CIBERSEGURIDAD

15/10/2025

Tema 1 Amenazas y vulnerabilidades informáticas

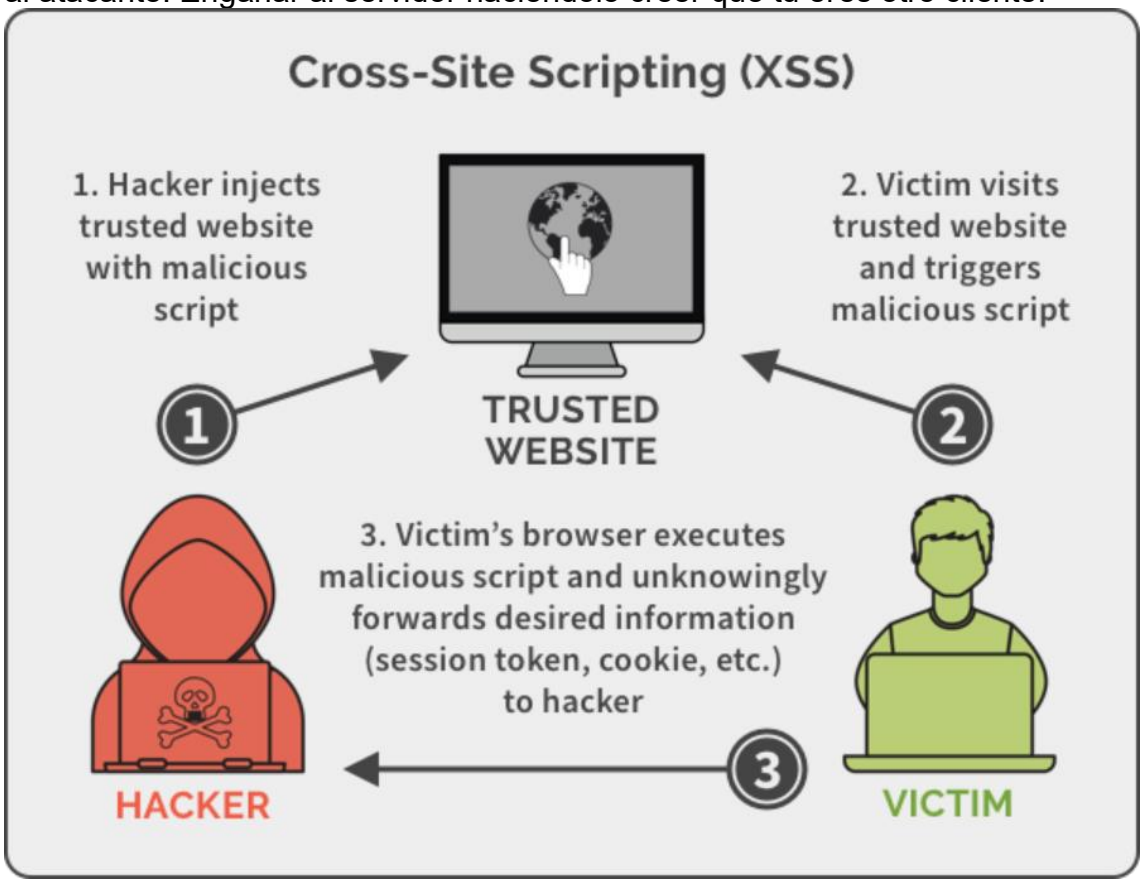
Cifrar:

Es la conversión de datos legibles a unos cifrados y solo se puede descifrar con una clave de cifrado.

Confidencialidad:

Garantizarían de nivel necesario de secretismo a la información y de su tratamiento, para prevenir su divulgación no autorizada.

Cross-Site Scripting (XSS): Es un ataque que logra inyectar código malicioso en una web donde ha encontrado un agujero de seguridad para luego pasar el enlace a los usuarios para luego ser ejecutado y enviar la información al atacante. Engañar al servidor haciéndolo creer que tú eres otro cliente.



Disponibilidad: Asegura que los usuarios autorizados puedan acceder a la información cuando lo necesiten.

DoS: Hacer que una web no esté disponible sobrecargándola con peticiones. Tirar una página a fuerza bruta.

DDoS: Es lo mismo que DoS (Denial of Service) pero con la contribución de muchos equipos.

