidiría con la regla 3.

Fuente: https://www.iukanet.com/es/blog/que-son-los-firewall

➢ Filtrado de puertos y protocolos:

Es una función de los firewalls que **inspecciona los paquetes de datos** entrantes y **salientes para permitir o bloquear su paso** basándose en el número de puerto (TCP o UDP) y el protocolo (como IP) utilizado. Esta técnica es fundamental para proteger las redes, ya que permite definir qué servicios de red estarán disponibles y por cuáles puertos, gestionando así el flujo de tráfico y previniendo el acceso no autorizado y las amenazas de malware.



Fuente: https://www.paloaltonetworks.es/cyberpedia/what-is-a-packet-filtering-firewall

➢ 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).

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.

Fuentes:https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf; https://www.youtube.com/watch?v=8Py5-otzhD4

➢ Herramientas de detección y monitoreo:

Su función es **identificar amenazas activas**, comportamientos anómalos o eventos sospechosos en tiempo real. Las herramientas de detección también ayudan a identificar vulnerabilidades en tiempo real, permitiendo una respuesta rápida y efectiva.

Las amenazas no siempre se bloquean en el perímetro. Muchas veces logran ingresar y se mantienen ocultas por semanas o meses. Las herramientas de detección permiten descubrirlas antes de que causen daños mayores. Además, realizar pruebas de penetración es crucial para evaluar la seguridad de los sistemas y detectar posibles vulnerabilidades.

Ejemplos concretos y cómo se usan:

- **SIEM (Security Information and Event Management):** soluciones como Splunk, QRadar o Elastic Security recopilan y correlacionan registros de múltiples fuentes para detectar patrones anómalos. Por ejemplo, accesos desde ubicaciones no habituales o aumento repentino de tráfico en un servidor.
- **IDS/IPS (Intrusion Detection/Prevention Systems):** como Snort detecta firmas de ataques conocidos y los bloquea en tiempo real. Ideal para servidores con alta exposición a internet.
- **Threat Intelligence Platforms:** como Recorded Future, agregan datos externos sobre amenazas emergentes, proporcionando contexto adicional para decisiones rápidas.

Aplicación moderna: En empresas con trabajo híbrido, estas herramientas permiten monitorear dispositivos que operan fuera del perímetro clásico, integrando eventos desde la nube, redes locales y endpoints remotos.

Ejemplo de uso: Un SIEM detecta múltiples intentos de login desde una IP extranjera hacia cuentas administrativas. La correlación con datos de inteligencia revela que la IP está asociada a una botnet activa. Se bloquea automáticamente y se activa protocolo de revisión de accesos. Relacionado: Detección y prevención de amenazas

Fuente: https://preyproject.com/es/blog/herramientas-de-ciberseguridad

3. Análisis de los Incidentes de Seguridad.

➢ Incidentes de Seguridad

Un incidente de Seguridad es un evento que compromete la confidencialidad, integridad o disponibilidad de la información o los sistemas digitales de una organización. Estos incidentes pueden ser causados por ataques malintencionados, como el ransomware o el phishing, errores humanos, vulnerabilidades en el software o fallos técnicos.

Algunos ejemplos comunes de incidentes incluyen:

- **Ataques de malware:** programas dañinos diseñados para robar, cifrar o destruir datos.
- **Filtraciones de datos:** acceso no autorizado a información sensible.
- **Ataques de denegación de servicio (DDoS):** sobrecarga de los sistemas para inutilizarlos.

Los incidentes de ciberseguridad pueden tener consecuencias graves, como pérdidas financieras, daños a la reputación, interrupciones operativas y sanciones legales. Por eso, es fundamental contar con medidas preventivas y planes de respuesta para mitigar su impacto.

Fuente: https://www.pmg-ssi.com/2024/11/5-incidentes-de-ciberseguridad-mas-importantes/

➢ Ciclo de vida de un incidente:

- **Preparación**
  El **CSIRT** (Equipos de Respuesta a Incidentes de Seguridad Informática) define procedimientos y herramientas para responder rápidamente. Identifica vulnerabilidades de la red y prioriza los posibles incidentes según su impacto potencial en el negocio. Realiza **simulaciones de ataque** (*"juegos de guerra"*) para crear plantillas de respuestas eficaces. El resultado es la creación o actualización de **planes de respuesta a incidentes** basados en evaluaciones de riesgo completas.

