# Introducción a la seguridad informática

## Objetivos

Los objetivos de esta introducción a la seguridad informática son los siguientes:

1. Comprender los conceptos básicos de seguridad y seguridad informática.
2. Diferenciar entre medidas de seguridad activa y pasiva.
3. Reconocer la necesidad de la seguridad en redes.
4. Identificar diferentes tipos de software malicioso (malware) y sus clasificaciones.
5. Conocer las herramientas de protección y desinfección de malware.
6. Reflexionar sobre la paradoja de la seguridad.

## Mapa conceptual

- **Seguridad**: concepto general.
    - **Seguridad Informática**: protección de la información y sistemas.
        - **Medidas de seguridad**:
            - **Activa**
            - **Pasiva**
        - **Seguridad en redes**
        - **Software malicioso (malware)**:
            - **Clasificación de malware**
            - **Herramientas de protección y desinfección**

- **Paradoja de la seguridad**

# Glosario

- **Seguridad**: Estado en el cual se está libre de peligro o daño.
- **Seguridad Informática**: Protección de la información digital y los sistemas de información contra accesos no autorizados, ataques, o daños.
- **Medidas de seguridad activa**: Acciones preventivas diseñadas para impedir ataques y accesos no autorizados.
- **Medidas de seguridad pasiva**: Acciones reactivas que minimizan el impacto de un ataque después de que ha ocurrido.
- **Red**: Conjunto de equipos informáticos interconectados para compartir recursos.
- **Malware**: Software malicioso diseñado para dañar, interferir o acceder a sistemas informáticos sin el consentimiento del usuario.

# 1.1. Introducción

La seguridad informática es un campo vital que abarca la protección de sistemas, redes y datos contra amenazas y ataques. Con el incremento del uso de la tecnología en todas las áreas de la vida, la seguridad informática se ha convertido en una necesidad fundamental para proteger la integridad y confidencialidad de la información.

# 1.2. Los conceptos de seguridad y seguridad informática

La seguridad, en términos generales, se refiere a la protección contra el peligro o daño. En el contexto de la informática, la seguridad informática se centra en proteger los sistemas y la información digital contra accesos no autorizados, alteraciones y destrucción. Esto incluye la implementación de medidas preventivas y reactivas para asegurar la confidencialidad, integridad y disponibilidad de los datos.

# 1.3. Tipos de medidas de seguridad: activa y pasiva

## 1.3.1. Seguridad activa

Las medidas de seguridad activa están diseñadas para prevenir los ataques antes de que ocurran. Incluyen técnicas y herramientas como:

- **Firewalls**: Dispositivos que filtran el tráfico de red no autorizado.
- **Antivirus**: Software que detecta y elimina virus y otros tipos de malware.
- **Sistemas de Detección y Prevención de Intrusos (IDS/IPS)**: Monitorean la red y los sistemas en busca de actividades sospechosas y bloquean posibles amenazas.

## 1.3.2. Seguridad pasiva

Las medidas de seguridad pasiva están destinadas a minimizar el daño y recuperarse después de un ataque. Incluyen:

- **Copias de seguridad (Backups)**: Realización de copias de los datos para restaurarlos en caso de pérdida o daño.
- **Sistemas de recuperación ante desastres**: Procedimientos y tecnologías para recuperar sistemas y datos después de un evento catastrófico.
- **Registro y monitorización**: Mantener registros detallados de las actividades del sistema para analizar y responder a incidentes de seguridad.

# 1.4. Necesidad de la seguridad en red

Las redes son una parte integral de las infraestructuras tecnológicas actuales. La seguridad en red es crucial para proteger la información en tránsito, prevenir accesos no autorizados y mantener la integridad y disponibilidad de los servicios. Esto es especialmente importante en entornos empresariales donde la interrupción de los servicios de red puede resultar en pérdidas significativas.

# 1.5. Software malicioso

El malware, o software malicioso, se refiere a cualquier programa diseñado para causar daño a una computadora, red o usuario. El malware puede robar información, destruir datos, espiar a los usuarios o tomar el control de los sistemas infectados.

## 1.5.1. Clasificación de malware

El malware puede clasificarse en varias categorías según su comportamiento y método de propagación:

- **Virus**: Programas que se adhieren a otros archivos y se propagan al ejecutarse el archivo infectado.

- **Gusanos**: Programas que se replican automáticamente y se propagan a través de redes sin necesidad de intervención humana.
- **Troyanos**: Programas maliciosos que se disfrazan de software legítimo para engañar a los usuarios y obtener acceso a sus sistemas.
- **Spyware**: Software que recopila información sobre un usuario sin su conocimiento.
- **Ransomware**: Malware que cifra los archivos de la víctima y exige un rescate para liberar los datos.
- **Adware**: Software que muestra anuncios no deseados y puede recopilar información sobre los hábitos de navegación del usuario.
- **Rootkits**: Programas que proporcionan acceso no autorizado a un sistema y ocultan su presencia.

## 1.5.2. Herramientas de protección y desinfección de malware

Existen diversas herramientas para protegerse contra el malware y eliminar infecciones:

- **Antivirus**: Detecta y elimina virus y otros tipos de malware.
- **Anti-spyware**: Identifica y elimina spyware.
- **Firewalls**: Filtran el tráfico de red y bloquean accesos no autorizados.
- **Herramientas de Remoción de Ransomware**: Desencriptan archivos secuestrados por ransomware.
- **Actualizaciones de Seguridad**: Mantener el software actualizado para protegerse contra vulnerabilidades conocidas.

# 1.6. La paradoja de la seguridad

La paradoja de la seguridad se refiere a la tensión entre la necesidad de seguridad y la facilidad de uso. A medida que se implementan medidas de seguridad más estrictas, a menudo se dificulta el acceso y uso de los sistemas. Encontrar un equilibrio entre seguridad y usabilidad es un desafío constante en la gestión de la seguridad informática.

La seguridad informática es un campo dinámico y en constante evolución. La comprensión y aplicación de medidas de seguridad adecuadas son esenciales para proteger la información y los sistemas en el mundo digital actual.