ISEMED
MARÍA AUXILIADORA
SAN PEDRO SULA

Seguridad Informática

Informática I

Decimo grado

1. Introducción a la Seguridad Informática

La **seguridad informática** se refiere a la protección de sistemas informáticos (hardware y software), redes y datos contra el robo, daño, acceso no autorizado o cualquier otra forma de interrupción o mal uso. Su objetivo es mantener la **confidencialidad, integridad y disponibilidad** (CIA) de la información.

- **Confidencialidad:** Garantizar que solo los usuarios autorizados puedan acceder a la información.
- **Integridad:** Asegurar que la información no sea alterada o destruida de forma no autorizada.
- **Disponibilidad:** Permitir que los usuarios autorizados accedan a la información y los sistemas cuando lo necesiten.

2. ¿Qué es el Malware?

El término **Malware** es una abreviatura de "Malicious Software" (Software Malicioso). Engloba a cualquier tipo de programa, código o archivo diseñado específicamente para causar daño, interrupción, robo de datos o realizar acciones no deseadas en un sistema informático, servidor, tablet o dispositivo móvil. Su instalación se produce generalmente sin el consentimiento o conocimiento del usuario.

2.1. Objetivos Comunes del Malware

- **Robo de Información:** Datos personales, bancarios, contraseñas.
- **Daño al Sistema:** Corrupción de archivos, ralentización del equipo, borrado de datos.
- **Control Remoto:** Permitir a un atacante tomar el control del dispositivo.
- **Extorsión:** Bloquear el acceso a archivos o al sistema hasta que se pague un rescate.
- **Espionaje:** Monitorear la actividad del usuario.
- **Propagación:** Infectar otros sistemas en una red.

3. Tipos Comunes de Malware

El malware ha evolucionado y se presenta en múltiples formas, cada una con métodos de operación y objetivos específicos.

3.1. Virus Informáticos

- **Descripción:** Programas maliciosos que se adjuntan a archivos o programas legítimos (huéspedes). Requieren que el usuario ejecute el programa infectado para que el virus se active y se propague.
- **Propagación:** Se insertan en ejecutables, documentos (macros), o sectores de arranque.
- **Acciones Típicas:** Corromper archivos, ralentizar sistemas, mostrar mensajes no deseados.
- **Analogía:** Como un virus biológico, necesita una "célula huésped" para reproducirse y causar daño.

3.2. Gusanos (Worms)

- **Descripción:** Programas maliciosos que tienen la capacidad de replicarse a sí mismos y propagarse a través de redes sin necesidad de adjuntarse a un programa huésped o de la intervención humana directa.
- **Propagación:** Exploran vulnerabilidades en la red (puertos abiertos, configuraciones débiles) para infectar otros equipos.
- **Acciones Típicas:** Consumir ancho de banda de la red, agotar recursos del sistema, actuar como "puerta trasera" para otro malware.
- **Analogía:** Como un "parásito de red" que se mueve de forma autónoma.

3.3. Troyanos (Trojan Horses)

- **Descripción:** Software malicioso que se disfraza de programa legítimo, útil o inofensivo para engañar al usuario y que lo instale. No se replican por sí mismos como virus o gusanos.
- **Propagación:** Descargas de software pirata, adjuntos de correo, sitios web fraudulentos.
- **Acciones Típicas:** Una vez ejecutados, abren "puertas traseras" (backdoors) para permitir el acceso remoto no autorizado al sistema, robar datos, o descargar más malware.
- **Analogía:** Como el caballo de Troya, parece un regalo, pero oculta enemigos dentro.

3.4. Spyware

- **Descripción:** Software diseñado para recopilar información sobre las actividades de un usuario sin su conocimiento ni consentimiento, y luego enviar esta información a un tercero.
- **Acciones Típicas:** Registrar pulsaciones de teclas (keyloggers), capturar pantallas, monitorear sitios web visitados, robar credenciales.
- **Propagación:** A menudo se instala junto con software gratuito o shareware.
- **Impacto:** Riesgos de privacidad y robo de identidad.