- **Detección y análisis**
  Los miembros del **equipo vigilan la red en busca de actividad sospechosa** y amenazas potenciales. Analizan datos de registros de dispositivos y herramientas de seguridad (antivirus, firewall) para identificar incidentes en curso. Trabajan para filtrar los falsos positivos y clasificar las alertas reales según su gravedad. Una vez determinada la amenaza, el CSIRT notifica al personal apropiado, activando el plan de comunicación.

- **Contención**
  El equipo toma medidas para **impedir que la brecha se propague** y cause más daño a la red. La mitigación a **corto plazo** implica aislar los sistemas infectados (ej. desconectar dispositivos). La contención a **largo plazo** se centra en proteger sistemas no afectados, implementando controles de seguridad más estrictos (ej. segmentación de bases de datos). En esta etapa, se crean copias de seguridad de sistemas afectados y no afectados para evitar pérdidas de datos y **capturar pruebas forenses**.

- **Erradicación**

Una vez contenida la amenaza, el equipo **pasa a la corrección y a la eliminación completas de la amenaza del sistema**. Esto podría incluir la eliminación de malware o la expulsión de la red de un usuario no autorizado o malicioso. El equipo también revisa tanto los sistemas afectados como los no afectados para garantizar que no queden rastros de la brecha.

- **Recuperación**
  Cuando el equipo de respuesta a incidentes está seguro de que la amenaza se erradicó por completo, **restaura los sistemas afectados a las operaciones normales**. Esta corrección podría implicar el despliegue de parches, la reconstrucción de sistemas a partir de copias de seguridad y la puesta en marcha de sistemas y dispositivos. Se conserva un registro del ataque y su resolución para su análisis y mejora del sistema.

- **Revisión posterior al incidente**
  El CSIRT revisa toda la evidencia recopilada y la documentación de cada fase para obtener "lecciones aprendidas". Se busca determinar la causa principal del ataque y cómo se explotó la vulnerabilidad de la red. El equipo resuelve las vulnerabilidades identificadas para evitar que incidentes similares se repitan en el futuro. Finalmente, se revisa qué salió bien y se proponen mejoras en los sistemas, herramientas y procesos de respuesta.

Fuente: https://www.ibm.com/mx-es/think/topics/incident-response

➢ Indicadores de compromiso (IoC):

Los indicadores de riesgo (IoC) son **información sobre un fallo de seguridad** concreto que puede ayudar a los equipos de seguridad a determinar si se ha producido un ataque. Estos datos pueden incluir detalles sobre el ataque, como el tipo de malware utilizado, las direcciones IP implicadas y otros detalles técnicos. Señal, rastro o pista de que el sistema ha sido comprometido.

Los IoC pueden obtenerse por varios métodos, entre los que se incluyen:

- **Observación:** observar actividades o comportamientos anormales en sistemas o dispositivos
- **Análisis:** determinar las características de la actividad sospechosa y analizar su impacto
- **Firmas:** identificar las firmas de software malicioso conocidas

Hay varios tipos diferentes de IoC que pueden utilizarse para detectar incidentes de seguridad. Estos incluyen:

- **Los IoC basados en la red**, como direcciones IP, dominios o URL maliciosos, también pueden incluir patrones de tráfico de red, actividad inusual del puerto, conexiones de red a hosts maliciosos conocidos o patrones de exfiltración de datos.
- Los **IoC basados en el servidor** están relacionados con la actividad en una estación de trabajo o servidor. Los nombres de archivo o hash, las claves de registro o los procesos sospechosos que se ejecutan en el servidor son ejemplos de IoC basados en el servidor.
- Los **IoC basados en archivos** incluyen archivos maliciosos, tales como malware o scripts.

- Los **IoC de comportamiento** cubren varios tipos de comportamiento sospechoso, como comportamientos extraños de los usuarios, patrones de inicio de sesión, patrones de tráfico de red e intentos de autenticación.
- Los **IoC de metadatos** tienen que ver con los metadatos asociados a un archivo o documento, como el autor, la fecha de creación o los detalles de la versión.

