2025

FUNDAMENTOS DE CIBERSEGURIDAD

ALEJANDRO DE LA HUERGA FERNANDEZ

GLOSARIO

29-10-2025

Contenido

INTRODUCCIÓN 2

GLOSARIO: 3

1. Amenazas y Vulnerabilidades informáticas. 3
2. Medidas de protección básicas. 8
3. Análisis de los incidentes de seguridad 11
4. Herramientas y tecnologías de aplicación 13
5. Normativa y buenas prácticas de uso 16

INTRODUCCIÓN

El siguiente documento es un glosario con los términos básicos necesarios para entender la base de la ciberseguridad y todos aquellos términos necesarios a la hora de introducirse en esté área de la tecnología.

Al final del documento se aportara toda la información necesaria sobre la obtención de información e imágenes además de algunos recursos de interés para todos aquellos que necesiten más información.

Los términos serán organizados en temas para así poder mantener la organización a lo largo del mismo.

GLOSARIO:

1. Amenazas y Vulnerabilidades informáticas.

- **Amenazas:** Cualquier situación o caso que pueda tener consecuencias negativas para las operaciones, funciones, marca, reputación o imagen percibida de una empresa (son externas a nosotros).

- **Vulnerabilidades:** Una vulnerabilidad es un fallo técnico o deficiencia de un programa que puede permitir que un usuario no legitimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota (son internas , un punto débil propio).

https://www.youtube.com/watch?v=VkS56Zz-iEo

Video sobre malware del Instituto Nacional de Ciberseguridad.

LA TRIADA CIA *(Confidentiality – Integrity – Availability)*

- **Confidencialidad:** Protección de la información sensible de modo que solo sea visible para aquellos que tienen permiso para verla, su objetivo es evitar el acceso no autorizado.

- **Disponibilidad:** Garantizar que los sistemas, redes y datos estén accesibles para los usuarios autorizados cuando los necesiten, su objetivo es asegurar el acceso ininterrumpido de la información.

- **Integridad:** Mantener la precisión, consistencia y fiabilidad de la información a lo largo de todo su ciclo de vida, su objetivo es prevenir la alteración o eliminación de la información no autorizada.

- **Malware:** cuya principal característica es que se ejecuta sin el conocimiento ni autorización del propietario o usuario del equipo infectado y realiza funciones en el sistema que son perjudiciales para el usuario y/o para el sistema.

  https://youtu.be/11Ww1WF0-0s

  Video sobre malware del Instituto Nacional de Ciberseguridad.

- **Ingeniería social:** La ingeniería social es el conjunto de técnicas de manipulación psicológica que los ciberdelincuentes utilizan para engañar a las personas y obtener información confidencial, acceso a sistemas o que realicen acciones en su perjuicio. A diferencia de los ataques técnicos, la ingeniería social se basa en el comportamiento y la psicología humana para explotar la confianza o la urgencia, haciendo que la víctima revele datos.

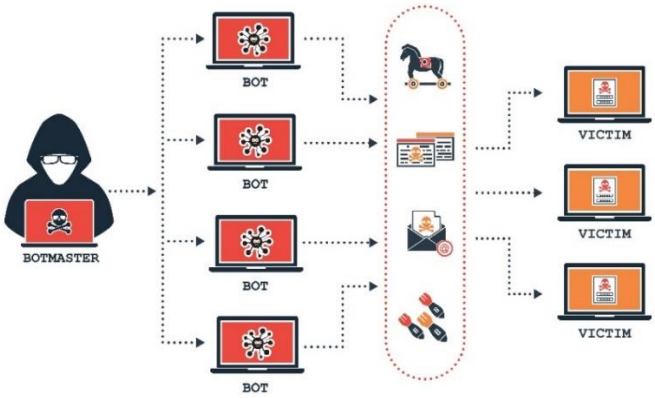
ATAQUES A LA RED:

- **DoS:** Un ataque de denegación de servicio, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado.

  Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.

  En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP.

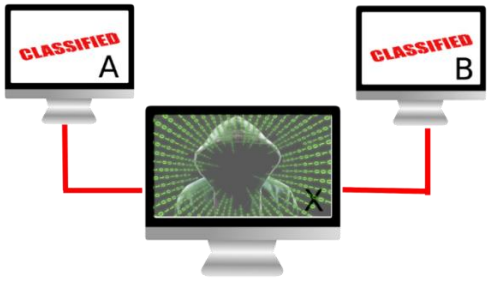
- **DDos:** Este tipo de ataque de denegación de servicios en cuanto a la base es exactamente igual que el ataque DoS, pero en este caso los ataques DDoS, se realizan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP.



https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos

Articulo interesante del "incibe" sobre los ataques de denegación de servicios.