3.5. Adware

- **Descripción:** Software que muestra publicidad no deseada al usuario, a menudo en forma de ventanas emergentes, banners intrusivos o modificando la página de inicio del navegador.
- **Acciones Típicas:** Bombardear con anuncios, redirigir búsquedas a sitios patrocinados, ralentizar el navegador.
- **Propagación:** Frecuentemente incluido en instaladores de software gratuito.
- **Impacto:** Molestias, ralentización del sistema, posible puerta de entrada a otros malwares.

3.6. Ransomware

- **Descripción:** Un tipo de malware que cifra los archivos de un usuario o bloquea el acceso a su sistema, exigiendo un "rescate" (generalmente en criptomonedas) a cambio de la clave de descifrado o la restauración del acceso.
- **Acciones Típicas:** Cifrado de documentos, fotos, videos; bloqueo total del sistema.
- **Impacto:** Pérdida total o temporal de datos y operación del sistema, coste económico.
- **Una de las amenazas más rentables y devastadoras actualmente.**

4. Vectores de Infección del Malware

El malware utiliza diversas vías para infiltrarse en los sistemas. La mayoría de las infecciones ocurren debido a la interacción del usuario o la explotación de vulnerabilidades.

- **Correos Electrónicos (Phishing y Spam):**
  - **Phishing:** Correos que simulan ser de entidades legítimas (bancos, redes sociales, servicios conocidos) con el fin de engañar al usuario para que revele información sensible o haga clic en enlaces maliciosos.
  - **Adjuntos y Enlaces Maliciosos:** Archivos adjuntos infectados o enlaces que dirigen a sitios web comprometidos que descargan malware automáticamente.
- **Sitios Web Maliciosos o Comprometidos:**
  - **Descargas Falsas:** Sitios que ofrecen software pirata, cracks, o programas "gratuitos" que en realidad contienen malware.
  - **Exploits Kit (Drive-by Downloads):** Visitar un sitio web infectado puede llevar a la descarga e instalación automática de malware sin ninguna acción por parte del usuario, explotando vulnerabilidades en el navegador o complementos.
- **Dispositivos de Almacenamiento Externos:**
  - Unidades USB, discos duros externos o tarjetas de memoria infectadas pueden transferir malware al conectarse a un ordenador.
- **Redes y Conexiones Inseguras:**
  - **Redes Wi-Fi Públicas:** Conectarse a redes Wi-Fi abiertas y no seguras puede exponer el dispositivo a ataques "Man-in-the-Middle" o a la inyección de malware.
  - **Compartición de Archivos P2P:** La descarga de archivos de redes peer-to-peer (P2P) no controladas a menudo contiene malware.
- **Vulnerabilidades de Software:**
  - **Software Obsoleto:** Sistemas operativos, navegadores web y aplicaciones con versiones desactualizadas que contienen fallos de seguridad conocidos que los atacantes pueden explotar.

5. ¿Qué es un Antivirus?

Un **Antivirus** es un programa informático diseñado específicamente para **detectar, prevenir, identificar y eliminar** software malicioso de los sistemas. Actúa como la primera línea de defensa para proteger la integridad y la seguridad de los datos y el funcionamiento de los dispositivos.

5.1. Funciones Clave de un Antivirus

- **Escaneo y Detección:** Analiza archivos, programas y sistemas en busca de firmas o comportamientos asociados con malware.
- **Eliminación y Cuarentena:** Una vez detectado, el antivirus puede eliminar el malware, ponerlo en cuarentena (aislarlo para que no cause daño) o intentar repararlo.
- **Protección en Tiempo Real:** Monitoriza continuamente la actividad del sistema para detectar y bloquear amenazas en el momento en que intentan infectar.
- **Actualizaciones:** Recibe y descarga constantemente nuevas definiciones de virus (firmas) y mejoras de motor para reconocer las amenazas más recientes.
- **Cortafuegos (Firewall):** Muchos antivirus modernos incluyen funcionalidades de firewall para controlar el tráfico de red entrante y saliente, bloqueando accesos no autorizados.

