Introducción a la ciberseguridad

1. Introducción a la ciberseguridad.

1.1. El Mundo de la Ciberseguridad.

1.1.1. ¿Qué es la Ciberseguridad?

La **ciberseguridad** es el **conjunto de prácticas, tecnologías y procesos aplicados de forma continua** para proteger a personas, organizaciones y gobiernos frente a **ataques digitales**, garantizando la **seguridad de los sistemas informáticos y de los datos en red** frente a accesos, usos, alteraciones o daños no autorizados.

La ciberseguridad actúa en distintos niveles:

- **Nivel personal**: protege la identidad digital, los datos personales y los dispositivos informáticos de los usuarios.
- **Nivel organizacional**: es una responsabilidad compartida dentro de la empresa y tiene como objetivo proteger la información, los clientes, los sistemas y la reputación de la organización.
- **Nivel gubernamental**: adquiere una importancia crítica, ya que la protección de la información digital está directamente relacionada con la seguridad nacional, la estabilidad económica y el bienestar de los ciudadanos.

1.1.2. Protegiendo su Data Personal

Los **datos personales** son cualquier información que permite **identificar directa o indirectamente a una persona**, y pueden existir tanto **fuera de línea** como **en línea**. Su protección es fundamental para evitar fraudes, suplantaciones de identidad y otros delitos digitales.

Identidad fuera de línea

La **identidad fuera de línea** corresponde a la persona en el mundo físico y a la información que se comparte en entornos cotidianos como el hogar, la escuela o el trabajo. Incluye datos como el nombre completo, la edad, la dirección u otros detalles personales conocidos por familiares, amigos o compañeros.

La protección de esta identidad es esencial, ya que los delincuentes pueden obtener información personal mediante descuidos, documentos físicos o interacciones cotidianas.

Identidad en línea

La **identidad en línea** representa cómo una persona se muestra y se relaciona en Internet. Incluye los nombres de usuario, alias, perfiles digitales y la identidad social que se construye en plataformas, comunidades y sitios web.

Es fundamental **limitar la información personal compartida en línea**, ya que un exceso de datos públicos facilita la suplantación de identidad y otros ataques basados en ingeniería social.

1.1.3. Su Data

Los **datos personales** comprenden cualquier información que describe o permite identificar a una persona. Incluyen, entre otros, el nombre, número de identificación oficial, fecha y lugar de nacimiento, datos familiares, así como fotografías, mensajes y comunicaciones privadas.

El uso indebido de estos datos por parte de ciberdelincuentes puede dar lugar a **suplantación de identidad**, violaciones de la privacidad y **daños graves a la reputación personal y profesional**.

Los datos personales pueden clasificarse en las siguientes categorías:

- **Registros médicos**

Los **registros médicos** contienen información sensible sobre la salud física y mental de una persona y su bienestar general. Actualmente, gran parte de estos datos se almacenan en **registros médicos electrónicos (EHR)**, lo que incrementa la necesidad de protegerlos adecuadamente.

Además, dispositivos y aplicaciones de monitorización de la salud, como relojes inteligentes o monitores de actividad física, recopilan datos clínicos (frecuencia cardíaca, presión arterial, niveles de glucosa, entre otros) que se almacenan y procesan en la nube, formando parte del historial médico digital del usuario.

- **Registros educativos**

Los **registros educativos** incluyen información académica como calificaciones y logros, así como datos personales asociados, tales como información de contacto, asistencia, informes disciplinarios, datos de salud, vacunación y, cuando corresponda, información relacionada con programas de educación especial.

- **Registros laborales y financieros**

Los **registros laborales** pueden contener información sobre empleos anteriores, puestos desempeñados y evaluaciones de rendimiento, datos que pueden resultar de alto valor para los ciberdelincuentes.

Los **registros financieros** incluyen información sobre ingresos, gastos, cuentas bancarias, tarjetas de crédito, historial crediticio y declaraciones fiscales. La falta de protección de estos datos puede permitir fraudes económicos y otros delitos financieros.

1.1.4. ¿Dónde están sus datos?

Los **datos personales** no permanecen únicamente en los dispositivos del usuario. Cada vez que se crean, almacenan o comparten, pueden **replicarse y distribuirse automáticamente** a través de múltiples dispositivos, sistemas y ubicaciones geográficas.

Por ejemplo, al capturar una imagen con un dispositivo móvil, los datos se almacenan localmente en el equipo. Al compartirla con otras personas, se generan **copias adicionales** en los dispositivos de los destinatarios. Si posteriormente estos datos se publican en Internet o en redes sociales, pasan a almacenarse en **servidores remotos**, generalmente ubicados en distintos países y gestionados por terceros.

Como consecuencia, el usuario **pierde el control directo** sobre sus datos, que pueden quedar accesibles para personas no autorizadas y sujetos a políticas de uso, almacenamiento y protección ajenas a su voluntad.

1.1.5. ¿Que más hay?

Cada vez que se **recopilan, almacenan o comparten datos personales**, es necesario considerar los **riesgos asociados a la privacidad y la seguridad de la información**. Aunque existen leyes y normativas que protegen los datos personales, el usuario debe ser consciente de **quién tiene acceso a sus datos, con qué finalidad y dónde se almacenan**.

En muchos casos, los datos personales se comparten con **terceros** como parte de procesos legítimos, lo que incrementa su exposición y reduce el control directo del titular. Algunos ejemplos comunes incluyen:

- **Datos médicos**: tras una consulta, la información sanitaria se incorpora a la historia clínica y puede compartirse, total o parcialmente, con compañías aseguradoras para fines administrativos o de facturación.
- **Datos de consumo**: las tarjetas de fidelización permiten obtener beneficios comerciales, pero también se utilizan para recopilar y analizar hábitos de compra, creando perfiles de consumo que pueden compartirse con socios comerciales o utilizarse para marketing dirigido.

Por ello, la protección de los datos personales no depende únicamente de la legislación, sino también del **conocimiento y la responsabilidad del usuario** sobre el uso y la circulación de su información.

1.1.6. Dispositivos inteligentes

Los **dispositivos inteligentes** son equipos informáticos conectados a la red que permiten al usuario **acceder, gestionar y transferir datos personales** a través de aplicaciones y servicios digitales, como la banca electrónica, los pagos en línea o la consulta de información privada.

Además de facilitar el acceso a la información, estos dispositivos **recopilan y generan datos de manera continua** sobre el usuario. Tecnologías portátiles, como relojes inteligentes y dispositivos de seguimiento de actividad, registran información relacionada con la salud, el

estado físico y los hábitos diarios, que suele almacenarse y procesarse en **plataformas externas o servicios en la nube**.

El crecimiento del uso de dispositivos inteligentes y tecnologías portátiles **incrementa la superficie de ataque**, así como los riesgos para la **privacidad y la seguridad de los datos personales**, lo que hace imprescindible la adopción de medidas de protección adecuadas.

2. Ataques, Conceptos y Técnicas

2.1. Analizando un ciberataque

2.1.1. Tipos de malware:

Spyware:

El **spyware** es un tipo de software malicioso diseñado para **rastrear y monitorear la actividad del usuario** sin su consentimiento. Puede registrar pulsaciones de teclado, recopilar datos personales sensibles, como información bancaria, y capturar gran parte de la información almacenada en el dispositivo.

Generalmente, el spyware **modifica la configuración de seguridad del sistema** para operar de manera encubierta y a menudo se distribuye junto con software legítimo o mediante **troyanos**.

Adware:

El **adware** es un tipo de software diseñado para **mostrar anuncios de forma automática** en el dispositivo del usuario, normalmente a través de navegadores web. Su presencia se manifiesta mediante **ventanas emergentes o publicidad intrusiva** que puede afectar la experiencia del usuario.

A menudo, el adware se **instala junto con otro software** y puede estar vinculado a spyware, aumentando los riesgos de privacidad y recopilación de datos personales.

Puerta trasera:

Una puerta trasera es un tipo de malware que permite acceso no autorizado a un sistema al eludir los mecanismos de autenticación normales.

A través de ella, los atacantes pueden controlar remotamente aplicaciones o recursos del sistema, ejecutar comandos y manipular la información sin el conocimiento del usuario.

Las puertas traseras operan en segundo plano y son difíciles de detectar, lo que las convierte en una amenaza persistente para la seguridad de los sistemas.

Ransonware:

El **ransomware** es un tipo de malware que **secuestra sistemas o datos** hasta que se realiza un pago exigido por el atacante. Su método más común consiste en **cifrar los archivos del usuario**, impidiendo su acceso.

Algunas variantes pueden **explotar vulnerabilidades del sistema** para bloquear completamente el equipo. El ransomware se **propaga principalmente mediante correos electrónicos de phishing** con archivos maliciosos o mediante la explotación de fallos de seguridad en el sistema.

Scareware:

El **scareware** es un tipo de malware que utiliza **tácticas de miedo** para engañar al usuario y que realice acciones específicas. Generalmente se manifiesta mediante **ventanas emergentes falsas** que alertan sobre supuestos problemas de seguridad o fallos del sistema, instando al usuario a descargar o ejecutar un programa.

