# ACTIVIDAD FUNDAMENTAL 4

Oscar Eduardo Hernández Córdova 1960609 ITS

Rodolfo Rosas Andrade 1945699 IAS

Asael Abisai Scott Garza 1947203 ITS

# Introducción a la Seguridad Informática

- La seguridad informática es la práctica de proteger los sistemas de información y los datos que contienen de amenazas externas e internas.
- En un mundo cada vez más digital, la seguridad informática se ha convertido en una necesidad crítica para individuos, empresas y gobiernos.
- La seguridad informática abarca desde la protección contra virus y malware hasta la prevención de ciberataques sofisticados.

# Historia de las Amenazas Informáticas

- Las amenazas informáticas existen desde los primeros días de la informática.
- El primer virus informático conocido, llamado "Creeper", fue creado en 1971 por un programador llamado Robert Thomas. Desde entonces, las amenazas informáticas han evolucionado y se han vuelto cada vez más sofisticadas.
- En la década de 1990, los gusanos informáticos como el "ILOVEYOU" y el "Melissa" causaron estragos en todo el mundo, y en la década de 2000, los troyanos y el malware se convirtieron en amenazas comunes. Hoy en día, los ataques de ransomware son una de las amenazas de seguridad más peligrosas para los individuos y las empresas.

# Tipos de Amenazas Informáticas

Existen varios tipos de amenazas informáticas, cada una con sus propias características y formas de propagación. Los tipos de amenazas más comunes incluyen:

- Virus informáticos.
- Malware.
- Gusanos informáticos.
- Troyanos.
- Spyware.
- Adware.
- Ransomware.

# Virus Informáticos


- Los virus informáticos son programas que se propagan al adjuntarse a archivos legítimos y que pueden causar daño a los sistemas. Los virus informáticos pueden ser propagados por medios como correo electrónico, descargas de archivos, discos de almacenamiento y redes.

- Algunos de los efectos dañinos de los virus informáticos pueden incluir la eliminación de archivos, el robo de información personal, la interrupción de la red y la degradación del rendimiento de la computadora.

- Es importante tener un software antivirus actualizado y escanear regularmente los sistemas para detectar y eliminar virus informáticos. Además, es importante tener precaución al abrir correos electrónicos de remitentes desconocidos o al descargar archivos de sitios web no confiables.

# Malware

- ✓ El malware es un término que se utiliza para referirse a programas maliciosos diseñados para dañar o tomar el control de una computadora. El malware puede ser propagado por medios como correo electrónico, sitios web, descargas de archivos y redes.
- ✓ Los tipos comunes de malware incluyen virus, gusanos, troyanos, spyware, adware y ransomware. El malware puede causar problemas como la eliminación de archivos, la degradación del rendimiento del sistema, la interrupción de la red y la captura de información personal.
- ✓ Es importante tener un software de seguridad actualizado y escanear regularmente los sistemas para detectar y eliminar malware. Además, es importante tener precaución al abrir correos electrónicos de remitentes desconocidos o al descargar archivos de sitios web no confiables.

# Gusanos Informáticos

- Los gusanos informáticos son programas que se propagan a través de redes y sistemas, replicándose y consumiendo recursos de la computadora. Los gusanos pueden ser propagados por medios como correo electrónico, sitios web, mensajería instantánea y redes sociales.

- Los gusanos informáticos pueden causar problemas como la ralentización de la red, la degradación del rendimiento del sistema y el robo de información personal. Algunos gusanos incluso pueden abrir puertas traseras en el sistema, permitiendo que los atacantes tomen el control remoto de la computadora.

- Es importante tener un software de seguridad actualizado y escanear regularmente los sistemas para detectar y eliminar gusanos informáticos. Además, es importante tener precaución al abrir correos electrónicos de remitentes desconocidos o al hacer clic en enlaces desconocidos.

# Troyanos

- Los troyanos son programas maliciosos que se disfrazan como software legítimo para engañar a los usuarios y hacer que instalen el programa en su computadora. Los troyanos pueden ser propagados por medios como correo electrónico, descargas de software y sitios web comprometidos.

- Una vez instalado, el troyano puede dar a los atacantes acceso remoto a la computadora y permitirles controlarla. Los troyanos también pueden ser diseñados para robar información personal, como contraseñas, información bancaria y de tarjetas de crédito.