- **Man-in-the-Middle:** Consiste en interceptar la comunicación entre 2 o mas interlocutores , por ejemplo la comunicación entre el cliente y el servidor , el anónimo se colocara en el medio de la comunicación conociendo la información y haciendo que transcurra con normalidad.



https://share.google/e3WV40wDXEN1lJ7ba

Video explicativo de manera gráfica de en que consiste un ataque Man-in-the-middle.

- **Exploits:** Programa informático o parte de un software que aprovecha un error o una vulnerabilidad como bien indica su nombre en inglés para explotarla.

A tener en cuenta tenemos el programa Metasploit un proyecto de código abierto para la seguridad informática que proporciona información acerca de vulnerabilidades.

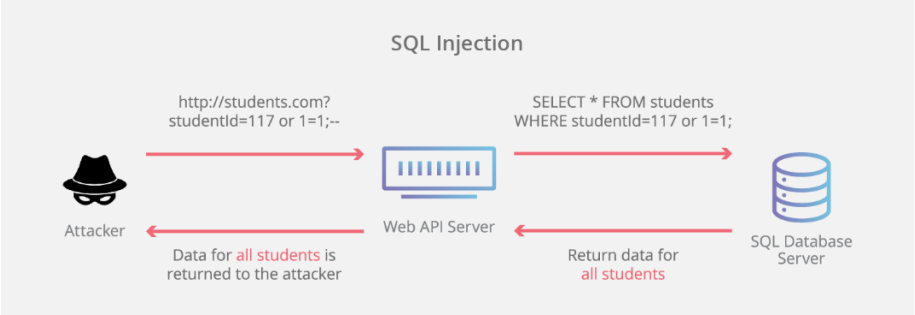
Web Oficial:

https://www.metasploit.com/

- **Inyección SQL:** Tipo de ataque mediante el cual los cibercriminales intentan explotar vulnerabilidades en el código de una aplicación mediante una consulta SQL en campos de entrada o formularios regulares.

Video de realización de inyección SQL en entorno controlado:

https://share.google/jLPyfi3okTSjomo3A



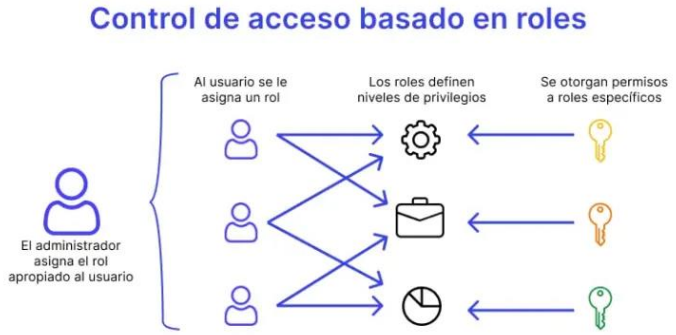
- **Cross-Site Scripting (XSS):** Tipo de ataque que aprovecha fallas de seguridad de los sitios web y que permite a los atacantes implementar scripts maliciosos en el sitio web (también víctima del atacante) para ejecutarlo en el navegador del usuario que ingresa a dicha web.

2. Medidas de protección básicas.

- **Autenticación Multifactor (MFA):** Capa de seguridad que exige dos o mas pruebas de identidad para acceder a una cuenta, en lugar de solo una contraseña, utilizando diferentes categorías de factores (huella digital, reconocimiento facial).

- **Roles:** Conjuntos de permisos que se agrupan y se asignan a usuarios o grupos. Por ejemplo, los roles de “administrador”, ”usuario” o “auditor”.
  Los roles definen distintos niveles de acceso y capacidades.

- **Permisos:** Son las acciones especificas que un rol puede realizar, como leer, escribir, ejecutar o modificar un recurso.



- **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. Las reglas pueden ser para permitir todo, denegar todo, permitir accesos específicos o denegar accesos específicos.

Para crear una regla, se definen condiciones (como IP, puerto, aplicación) y una acción (permitir o denegar) que el firewall aplicará cuando el tráfico coincida con esas condiciones.