Fuente: https://www.cloudflare.com/es-es/learning/security/what-are-indicators-of-compromise/

➢ Estrategias proactivas

El enfoque proactivo de ciberseguridad va mucho más allá de responder a los incidentes o corregir las vulnerabilidades después de un ataque. Se trata de una **estrategia integral que se centra en anticipar, prevenir y mitigar rápidamente las ciberamenazas**, antes de que puedan causar daños.

En lugar de esperar las alertas, la ciberseguridad proactiva se puede hacer hincapié en:

- Evaluaciones de riesgos y gestión de vulnerabilidades continuas.
- Recopilación y análisis de inteligencia sobre ciberamenazas.
- Programas de capacitación y concientización de empleados.
- Implementar y probar planes sólidos de respuesta a incidentes

Fuente: https://www.startupdefense.io/es-us/blog/enfoque-proactivo-de-ciberseguridad

➢ Análisis forense(Peritaje informático):

es una técnica de seguridad **pasiva** utilizada para **investigar y analizar incidentes** de seguridad informática, como intrusiones, robos de datos o ciberataques. Este proceso involucra la recopilación, preservación y análisis de datos digitales para determinar qué sucedió durante un incidente de seguridad y quién es el responsable.

El análisis forense en ciberseguridad se lleva a cabo en un ambiente controlado y seguido de cerca para garantizar la integridad de los datos y evitar contaminación. Los expertos en análisis forense utilizan herramientas especializadas y técnicas para examinar el sistema afectado y buscar pistas que puedan ayudar a identificar al atacante y comprender cómo se produjo el incidente.

La herramienta la más importante en estos casos está en los ficheros de log, que son los que recogen la información de los

Fuente: https://iddigitalschool.com/bootcamps/que-es-el-analisis-forense-en-ciberseguridad/

4. Herramientas y tecnologías de aplicación.

➢ Cortafuegos:

➢ Tipos de Cortafuegos.

Es un dispositivo especializado en limitar o impedir la comunicación entre dispositivos de redes diferentes.

Los firewalls de red: implican el **uso de uno o más firewalls entre las redes externas y las redes internas privadas**. Estos regulan el tráfico de red entrante y saliente, y separan las redes públicas externas (como el Internet global) de las redes internas, como las redes de wifi domésticas y las intranets de empresas o nacionales. Los firewalls de red pueden tener cualquiera de los siguientes formatos: hardware dedicado, software y virtual.

Los firewalls de host o "firewalls de software": requieren el **uso de firewalls en dispositivos de usuario individuales y otros puntos de conexión de red privados** como barreras entre los dispositivos dentro de la red. Estos dispositivos, o hosts, reciben una regulación adaptada del tráfico desde y hacia aplicaciones de la computadora específicas. Los firewalls de host pueden ejecutarse en dispositivos locales como un servicio del sistema operativo o una aplicación de seguridad de punto de conexión. Los firewalls de host pueden acceder de manera más profunda al tráfico web, el filtrado basado en HTTP y otros protocolos de red, lo que permite administrar el contenido que recibe el equipo, en lugar de solo saber de dónde viene.

Fuente: https://latam.kaspersky.com/resource-center/definitions/firewall

➢ IDS /IPS

IDS (Intrusion Detection System): Es una **aplicación usada para detectar accesos no autorizados a un ordenador o a una red**. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia.

IPS (Intrusion Prevention System): El sistema de prevención de intrusiones es un **software que se utiliza para proteger a los sistemas de ataques y abusos**. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos

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

➢ Antivirus vs Antimalware:

El **software antivirus** es una herramienta que **ayuda a escanear, detectar y eliminar virus**. Actúa como un escudo para el dispositivo, protegiéndolo contra los virus. Los virus pueden replicarse y propagarse en tu sistema, causando daños y robando información. Pueden **corromper** archivos, **interrumpir** programas e incluso **dar a los hackers acceso a tus datos personales.**

- **Escanea el dispositivo en busca de actividad sospechosa**, incluidos correos electrónicos, descargas e incluso sitios web que visitas.
- **Aisla actores maliciosos o los elimina**.