5.2. Cómo Funciona un Antivirus

Los antivirus emplean una combinación de técnicas para identificar el malware:

- **Detección Basada en Firmas:**
  - **Descripción:** Es el método más tradicional y eficaz para malware conocido. El antivirus mantiene una base de datos (diccionario de firmas) de patrones de código únicos de miles de programas maliciosos. Cuando escanea un archivo, compara su código con estas firmas.

- **Limitación:** Solo detecta malware cuyas firmas ya están en su base de datos. Las nuevas amenazas (conocidas como "zero-day") pueden pasar desapercibidas hasta que se actualiza la base de datos.
- **Detección Heurística:**
- **Descripción:** Analiza el código de un programa en busca de características o instrucciones que son comunes en el malware, incluso si no coinciden con una firma exacta. Busca patrones sospechosos.
- **Ventaja:** Puede detectar malware nuevo o variantes de malware existentes para las que aún no hay una firma.
- **Limitación:** Mayor probabilidad de "falsos positivos" (identificar un programa legítimo como malware).
- **Análisis de Comportamiento:**
- **Descripción:** Ejecuta (o simula la ejecución de) programas en un entorno seguro (sandbox) y monitoriza sus acciones. Si un programa intenta realizar actividades sospechosas (ej., modificar archivos del sistema, conectarse a direcciones IP inusuales), el antivirus lo marca como malware.
- **Ventaja:** Muy efectivo contra malware de día cero y amenazas polimórficas (que cambian su código para evadir la detección por firmas).
- **Análisis Basado en la Nube:**
- **Descripción:** Envía información sobre archivos sospechosos a servidores en la nube para un análisis más rápido y el acceso a bases de datos de amenazas masivas y en tiempo real.

6. Mejores Prácticas para Protegerse

La ciberseguridad no es solo una herramienta, es una disciplina que requiere hábitos y conciencia.

- **Instalar y Mantener un Antivirus Actualizado:**
- Es la primera línea de defensa. Asegúrese de que esté siempre activo, con sus definiciones de virus actualizadas automáticamente.
- **Mantener el Sistema Operativo y Aplicaciones Actualizados:**
- Las actualizaciones de software (Windows Update, macOS updates, actualizaciones de navegador, etc.) a menudo incluyen parches de seguridad para vulnerabilidades descubiertas. Active las actualizaciones automáticas.
- **Ser Cauteloso con Correos Electrónicos y Enlaces:**
- No abra adjuntos ni haga clic en enlaces de correos electrónicos de remitentes desconocidos o sospechosos.
- Verifique la dirección del remitente y pase el ratón sobre los enlaces antes de hacer clic para ver la URL real.
- **Descargar Software de Fuentes Confiables:**
- Utilice solo las tiendas de aplicaciones oficiales (Google Play Store, Apple App Store, Microsoft Store) o los sitios web oficiales de los desarrolladores.
- Evite las descargas de sitios de terceros no verificados o de software pirata.
- **Usar Contraseñas Fuertes y Únicas:**
- Utilice combinaciones complejas de letras mayúsculas y minúsculas, números y símbolos.
- Evite reutilizar la misma contraseña para múltiples cuentas. Considere usar un gestor de contraseñas.
- **Realizar Copias de Seguridad (Backups) Regularmente:**
- Guarde sus datos importantes (documentos, fotos, videos) en un lugar separado del dispositivo principal (ej., en la nube, en un disco duro externo). Esto es crucial en caso de un ataque de ransomware o fallo del sistema.
- **Habilitar el Cortafuegos (Firewall):**

- El firewall (integrado en el sistema operativo o en su antivirus) controla el tráfico de red para bloquear accesos no autorizados a su equipo.