- **Filtrado de puertos y protocolos:** técnica de seguridad de red que bloquea o permite el paso de paquetes de datos basándose en los números de puerto y los protocolos (como TCP o UDP) que utilizan.

FUNCIONAMIENTO:

1. **Inspección de paquetes:** Los dispositivos de seguridad (firewalls) examinan los paquetes de datos entrantes y salientes.

2. **Basado en reglas:** Se aplican reglas predefinidas para determinar si un paquete debe ser permitido o bloqueado.

3. **Criterios de filtrado:** Basados en puertos, protocolos y direcciones IP.

- **Router:** Es un dispositivo que conecta tu red doméstica (LAN) a Internet (WAN), actuando como un centro de distribución para el tráfico de datos. Su función principal es recibir la conexión de Internet (generalmente a través de un módem) y dirigir los paquetes de datos hacia los dispositivos adecuados, como ordenadores, teléfonos...
  Es crucial en ciberseguridad funciona como la primera línea de defensa de una red, controlando el tráfico de datos entre Internet y los dispositivos locales.

- **Monitoreo:** El monitoreo en ciberseguridad es la vigilancia constante y el análisis de redes, sistemas y dispositivos para detectar y responder a amenazas en tiempo real. Este proceso utiliza herramientas como firewalls y sistemas de detección de intrusiones, apoyándose en la labor de especialistas para identificar actividades sospechosas, vulnerabilidades y patrones inusuales.

- **Auditoria:** Una auditoría es un proceso que consiste en revisar y evaluar cómo se protegen los equipos, sistemas y datos. Esta trata de detectar cuáles son los fallos de seguridad informática, generalmente en una empresa, ya sea en sus sistemas, redes o aplicaciones que podrían aprovechar los atacantes.

TIPOS DE AUDITORIAS:

1. **Auditorias de vulnerabilidades:** Se centran en identificar puntos débiles en los sistemas.
2. **Auditorias de código:** Analizan el código fuente de las aplicaciones para detectar fallos en la aplicación.
3. **Auditorias de redes:** Evalúan la configuración de la infraestructura de red.
4. **Auditorias forenses:** Se realizan después de un incidente para evaluar que ocurrió.
5. **Auditorias de hacking ético:** consisten en simular ataques reales para encontrar debilidades antes que los ciberdelincuentes.

INCIBE Articulo sobre las Auditorías

El artículo sobre auditorias de la INCIBE es muy completo y aporta información de mucho valor.

3. Análisis de los incidentes de seguridad

- **Incidentes de seguridad:** Cualquier evento que compromete la confidencialidad, integridad o disponibilidad de la información o los sistemas informáticos, como la pérdida de datos, accesos no autorizados o interrupciones del servicio.

- **Ciclo de vida de un incidente (detección, análisis, contención, erradicación, recuperación y aprendizaje):**

    1. **Detección:** Suele comenzar con herramientas de supervisión y alertas. aunque a veces la primera noticia de un incidente puede llegar por cualquier otro medio.
    2. **Análisis:** Recopilar información para comprender el alcance y la gravedad y el impacto del incidente.
    3. **Contención:** Contener el incidente para evitar daños mayores aislando los sistemas afectados y bloqueando el tráfico malicioso.
    4. **Erradicación:** Tome medidas correctivas para resolver el incidente, incluida la erradicación del malware y la restauración de datos.
    5. **Recuperación:** Restaurar las operaciones normales verificando la funcionalidad del sistema y restableciendo las operaciones comerciales normales.
    6. **Aprendizaje:** Identificar las causas fundamentales del incidente y actualizar el plan de respuesta al incidente en consecuencia.

- **Indicadores de compromiso (IoC):** Son pistas o pruebas forenses que señalan una posible actividad maliciosa en sistemas o redes, ayudando a los equipos de ciberseguridad a detectar y responder a un incidente, los indicadores pueden incluir direcciones IP maliciosas, firmas de malware…

- **Estrategias proactivas:**

    1. **Mantener el software actualizado:** Tener todos los sistemas operativos y aplicaciones actualizados.
    2. **Usar software de seguridad:** firewalls, antimalware…
    3. **Cifrar la información:** Proteger la información confidencial.
    4. **Implementación de control de acceso**
    5. **Gestión de contraseñas.**

- **Análisis forense:** Medida de ciberseguridad pasiva, física y pasiva la cual investiga y reconstruye los incidentes de ciberseguridad mediante la recopilación, el análisis y la preservación de pruebas digitales, es decir los rastros que dejan los actores de las amenazas.