El **antimalware** es un tipo de **software diseñado para combatir una gama más amplia de malware**, no solo los virus.

P**rotege contra spywares** que roban los datos, ransomwares que bloquean los archivos o **troyanos** que se camuflan como programas legítimos.

La protección contra malware es una excelente manera de hacer frente a estas amenazas. Un buen programa de antimalware puede ayudarte a:

- **Identifica y elimina diversas amenazas de malware** mediante técnicas como la detección basada en firmas (que busca patrones de malware conocidos) y el análisis de comportamiento (que monitoriza programas en busca de actividades sospechosas).
- **Protege en tiempo real** al escanear constantemente tu dispositivo en busca de nuevas amenazas.

5. Normativas y buenas prácticas de uso.

➢ Reglamento General de Protección de Datos (RGPD). ISO/IEC 27001.

Tiene como objeto la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y la libre circulación de los mismos.

Entre las principales características de este Reglamento, subrayamos las siguientes:

- Consentimiento: debe ser explícito y claro. No se permite el consentimiento tácito o por omisión.
- Derechos de los sujetos: acceso, rectificación, olvido, portabilidad de datos, limitación del tratamiento y oposición.
- Proactividad de las organizaciones.
- Transparencia y notificación.
- Transferencias internacionales de datos: existen normas estrictas para la transferencia de datos personales fuera del Espacio Económico Europeo para asegurar que el nivel de protección de datos no se vea comprometido.

➢ Esquema Nacional de Seguridad (ENS).

Como principios básicos del ENS se consagran los siguientes:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en riesgos, reforzando el gobierno de la ciberseguridad y el gobierno TI.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua y reevaluación periódica.
- Diferenciación de responsabilidades dentro de la organización.

En las mismas líneas, también se definen los requisitos mínimos, tales como:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

Convergencia entre ENS y RGPD:

El ENS y el RGPD son dos normativas que impactan en la seguridad y el tratamiento de datos en el ámbito digital. El ENS establece medidas de seguridad para los sistemas de información utilizados por las entidades del sector público, siendo una de estas medidas la protección de datos personales, regulada en el RGPD.

Fuente: https://ciberso.com/blog/gobierno-de-la-ciberseguridad/que-es-esquema-nacional-seguridad-ens-convergencias-rgpd/

➢ Datos sensibles.

Los datos sensibles **incluyen diferentes tipos de información de identificación personal (PII) asociados a su identidad**. Los siguientes son ejemplos de datos sensibles:

- Número de la Seguridad Social
- Número de identificación del permiso de conducir
- Número de pasaporte
- Número de cuenta bancaria
- Historial médico
- Número de tarjeta de crédito o débito
- Fecha de nacimiento
- Nombre legal completo
- Nombres de usuario y contraseñas
- Dirección postal

Los datos personales, financieros, sanitarios y empresariales se consideran datos sensibles porque no están disponible en los registros públicos y se guardan como confidenciales. Pero si los datos sensibles se ven vulnerados, pueden producirse robos de identidad, solicitudes de préstamos a nombre de otra persona y grandes fraudes con tarjetas de crédito.

6 maneras de proteger sus datos sensibles:

- Cree contraseñas seguras para todas sus cuentas en línea
- Configure la autenticación multifactor (MFA)
- Utilice una VPN en redes Wi-Fi públicas
- Habilite el cifrado de datos
- Haga copias de seguridad de sus datos con frecuencia
- Invierta en un gestor de contraseñas

Fuente: https://www.keepersecurity.com/blog/es/2024/08/19/how-to-protect-sensitive-data/

➢ Políticas de acceso.

El **control de acceso en ciberseguridad** se refiere al conjunto de tecnologías, políticas y procedimientos que determinan **quién puede entrar, a qué recursos y bajo qué condiciones**, dentro de un entorno digital.

Este sistema no solo protege el acceso a archivos o carpetas, sino también a servidores, bases de datos, software corporativo y sistemas críticos.

El modelo de control que adopta una organización dependerá de su tamaño, tipo de datos, infraestructura tecnológica y grado de madurez en seguridad. Estos son los tipos más comunes:

- **Control de acceso discrecional (DAC)**
  Permite al propietario del recurso decidir quién tiene acceso. Es flexible, pero potencialmente inseguro si no se controla de forma centralizada.