- **Educación y Conciencia:**
- La mejor defensa es un usuario informado. Manténgase al tanto de las últimas amenazas y técnicas de ingeniería social

II. Medidas de Almacenamiento

1. Medidas de Almacenamiento: El Tamaño de los Datos

La información en las computadoras se almacena y procesa utilizando el **sistema binario**, que se basa en dos estados: 0 o 1. A partir de esta unidad mínima, se construyen todas las demás medidas.

1.1. Unidades Fundamentales

- **Bit (Binary Digit):**
- Es la **unidad más pequeña de información** en un sistema informático.
- Puede representar solo uno de dos valores: **0** (apagado) o **1** (encendido).
- Es el "átomo" de los datos digitales.
- **Byte:**
- Un grupo de **8 bits**.
- Es la **unidad básica** para almacenar un solo carácter (como una letra, un número o un símbolo). Por ejemplo, la letra 'A' en el código ASCII se representa con un byte.
- Es la medida más pequeña que la mayoría de los sistemas de almacenamiento pueden direccionar.

1.2. Jerarquía de Medidas de Almacenamiento (Basado en Potencias de 2 o 10)

Aunque tradicionalmente se usan potencias de 10 (1 KB = 1000 Bytes) para simplificar, en informática es más preciso usar potencias de 2 (1 KiB = 1024 Bytes). Para propósitos generales y de marketing de hardware, se suele usar la base 10. Para este contexto, usaremos la aproximación más común (base 1000 para simplicidad, pero con la base 1024 en mente para precisión técnica).

- **Kilobyte (KB):**
- Aproximadamente **1,000 Bytes** (10^3 Bytes). Técnicamente, 1 KiB = 1,024 Bytes.
- **Ejemplo:** Un documento de texto corto, una imagen muy pequeña.
- **Megabyte (MB):**
- Aproximadamente **1,000 Kilobytes** (10^6 Bytes). Técnicamente, 1 MiB = 1,024 KiB.
- **Ejemplo:** Una canción en formato MP3, una imagen de alta resolución, un documento PDF con varias páginas.
- **Gigabyte (GB):**
- Aproximadamente **1,000 Megabytes** (10^9 Bytes). Técnicamente, 1 GiB = 1,024 MiB.
- **Ejemplo:** Una película en calidad estándar, un software de aplicación, la capacidad de un USB común.

- **Terabyte (TB):**
  - Aproximadamente **1,000 Gigabytes** (10^12 Bytes). Técnicamente, 1 TiB = 1,024 GiB.
  - **Ejemplo:** La capacidad de los discos duros modernos para computadoras personales, grandes colecciones de videos o fotografías.
- **Petabyte (PB):**
  - Aproximadamente **1,000 Terabytes** (10^15 Bytes).
  - **Ejemplo:** Almacenamiento a gran escala en centros de datos, grandes bases de datos.
- **Exabyte (EB):**
  - Aproximadamente **1,000 Petabytes** (10^18 Bytes).
  - **Ejemplo:** El volumen total de datos en internet o en grandes infraestructuras de nube.

2. Formatos de Archivos: El Lenguaje de los Datos

Un **formato de archivo** es un método estándar para organizar y almacenar datos digitales. Define la estructura interna de un archivo, lo que permite a los programas informáticos reconocer, leer y procesar correctamente la información contenida en él. La **extensión de archivo** (las letras después del punto en el nombre del archivo, ej., .txt, .jpg) es un indicador visual común del formato.

2.1. Importancia de los Formatos de Archivos

- **Compatibilidad:** Asegura que diferentes programas puedan abrir y trabajar con el mismo tipo de archivo.
- **Funcionalidad:** Determina qué tipo de datos puede almacenar un archivo (texto, imagen, audio, video) y qué características especiales puede soportar (compresión, transparencia, animación).
- **Optimización:** Algunos formatos están diseñados para ahorrar espacio (compresión) o para preservar la calidad.