Si el usuario ejecuta el programa indicado, su sistema **se infecta con malware**, comprometiendo la seguridad y la privacidad de los datos.

Rootkit:

Un **rootkit** es un tipo de malware diseñado para **modificar el sistema operativo** y crear una **puerta trasera** que permita a un atacante **acceso remoto y persistente** al equipo.

La mayoría de los rootkits **aprovecha vulnerabilidades del software** para obtener privilegios elevados (escalada de privilegios) y **alterar archivos del sistema**. Además, pueden **deshabilitar o manipular herramientas de monitoreo y análisis forense**, lo que dificulta su detección.

En muchos casos, la **única forma segura de eliminar un rootkit** es **formatear el equipo y reinstalar el software** necesario desde cero.

Virus:

Un **virus** es un programa informático que, al ejecutarse, se **autorreplica y se inserta en otros archivos ejecutables**, incorporando su propio código. La mayoría requiere **interacción del usuario** para activarse y puede estar programado para ejecutarse en una **fecha u hora específica**.

Los virus pueden ser **inofensivos o destructivos**, afectando archivos, datos o sistemas completos. Algunos incluyen mecanismos de **mutación** para evitar la detección por software de seguridad.

Actualmente, los virus se propagan principalmente a través de **unidades extraíbles (USB, discos ópticos), recursos de red compartidos y correos electrónicos**.

Troyanos:

Un **troyano** es un tipo de malware que **realiza acciones maliciosas mientras oculta su verdadera intención**. Suele presentarse como un archivo o programa legítimo (por ejemplo, imágenes, audio o juegos) para **engañar al usuario y ejecutar software dañino**.

A diferencia de los virus, los troyanos **no se replican por sí mismos**, sino que dependen de la interacción del usuario para infiltrarse en el sistema y aprovechar sus privilegios.

Gusanos:

Un **gusano** es un tipo de malware que **se replica y se propaga de manera autónoma** entre computadoras, sin necesidad de un programa anfitrión ni de interacción del usuario.

A diferencia de los virus, los gusanos **pueden ejecutarse por sí mismos** y propagarse rápidamente a través de redes, aprovechando **vulnerabilidades del sistema**. Contienen una **carga útil maliciosa** diseñada para afectar sistemas o redes.

Los gusanos han sido responsables de algunos de los **ataques más rápidos y devastadores en Internet**, como el gusano *Code Red* en 2001, que infectó más de 300.000 servidores en solo 19 horas.

2.2. Métodos de infiltración.

2.2.1. Ingeniería Social

La **ingeniería social** es la manipulación de personas para que **realicen acciones o divulguen información confidencial** mediante técnicas engañosas, explotando la confianza o la urgencia percibida.

Algunos ejemplos de técnicas comunes incluyen:

- **Tailgating**: un atacante sigue a una persona autorizada para acceder a un área segura sin credenciales propias, aprovechando que la puerta se abre para el usuario legítimo.
- **Intercambio de beneficios**: el atacante ofrece incentivos, regalos o favores para que la víctima revele información valiosa.
- **Suplantación de identidad (pretexting)**: hacerse pasar por una entidad confiable, como una compañía telefónica o un banco, para solicitar datos personales bajo pretextos falsos.

El objetivo de la ingeniería social es **obtener acceso a información o sistemas sin recurrir a vulnerabilidades técnicas**, confiando en la interacción humana.

.

2.2.2. Denegación de servicio.

La **denegación de servicio (DoS)** es un ataque dirigido a **interrumpir o degradar el funcionamiento de un servicio o sistema** mediante acciones maliciosas. Puede ejecutarse incluso por atacantes sin conocimientos avanzados y se manifiesta principalmente de dos formas:

1. **Sobrecarga de tráfico**: el atacante envía un **volumen excesivo de datos** a un sitio o servidor, provocando que no pueda procesarlos, lo que resulta en **lentitud, interrupción parcial o caída del servicio**.

2. **Explotación de fallos en paquetes**: se envían **paquetes malformados o con errores** que el sistema no puede procesar correctamente, ralentizando aplicaciones o provocando fallos. Esto incluye paquetes que no cumplen las reglas estándar de protocolos como **IP, TCP, UDP o ICMP**.

El objetivo de un ataque DoS es **hacer inaccesible un servicio legítimo**, afectando a usuarios y sistemas sin necesidad de comprometerlos directamente.

2.2.3. DoS distribuido.

La **denegación de servicio distribuida (DDoS)** es un ataque similar al DoS, pero ejecutado de forma **coordinada desde múltiples fuentes** para aumentar su impacto y dificultar su mitigación.

El ataque se basa en una **botnet**, formada por dispositivos infectados, denominados **zombis**, que son controlados remotamente por el atacante. Estos equipos comprometidos pueden continuar infectando nuevos hosts, ampliando el tamaño de la botnet.

Cuando el atacante lo decide, envía instrucciones a los sistemas de control para que los dispositivos zombis **generen grandes volúmenes de tráfico o solicitudes maliciosas**, provocando la **saturación y caída del servicio objetivo**.

2.2.4. Botnet.

Una **botnet** es un conjunto de dispositivos infectados (**bots**) conectados a través de Internet y controlados por un atacante o grupo malintencionado. Puede abarcar desde decenas hasta **cientos de miles de equipos**, gestionados mediante un **servidor de comando y control (C&C)**.

Los dispositivos se infectan generalmente al **visitar sitios web comprometidos o abrir archivos maliciosos adjuntos en correos electrónicos**.

Las botnets se utilizan para fines delictivos como:

- **Distribución de malware**
- **Ataques de denegación de servicio (DoS/DDoS)**
- **Ataques de fuerza bruta a contraseñas**

En muchos casos, los ciberdelincuentes **alquilan botnets** a terceros para actividades ilícitas.

Existen herramientas de seguridad, como los **firewalls con detección de bots** (por ejemplo, Cisco), que permiten **filtrar tráfico malicioso, prevenir ataques y localizar dispositivos infectados**.

2.2.5. Ataques en el camino.

Un **ataque en el camino** o **Man-in-the-Middle (MitM)** ocurre cuando un atacante **intercepta la comunicación entre dos dispositivos**, como un cliente y un servidor, con el objetivo de **obtener información o suplantar a una de las partes**.

En estos ataques, el ciberdelincuente **controla un dispositivo o la conexión de red sin que el usuario lo perciba**, lo que le permite capturar datos sensibles antes de que lleguen a su destino. Esto se utiliza frecuentemente para **robo de información financiera, credenciales de acceso o datos personales**.

Una variante específica, conocida como **Man-in-the-Mobile (MitMo)**, afecta a **dispositivos móviles**. El malware en el dispositivo filtra información personal y la envía al atacante. Por ejemplo, paquetes de malware como **Zeus** interceptan silenciosamente **SMS de verificación en dos pasos** para vulnerar cuentas protegidas por autenticación multifactor.

2.2.6. Envenenamiento de SEO.

El **SEO malicioso** es una técnica en la que los atacantes **manipulan los motores de búsqueda** para que **sitios web maliciosos aparezcan en los primeros resultados**. El objetivo es **incrementar el tráfico hacia estos sitios**, exponiendo a los usuarios a malware, phishing u otras amenazas.

2.2.7. Descifrado de contraseña de WI-FI.

El **descifrado de contraseñas Wi-Fi** es un ataque mediante el cual un atacante **obtiene acceso no autorizado a una red inalámbrica privada**.

Los métodos más comunes incluyen:

- **Fuerza bruta**: probar sistemáticamente combinaciones de contraseñas hasta adivinar la correcta.
- **Rastreo de red (packet sniffing)**: interceptar y capturar los paquetes de datos transmitidos por la red.

Si la contraseña está cifrada, el atacante puede usar **herramientas de decodificación o cracking de contraseñas** para revelar la clave y acceder a la red.

2.2.8. Ataque de contraseñas.

Un **ataque de contraseñas** es un intento por parte de un ciberdelincuente de **obtener acceso no autorizado a cuentas de usuario** mediante la obtención o adivinanza de las credenciales (usuario y contraseña).

Las técnicas más comunes incluyen:

1. **Pulverización de contraseñas (Password Spraying)**: se prueban contraseñas comunes (por ejemplo, password123 o qwerty) contra múltiples nombres de usuario, evitando bloqueos frecuentes por intentos fallidos.
2. **Ataques de diccionario**: el atacante utiliza una lista de palabras comunes o previamente filtradas como posibles contraseñas para acceder a cuentas protegidas.