- **Control de acceso basado en roles (RBAC)**

Asigna permisos según funciones o jerarquías dentro de la empresa. Es el más utilizado en empresas medianas y grandes, y permite automatizar parte de la gestión.

- **Control de acceso obligatorio (MAC)**

Aquí, las políticas de acceso son definidas por una autoridad central (como el administrador de seguridad) y no pueden modificarse libremente. Se usa en entornos de alta confidencialidad.

- **Control de acceso basado en atributos (ABAC)**

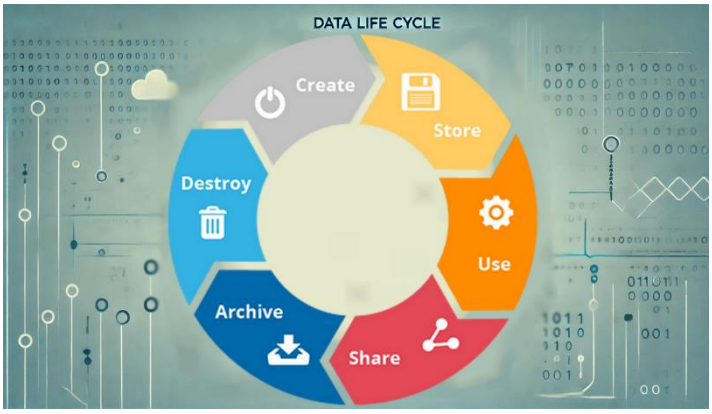
Permite definir condiciones basadas en atributos como la ubicación, tipo de dispositivo, nivel de riesgo, etc. Es más dinámico, ideal para entornos híbridos o en la nube.

Fuente: https://www.deletetechnology.com/blog/control-de-acceso-en-ciberseguridad-qu%C3%A9-es-tipos-normas-y-c%C3%B3mo-aplicarlo

➢ Ciclo de vida de la información.

Existen seis fases principales en el ciclo de vida de la información:

- **Creación:** Generar nuevos datos, como documentos, correos electrónicos o registros académicos.
- **Almacenamiento:** Guardar de forma segura estos datos en formatos físicos (papel) o digitales (servidores, nubes, etc.).
- **Uso:** Acceder y utilizar la información para realizar actividades académicas o administrativas.
- **Compartición:** Distribuir los datos de manera segura a usuarios autorizados, como docentes, alumnos o personal administrativo.
- **Archivo:** Mover la información a un almacenamiento de largo plazo para mantener un registro histórico o para cumplir con obligaciones legales.
- **Destrucción:** Eliminar los datos de manera segura cuando ya no se necesiten, asegurándose de que no se puedan recuperar.



Fuente: https://ciberseguridad.comillas.edu/ciclo-de-vida-de-la-informacion

➢ 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.

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

➢ Propuestas de mejora.

Con el objetivo de **reducir la posibilidad de sufrir ataques por parte de hackers** que afecten la integridad, disponibilidad y confidencialidad de tus datos, estas son algunas de las medidas más eficaces para resguardar la información de los negocios:

- **Capacitar al personal**

  Según el informe The Global Risks Report 2022, el 95% de los problemas de ciberseguridad se originan por fallos humanas. Por lo mismo, **resulta imprescindible que el personal adquiera competencias en seguridad digital**.

  En este sentido, es necesario capacitar a los colaboradores en esta materia para que realicen un uso adecuado de contraseñas, eviten hacer click en enlaces sospechosos y solo visiten páginas que cuenten con el protocolo *https* en su URL.

- **Usar antivirus y antimalware**

  La óptima seguridad en la red de la empresa también demanda que los **equipos computacionales se mantengan actualizados en el uso de soluciones como antivirus, antimalware y firewall**. De esta manera, se podrá reducir la posibilidad de que el negocio se vea perjudicado por el ataque de un actor malicioso.

- **Utilizar VPN**

  Una red privada virtual o VPN permite establecer una **conexión segura entre un servidor privado y los equipos de un cliente** al utilizar redes públicas. Esto implica que, al navegar por internet, los datos enviados y recibidos son encriptados con el fin de que terceras personas no puedan leerlos ni robarlos, manteniendo lejos a los cibercriminales.