2.2. Tipos Comunes de Archivos por Categoría

2.2.1. Archivos de Documentos y Texto

- **Texto Plano (.txt):**
  - Contiene solo caracteres de texto sin ningún tipo de formato (negrita, cursiva, fuentes, colores).
  - **Ventajas:** Muy ligero, universalmente compatible, fácil de abrir con cualquier editor de texto.
- **Documento de Word (.doc, .docx):**
  - Formato propietario de Microsoft Word. Permite formato avanzado (fuentes, colores, tablas, imágenes), objetos incrustados, y más.
  - **.doc:** Formato antiguo (hasta Word 2003).
  - **.docx:** Formato moderno basado en XML, más compacto y robusto.
- **Documento PDF (.pdf - Portable Document Format):**
  - Desarrollado por Adobe. Mantiene el diseño, fuentes, imágenes y gráficos del documento original, independientemente del software o hardware utilizado para verlo.
  - **Ventajas:** Ideal para compartir documentos que deben mantener su apariencia exacta.
- **Hoja de Cálculo (.xls, .xlsx):**
  - Formatos para almacenar datos tabulares, fórmulas, gráficos y funciones. Usados principalmente por Microsoft Excel.

- **.xls:** Formato antiguo.
- **.xlsx:** Formato moderno basado en XML.

- **Presentación (.ppt, .pptx):**
- Formatos para crear diapositivas con texto, imágenes, audio, video y transiciones. Usados principalmente por Microsoft PowerPoint.
- **.ppt:** Formato antiguo.
- **.pptx:** Formato moderno basado en XML.

2.2.2. Archivos Multimedia

- **Imágenes:**
- **.jpg / .jpeg:** (Joint Photographic Experts Group) Ideal para fotografías digitales. Utiliza compresión con pérdida, lo que significa que reduce el tamaño del archivo a expensas de una pequeña pérdida de calidad (generalmente imperceptible).
- **.png:** (Portable Network Graphics) Ideal para gráficos, logos, imágenes con transparencias. Utiliza compresión sin pérdida, manteniendo la calidad original.
- **.gif:** (Graphics Interchange Format) Soporta animaciones cortas y transparencias simples. Ideal para imágenes web pequeñas y animaciones repetitivas.

- **Audio:**
- **.mp3:** (MPEG-1 Audio Layer 3) Formato más popular para música digital. Utiliza compresión con pérdida para reducir drásticamente el tamaño del archivo manteniendo una calidad aceptable.
- **.wav:** (Waveform Audio File Format) Formato de audio sin comprimir desarrollado por Microsoft. Ofrece alta calidad de sonido, pero los archivos son muy grandes.

- **Video:**
- **.mp4:** (MPEG-4 Part 14) Formato versátil y ampliamente utilizado. Permite alta compresión sin mucha pérdida de calidad, ideal para streaming y dispositivos móviles.
- **.avi:** (Audio Video Interleave) Desarrollado por Microsoft. Puede contener audio y video en diferentes códecs, pero los archivos tienden a ser grandes.
- **.mov:** (QuickTime File Format) Desarrollado por Apple. Comúnmente usado en productos Apple.

2.2.3. Archivos Comprimidos y Ejecutables

- **Archivos Comprimidos (.zip, .rar, .7z):**
  - Contenedores que agrupan uno o más archivos y carpetas en un solo archivo, a menudo reduciendo su tamaño para facilitar el almacenamiento y la transferencia.
  - Requieren un programa de descompresión (ej., WinRAR, 7-Zip) para acceder a su contenido.
- **Archivos Ejecutables (.exe, .app, .msi):**
  - Contienen instrucciones de programa que un sistema operativo puede ejecutar directamente.
  - **.exe:** Común en Windows.
  - **.app:** Común en macOS.
  - **.msi:** Instaladores de Windows.
  - **Advertencia:** Son un vector común para malware, por lo que deben tratarse con precaución y solo descargarse de fuentes confiables.

3. Navegación entre Archivos: Organizando tu Espacio Digital

La **navegación entre archivos** se refiere al proceso de moverse a través de la estructura de directorios y archivos de un sistema informático para localizar, acceder y gestionar la información. El **sistema de archivos** es la manera en que el sistema operativo organiza y controla cómo se almacenan y recuperan los datos en un dispositivo de almacenamiento.