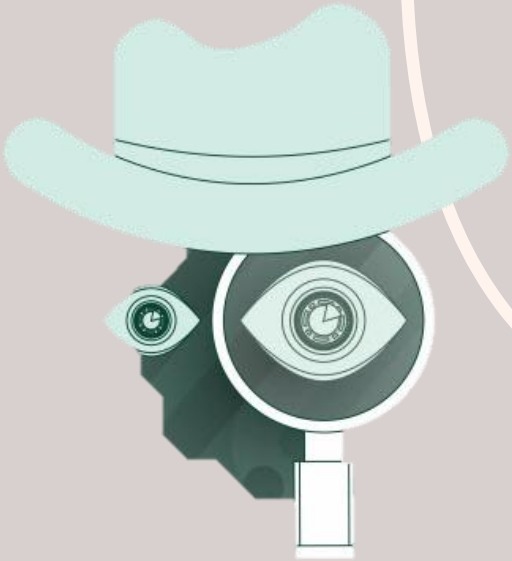
- Es importante tener precaución al descargar e instalar software de fuentes desconocidas. Además, es importante tener un software de seguridad actualizado y escanear regularmente los sistemas para detectar y eliminar troyanos.

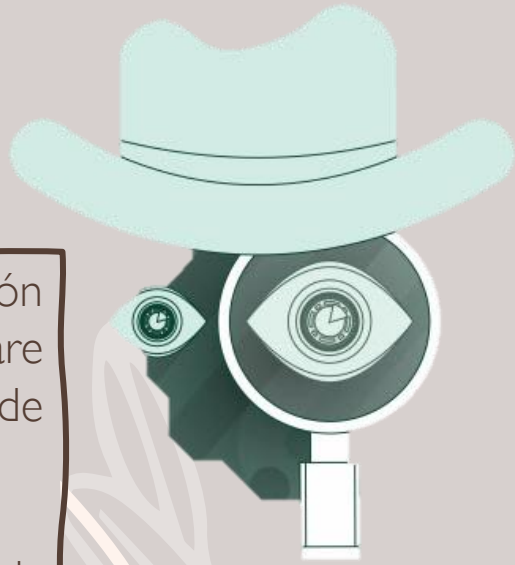
# Spyware

- El spyware es un software malicioso diseñado para recopilar información personal del usuario sin su conocimiento o consentimiento. El spyware puede ser propagado por medios como correo electrónico, descargas de software y sitios web comprometidos.

- Los efectos del spyware pueden incluir la ralentización del sistema, la aparición de anuncios emergentes no deseados y la recopilación de información personal, como contraseñas y datos bancarios.

- Es importante tener un software de seguridad actualizado y escanear regularmente los sistemas para detectar y eliminar spyware. Además, es importante tener precaución al descargar e instalar software de fuentes desconocidas y al hacer clic en enlaces desconocidos.





# Adware

- El adware es un software malicioso que muestra anuncios no deseados en la computadora del usuario. El adware puede ser propagado por medios como correo electrónico, descargas de software y sitios web comprometidos.

- Los efectos del adware pueden incluir la ralentización del sistema, la aparición de anuncios emergentes no deseados y la recopilación de información personal.

- Es importante tener un software de seguridad actualizado y escanear regularmente los sistemas para detectar y eliminar adware. Además, es importante tener precaución al descargar e instalar software de fuentes desconocidas y al hacer clic en enlaces desconocidos.

# Ransomware

- El ransomware es un tipo de software malicioso que encripta los archivos de la computadora del usuario y exige un rescate para restaurar el acceso a los archivos. El ransomware puede ser propagado por medios como correo electrónico, descargas de software y sitios web comprometidos.

- Los efectos del ransomware pueden incluir la pérdida permanente de datos y la interrupción de las operaciones comerciales y personales. Los ataques de ransomware son comunes en empresas y organizaciones gubernamentales.

- Es importante tener precaución al descargar e instalar software de fuentes desconocidas y tener un software de seguridad actualizado y escanear regularmente los sistemas para detectar y eliminar ransomware. Además, se recomienda realizar copias de seguridad de los datos importantes en caso de un ataque de ransomware.

# Tipos de intrusos

# Hackers

Son individuos con habilidades técnicas que utilizan sus conocimientos para acceder a sistemas informáticos sin autorización. Pueden ser motivados por fines financieros, políticos o simplemente por el desafío técnico. Los hackers pueden ser clasificados en tres tipos principales: white hat (éticos), grey hat (neutrales) y black hat (maliciosos).

# Crackers

Son individuos con habilidades técnicas que utilizan sus conocimientos para acceder a sistemas informáticos sin autorización. Pueden ser motivados por fines financieros, políticos o simplemente por el desafío técnico. Los hackers pueden ser clasificados en tres tipos principales: white hat (éticos), grey hat (neutrales) y black hat (maliciosos).