- **Implementar sistemas de autenticación**

  Otra buena medida en materia de seguridad informática consiste en implementar sistemas de autenticación para **verificar la identidad digital de una persona** al acceder a una cuenta en línea de la empresa.

  De esta manera, a través de soluciones como contraseñas, herramientas biométricas, notificaciones al teléfono celular o preguntas secretas, es posible restringir el ingreso de terceros no autorizados.

- **Contar con copias de seguridad**

Ante ataques consumados, las copias de seguridad o *backup* representan la mejor solución para **no perder de forma definitiva la información del negocio**. Asimismo, esta herramienta de respaldo en la nube resulta de gran utilidad en el caso de robo de los equipos, cortocircuitos, incendios o cualquier otra eventualidad que afecte a los computadores.

- **Ejecutar pruebas de vulnerabilidad**

Estas evaluaciones implican la simulación planificada de ataques a los sistemas de ciberseguridad, por parte del equipo informático, con el fin de **detectar debilidades, vulnerabilidades y riesgos**. Así, se pueden implementar medidas correctivas que permitan incrementar la seguridad digital de tu empresa frente a ciberataques reales.

- **Solicitar la asesoría de expertos**

Finalmente, la mejor manera de asegurar que los sistemas estén constantemente preparados para cualquier eventualidad y que las anteriores medidas se apliquen de forma correcta, es obtener la asesoría de expertos en seguridad informática.

➢ Registro de incidencias

Un incidente bien documentado y notificado ayuda a comprender la causa raíz, evaluar la respuesta y prevenir futuras incidencias.

1. Preparación y respuesta inicial

- Identificar al personal clave: Antes de que se produzca un incidente, asegurarse de que se cuenta con un equipo de respuesta a incidentes (IRT) designado. Este equipo debe incluir individuos de TI, legales, de cumplimiento y de relaciones públicas, entre otros. Asignar funciones y responsabilidades con claridad.
- Establecer un plan de respuesta a incidentes: Desarrollar y mantener un plan integral de respuesta a incidentes (IRP) que describa los procedimientos para identificar, responder y registrar los incidentes de seguridad. Asegurarse de que este plan sea accesible y se actualice periódicamente.
- Detección de incidentes: Utilizar herramientas de supervisión automatizadas y procesos manuales para detectar posibles incidentes de seguridad. Estas herramientas pueden incluir sistemas de detección de intrusos (IDS), software antivirus y sistemas de gestión de eventos e información de seguridad (SIEM).

2. Identificación del incidente

- Verificar el incidente: Una vez detectado un posible incidente, verificar su autenticidad. Analizar los indicadores iniciales y validarlo frente a las amenazas conocidas. Esto podría implicar la comprobación de registros, alertas del sistema y otras fuentes de datos relevantes.
- Clasificar el incidente: Una vez detectado, el incidente debe clasificarse en función de su gravedad y tipo. Las categorías comunes incluyen ataques de malware, intentos de phishing, violaciones de datos y ataques de denegación de servicio. Asigne un nivel de gravedad como bajo, medio o alto para priorizar el esfuerzo de respuesta.

3. Contención

- Acciones inmediatas: Tomar medidas inmediatas para contener el incidente. Esto podría implicar aislar los sistemas afectados, bloquear las direcciones IP maliciosas o desactivar las cuentas comprometidas. El objetivo es evitar que el incidente cause más daños.
- Contención a corto plazo: Aplicar medidas de contención a corto plazo para estabilizar la situación. Por ejemplo, se podría redirigir el tráfico de la red, aplicar correcciones temporales o utilizar técnicas de cuarentena para limitar el impacto.

4. Erradicación

- Identificar la causa raíz: Llevar a cabo una investigación exhaustiva para identificar la causa raíz del incidente. Esto implica analizar los registros, examinar los sistemas afectados y consultar las fuentes de inteligencia sobre amenazas.
- Eliminar la amenaza: Una vez identificada la causa raíz, tomar medidas para eliminar la amenaza por completo. Esto podría implicar la eliminación del malware, el cierre de vulnerabilidades y la aplicación de parches. Asegurarse de que todos los sistemas afectados estén limpios y seguros.