3. **Fuerza bruta (Brute Force)**: consiste en probar **todas las combinaciones posibles** de letras, números y símbolos hasta encontrar la contraseña correcta.
4. **Ataques de tabla arcoíris (Rainbow Table Attacks)**: las contraseñas no se almacenan en texto plano, sino como **hashes**. Una tabla arcoíris es un conjunto de **hashes precalculados y sus contraseñas originales**. El atacante compara los hashes de la base de datos con la tabla hasta encontrar coincidencias y descubrir la contraseña. Actualmente, el uso de **salts** (datos aleatorios añadidos antes de hashear) dificulta significativamente estos ataques.
5. **Interceptación de tráfico (Traffic Sniffing)**: si las contraseñas se transmiten o almacenan en **texto plano**, pueden ser capturadas por atacantes que monitorean la red o acceden a dispositivos comprometidos.

2.2.9. Tiempos de craqueo.

Un **ataque de fuerza bruta** consiste en **probar sistemáticamente todas las combinaciones posibles** para adivinar una contraseña. Este método puede usar **listas de palabras comunes** o intentar **todas las combinaciones de letras, números y símbolos** hasta encontrar la correcta.

Existen herramientas especializadas que automatizan este proceso, como **Ophcrack, L0phtCrack, Hydra, RainbowCrack y Medusa**.

La **eficacia del ataque** depende de la **longitud y complejidad de la contraseña**: cuanto más larga y compleja sea, más tiempo y recursos requerirá para descifrarla.

2.2.10. Amenazas persistentes avanzadas

Las **Amenazas Persistentes Avanzadas (APT)** son **campañas de ataque altamente sofisticadas**, sigilosas y **estructuradas en múltiples fases**, que se ejecutan **durante largos periodos de tiempo** contra un **objetivo específico**.

Debido a su complejidad técnica, planificación y necesidad de recursos, **una sola persona normalmente no dispone de las capacidades necesarias para llevar a cabo un APT**. Por ello, estos ataques suelen ser realizados por **grupos criminales altamente organizados** o **actores estatales**, con fines **económicos, estratégicos, militares o políticos**.

El objetivo principal de una APT es **comprometer uno o varios sistemas mediante malware personalizado**, **mantener el acceso de forma persistente** y **evitar la detección** el mayor tiempo posible, permitiendo el robo de información, el espionaje o el sabotaje continuo del sistema afectado.

2.3. Aprovechamiento de las vulnerabilidades de seguridad.

Exploit: Todo programa escrito con el fin de aprovecharse de una vulnerabilidad de un sistema se conoce como exploit.

2.3.1. Vulnerabilidades de hardware.

Las **vulnerabilidades de hardware** suelen surgir por fallos en el diseño físico de los componentes. Un ejemplo clásico es **Rowhammer**, descubierto cuando se observó que los condensadores de la RAM están tan próximos que alterar repetidamente (o "martillar") una fila de memoria puede provocar interferencias eléctricas y corromper los datos de las filas vecinas.

Meltdown y Spectre

Otro caso destacado son **Meltdown y Spectre**, vulnerabilidades reveladas por Google que afectan a la mayoría de CPUs fabricadas desde 1995, presentes en PCs, portátiles, servidores, móviles y servicios en la nube.
Estos ataques, considerados **ataques de canal lateral**, permiten acceder a información sensible:

- **Meltdown** puede leer toda la memoria del sistema.
- **Spectre** puede acceder a datos procesados por otras aplicaciones.

Ambas fallas son peligrosas porque pueden repetirse muchas veces sin causar fallos visibles en el sistema, lo que facilita la extracción masiva de datos.
En general, las vulnerabilidades de hardware son específicas de ciertos modelos o arquitecturas y suelen aprovecharse en ataques altamente dirigidos.

2.3.2. Vulnerabilidad de software.

Una **vulnerabilidad de software** es un **fallo o error en el sistema operativo o en el código de una aplicación** que puede ser **explotado por un atacante para comprometer un sistema**.

Un ejemplo es **SynFUL Knock**, que permitió a los atacantes **tomar el control de routers empresariales**, como los **Cisco ISR**, para **monitorear comunicaciones de red e infectar otros dispositivos**. Esta vulnerabilidad se originó cuando **se instaló una versión de IOS alterada** en los routers.

Para mitigar riesgos, se recomienda:

- **Verificar la autenticidad de las imágenes de software** antes de instalarlas.
- **Restringir el acceso físico a los dispositivos** únicamente a personal autorizado.
- Mantener el software **actualizado con parches oficiales** y buenas prácticas de configuración.

2.3.3. Categorización de vulnerabilidades de software.

La mayoría de las vulnerabilidades de seguridad del software se pueden clasificar en las siguientes categorías:

1. **Desbordamiento de búfer (Buffer Overflow)**
   Un búfer es un espacio de memoria reservado para una aplicación. La vulnerabilidad ocurre cuando se escriben más datos de los que puede contener, sobrescribiendo memoria adyacente. Esto puede causar **fallos del sistema, robo de datos o permitir que un atacante obtenga control adicional sobre el sistema**.

2. **Entrada no validada (Improper Input Validation)**
   Se produce cuando una aplicación acepta datos sin verificar su **validez, formato o seguridad**. Esto permite que un atacante envíe información malformada, como una imagen con dimensiones manipuladas, provocando **fallos, ejecución inesperada de código o vulnerabilidades explotables**.

3. **Condiciones de carrera (Race Conditions)**
   Surgen cuando dos o más procesos dependen de un **orden específico de ejecución**. Si ese orden se altera —por ser demasiado rápido, lento o fuera de secuencia— el sistema puede comportarse de forma inesperada, generando **fallos o vulnerabilidades que un atacante puede aprovechar**.

4. **Debilidades en prácticas de seguridad (Security Misconfigurations / Weak Practices)**
   Los sistemas y datos confidenciales requieren **autenticación, autorización y cifrado adecuados**. Los desarrolladores deben utilizar **bibliotecas y algoritmos de seguridad probados y verificados**, evitando crear sus propios métodos, ya que esto aumenta la probabilidad de generar nuevas vulnerabilidades.

5. **Problemas de control de acceso (Access Control Issues)**
   El control de acceso regula quién puede usar qué recursos y qué acciones puede realizar (lectura, modificación o eliminación de archivos, acceso físico, etc.).

   - Una **configuración incorrecta** es un riesgo importante.
   - Incluso con controles estrictos, un **acceso físico no autorizado** puede permitir eludir el sistema operativo y acceder directamente a los datos.
     Por ello, además de configurar correctamente los permisos, es crucial **restringir el acceso físico y usar cifrado** para proteger la información de robo o manipulación.

2.3.4. Actualizaciones de software

Las **actualizaciones de software** son parches y mejoras lanzados por desarrolladores para **corregir vulnerabilidades, errores y mantener los sistemas seguros**. Empresas como **Microsoft, Apple** y desarrolladores de aplicaciones, navegadores o servidores web publican **actualizaciones periódicas** para reparar fallos y proteger a los usuarios.

A pesar de estos esfuerzos, **siempre surgen nuevas vulnerabilidades**, por lo que muchas compañías **contratan investigadores externos** o crean **equipos internos especializados** en identificar fallos antes de que sean explotados.

Un ejemplo destacado es **Project Zero de Google**, un equipo permanente dedicado a **descubrir vulnerabilidades en software utilizado por millones de usuarios**, con el objetivo de **prevenir ataques antes de que ocurran**.

2.4. El panorama de la ciberseguridad

2.4.1. Criptomoneda

Las criptomonedas usan cifrado fuerte para asegurar las transacciones en línea. Los usuarios las guardan en **billeteras virtuales encriptadas**, y las transacciones se registran en un **libro mayor descentralizado o blockchain**, lo que permite operar con cierto anonimato y sin intermediarios como bancos o gobiernos.

Cada cierto tiempo, computadoras especiales agrupan las últimas transacciones y las transforman en **acertijos matemáticos** que deben resolverse mediante un proceso complejo llamado **minería**. Los "mineros", con equipos potentes, verifican las transacciones y actualizan el libro mayor, que se distribuye electrónicamente por toda la red, completando así la operación de forma segura y transparente.

2.4.2. Criptojacking

Es una amenaza emergente que puede infectar cualquier dispositivo: PC, móvil o tablet. Consiste en **aprovechar los recursos del dispositivo** —CPU, GPU, memoria— para **minar criptomonedas sin el consentimiento del usuario**.
A menudo, las víctimas **no se dan cuenta** hasta que el rendimiento del dispositivo disminuye drásticamente, se calienta, la batería se agota rápido o la factura de electricidad aumenta.

3. Protegiendo sus datos y su Privacidad

3.1. Protegiendo los dispositivos y la red

Al adquirir un **nuevo dispositivo**, las medidas básicas de seguridad que se deben implementar incluyen:

1. **Configurar o verificar el firewall** del sistema para controlar y filtrar el tráfico de red no autorizado.
2. **Instalar software de protección**, como **antivirus y antiespías**, para detectar y bloquear malware y amenazas en tiempo real.
3. **Administrar el sistema operativo y el navegador web**, aplicando **actualizaciones, parches de seguridad y configuraciones recomendadas**.
4. **Configurar protecciones de contraseña**, asegurando **contraseñas fuertes, únicas y gestionadas mediante gestores de contraseñas** para proteger el acceso a cuentas y servicios.