Exploits: Un software de aprovechamiento de vulnerabilidades para alterar el funcionamiento normal de una web que tú ejecutas. Para poder escribir uno de estos debes ser excelente en sistemas operativos y redes. Para ejecutarlos solo necesitas dinero. Hacer estos programas no son delitos, pero usarlos sí. Hay varios tipos de exploits

1. Exploits de día 0: Son los más peligrosos ya que aprovechan fallos desconocidos para el fabricante o sin parche disponible.
2. Exploit kits: Son paquetes automatizados que combinan exploits y payloads (codigo malicioso que se ejecuta **tras** lograr el acceso)

3. Data exploit: Son los que atacan directamente a la base de datos para extraer información confidencial.

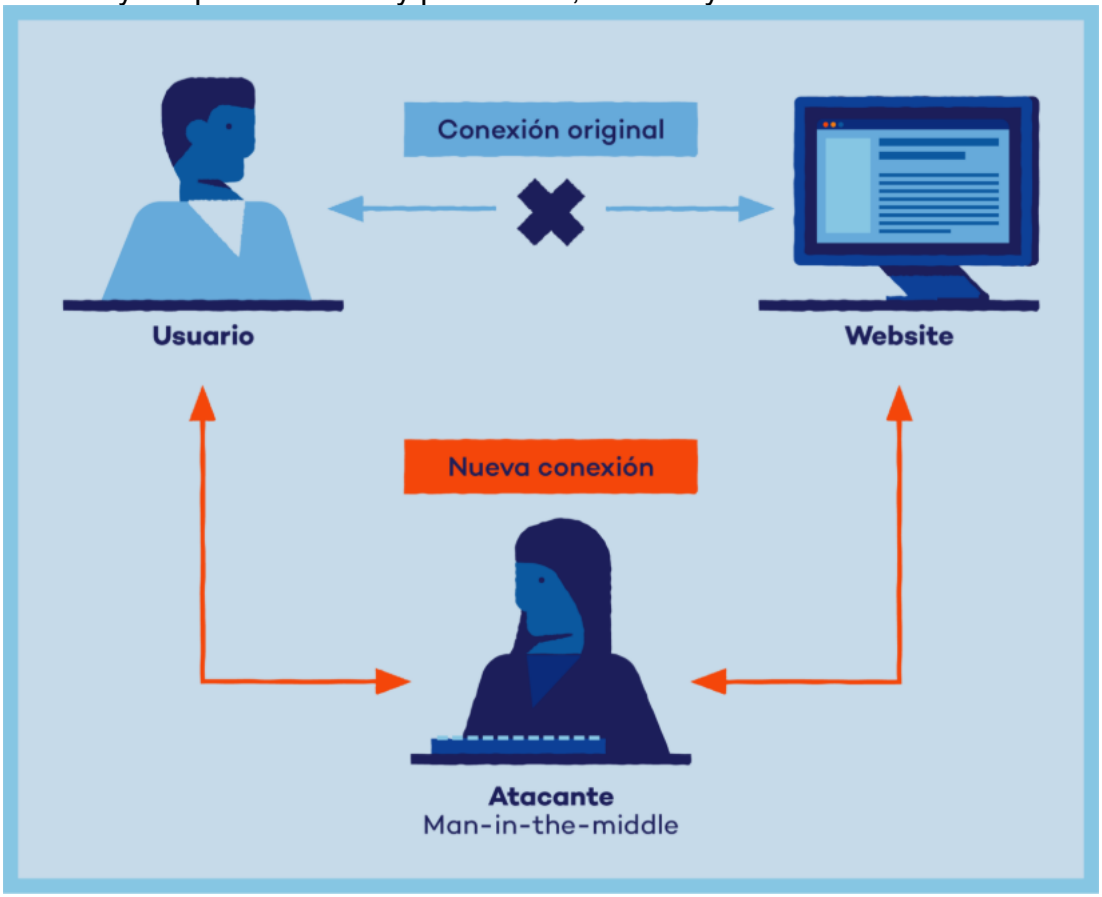
Ingeniería social: Técnicas de manipulación usada para obtener información confidencial. Por ejemplo, haciéndose pasar por tu empresa bancaria diciendo que ha habido un problema en tu cuenta y te pide identificarte (para robarte los datos).

Integridad: La capacidad para garantizar la fiabilidad de los datos y asegurar que no se han modificado ni manipulado.

Inyección SQL: Infiltración de código mediante una vulnerabilidad en el nivel de validación para realizar operaciones sobre la base de datos. Escribir sentencias sql en el registro de usuario para conseguir ejecutar instrucciones SQL.

Malware: Programa maligno que se ejecuta sin ser detectado y realiza funciones perjudícales.

Man-in-the-Middle: Es un ataque donde el criminal se posiciona entre el usuario y la aplicación web y puede leer, insertar y/o modificar.