# Insiders

Son personas con acceso legítimo a un sistema o red, como empleados o contratistas, que utilizan su acceso para realizar actividades maliciosas. Los insiders pueden ser clasificados en dos tipos principales: los que actúan intencionalmente y los que actúan sin saberlo.

# Phishers

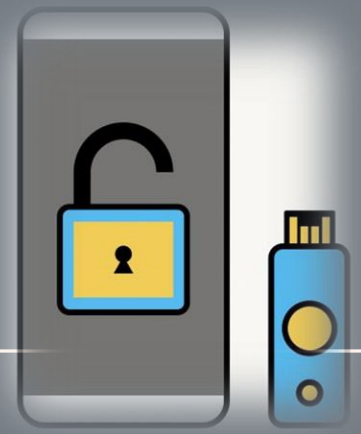
Son individuos que utilizan técnicas de ingeniería social para obtener información confidencial, como contraseñas o información financiera, de los usuarios. Los phishers a menudo utilizan correos electrónicos o sitios web falsos para engañar a los usuarios y hacerles revelar información.

# Tipos de autentificaciones

1. Autenticación por contraseña: Es el tipo de autenticación más común y se basa en el uso de una contraseña o clave secreta para verificar la identidad de un usuario. La contraseña es comparada con una versión almacenada en el sistema y si coincide, se permite el acceso.
2. Autenticación de dos factores (2FA): Este método de autenticación requiere que el usuario proporcione dos formas diferentes de verificación de identidad, como una contraseña y un código enviado a través de SMS o una aplicación de autenticación.


# Tipos de autentificaciones

3. Autenticación de token: Este método utiliza un dispositivo físico, como una llave USB o una tarjeta inteligente, para verificar la identidad del usuario. El token contiene información que identifica al usuario y se utiliza para acceder a sistemas o recursos en línea.
4. Autenticación basada en la red: Este tipo de autenticación utiliza la dirección IP del usuario o la ubicación geográfica para verificar la identidad del usuario y permitir el acceso a recursos o sistemas en línea.



# Nivel de seguridad de usuario:

- Implementar autenticación de dos factores.
- Utilizar contraseñas seguras y cambiarlas regularmente.
- Instalar software de seguridad, como un antivirus, un firewall personal, y software de cifrado.
- Mantener el software actualizado para corregir posibles vulnerabilidades.
- Evitar el uso de redes Wi-Fi públicas y desconocidas.
- Realizar copias de seguridad regularmente de los datos importantes.
- Deshabilitar o eliminar cuentas de usuario inactivas o no utilizadas..

# Red

- Utilizar firewalls para proteger los accesos a la red.
- Segmentar la red para reducir el impacto de una posible brecha de seguridad.
- Establecer políticas de acceso a la red y utilizar sistemas de autenticación seguros.
- Monitorear constantemente la red para detectar posibles amenazas o brechas de seguridad.
- Implementar una política de actualizaciones y parches para corregir posibles vulnerabilidades en el software.
- Realizar pruebas de penetración para evaluar la seguridad de la red.

# Empresa

- Establecer una política de seguridad clara y efectiva para toda la organización.
- Educar a los empleados sobre las amenazas de seguridad y cómo prevenirlas.
- Implementar medidas de seguridad física, como el control de acceso a las instalaciones y la protección de los activos.
- Establecer una política de copias de seguridad y recuperación de datos en caso de una posible brecha de seguridad.
- Realizar auditorías de seguridad periódicas para evaluar la efectividad de las medidas de seguridad implementadas.
- Establecer un plan de respuesta ante posibles incidentes de seguridad.
- Utilizar tecnologías avanzadas de seguridad, como la detección de intrusiones y el análisis de comportamiento de la red.

# Análisis de posibles problemas

El análisis de riesgos permite conocer todos los activos relacionados con la información de la empresa, identificando amenazas y vulnerabilidades que permitan definir los riesgos reales a los que se expone la información y los sistemas.