Estas acciones iniciales **minimizan el riesgo de ataques y vulnerabilidades**, garantizando que el dispositivo esté protegido desde el primer momento.

3.1.1. Proteger los dispositivos informáticos

Para proteger sus dispositivos informáticos y los datos que contienen, se recomienda seguir estas prácticas fundamentales:

1. **Activar el firewall**
    - **Utilice al menos un firewall, ya sea de software o hardware, para controlar y filtrar el tráfico de red no autorizado.**
    - **Mantenga el firewall activado y actualizado constantemente para evitar que los atacantes accedan a información personal o corporativa.**
2. **Instalar antivirus y antiespías**
    - **El malware, como virus o spyware, puede acceder a sus datos sin permiso, destruir información, ralentizar el equipo o enviar correos no deseados.**
    - **El spyware también puede monitorizar su actividad en línea y mostrar anuncios intrusivos.**
    - **Para protegerse:**
        - **Descargue software solo de sitios confiables.**
        - **Use antivirus con funciones antiespías que analicen su PC y correo electrónico en busca de amenazas y las eliminen.**
        - **Mantenga el software actualizado para defenderse de malware nuevo y emergente.**
3. **Administrar el sistema operativo y el navegador web**
    - **Los atacantes buscan vulnerabilidades en el sistema operativo (Windows, macOS, Linux, etc.) o en el navegador web.**
    - **Establezca la configuración de seguridad en niveles medios-altos.**
    - **Mantenga el sistema operativo y los navegadores actualizados, instalando parches de seguridad de manera periódica.**
4. **Configurar la protección de contraseñas**
    - **Todos los dispositivos deben estar protegidos con contraseñas seguras para evitar accesos no autorizados.**
    - **La información sensible debe cifrarse, especialmente datos confidenciales.**
    - **Almacene solo la información estrictamente necesaria en el dispositivo, ya que un robo o pérdida del equipo podría comprometer los datos, incluso si están sincronizados en la nube.**

3.1.2. Seguridad de la red inalámbrica en casa

Las **redes Wi-Fi** permiten que dispositivos como PCs, tablets y móviles se conecten a Internet mediante un **identificador de red (SSID, Service Set Identifier)**. Aunque algunos routers permiten ocultar el SSID, esto **no es suficiente como medida de seguridad**, ya que los atacantes pueden descubrirlo con herramientas especializadas o mediante los valores predeterminados del dispositivo.

Es fundamental **cambiar el SSID y la contraseña predeterminada** por valores **únicos y robustos**, y habilitar la **encriptación de la red inalámbrica**, preferiblemente **WPA2 o superior**, para proteger la comunicación entre los dispositivos y el router.

Sin embargo, incluso con WPA2 activado, las redes Wi-Fi pueden presentar vulnerabilidades. Por ejemplo, el **ataque KRACK (Key Reinstallation Attack)** explota debilidades en el protocolo de cifrado, permitiendo a un intruso **interceptar o modificar datos transmitidos**. Esto demuestra que el cifrado por sí solo **no garantiza protección total**.

Medidas recomendadas para proteger la red Wi-Fi doméstica:

- Mantener **firmware del router y dispositivos actualizado** ante vulnerabilidades conocidas.
- Cambiar **SSID y contraseñas predeterminadas** por valores complejos y únicos.
- Preferir **conexiones por cable** para dispositivos críticos cuando sea posible.
- Usar un **servicio VPN confiable** al conectarse a redes públicas o compartidas, para cifrar la información transmitida.
- **Revisar periódicamente** los dispositivos conectados y la configuración de seguridad del router para detectar accesos sospechosos.

3.1.3. Riesgo del Wi-Fi publico

Al conectarse a una **red Wi-Fi pública**, se **desaconseja enviar información personal o sensible**, ya que estas redes suelen ser menos seguras y vulnerables a ataques.

Para protegerse:

- Verifique que su dispositivo **no esté configurado para compartir archivos, carpetas o medios** con otros usuarios de la red.
- Asegúrese de que las conexiones requieran **autenticación y cifrado** siempre que sea posible.
- Utilice un **servicio VPN encriptado**, que cifra la conexión entre su dispositivo y el servidor VPN, garantizando un **acceso seguro a Internet**.
    - Incluso si un atacante intercepta los datos transmitidos en un **túnel VPN**, no podrá **descifrarlos** gracias al cifrado.

Estas medidas reducen significativamente el riesgo de **intercepción, robo de datos o ataques maliciosos** al usar redes públicas.

3.1.4. Contraseña segura

Para proteger sus cuentas y dispositivos, se recomienda crear contraseñas que cumplan con los siguientes criterios:

- **Evite palabras del diccionario o nombres propios**, ya que son fáciles de adivinar.
- **No use errores ortográficos comunes** de palabras conocidas, pues los atacantes también los prueban.
- **Incluya caracteres especiales** como ¡ ” · $ % & para aumentar la complejidad.
- **No utilice nombres de equipos, cuentas o información personal** fácilmente identificable.
- **Cree contraseñas largas**, preferiblemente **de más de diez caracteres**, combinando letras mayúsculas y minúsculas, números y símbolos.

Estas prácticas **hacen que las contraseñas sean más resistentes a ataques de fuerza bruta, diccionario y otras técnicas de descifrado**.

3.1.5. Uso de una frase de contraseña.

Para proteger sus cuentas y dispositivos, se recomienda utilizar **frases de contraseña**, que son contraseñas largas basadas en palabras o combinaciones de palabras adaptadas con caracteres especiales, números o mayúsculas, por ejemplo: @mo l0s P€rros..

Las **ventajas de las frases de contraseña** son:

- **Más fáciles de recordar** que cadenas aleatorias de caracteres.
- **Más resistentes a ataques de diccionario y de fuerza bruta**, gracias a su longitud y complejidad.

Precaución: No utilice frases conocidas públicamente, como letras de canciones populares o citas célebres, ya que pueden ser adivinadas fácilmente por atacantes.

3.1.6. Guias para las contraseñas

El **NIST (Instituto Nacional de Estándares y Tecnología de Estados Unidos)** publica recomendaciones para la creación y gestión de contraseñas. Aunque están orientadas a aplicaciones gubernamentales, sus pautas también son útiles como estándar general:

- Las contraseñas deben tener **al menos 8 caracteres y un máximo de 64**.
- Evitar **contraseñas comunes o fáciles de adivinar**, como "contraseña" o "123456".

- **No es necesario imponer reglas de composición estrictas**, como incluir obligatoriamente números o mayúsculas.
- Los usuarios deben poder **ver la contraseña mientras la escriben**, para reducir errores de digitación.
- Se deben permitir **todos los caracteres imprimibles y espacios**, aumentando la complejidad y seguridad.
- **No se deben proporcionar sugerencias de contraseña** que puedan facilitar ataques.
- **No se recomienda la expiración periódica de contraseñas**, salvo indicaciones específicas de seguridad.
- **No se debe basar la autenticación en conocimiento secreto**, como respuestas a preguntas personales o historial de transacciones, ya que son fáciles de adivinar o interceptar.

Estas normas buscan **equilibrar seguridad y usabilidad**, promoviendo contraseñas seguras sin complicar innecesariamente la experiencia del usuario.

3.2 Mantenimiento de datos.

3.2.1. Que es el cifrado?

Es el proceso de convertir información en un formato **ilegible para personas no autorizadas**. Solo quienes poseen la **clave o contraseña correcta** pueden descifrar los datos y acceder a su contenido original.

El cifrado **no evita que los datos sean interceptados**, solo protege que su contenido sea leído por terceros. Por eso, los ciberdelincuentes pueden **secuestrar datos cifrándolos** y exigir un rescate para restaurarlos (ransomware).

3.2.2 Como se cifran sus datos?

El cifrado de datos utiliza **software especializado** para proteger archivos, carpetas o incluso unidades completas, asegurando que solo usuarios autorizados puedan acceder a la información.

En **Windows**, el sistema **EFS (Encrypting File System)** permite cifrar datos vinculándolos directamente a la cuenta de usuario. Solo el usuario que realiza el cifrado puede acceder posteriormente a los archivos o carpetas protegidas.

Pasos para cifrar un archivo o carpeta con EFS:

1. Seleccione el archivo o carpeta que desea proteger.
2. Haga clic derecho y seleccione **Propiedades**.
3. Haga clic en **Avanzado**.

4. Active la casilla **Encriptar contenido para proteger datos**.
5. Los archivos y carpetas cifrados con EFS se mostrarán en **verde**, indicando que están protegidos.

Este método **garantiza la confidencialidad de los datos**, evitando el acceso no autorizado incluso si alguien obtiene acceso físico al dispositivo.

3.2.3 Realice un respaldo de sus datos

Tener copias de seguridad protege información irremplazable, como fotos familiares, frente a pérdida accidental o fallos del dispositivo. Un respaldo requiere **una ubicación adicional** y **copias periódicas, preferiblemente automáticas**.