3.1. Estructura Jerárquica del Sistema de Archivos

Los sistemas de archivos modernos (como NTFS en Windows, HFS+ y APFS en macOS, o ext4 en Linux) organizan los datos en una estructura de **árbol o jerárquica**:

- **Carpetas (Directorios):** Son contenedores que pueden almacenar archivos y otras carpetas (subcarpetas). Ayudan a organizar lógicamente la información.
- **Carpeta Raíz:** Es el punto de inicio de la jerarquía de una unidad de almacenamiento.
    - En Windows, cada unidad tiene su propia raíz (ej., C:\, D:\).
    - En Linux/macOS, hay una única raíz / de la que cuelgan todos los demás directorios.

3.2. Rutas de Archivos

Una **ruta de archivo** es una cadena de texto que especifica la ubicación única de un archivo o carpeta dentro del sistema de archivos.

- **Ruta Absoluta:**
    - Define la ubicación completa del archivo desde la **carpeta raíz** de la unidad.
    - **Ejemplo (Windows):** C:\Usuarios\Documentos\Informes\informe_ventas.xlsx
    - **Ejemplo (Linux/macOS):** /home/usuario/documentos/informes/informe_ventas.xlsx
    - Siempre apuntan a la misma ubicación, sin importar dónde se encuentre el usuario actualmente.
- **Ruta Relativa:**
    - Define la ubicación del archivo en relación con el **directorio de trabajo actual** (la carpeta donde se encuentra el usuario en ese momento).
    - **./**: Representa el directorio actual.
    - **../**: Representa el directorio padre (un nivel arriba).
    - **Ejemplo:** Si estás en C:\Usuarios\Documentos y quieres acceder a C:\Usuarios\Documentos\Informes\factura.pdf, la ruta relativa sería .\Informes\factura.pdf o simplemente Informes\factura.pdf.
    - Si estás en C:\Usuarios\Documentos\Informes y quieres acceder a C:\Usuarios\Musica\cancion.mp3, la ruta relativa sería ..\..\Musica\cancion.mp3.

3.3. Gestión de Archivos con el Explorador de Archivos (Windows) / Finder (macOS)

Estas son las interfaces gráficas principales para interactuar con el sistema de archivos:

- **Crear Carpetas y Archivos:**
    - Haz clic derecho en un espacio vacío en la carpeta deseada, selecciona "Nuevo" y elige "Carpeta" o el tipo de documento.
- **Eliminar:**
    - Selecciona el archivo o carpeta y presiona la tecla Supr (Delete) o arrástralo a la "Papelera de Reciclaje" (Windows) / "Papelera" (macOS). Los elementos en la papelera se pueden restaurar antes de ser eliminados permanentemente.

- **Renombrar:**
    - Selecciona el archivo o carpeta, haz clic derecho y elige "Cambiar nombre", o selecciona y presiona la tecla F2 (en Windows) o Enter (en macOS, después de seleccionar).
- **Mover (Cortar y Pegar):**
    - **Cortar:** Selecciona el elemento y usa Ctrl+X (Windows) / Cmd+X (macOS).
    - **Pegar:** Ve a la ubicación de destino y usa Ctrl+V (Windows) / Cmd+V (macOS). El elemento se moverá de su ubicación original a la nueva.
- **Copiar (Copiar y Pegar):**
    - **Copiar:** Selecciona el elemento y usa Ctrl+C (Windows) / Cmd+C (macOS).
    - **Pegar:** Ve a la ubicación de destino y usa Ctrl+V (Windows) / Cmd+V (macOS). Se creará una copia del elemento en la nueva ubicación, manteniendo el original.
- **Buscar:**
    - Utiliza la barra de búsqueda integrada en la parte superior del explorador para encontrar archivos o carpetas por nombre, tipo, fecha de modificación, etc.