5. Recuperación

- Restaurar sistemas: Una vez eliminada la amenaza, se debe comenzar el proceso de restauración de los sistemas para que vuelvan a funcionar con normalidad. Esto incluye recuperar los datos de las copias de seguridad, reinstalar el software y verificar que los sistemas funcionan correctamente.
- Supervisar si hay más problemas: Una vez restablecidos los sistemas, continuar vigilándolos de cerca para detectar cualquier signo de problemas residuales o nuevos ataques. Asegurarse de que todos los sistemas son plenamente operativos y seguros.

6. Documentación e informes

- Registrar los detalles del incidente: Documentar con precisión todos los detalles del incidente. Esto debe incluir:
  - Fecha y hora: Cuándo se detectó, contuvo, erradicó y resolvió el incidente.
  - Descripción: Una descripción detallada del incidente, incluyendo cómo se detectó y los sistemas afectados.
  - Acciones emprendidas: Una relación paso a paso de las acciones llevadas a cabo durante la respuesta, incluyendo los esfuerzos de contención, erradicación y recuperación.
  - Impacto: Una evaluación del impacto en la organización, incluyendo la pérdida de datos, los costes financieros y las interrupciones operativas.
  - Análisis de la causa raíz: Un análisis detallado de la causa raíz y de los factores que han contribuido a ella.
- Crear un informe de incidentes: Compilar los detalles registrados en un informe exhaustivo del incidente. Este informe debe ser claro, conciso y accesible para todas las partes interesadas. Incluir las lecciones aprendidas y las recomendaciones para mejorar la respuesta al incidente en el futuro.
- Informes legales y reglamentarios: Si el incidente implica la violación de datos u otros problemas reglamentarios, asegurarse de que se realizan rápidamente todas las notificaciones legales y reglamentarias necesarias. Esto podría incluir la notificación a las personas afectadas, a los organismos reguladores y a las fuerzas del orden.

7. Revisión posterior al incidente

- Realice una revisión posterior al incidente: Se debe celebrar una reunión de revisión posterior al incidente con el equipo de respuesta al incidente y otras partes interesadas. Discutir lo sucedido, lo que se hizo bien y lo que podría mejorarse.
- Actualizar políticas y procedimientos: Basándose en la revisión, actualizar el plan de respuesta a incidentes, las políticas de seguridad y los procedimientos. Implementar los cambios necesarios para prevenir incidentes similares en el futuro.

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

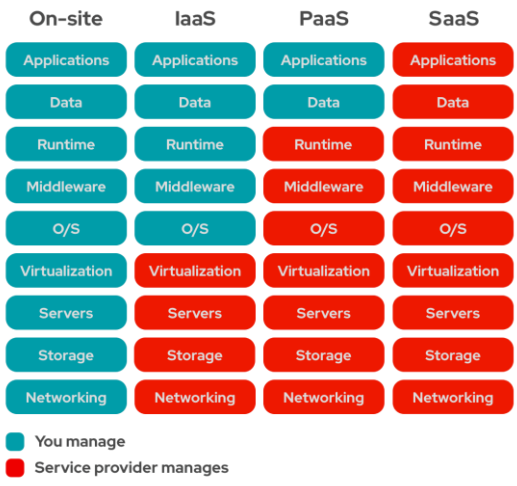
➢ Diferencias entre IaaS, PaaS, SaaS y su impacto en la ciberseguridad

Los tres modelos comparten el enfoque "como servicio": en lugar de que las organizaciones compren y gestionen su propia infraestructura, un proveedor ofrece recursos de TI en la nube mediante suscripción o pago por uso. Esto reduce costes y aumenta la flexibilidad.