Opciones de almacenamiento:

- **Red doméstica:** guardar los datos localmente da **control total**, pero requiere responsabilidad sobre mantenimiento y costos.
- **Dispositivo secundario:** usar NAS, disco duro externo, USB, CD o cintas; puedes respaldar todo o solo carpetas importantes.
- **Nube:** servicios como AWS permiten acceder a tus datos desde cualquier lugar y protegen contra fallos físicos, incendios o robos; el costo depende del espacio contratado.

Mantener **copias actualizadas en más de un lugar** aumenta la seguridad de tus datos frente a cualquier eventualidad.

3.2.4 Realmente se han ido?

Cuando eliminas un archivo y luego vacías la **papelera de reciclaje**, en realidad solo se elimina la referencia al archivo en el sistema operativo. Los datos permanecen en el **disco duro** hasta que se sobrescriben.

Con **herramientas forenses especializadas**, es posible **recuperar estos archivos** debido a los rastros magnéticos que quedan en el disco, incluso después de haber sido eliminados aparentemente.

Conclusión: El borrado estándar no garantiza la eliminación completa; para proteger información sensible, se recomienda utilizar métodos de **borrado seguro o software de destrucción de datos** que sobrescriba varias veces la información.

3.2.5 Como eliminar datos de forma permanente.

Para que un archivo **no pueda recuperarse**, no basta con simplemente eliminarlo. Es necesario **sobrescribirlo varias veces** con patrones de datos (unos y ceros) utilizando herramientas especializadas.

Ejemplos de herramientas:

- **Windows:** SDelete
- **Linux:** shred
- **macOS:** Secure Empty Trash

Aunque estas herramientas reducen significativamente el riesgo de recuperación, **ninguna garantiza un 100% de irrecuperabilidad**. La única forma totalmente segura de eliminar datos es **destruir físicamente el disco o dispositivo de almacenamiento**, ya que muchos atacantes han recuperado información de equipos que se creían "limpios" pero no fueron destruidos.

Además, es importante **considerar el borrado de archivos en la nube**, ya que los datos almacenados en servidores remotos requieren métodos de eliminación específicos proporcionados por el proveedor del servicio.

3.3. A quien le pertenecen sus datos

3.3.1 Términos del servicio

Los **términos de servicio** son un contrato legal que regula la relación entre usted, el proveedor y otros usuarios del servicio, incluyendo derechos, responsabilidades, limitaciones de responsabilidad y reglas sobre la cuenta.

- **Política de uso de datos:** explica cómo el proveedor recopila, usa y comparte su información.
- **Configuración de privacidad:** permite controlar quién puede ver su información y acceder a su perfil o cuenta.
- **Política de seguridad:** detalla las medidas que la empresa aplica para proteger los datos que recopila.

3.3.2. Antes de registrarse

Antes de registrarse en un servicio en línea, es fundamental evaluar cómo se manejarán tus datos personales. Entre los factores clave a considerar están:

- **Lectura de términos de servicio:** ¿Has leído y comprendido el acuerdo de uso del servicio?
- **Derechos sobre tus datos:** ¿Qué derechos tienes respecto a la recopilación, almacenamiento y uso de tus datos personales?
- **Acceso a tus datos:** ¿Puedes solicitar una copia de la información que el servicio posee sobre ti?
- **Uso de los datos por el proveedor:** ¿Qué puede hacer el proveedor con la información que cargas o compartes en la plataforma?
- **Destino de los datos al cerrar la cuenta:** ¿Qué sucede con tus datos si decides eliminar o cerrar tu cuenta?

Conclusión: Revisar estos aspectos antes de registrarse ayuda a proteger tu privacidad y a tomar decisiones informadas sobre qué servicios usar.

3.3.3. Para proteger sus datos

Para mantener tus datos personales seguros, se recomienda seguir estas pautas:

- **Revisar términos y condiciones:** Antes de registrarse, lee los términos de servicio para decidir si estás dispuesto a ceder ciertos derechos sobre tus datos a cambio del uso del servicio.
- **Configurar la privacidad:** No aceptes la configuración predeterminada; ajusta las opciones de privacidad según tus necesidades.
- **Controlar el acceso a tu contenido:** Limita el grupo de personas con las que compartes información o archivos.
- **Evaluar la política de seguridad del proveedor:** Comprende cómo gestionan y protegen tus datos para evitar riesgos innecesarios.
- **Fortalecer la seguridad de la cuenta:** Cambia contraseñas periódicamente, utiliza contraseñas complejas y activa la **autenticación en dos pasos** siempre que sea posible.

Conclusión: Aplicar estas medidas reduce significativamente la exposición de tus datos y protege tu privacidad en línea.

3.4 Protección de la privacidad en línea

3.4.1 Autenticación de doble factor

La **autenticación de doble factor (2FA)** es un método de seguridad que agregan grandes empresas como Google, Facebook o Apple para proteger las cuentas de los usuarios.

Además de solicitar **nombre de usuario y contraseña** (o un patrón), 2FA requiere un **segundo factor** para verificar la identidad, que puede ser:

- **Objeto físico:** por ejemplo, una tarjeta de seguridad o el teléfono móvil.
- **Verificación biométrica:** huella dactilar, reconocimiento facial u otros datos biométricos.
- **Código de un solo uso:** enviado por SMS, correo electrónico o generado por aplicaciones de autenticación.

Beneficio: Esta capa adicional dificulta que los atacantes accedan a la cuenta incluso si conocen la contraseña, aumentando significativamente la seguridad de los datos.

3.4.2 Autorización abierta

OAuth (Open Authorization) es un protocolo abierto que permite a un usuario conceder acceso limitado a aplicaciones de terceros sin compartir su contraseña.

Por ejemplo, cuando inicias sesión en un sitio usando tu cuenta de Google, Facebook u otro proveedor:

- **La aplicación recibe solo los permisos necesarios para funcionar.**
- **Tu contraseña nunca se expone ni se comparte.**

Beneficio: Permite integrar servicios de manera segura, protegiendo la información confidencial del usuario.

3.4.3 Social sharing

Para **proteger la privacidad en redes sociales**, es fundamental **limitar la cantidad de información personal** que se comparte.
Cuanta más información divulgue en línea, **más fácil será que terceros creen un perfil sobre usted** y lo utilicen para fines maliciosos, ya sea en el mundo digital o en la vida real.

3.4.4. Privacidad de correo electrónico y navegadores web

El uso del **modo de navegación privada** en los navegadores ayuda a **minimizar la recopilación de datos personales durante la navegación**. Cada navegador lo llama de manera diferente:

- **Chrome:** Incógnito
- **Mozilla Firefox:** Pestaña privada
- **Safari:** Navegación privada

Cuando se activa este modo, **las cookies se desactivan** y todos los archivos temporales e historial de navegación se eliminan al cerrar la ventana o el navegador. Esto reduce la posibilidad de que las empresas rastreen sus actividades en línea o muestren anuncios personalizados.

Sin embargo, **no garantiza anonimato completo**, ya que algunas entidades, como los proveedores de Internet o los routers, aún pueden recopilar información sobre el historial de navegación.

3.5 Anotaciones LAB.

- **Cuidado con lo que publicas:** Evite compartir información sensible en redes sociales, como su dirección o planes de viaje, ya que puede facilitar robos o fraudes si se sabe que no está en casa.

- **Contraseñas únicas y seguras:** Use una contraseña diferente para cada sitio web o aplicación. Como recordar tantas contraseñas puede ser complicado, lo más recomendable es emplear un **gestor de contraseñas**, que almacena sus credenciales de forma segura y cifrada, permitiéndole acceder a ellas fácilmente cuando las necesite.

4. Protegiendo a la organización.

4.1 Dispositivos y tecnologías de ciberseguridad

4.1.1 Dispositivos de seguridad

Los dispositivos de seguridad pueden ser hardware independiente, como un enrutador, o software que se ejecuta en un dispositivo de red. Generalmente se dividen en seis categorías principales:

- **Routers:** Su función principal es conectar distintos segmentos de red, pero muchos incluyen filtrado básico de tráfico. Esto permite controlar qué dispositivos pueden comunicarse entre sí, proporcionando una primera capa de seguridad y control de la red.
- **Firewalls:** Analizan el tráfico de red en profundidad y aplican políticas de seguridad avanzadas para bloquear actividades maliciosas. Protegen contra ataques más complejos que los simples filtros básicos de routers, supervisando todo el tráfico que atraviesa la red.
- **Sistemas de prevención de intrusiones (IPS):** Monitorean el tráfico en tiempo real y bloquean automáticamente cualquier actividad maliciosa. Combinan firmas de ataques conocidos, detección de anomalías y análisis de comportamiento para identificar amenazas. Cuando detectan un intento de intrusión, interrumpen el tráfico, bloquean conexiones o aplican reglas de seguridad, evitando que el ataque afecte a sistemas o datos.
- **Redes privadas virtuales (VPN):** Crean un túnel cifrado entre un dispositivo y la red de la organización, protegiendo la información incluso a través de Internet. Permiten a empleados remotos acceder a recursos internos como si estuvieran físicamente en la oficina y conectan de manera segura distintas sedes bajo un canal protegido.
- **Antimalware o antivirus:** Detectan y bloquean malware mediante firmas de amenazas conocidas, análisis heurístico de comportamientos sospechosos, monitorización en tiempo real y ejecución en entornos aislados (sandbox). Las amenazas detectadas se bloquean, se ponen en cuarentena o se eliminan, manteniendo la red y los dispositivos protegidos.
- **Otros dispositivos de seguridad:** Incluyen herramientas de seguridad web y de correo electrónico, dispositivos de descifrado, servidores de control de acceso de clientes y sistemas de gestión de seguridad, que complementan la protección de la red y los datos.