Ransomware: Es un programa que restringe el acceso a determinadas partes mediante cifrado y pide un rescate para quitar esa restricción.

Tema 2. Medidas de protección básicas.

Autenticación Multifactor (mfa)

La autenticación multifactor se basa en el concepto de usar algo que sabemos y algo que tenemos para aumentar la seguridad. Normalmente usamos una contraseña (algo que sabemos) y nuestro dispositivo móvil (algo que tenemos). También podemos usar el tercer factor, que sería algo que somos. Los ejemplos más comúnes son la huella dactilar o el reconocimiento biométrico (más conocido como reconocimiento facial)

Roles y permisos

Es una estrategia de autorización que organiza los privilegios en función de un rol. La asignación de estos roles a cada usuario garantiza que solo tengan los permisos requeridos para su trabajo.

- Roles: conjuntos de perimisos que agrupan privilegios para una función especifica
- Permisos: Acciones que puede realizar un usuario

Reglas de firewall

Las reglas de firewall son las instrucciones que determinan que tráfico de red puede pasar o no. Es decir, si el firewall recibe tráfico de red, revisará si ese tráfico cumple con alguna de las reglas de firewall, y si no, no se le permite el acceso.

Filtrado de puertos y protocolos

Se basa en la inspección de los paquetes tanto de entrada como de salida basándose en su puerto y protocolo. Gracias a esto se puede gestionar que servicios estarán disponibles y sobre que puertos actuarán.

Routers

Un router es un dispositivo que conecta varias redes entre sí y gestiona el tráfico de datos entre los distintos dispositivos. Distribuye la conexión a internet comprobando las direcciones de destino de los paquetes para decidir porque ruta serán enviados.

Monitoreo y auditoría

Su función es la identificar amenazas activas **en nuestro sistema,** analizando comportamientos o eventos sospechosos. A veces las amenazas no actuan

hasta meses después de introducirse en nuestro dispositivo. Con estas herramientas podemos detectarlas antes de sufrir daños graves.

Tema 3: Análisis de los incidentes de seguridad

Ciclo de vida de un incidente:

- Detección: Vigilancia en la red de actividades sospechosas y amenazas potenciales.
- Análisis: Analisis de datos, notificacions y alertas recopiladas de dispositivos y herramientas de seguridad
- Contención: Toma de medidas para impedir más daños a la red
    - A corto plazo: evitar que la amenaza actual se propague aislando los sistemas
    - A largo plazo: protección de los sistemas no afectados mediante la colocación de controles de seguridad.
- Erradicación: Una vez contenida la amenaza, se pasa a la eliminación completa de la amenaza
- Recuperación: Cuando el equipo está seguro, se restauran los sistemas con las copias de seguridad. Se conserva un registro del ataque
- Aprendizaje: A lo largo de cada fase del incidente, se recopila la evidencia de la violación y documenta los pasos que toma para contener y erradicar la amenaza.

Indicadores de compromiso:

Son información sobre un fallo de seguridad que puede ayudar a determinar si se ha producido un ataque.

Los IoC pueden obtenerse a través de:

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

Hay varios tipos de IoC:

1. Los IoC Basados en archivos:
   Son como las "huellas" 👣 que dejan los archivos maliciosos en nuestros sistemas. Esto puede verse de diversas formas, como extensiones de archivo inusuales (por ejemplo, un documento de texto con la terminación ".exe" en lugar de ".docx"), nombres de archivo y ubicaciones sospechosas (como un archivo llamado "virus_peligroso.exe" 😳 guardado en una carpeta temporal), las "huellas digitales" únicas de los virus conocidas como hashes (que

permiten identificar un archivo malicioso específico), o incluso un cambio drástico en el tamaño de un archivo sin explicación lógica.

2. Los IoC basados en red:
   Estos se centran en las actividades sospechosas que ocurren durante la comunicación en nuestra red 🌐. Incluye: la identificación de direcciones IP maliciosas como nombres de dominio o URLs que parecen fraudulentas o que se sabe que distribuyen software malicioso
   Ejemplo: Un aumento repentino y sin motivo aparente en la cantidad de información que entra o sale de nuestra red también puede ser un IoC de este tipo.
3. Los IoC de comportamiento
   Estos se fijan en las acciones extrañas tanto de nuestros sistemas como de los usuarios 🕵️. Algunos ejemplos serían:
   - Múltiples intentos fallidos de iniciar sesión en una cuenta
   - La actividad inusual de un empleado accediendo a archivos importantes fuera de su horario laboral habitual sin justificación
   - Los bloqueos inesperados de ordenadores o servidores
   - Las conexiones de red con servidores ubicados en países desconocidos
   - Un programa que de repente comienza a consumir una cantidad excesiva de memoria del sistema
4. Los IoC basados en registros
   Estos se refieren a modificaciones sospechosas en el "registro" de Windows, una base de datos que almacena la configuración del sistema operativo. Por ejemplo, la eliminación de claves importantes 🔐 dentro de este registro o la aparición de valores de registro inusuales pueden ser indicios de un ciberataque.
5. Los IoC basados en host
   Son los que abarcan cualquier cambio sospechoso que se realice en la configuración general de un ordenador 🖥️ o servidor (el "host"), así como en los permisos de acceso a los archivos y en los procesos que se están ejecutando en el sistema 🪪.