- **IaaS (Infraestructura como Servicio)** Proporciona infraestructura de TI accesible por internet, incluyendo computación, analítica, machine learning, IoT y más. Funciona con modelo escalable y pago según uso, permitiendo desplegar soluciones en segundos. Ideal para empresas de cualquier tamaño y sector.
- **PaaS (Plataforma como Servicio)** Ofrece una plataforma completa para que los desarrolladores creen, ejecuten y administren aplicaciones sin preocuparse por la infraestructura subyacente. Incluye entornos de desarrollo, bases de datos, herramientas de análisis y seguridad. Perfecto para desarrollo de APIs, metodologías Agile y DevOps.
- **SaaS (Software como Servicio)** Distribuye software y aplicaciones ya desarrolladas a través de internet mediante suscripción. Los usuarios acceden directamente a aplicaciones listas para usar, con actualizaciones automáticas y costes predecibles. Ejemplos: Microsoft 365, Salesforce, HubSpot.

Diferencia clave

Cada modelo representa un equilibrio diferente entre la personalización/control que tiene el cliente y la responsabilidad de gestión que asume el proveedor.



	IaaS	PaaS	SaaS
Qué servicio ofrece	Recursos de infraestructura de TI para que los usuarios implementen y administren sus aplicaciones y datos.	Entorno completo para el desarrollo, ejecución y administración de aplicaciones.	Aplicaciones y software listos para usar, quedando cubiertas por el proveedor tanto infraestructura como desarrollo.
Nivel de control	Alto nivel de control sobre la infraestructura y configuración de entornos.	Los usuarios tienen control sobre las aplicaciones y los datos, no sobre la infraestructura.	Los clientes interactúan con la aplicación como usuario final, sin acceso directo a la infraestructura o las aplicaciones y códigos.
Desarrollo de aplicaciones	Requiere de la gestión de los entornos de desarrollo.	Se orienta a simplificar el proceso de desarrollo y despliegue al ofrecer el entorno adecuado.	Los usuarios se incorporan al proceso cuando la aplicación ya está desarrollada y se ofrece como servicio proporcionado por el proveedor.
Perfil de usuario	Equipos de TI con experiencia para configurar y ejecutar infraestructura. Buscan un dominio total sobre los sistemas operativos y configuraciones del servidor y son capaces de ocuparse de su gestión y mantenimiento, además de las aplicaciones y las plataformas de desarrollo.	Organizaciones que buscan un control total sobre el desarrollo de una aplicación y, a su vez, liberarse de la gestión de infraestructura.	Organizaciones que desean implementar una aplicación o software sin tener que ocuparse de su gestión. No les resulta problemático ceder el control sobre la infraestructura subyacente o la personalización de la plataforma.

Principal beneficio	Mejorar la flexibilidad y la agilidad de la infraestructura de TI sin incurrir en grandes costos de capital.	Crear, probar y desplegar aplicaciones de manera rápida y eficiente sin preocuparse por la configuración y gestión de la infraestructura subyacente.	Acceder a software empresarial de calidad sin la necesidad de invertir en hardware o infraestructura de TI.
Ciberseguridad	El proveedor se encarga de proteger la infraestructura física y la virtualización subyacente. No obstante, el usuario tiene importantes responsabilidades, como asegurar los sistemas operativos, las aplicaciones y los datos que se ejecutan en la infraestructura. Los usuarios tienen un alto control de las configuraciones de seguridad. Mayor exposición a riesgos vinculados a una configuración incorrecta.	El proveedor de servicios asume una mayor responsabilidad en cuanto a la seguridad de la plataforma subyacente. Menor control sobre la configuración de seguridad de la plataforma, en comparación con IaaS. Los usuarios se centran en la seguridad de las aplicaciones, siendo responsables de asegurar el código y los datos de las aplicaciones que desarrollan y ejecutan en la plataforma.	La ciberseguridad recae en gran medida en el proveedor de servicio, que se ocupa de desarrollar, mantener y gestionar la aplicación y los datos asociados. Los usuarios están sujetos en un alto grado a las políticas de seguridad del proveedor de servicios en la nube.

Una de las claves para comprender la **ciberseguridad en entornos cloud** y en los modelos **IaaS, PaaS y SaaS** es el concepto de responsabilidad compartida.

Este término se refiere a la necesidad de **dividir claramente las responsabilidades de seguridad** entre el proveedor de servicios en la nube y el cliente, en vistas a comprender quién es responsable de proteger qué aspectos de los datos, aplicaciones, sistemas y redes en el entorno de la nube.

Fuente : https://s2grupo.es/iaas-paas-y-saas-en-que-se-diferencian-y-ejemplos/