4.1.2 Firewalls

Los firewalls están diseñados para controlar y filtrar las comunicaciones que se permiten dentro y fuera de un dispositivo o red. Pueden instalarse en una sola computadora para protegerla (firewall basado en host) o como dispositivos de red independientes que protegen toda una red y sus dispositivos conectados (firewall basado en red).

A medida que los ataques se han vuelto más sofisticados, se han desarrollado distintos tipos de firewalls adaptados a necesidades específicas:

- **Firewall de la capa de red:** Filtra las comunicaciones según las direcciones IP de origen y destino.
- **Firewall de la capa de transporte:** Filtra según los puertos de datos de origen y destino, así como el estado de las conexiones.
- **Firewall de la capa de aplicación:** Filtra el tráfico en función de aplicaciones, programas o servicios específicos.
- **Firewall de capa sensible al contexto:** Filtra comunicaciones considerando el usuario, el dispositivo, la función, el tipo de aplicación y el perfil de amenaza.
- **Servidor proxy:** Filtra solicitudes de contenido web, incluyendo URL, nombres de dominio y tipos de medios.
- **Servidor proxy inverso:** Ubicado frente a servidores web, protege, oculta, descarga y distribuye el acceso a los servidores web.
- **Firewall de traducción de direcciones de red (NAT):** Oculta o enmascara las direcciones privadas de los hosts de la red, protegiendo su identidad en Internet.
- **Firewall basado en host:** Filtra puertos y llamadas a servicios del sistema en un solo sistema operativo, proporcionando protección directa al equipo individual.

4.1.3 Análisis de puertos

En **redes**, cada aplicación que se ejecuta en un dispositivo recibe un **identificador llamado número de puerto**, que se utiliza en ambos extremos de la comunicación para asegurar que los datos lleguen a la aplicación correcta. El **escaneo de puertos** es el proceso de inspeccionar una computadora, servidor u otro host de red para identificar qué puertos están abiertos. Puede usarse **con fines maliciosos**, como herramienta de reconocimiento para descubrir el sistema operativo y los servicios activos, o de manera **legítima**, por un administrador de red, para verificar la seguridad y las políticas de la red.

Ejemplo: un escaneo de puertos podría revelar que el puerto 80 (HTTP) está abierto en un servidor web, indicando que el servicio web está activo y disponible para conexiones.

4.1.4 La importancia del escaneo puertos en tu pc

Un **puerto abierto** es un punto de comunicación en un dispositivo donde un programa o servicio está escuchando y aceptando conexiones externas. Esto significa que otras redes

pueden interactuar con ese servicio. Si el servicio tiene vulnerabilidades, un atacante podría explotarlas para acceder al equipo o a la red. Por eso, el **escaneo de puertos** debe considerarse un paso previo a un ataque y **nunca debe realizarse en sistemas ajenos sin autorización**, ya que podría ser ilegal y peligroso.

4.1.5 Sistemas de detección y prevención de intrusiones

Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) son medidas de seguridad implementadas en una red para detectar y prevenir actividades maliciosas.

- **IDS:** Un **IDS (Intrusion Detection System)** es un sistema que puede ser un dispositivo de red independiente o una herramienta dentro de un servidor, firewall o sistema operativo (Windows, Linux). Su función es **escanear el tráfico de la red** comparándolo con una base de firmas o reglas de ataques para detectar actividad maliciosa.
  Cuando se detecta un ataque, el IDS **registra la incidencia y genera una alerta** para el administrador de la red, pero **no bloquea el ataque**; su trabajo es **detectar, registrar y reportar**.
  Para evitar que el análisis ralentice la red, el IDS suele colocarse **fuera de línea**, recibiendo una copia del tráfico mediante un switch, permitiendo la inspección sin afectar la comunicación normal.
- **IPS:** Un **IPS (Intrusion Prevention System)** puede **bloquear o denegar tráfico** según reglas o coincidencias de firmas. Uno de los IPS/IDS más conocidos es **Snort**, cuya versión comercial es **Sourcefire de Cisco**. Sourcefire permite **analizar tráfico y puertos en tiempo real**, detectar sondas, ataques y escaneos, registrar y comparar contenido, y se integra con otras herramientas para informes y análisis de rendimiento.

NOTA: Cuando los atacantes, realizan ataques a sistemas antes de que los propios creadores del software tengas oportunidad de solucionarlas se dice que los hacker llevaron a cabo un ataque de día cero.

La capacidad de detectar estos ataques en tiempo real y detenerlos de inmediado es el objetivo final

4.1.6 Detección en tiempo real

Hoy en día, muchas organizaciones no detectan ataques hasta días o meses después. La **detección en tiempo real** requiere un análisis activo mediante **firewalls**, **IDS/IPS** y software de detección de malware de próxima generación, conectado a centros de amenaza globales. Estos sistemas identifican **anomalías y comportamientos sospechosos** en la red antes de que el daño se produzca.

Los ataques **DDoS** representan una de las mayores amenazas que necesitan respuesta inmediata, ya que pueden paralizar servidores y la disponibilidad de la red. Su defensa es complicada porque los ataques provienen de cientos o miles de hosts comprometidos y se parecen a tráfico legítimo.

4.1.7 Protección contra software malicioso

Para defenderse de ataques de día cero y **APT (Amenazas Persistentes Avanzadas)** se utilizan soluciones avanzadas de detección de malware a nivel empresarial, como la **Advanced Malware Protection (AMP) de Cisco**.

Este software, que funciona en clientes y servidores, puede desplegarse en **puntos finales** como servidores, PCs o dispositivos de seguridad de red. Analiza millones de archivos y los compara con **cientos de millones de artefactos de malware** para detectar comportamientos sospechosos que indiquen una amenaza avanzada. Este enfoque permite tener una **visión global de los ataques**, sus campañas y distribución.

THREAT GRID

- Equipo del Centro de Operaciones de Seguridad (SOC): recopila datos precisos y procesables sobre amenazas para mejorar la vigilancia y la toma de decisiones.
- Equipo de Respuesta a Incidencias (IRT): accede a información forense detallada para analizar y comprender rápidamente comportamientos sospechosos y responder a incidentes de manera efectiva.
- Equipo de Inteligencia de Amenazas: utiliza el análisis de datos para anticipar ataques y mejorar proactivamente la infraestructura de seguridad de la organización.
- Equipo de Ingeniería de Infraestructura de Seguridad: aplica la información sobre amenazas de forma rápida y, a menudo, automatizada, fortaleciendo la protección de los sistemas y redes.

4.1.8 Mejores prácticas de seguridad

Muchas organizaciones, nacionales y profesionales, han publicado listas de **buenas prácticas de seguridad**. Algunos de los repositorios más completos se encuentran en el **Centro de Recursos de Seguridad Informática del NIST**.

Principales pautas de seguridad:

1. **Evaluación de riesgos:** Conocer y valorar los activos protegidos ayuda a justificar la inversión en seguridad.
2. **Política de seguridad:** Definir reglas, roles, responsabilidades y expectativas de los empleados.
3. **Seguridad física:** Restringir el acceso a armarios de red, servidores y equipos críticos; incluir sistemas contra incendios.
4. **Seguridad de recursos humanos:** Realizar verificaciones de antecedentes y evaluaciones para todos los empleados.

5. **Copias de seguridad:** Realizar backups periódicos y probar la recuperación de datos.
6. **Actualizaciones y parches:** Mantener sistemas operativos, aplicaciones y dispositivos de red siempre actualizados.
7. **Controles de acceso:** Configurar roles de usuario, niveles de privilegio y autenticación sólida.
8. **Respuesta a incidentes:** Contar con un equipo de respuesta a incidentes y probar escenarios de emergencia regularmente.
9. **Monitoreo y análisis de red:** Implementar herramientas que integren monitoreo, análisis y gestión de seguridad.
10. **Dispositivos de seguridad de red:** Usar firewalls, routers y dispositivos de seguridad de próxima generación.
11. **Seguridad de endpoints:** Instalar software antivirus, antimalware y soluciones de protección empresarial.
12. **Educación de usuarios:** Capacitar a los empleados en procedimientos y buenas prácticas de ciberseguridad. *(Ejemplo de institución: SANS Institute)*
13. **Cifrado de datos:** Proteger la información confidencial, incluyendo correos electrónicos y documentos críticos.