Fuente -> https://www.manageengine.com/latam/blog/general/que-son-los-ioc-en-ciberseguridad.html

Estrategias proactivas:

Se trata en anticipar, prevenir y mitigar las ciberamenazas. Se hace 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

Análisis forenses: Es una técnica de seguridad pasiva (porque se usa después de tener el problema) y física/lógica (físico=hardware, lógico=software) que se basa en el análisis de los dispositivos y rastro de uso de estos para saber que ha pasado y que no vuelva a pasar. La parte lógica se basa en revisar los logs (lo escribe el servidor web) y de la trazabilidad (traza= la aplicación web también apunta cosas).

Casos reales:

AWS: https://www.computing.es/infraestructuras/fallo-aws-20-octubre-2025-gran-corte-nube/

Tema 4: Herramientas y tecnologías de aplicación.

Cortafuegos

Programa especializado en limitar/impedir que ordenadores que están en redes distintas se comuniquen.

Cortafuegos: basados en red y cortafuegos basados en host

Los cortafuegos basados en red son los proxys de la capa de aplicación. Son cortafuegos que escuchan las peticiones, más allá de revisar una serie de reglas preestablecidas. Hay un tipo de proxy que guarda toda la información sin avisarte. Se llama proxy transparente

Los cortafuegos basados en host funcionan en un solo dispositivo dentro de una red. Complementan las soluciones perimetrales. Esto hace que, aunque superen las defensas de red primarias y generales, cada ordenador permanezca blindado.

IDS/IPS

IDS: (Puede ser tanto hardware como software). Utiliza firmas de intrusión conocidas para analizar el tráfico de red entrante y saliente en busca de actividades anormales.

Un IDS puede expulsar a un usuario, pero también tiene sus inconvenientes como que las amenazas 0 Day pueden ser desapercibidas al no tener todavía la firma atacante. Además, solo detecta ataques continuos

IPS: Complementa la configuración IDS mediante la inspección proactiva del tráfico entrante. Evita ataques al descartar paquetes maliciosos, bloquear IPs y alerta al personal de seguridad. Algo negativo que tienen que es son excesivamente dependientes de las reglas predefinidas, pudiendo dar falsos positivos.

Antivirus

Es seguridad activa cuando te avisa que un fichero podría tener un virus.

Es pasiva cuando detecta que ya tenemos un virus haciendo cosas maliciosas.

Una de las 3 patas del control de acceso la cual se ocupa de defender al dispositivo de los programas que estén dentro del mismo. Es decir, nos defiende de los virus que ya tenemos instalados.

Antimalware

El antimalware está diseñado para combatir una gama más amplia de malware que el antivirus, como, por ejemplo, contra spyware, ransomware o troyanos.

Identifica y elimina amenazas de malware mediante la detección basada en firmas y el análisis de comportamiento.

Protege en tiempo real al escanear constantemente tu dispositivo.

Tema 5: Normativa y buenas prácticas de uso.

Reglamento General de Protección de Datos (RGPD).

El Reglamento General de Protección de Datos (RGPD) es una normativa europea que trata de regular el tratamiento de datos personales para proteger la privacidad de los derechos de las personas. Establece obligaciones para las empresas sobre cómo gestionar dichos datos personales, así como otorgando más control a los individuos sobre su información

ISO/IEC 27001.

La ISO/IEC 27001. es la norma internacional más conocida para sistemas de gestión de la seguridad de la información. A todos los tipos de empresas les interesa implementar esta norma, independientemente de su tamaño o actividad. El factor clave para decidir sobre la implantación de un sistema de gestión de la seguridad de la información radica en la importancia que los activos de información tienen dentro de una organización como elementos imprescindibles para la obtención de sus objetivos.