ENLACES DE INTERES:

INCIBE portal de Análisis Forense

En el siguiente enlace se pueden encontrar distintas noticias y apartados relacionados con el análisis forense y casos reales de ciberseguridad.

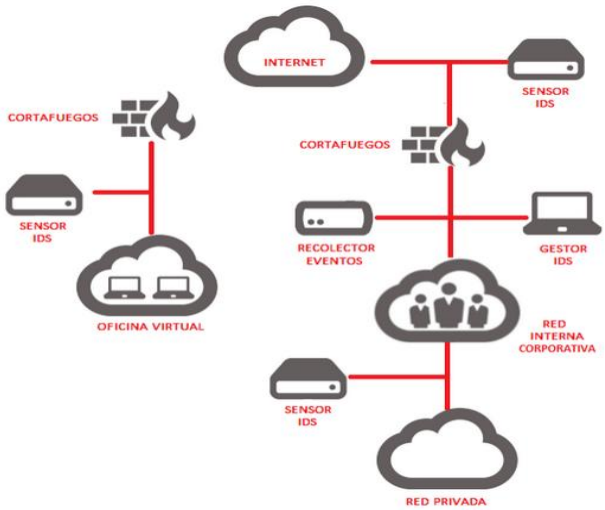
4. Herramientas y tecnologías de aplicación

- **Proxy:** Es un cortafuegos que para tomar la decisión de si decide darte paso o no, comprueba la información que quieres comunicar. Cuando el proxy esta en el lado del servidor su función es proteger el servidor (Reverse proxy).

- **Router:** Dispositivo especializado en comunicar.

- **Cortafuegos:** Un cortafuegos es un sistema de seguridad de red, tanto de hardware como de software, que actúa como una barrera entre una red interna de confianza y redes externas no confiables, como Internet. Su función principal es supervisar y filtrar el tráfico de red entrante y saliente según reglas predeterminadas para prevenir accesos no autorizados.

- **IDS/IPS:** Ambos son sistemas de protección de las comunicaciones que actúan monitorizando el tráfico que entra o sale de nuestra red, pero cada uno tiene unas características que les confieren ventajas e inconvenientes.



Esta imagen ha sido obtenida de la página web de INCIBE.

IDS: Sistema de detección de intrusos, es una aplicación utilizada para detectar **accesos no autorizados** a un ordenador o una red, son sistemas que monitorizan el tráfico entrante. Ante cualquier actividad sospechosa **emiten una alerta. No tratan de mitigar la intrusión** (Su actuación es reactiva).

IPS: Sistema de prevención de intrusiones: es un software que se utiliza para **proteger a los sistemas de ataques e intrusiones.** Llevan a cabo un análisis real

de las conexiones y los protocolos para determinar si se va a producir un incidente. **IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.**

ENLACE DE INTERES: Blog de INCIBE sobre SIEM, IPS, IDS

- **Antivirus:** Son programas de software diseñados para detectar, prevenir y eliminar malware como troyanos, gusanos, spyware y otras amenazas informáticas que pueden comprometer la seguridad de los dispositivos. **Proporcionan una defensa activa y constante.**

  ENLACE DE INTERES: Articulo de INCIBE sobre Antivirus

- **Tipos de Cortafuegos:** Los cortafuegos se pueden dividir en dos tipos:

  a. **Basados en Host:** Un firewall basado en host se instala en cada **dispositivo individual** (PC, servidor, etc.). Controlan el tráfico saliente y entrante de ese dispositivo en particular, estos firewall son parte del sistema operativo o son aplicaciones independientes.

  b. **Basados en Red:** Un firewall de red opera a nivel de red, filtrando y controlando el tráfico de **todos los dispositivos** conectados a una red. Normalmente, estos firewalls están implementados en routers, switches o dispositivos de seguridad dedicados. **Algunos ejemplos son:**

     Cisco ASA: Software que protege redes corporativas.

     SonicWall: Se usa para filtrar tráfico en pequeñas y medianas empresas.

     pfSense en modo router/firewall: Controla el tráfico de una red doméstica.