4.2 Comportamiento a seguir en la ciberseguridad

4.2.1 Seguridad basada en el comportamiento.

Es una forma de detección de amenazas que implica capturar y analizar el flujo de comunicación entre un usuario en la red local y un destino local o remoto. Cualquier cambio en los patrones normales de comportamiento se considera anomalía y puede indicar un ataque.

Honeypot:

Un **honeypot** es una herramienta de seguridad que funciona como un señuelo, diseñada para atraer a atacantes mediante la simulación de sistemas vulnerables. Aprovecha patrones de comportamiento malicioso esperados para capturar al intruso. Una vez que el atacante interactúa con el honeypot, el **administrador de red** puede **registrar, analizar y estudiar su comportamiento**, lo que permite **mejorar la defensa de la red** y detectar nuevas técnicas de ataque.

Arquitectura de la solución Cisco Cyber Threat Defense:

La **arquitectura Cisco Cyber Threat Defense** es un enfoque integral de seguridad que combina **detección basada en firmas y comportamiento**, proporcionando **visibilidad completa, contexto y control** sobre los ataques. Permite identificar **quién realiza el ataque, qué tipo de ataque es, dónde y cuándo ocurre, y cómo se está ejecutando**. Esta arquitectura integra

múltiples tecnologías de seguridad, incluyendo sistemas de detección de intrusiones, análisis de tráfico y correlación de eventos, para **anticipar y responder de manera proactiva a amenazas avanzadas**.

4.2.2 NetFlow

La tecnología NetFlow se utiliza para recopilar información sobre los datos que fluyen a través de una red, incluidos quienes, y que dispositivos están en la red, y cuando y como los usuarios y los dispositivos acceden a la red.

NetFlow es un componente importante del análisis y la detección basados en el comportamiento. Los conmutadores, enrutadores y firewalls equipados con NetFLow pueden reportar información sobre la entrada, salida y viaje de datos a través de la red.

Esta información se envía a los recopiladores de NetFlow, que se pueden utilizar para establecer comportamiento de referencia en más de 90 atributos, como la dirección IP de origen y destino.

4.2.3 Pruebas de Penetración (Pentesting)

Las pruebas de penetración son un proceso controlado y autorizado cuyo objetivo es evaluar la seguridad de un sistema informático, red, aplicación o infraestructura completa simulando ataques reales. Su finalidad no es solo detectar vulnerabilidades, sino comprobar hasta qué punto estas pueden ser explotadas y qué impacto real tendrían sobre la confidencialidad, integridad y disponibilidad de la información.

Una prueba de penetración busca pensar y actuar como un atacante real, analizando no solo la tecnología, sino también a las personas y los procesos, para identificar fallos que podrían comprometer la seguridad de la organización. La información obtenida se utiliza para reforzar las defensas, reducir la superficie de ataque y mejorar la resiliencia frente a amenazas futuras.

Proceso de una prueba lápiz o de pluma

1. Planificación y reconocimiento

En esta fase se define el alcance, los objetivos y las reglas de la prueba (qué se puede atacar, qué no, y hasta dónde se puede llegar). Posteriormente, el pentester recopila la mayor cantidad de información posible sobre el objetivo, utilizando reconocimiento pasivo y activo.

Incluye:

- Identificación de direcciones IP, dominios y subdominios.
- Mapeo de infraestructura y tecnologías utilizadas.
- Análisis preliminar de posibles vulnerabilidades.
- Recopilación de información pública (OSINT).

Esta etapa es crucial, ya que una buena recopilación de datos determina la eficacia de toda la prueba.

---

2. Escaneo y enumeración

Aquí se realiza un reconocimiento activo para identificar puntos débiles concretos que puedan ser explotados.

Incluye:

- Escaneo de puertos para detectar servicios expuestos.
- Identificación de versiones de software y sistemas operativos.
- Análisis de vulnerabilidades mediante herramientas automáticas y verificación manual.
- Enumeración de usuarios, recursos compartidos, políticas de seguridad y estructuras internas.

El objetivo es comprender cómo está construido el sistema y dónde existen fallos potenciales.

---

3. Explotación (obtención de acceso)

En esta fase se intenta comprometer el sistema utilizando las vulnerabilidades detectadas, simulando técnicas reales de ataque.

Entre los métodos utilizados pueden estar:

- Ejecución de exploits con cargas útiles (payloads).
- Ataques a aplicaciones web (SQL Injection, XSS, CSRF, etc.).
- Ingeniería social contra empleados.
- Bypass de controles de acceso.
- Ataques a configuraciones incorrectas de software y hardware.
- Compromiso de redes Wi-Fi con cifrado débil.
- Acceso físico no autorizado a instalaciones críticas.

El propósito no es causar daño, sino demostrar de forma controlada el nivel real de exposición.

---

4. Post-explotación y persistencia

Una vez obtenido el acceso, se evalúa hasta dónde puede llegar un atacante dentro del sistema comprometido.

Se analiza:

- Escalada de privilegios.
- Movimiento lateral dentro de la red.

- Acceso a datos sensibles.
- Capacidad de mantener persistencia sin ser detectado.

Para ello pueden simularse técnicas como el uso de puertas traseras, rootkits o canales encubiertos, siempre dentro del marco ético y autorizado del test.

---

5. Análisis y reporte

Fase crítica donde se transforma el ataque en valor estratégico.

Se entrega un informe detallado que incluye:

- Vulnerabilidades encontradas (clasificadas por severidad).
- Técnicas utilizadas para explotarlas.
- Impacto potencial sobre la organización.
- Evidencias técnicas.
- Recomendaciones concretas de mitigación.

Este informe sirve como guía para mejorar:

- Configuraciones técnicas.
- Políticas de seguridad.
- Procedimientos internos.
- Formación del personal.

4.2.4 Reducción del impacto

Aunque muchas organizaciones conocen las amenazas de seguridad más comunes y aplican medidas preventivas, **ningún sistema es completamente infalible**. Por ello, es esencial estar preparados para **minimizar el daño** cuando se produce una violación de seguridad y actuar con rapidez y eficacia.

Principios clave

- La **rapidez de respuesta** es crítica: cada minuto cuenta para limitar el impacto.
- La **transparencia** genera confianza interna y externa.
- La **responsabilidad y el aprendizaje continuo** transforman un incidente en una oportunidad de fortalecer la seguridad.

Pasos para reducir el impacto tras una violación de seguridad

1. **Comunicar el incidente**

- Internamente: informar a todos los empleados clave y establecer instrucciones claras de acción.
- Externamente: notificar a clientes y stakeholders mediante canales oficiales, explicando la situación de forma transparente.

2. **Ser sincero y asumir la responsabilidad**
    - Responder con honestidad y reconocer los errores de la organización.
    - La responsabilidad fortalece la reputación y facilita la cooperación con clientes, reguladores y autoridades.
3. **Proporcionar información detallada**
    - Explicar qué ocurrió, cómo ocurrió y qué información se vio comprometida.
    - Indicar las medidas inmediatas para mitigar el daño, incluyendo servicios de protección al cliente (como monitoreo de identidad) si es necesario.
4. **Identificar la causa raíz**
    - Investigar a fondo el incidente para entender cómo se produjo y qué permitió la infracción.
    - Puede requerir expertos forenses y análisis técnico detallado para detectar fallos en sistemas, procesos o personas.
5. **Aplicar lecciones aprendidas**
    - Incorporar las recomendaciones de la investigación para fortalecer políticas, procedimientos y controles.
    - Actualizar configuraciones, parches, autenticaciones y protocolos de seguridad para prevenir incidentes similares.
6. **Verificar la integridad de los sistemas**
    - Asegurarse de que no quedan puertas traseras ni rastros de accesos no autorizados.
    - Realizar auditorías exhaustivas para garantizar que todos los sistemas están limpios y seguros.
7. **Educar y sensibilizar**
    - Capacitar a empleados, socios y clientes sobre buenas prácticas de seguridad.
    - Promover una cultura de ciberseguridad que reduzca riesgos futuros y mejore la resiliencia de la organización.

Síntesis para apuntes

La reducción del impacto transforma un incidente inevitable en un aprendizaje estratégico: **rapidez, transparencia, responsabilidad y mejora continua** son la clave para proteger datos, reputación y confianza.

4.2.5 Que es la gestión de riesgo?

La **gestión de riesgo** es un proceso sistemático y continuo que permite **identificar, evaluar y controlar riesgos** con el objetivo de minimizar el impacto de amenazas y vulnerabilidades sobre los activos de una organización.
No se puede eliminar el riesgo por completo; el objetivo es **determinar niveles de riesgo aceptables** equilibrando el impacto potencial de una amenaza con el costo y la eficacia de los controles implementados. Un principio clave: **el costo de un control nunca debe superar el valor del activo protegido**.