Enlace con la norma española:
https://www.industriaconectada40.gob.es/difusion/Documents/Documento_Norma_UNE-EN_ISO-IEC_27001%20MINTUR.pdf

Esquema Nacional de Seguridad (ENS)

El Esquema Nacional de Seguridad es una normativa cuyo objetivo es establecer la política de seguridad en el uso de los medios electrónicos relacionados con la administración pública. Se definen cinco dimensiones de seguridad: Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad.

Clasificación de datos sensibles

Datos personales que se consideran sensibles según la Unión Europea:

- Origen racial o étnico
- Opiniones políticas
- Convicciones religiosas o filosóficas
- Afiliación social
- Datos genéticos, datos biométricos tratados únicamente para identificar un ser humano
- Datos relativos a la salud
- Datos relativos a la vida sexual o su orientación sexual

Cuáles son las condiciones en las que las empresas pueden tartar mis datos sensibles

- Con consentimiento explícito
- Se exige (en virtud de una ley europea o nacional o un convenio colectivo) tratar los datos para cumplir sus obligaciones y derechos en el ámbito laboral, de la seguridad social y la legislación sobre la protección social
- Los intereses vitales de una persona están en peligro
- Es un organismo sin ánimo de lucro.
- La persona ha hecho manifiestamente públicos los datos personales
- Para la formulación, ejercicio o defensa de las reclamaciones
- Son de interés público esencial
- Trata los datos para alguno de los fines siguientes: medicina preventiva u ocupacional; evaluación de la capacidad de trabajo del empleado; diagnóstico médico; prestación de servicios médicos, asistencia social o tratamientos, o la gestión de sistemas sanitarios o de asistencia social sobre la base del Derecho de la Unión o nacional, o sobre la base de un contrato como profesional sanitario.
- Trata los datos por razones de interés público en el ámbito de la salud pública sobre la base del Derecho de la UE o nacional.
- Trata los datos para fines de archivo, investigación científica o histórica o para fines estadísticos sobre la base del Derecho de la UE o nacional.

Puedes consultar ejemplos en el siguiente enlace.

https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data_es

Políticas de acceso

Es una combinación de reglas que controla quien puede acceder a que recursos y sobre qué condiciones. Su idea es que los usuarios solo accedan a la información que les corresponda. Una forma de hacerlo es con el control de acceso basado en roles.

Ciclo de vida de la información

Los datos pasan por diferentes etapas, desde su creación hasta su borrado

1. Creación de datos: Los datos se crean o se introducen en el sistema

2. Almacenamiento: Se almacenan de forma segura y organizada en sistemas de almacenamiento, bases de datos u otros repositorios
3. Procesamiento y análisis: Etapa para extraer información valiosa. Se usan técnicas como la minería de datos o el aprendizaje automático para descubrir patrones, tendencias y conocimientos
4. Distribución de acceso: Una vez analizados, los datos se entregan mediante informes o aplicaciones
5. Retención y copia de seguridad: En esta etapa se determina cuánto tiempo se debe conservar la información, además de hacerse copias de seguridad para garantizar que no se pierden los datos en caso de fallo técnico o sucesos inesperados
6. Archivado y gestión de datos históricos: Cuando los datos ya no son usados en el día a día se archivan, permitiendo su recuperación si fuera necesario
7. Eliminación segura: Los datos obsoletos deben eliminarse de forma segura para evitar riesgos de seguridad y cumplir con las normativas de seguridad. Se eliminan de forma que no se puedan volver a recuperar

Diagnóstico de fallos

El diagnóstico de fallos es el proceso sistemático para identificar y localizar la causa de un problema en el sistema.

- **Detección:** Se verifica si se ha producido un fallo en el sistema.
- **Aislamiento:** Se localiza el componente específico dentro del sistema donde ocurrió la falla.
- **Estimación:** Se determina la gravedad o magnitud del fallo.

Propuestas de mejora

Las propuestas de mejora son planes de acción para optimizar un proceso, servicio o sistema basado en identificar problemas y oportunidades para mejorar la eficiencia y la calidad

Registro de incidencias

Un registro de incidencias es un sistema para documentar problemas, incidentes o eventos inesperados.

Elementos clave que debe incluir el registro:

- Identificacion: nombre del proyecto
- Datos del incidente: fecha, hora y lugar exacto
- Descripción: Narración **detallada** de los hechos, en su secuencia cronológica
- Tipo de incidencia
- Personas involucradas
- Acciones tomadas
- Seguimiento y solución: Anotar las acciones realizadas para resolver el problema por completo

Glosario Incibe

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

OWASP

Open Web Application Security Project

https://owasp.org/