# Riesgos del hardware

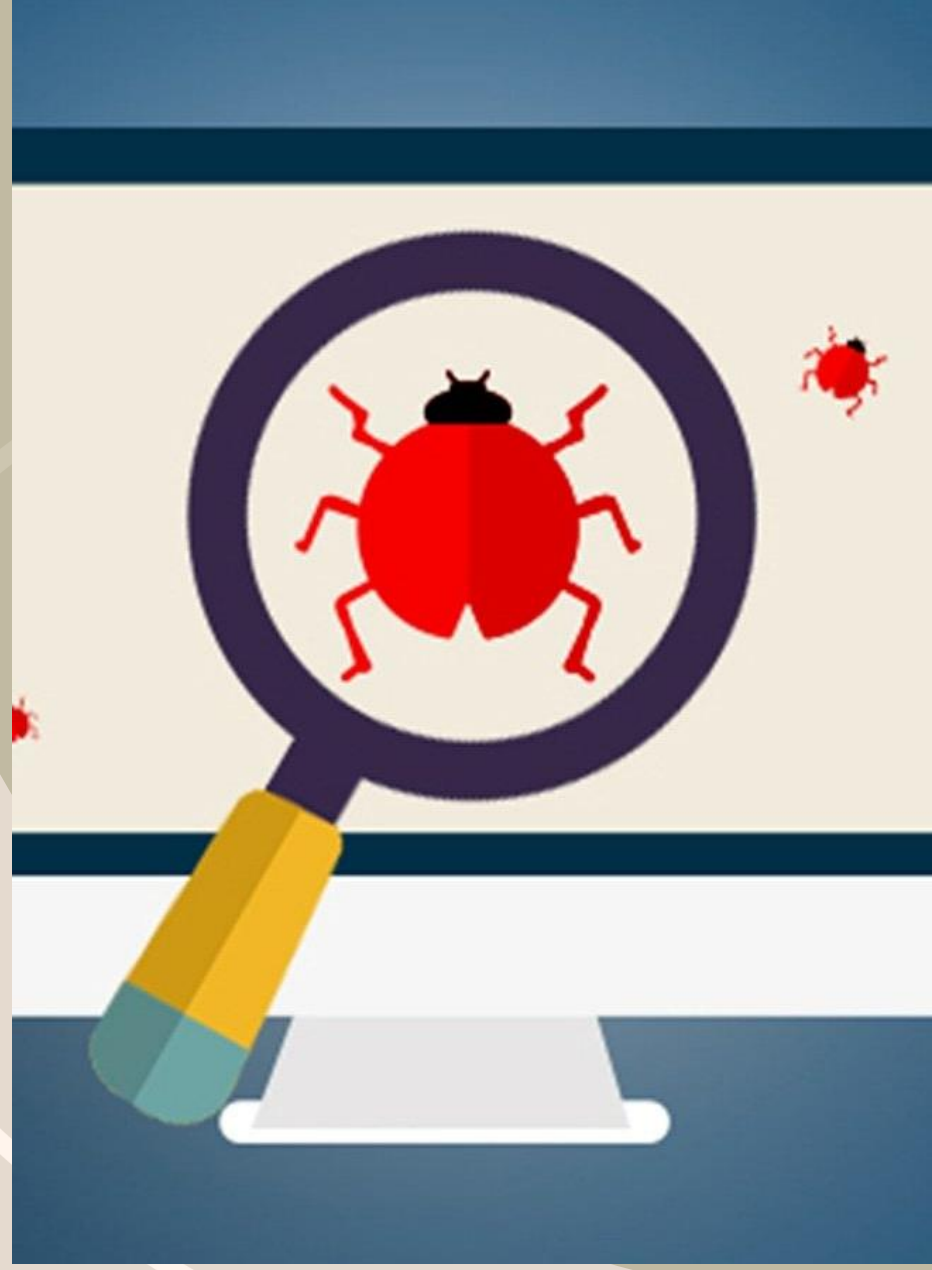
Se da la amenaza por fallas físicas que presente cualquiera de los elementos de hardware que conforman al sistema de cómputo. Estas fallas físicas pueden ser defectos de fabricación o mal diseño del hardware, pero también pueden ser el resultado de un mal uso y descuido en el mantenimiento.

# Problemas mas comunes del hardware

- Fallos en la tarjeta gráfica o el chip gráfico.
- Problemas de memoria RAM.
- Fallos en la CPU o microprocesador.
- Problemas en la placa base.
- Fallos de disco duro.

# Problemas con el sotfware

Un error de software, error o simplemente fallo (también conocido por el inglés, bug) es un problema en un programa de computador o sistema de software que desencadena un resultado indeseado.



# Principales problemas del sotfware

- Desconocimiento de la tecnología base del proyecto.
- Necesidad de tecnología inmadura.
- Alto nivel de complejidad técnica.
- Integraciones con sistemas externos desconocidos.

# Riesgos de archivos informaticos


- Ataques DDoS
- Phishing
- Robo de datos
- Spam
- Virus informático

# Riesgos de la red

Entre los principales hallazgos, se determinó que los mayores peligros de las redes sociales para las personas menores de edad son el ciberbulling, grooming, sexting y adicción, los cuales, sin una adecuada educación en seguridad cibernética, les hace más vulnerables.