# UD 1: Adopción de pautas de seguridad informática

## Introducción a la Seguridad Informática

\* Pilares fundamentales de la seguridad informática

\* Elementos vulnerables en el sistema informático

\* Análisis de las principales vulnerabilidades del sistema informático

\* Amenazas

\* Seguridad física y ambiental

\* Seguridad lógica

\* Análisis forense

## ¿Qué es un Sistema de Información? ¿Qué es un Sistema Informático?

### Sistema de Información (SI)

\* Definición: Conjunto de elementos organizados para facilitar el funcionamiento de una empresa.

\* Elementos:

\* Recursos (físicos y lógicos)

\* Equipo humano

\* Información (datos)

\* Actividades

### Sistema Informático

\* Definición: Conjunto de elementos físicos, lógicos y humanos.

## ¿Qué es la Seguridad Informática?

\* Definición: Disciplina que diseña normas, procedimientos, métodos y técnicas para un sistema de información seguro y confiable.

## Pilares Fundamentales de la Seguridad Informática

\* Integridad, Confidencialidad y Disponibilidad

### Integridad

\* Garantiza que los datos no se alteren de forma no autorizada.

### Confidencialidad

\* Asegura que la información solo esté disponible para personas autorizadas.

### Disponibilidad

\* Garantiza que los sistemas, servicios y datos estén accesibles cuando sea necesario.

### La Paradoja de la Seguridad

\* Equilibrio entre funcionalidad, usabilidad y seguridad.

## Elementos Vulnerables en el Sistema Informático

\* Hardware, Software, Datos y Redes

### Hardware

\* Componentes físicos del sistema.

\* Riesgos: Daños físicos, robo.

### Software

\* Sistema operativo y aplicaciones.

\* Riesgos: Errores de codificación, configuraciones inseguras, falta de actualizaciones.

### Datos

\* Activos valiosos.

\* Riesgos: Acceso no autorizado, falta de cifrado.

### Redes

\* Conectan componentes del sistema.

\* Riesgos: Intercepción de datos, ataques de denegación de servicio.

## Análisis de las Principales Vulnerabilidades de un Sistema Informático

\* Identificar y evaluar debilidades.

### Elementos a Estudiar en un Análisis de Riesgos

\* Activos

\* Amenazas

\* Vulnerabilidad (Debilidad)

\* Riesgo

\* Ataque

\* Impacto

### Vulnerabilidades Más Comunes

\* Errores de programación

\* Configuraciones inseguras

\* Vulnerabilidades no parcheadas

### Herramientas de Análisis de Vulnerabilidades

\* Nessus

\* OpenVAS

\* Nmap

## Tipos de Amenazas

\* Amenazas Físicas

\* Amenazas Lógicas

### Amenazas Físicas

\* Afectan al hardware e infraestructura física.

\* Incendios y desastres naturales

\* Cortes de suministro eléctrico

\* Robo de equipos

### Amenazas Lógicas

\* Afectan al software, datos y redes.

\* Virus y malware

\* Ransomware

\* Phishing

## Seguridad Física y Ambiental

\* Medidas para prevenir daños o robos.

### Ubicación y Protección Física de los Equipos y Servidores

\* Controles de acceso

\* Videovigilancia

\* Protección contra incendios

\* Sistemas de alimentación ininterrumpida (SAI)

## Seguridad Lógica

\* Medidas implementadas en el software y los datos.

### Criptografía

\* Cifrado simétrico

\* Cifrado asimétrico

\* Criptografía híbrida

### Listas de Control de Acceso (ACL)

\* ACE (Access Control Entry)

### Establecimiento de Política de Contraseñas

### Utilización de Sistemas Biométricos de Identificación

\* Ventajas

\* Desventajas

### Políticas de Almacenamiento

### Copias de Seguridad e Imágenes de Respaldo

\* Tipos de copias: Completa, incremental y diferencial

\* Tolerancia a fallos (RAID)

\* Imágenes de respaldo (Clonezilla o Acronis)

### Medios de Almacenamiento

### Recuperación de Datos

### Realización de Auditorías de Seguridad

\* Auditorías de seguridad en Windows

\* Auditorías de seguridad en Linux

\* Auditorías de seguridad en macOS

\* Auditorías de seguridad en red (Nmap, OpenVAS)

## Análisis Forense en Sistemas Informáticos

\* Proceso de investigar sistemas informáticos para recopilar y preservar evidencias.

### Recogida y Análisis de Evidencia

\* Asegurar la escena

\* Crear una imagen forense

\* Verificación

\* Análisis de la imagen

### Herramientas del Análisis

\* Para Windows: FTK Imager, EnCase, Volatility

\* Para Linux: The Sleuth Kit (TSK), Autopsy, Dd

\* Para macOS: MacQuisition, BlackLight

## Conclusión

\* Pilares fundamentales de la SI

\* Elementos vulnerables en el SI

\* Análisis de las principales vulnerabilidades

\* Amenazas

\* Seguridad física y ambiental

\* Seguridad lógica

\* Análisis forense