     ENLACE DE INTERES: Apuntes de sistemas y redes de gitbook

- **Diferencias entre IDS Y IPS:** La diferencia principal es que un **IDS** (Sistema de Detección de Intrusiones) **detecta y alerta sobre actividades sospechosas**, mientras que un **IPS** (Sistema de Prevención de Intrusiones) **detecta, alerta y,**

además, actúa automáticamente para bloquear o mitigar la amenaza en tiempo real. Un IDS es un sistema pasivo que requiere intervención humana, mientras que un IPS es un sistema activo que previene el ataque activamente.

- **Antimalware:** Es un software implementado en ciberseguridad esencial que protege sistemas y dispositivos de software malicioso como virus, ransomware y spyware, detectando, previniendo y eliminado amenazas en tiempo real.

Como funciona:

a. **Detección:** Utiliza detección basada en firmas.
b. **Prevención:** Bloquea el acceso a sitios web peligrosos.
c. **Eliminación:** Escanea continuamente el sistema.

Su papel en ciberseguridad:

a. **Protección integral:** Los programas antimalware están diseñados para combatir una gama más amplia de amenazas que los antivirus tradicionales.
b. **Línea de defensa:** Es una de las principales líneas de defensa contra ciberamenazas.
c. **Complemento a otras herramientas:** Aunque es fundamental, no es una solución única.

ENLACE DE INTERES: Articulo comparativo de Revisa Ciberseguridad

5. Normativa y buenas prácticas de uso.

- **Reglamento General de Protección de Datos (RGPD):** Exige medidas de ciberseguridad para proteger los datos personales contra accesos no autorizados, pérdida o alteración. No impone un conjunto específico de tecnologías, sino que requiere que las organizaciones implementen medidas técnicas.

- **ISO/IEC 27001:** Normal internacional la cual establece los requisitos para un Sistema de Gestión de la Seguridad de la información. Su propósito es ayudar a las organizaciones a gestionar la seguridad de los datos.

- **Esquema Nacional de Seguridad (ENS):** Marco normativo español que establece la política de seguridad para el uso de medios electrónicos en la administración pública y sus proveedores.

- **Datos sensibles:** Organizar la información según su nivel de confidencialidad para aplicar controles de seguridad adecuados, usando categorías como ***Público, Uso interno, Restringido y Confidencial/Altamente Confidencial.***

- **Políticas de acceso:** Combinación de reglas que controla el acceso de los usuarios a un recurso verificado, basándose en condiciones definidas, incluido si es necesario la autenticación del segundo factor (2FA).

  ENLACE DE INTERES: Articulo de IBM sobre políticas de acceso

- **Ciclo de vida de la información:** Conjunto de procesos y prácticas diseñadas para adquirir, organizar, almacenar, recuperar, proteger y utilizar la información de manera eficiente.

  Fases del ciclo de vida:

  - **Creación:** Es el punto de partida del ciclo de vida de la información, en esta fase los datos son recopilados o generados por primera vez.
  - **Almacenamiento:** Esta es una etapa esencial, una vez han sido creados es necesario almacenarlos de manera segura y accesible.
  - **Gestión:** Los datos almacenados son accesibles y utilizados por los usuarios autorizados dentro de la organización.
  - **Entrega y publicación:** La capacidad de compartir de manera segura y eficiente es fundamental.
  - **Eliminación:** Aquí la información llega al final de su ciclo de vida y se elimina de manera segura y definitiva.

- **Diagnostico de fallos:** Proceso el cual implica un proceso sistemático para identificar vulnerabilidades y riesgos en sistemas, redes y aplicaciones, que incluye la revisión de configuraciones, análisis de vulnerabilidades y pruebas de penetración. El objetivo es detectar debilidades antes de que sean explotadas.

- **Propuesta de mejora:** Una propuesta de mejora en ciberseguridad debe incluir la capacitación del personal en concienciación sobre amenazas como el phishing, la implementación de medidas técnicas como la autenticación de doble factor.

- **Registro de incidencias:** Es un proceso para detectar, responder y recuperarse de eventos de seguridad, minimizando el impacto en la organización. Para registrar una incidencia se puede contactar con el centro de empresa del **INCIBE.**

Registro de incidentes

ID de incidente	[illegible]	Fecha y hora		[illegible]
		Fecha	Hora	
2020_1	[illegible]	7/1/2020	4:55:00 PM	[illegible]
		7/5/2020	10:45:00 AM	
		7/5/2020	11:28:00 AM	
2020_2	[illegible]	7/5/2020	11:21:00 AM	[illegible]

Ejemplo de un documento de registro de incidentes.

ULTIMA ACTUALIZACIÓN: 29/10/2025