Proceso de gestión de riesgo

1. **Identificación del riesgo (Encuadre)**
    - Detectar y catalogar las amenazas que pueden aumentar el riesgo para la organización.
    - Ejemplos de amenazas: fallos de procesos, vulnerabilidades técnicas, ataques cibernéticos, interrupciones de servicios, pérdida de reputación, responsabilidad legal o fuga de propiedad intelectual.
2. **Evaluación del riesgo**
    - Determinar la gravedad y probabilidad de cada amenaza.
    - Se puede priorizar mediante:
        - **Análisis cuantitativo:** impacto financiero directo.
        - **Análisis cualitativo:** efecto sobre la operación, reputación o continuidad del negocio.
    - Permite enfocar recursos en los riesgos más críticos.
3. **Respuesta al riesgo**
    - Desarrollar estrategias para gestionar cada riesgo identificado:
        - **Eliminar:** eliminar la fuente de riesgo.
        - **Mitigar:** aplicar controles para reducir la probabilidad o impacto.
        - **Transferir:** delegar el riesgo a un tercero (seguros, outsourcing).
        - **Aceptar:** asumir el riesgo cuando el costo de mitigarlo supera su impacto.
4. **Monitoreo y revisión del riesgo**
    - Supervisar de manera continua la eficacia de las acciones implementadas.

- Evaluar riesgos aceptados y cambios en el entorno que puedan modificar la exposición.
- Ajustar estrategias según evolución tecnológica, regulatoria o de negocio.

Síntesis para apuntes

La gestión de riesgo es un ciclo constante: **identificar, evaluar, responder y monitorear**. No busca eliminar todos los riesgos, sino **gestionar su impacto de manera eficiente y proporcional al valor del activo protegido**.

4.3 Enfoque de Cisco para la ciberseguridad

4.3.1 CSIRT de Cisco

Muchas organizaciones grandes tienen un equipo de respuesta a incidentes de seguridad informática (CSIRT) para recibir, revisar y responder a los informes de incidentes de seguridad informática. Cisco CSIRT va un paso más allá y proporciona evaluación proactiva de amenazas, planificación de mitigación, análisis de tendencias de incidentes y revisión de la arquitectura de seguridad en un esfuerzo por evitar que ocurran incidentes de seguridad.

El CSIRT de Cisco adopta un enfoque proactivo, colaborando con el foro de equipos de seguridad y respuesta a incidentes (FIRST), el intercambio de información de seguridad nacional (NSIE), el intercambio de información de seguridad de defensa (DSIE) y el centro de análisis e investigación de operaciones de DNS (DNS-OARC) para asegurarnos de estar al día con los nuevos desarrollos.

Hay varias organizaciones CSIRT nacionales y públicas, como la División CERT del instituto de ingeniería de software de la universidad de Carnegie Mellon, que están disponibles para ayudar a las organizaciones y CSIRT nacionales a desarrollar, operar y mejorar sus capacidades de gestión de incidentes.

4.3.2 Libro de estrategias de seguridad

La mejor forma de prepararse para un incidente de seguridad es **anticiparlo**. Para ello, las organizaciones deben definir con claridad:

- Cómo **identificar riesgos** que afectan sistemas, activos, datos y capacidades críticas.
- Qué **salvaguardas técnicas y organizativas** aplicar, junto con la capacitación adecuada del personal.

- Un **plan de respuesta adaptable** que reduzca el impacto y acote el daño cuando ocurra una violación.
- Las **acciones posteriores al incidente**, incluyendo contención, erradicación, recuperación y mejora continua.

Toda esta información se consolida en un **Libro de Estrategias de Seguridad**, también conocido como *Security Playbook*.

¿Qué es un libro de estrategias de seguridad?

Es un **conjunto de procedimientos, consultas, flujos de trabajo y respuestas estandarizadas** diseñadas para detectar, analizar y responder a incidentes de seguridad de manera consistente, rápida y eficaz.
Un buen playbook elimina la improvisación y garantiza que cualquier miembro del equipo siga el mismo protocolo ante amenazas repetidas.

Características esenciales de un buen Security Playbook

- **Automatización de amenazas comunes**
  Explica cómo identificar y automatizar la respuesta a incidentes habituales:
  - Equipos infectados por malware
  - Actividad de red anómala
  - Intentos de autenticación sospechosos
  - Exfiltración de datos
  - Comportamientos inusuales de usuarios o sistemas
- **Definición clara del tráfico**
  Establece qué tráfico entrante y saliente es normal, qué no lo es y cómo debe tratarse cada patrón sospechoso.
- **Información sintetizada y accionable**
  Incluye paneles, tendencias, métricas y estadísticas que permitan tomar decisiones rápidas.
- **Acceso inmediato a métricas clave**
  Tiempos de detección, tiempos de respuesta, volumen de alertas, severidad, activos afectados, etc.
- **Correlación de eventos**
  Conecta datos provenientes de múltiples fuentes (SIEM, firewalls, endpoints, logs, IDS/IPS, aplicaciones, nube) para obtener una visión completa del ataque y evitar análisis aislados.

Síntesis clara para apuntes

Un playbook de seguridad es el **manual operativo** del equipo: define qué hacer, cómo hacerlo y en qué orden para detectar, responder y aprender de cualquier incidente, reduciendo al mínimo el impacto sobre la organización.

4.3.3 Herramientas para la prevención y la detección de incidentes

- **SIEM:** Un SIEM es una plataforma centralizada que **recopila, normaliza, correlaciona y analiza** registros, alertas y eventos de seguridad provenientes de toda la infraestructura (servidores, firewalls, endpoints, aplicaciones, servicios en la nube, etc.).
  Su objetivo principal es **detectar amenazas de forma temprana**, identificar patrones anómalos y proporcionar visibilidad completa del entorno mediante análisis en tiempo real e histórico. Es una herramienta clave para monitoreo, respuesta a incidentes y cumplimiento normativo.
- **DLP:** Un sistema DLP está diseñado para **prevenir la fuga, robo o uso indebido de información sensible**, aplicando políticas que supervisan y controlan cómo se accede, transmite o almacena la información.
  Protege los datos en sus tres estados fundamentales:
  - **Datos en uso:** información activa que está siendo manipulada por un usuario o proceso.
  - **Datos en movimiento:** información que viaja por la red (correo, transferencia, protocolos, APIs).
  - **Datos en reposo:** información almacenada en servidores, bases de datos, dispositivos o nubes.
  - Un DLP puede **bloquear acciones** que violen políticas de seguridad, alertar al personal, cifrar información o impedir transmisiones sospechosas.

4.3.4 ISE y TrustSec de Cisco

Cisco Identity SErvices Engine (ISE) y TrustSec aplican el acceso de los usuarios a los recuerdos de red mediante la creación de políticas de control de acceso basadas en roles

5. ¿Su futuro esta relacionado con la ciberseguridad?

5.1. Cuestiones legales y éticas

5.1.1. Cuestiones legales en ciberseguridad

Los profesionales de la ciberseguridad necesitan dominar muchas de las mismas técnicas que usan los atacantes. La diferencia es simple: **el profesional actúa dentro de la ley; el atacante, no**.
Entender los límites legales es tan importante como saber explotar una vulnerabilidad.

---

1. Asuntos legales personales

Tener habilidades para hackear no te da permiso para usarlas fuera de entornos autorizados.

- Acceder sin permiso a dispositivos, redes o cuentas ajenas es delito, aunque "solo sea por curiosidad".
- La mayoría de las intrusiones dejan rastros, y la atribución digital es cada vez más precisa.
- La ética profesional exige usar las habilidades para proteger, no para violar la privacidad o seguridad de otros.

Regla práctica: **Sin permiso explícito y documentado, no se toca nada.**

---

2. Asuntos legales corporativos

Las organizaciones operan bajo **leyes, normativas y estándares** que deben cumplirse (GDPR, leyes de protección de datos, normativas sectoriales, etc.).

Si un profesional comete acciones ilegales o no autorizadas mientras trabaja, las consecuencias pueden ser graves:

- Sanciones contra la empresa
- Despido inmediato
- Multas personales
- Procesos penales

Cuando exista duda sobre la legalidad de una acción:
Asume que es ilegal y consulta al departamento legal o a cumplimiento normativo antes de actuar.

---

3. Derecho internacional y ciberseguridad

El marco legal internacional en ciberseguridad es **complejo, difuso y en constante evolución**.
Razones:

- El ciberespacio no tiene fronteras físicas.
- La atribución de ataques es difícil; los actores pueden ocultar su origen con facilidad.
- Atacan gobiernos, empresas, grupos criminales y actores híbridos.

El derecho internacional se construye mediante:

- **Práctica estatal** (cómo actúan los países en el ciberespacio)
- **Opinio juris** (la convicción de que ciertas conductas son obligatorias según el derecho)
- **Tratados y acuerdos multilaterales** (como el Convenio de Budapest)

Aún no existe una "constitución del ciberespacio", pero se están definiendo normas sobre soberanía digital, uso legítimo de la fuerza, represalias, cooperación y responsabilidad entre estados.

Síntesis para memorizar

- **Lo que no está autorizado es ilegal.**
- **La empresa puede ser sancionada por tus errores. Tú también.**
- **A nivel internacional, las reglas del juego aún se están escribiendo.**