



DEPARTAMENTO DE INFORMÁTICA

SEGURIDAD INFORMÁTICA

2º Bachillerato

PROFESORA: ROSARIO RUIZ DE CENZANO
CURSO 2019-2020



Seguridad informática

- 
- ◆ **La seguridad de la información**
 - ◆ **Amenazas de la seguridad**
 - ◆ **Conductas de seguridad**
 - ◆ **Malware**
 - ◆ **Ataques a los sistemas informáticos**
 - ◆ **Protección contra el malware**
 - ◆ **Cifrado de la información**
 - ◆ **Firma electrónica y certificado digital**
 - ◆ **Navegación segura**
 - ◆ **Privacidad de la información**
 - ◆ **Protección de las conexiones en red**
 - ◆ **Seguridad en las conexiones inalámbricas**



La seguridad de la información

Objetivo:

- Proteger los recursos valiosos de una organización como la información, el hardware o el software
- Alcanzar un nivel aceptable de protección del usuario y de su información

Principios:

- Confidencialidad de la información
- Integridad de la información
- Disponibilidad de la información



Amenazas de la seguridad

Humanas

- Ataques pasivos
- Ataques activos

Lógicas

- Software malicioso o malware
- Vulnerabilidades del software

Físicas

- Fallos en los dispositivos
- Accidentes
- Catástrofes naturales



Conductas de seguridad

Seguridad activa

- Control de acceso
- Encriptación
- Software de seguridad
- Firmas y certificados digitales
- Protocolos seguros

Seguridad pasiva

- Herramientas de limpieza
- Copias de seguridad
- Sistemas de alimentación ininterrumpida (SAI)
- Dispositivos NAS
- Sistemas redundantes



Malware



- ◆ **Virus**
- ◆ **Gusano**
- ◆ **Troyano**
- ◆ **Spyware**
- ◆ **Adware**
- ◆ **Ransomware**
- ◆ **Rogue**
- ◆ **Rootkit**
- ◆ **Phishing**
- ◆ **Pharming**
- ◆ **Spam**
- ◆ **Hoax**



Ataques a los sistemas informáticos

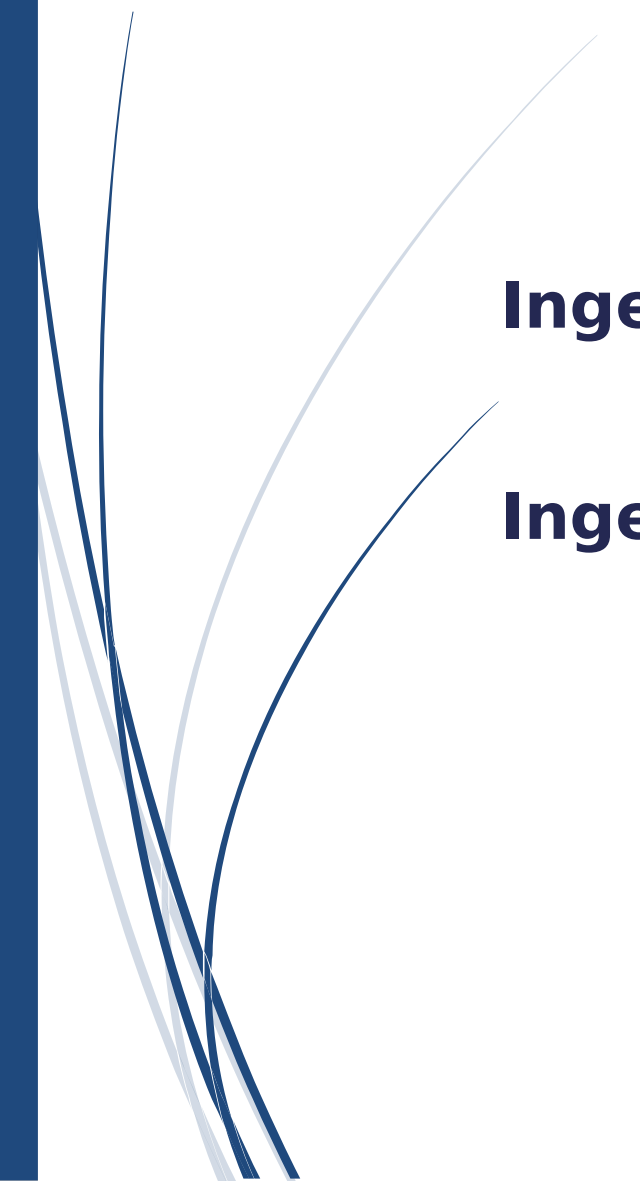


Tipos de ataque

- Interrupción
- Interceptación
- Modificación
- Suplantación



Ataques a los sistemas informáticos



Ingeniería social

Ingeniería social inversa



Ataques a los sistemas informáticos



Ataques remotos

- Inyección de código
- Escaneo de puertos
- Denegación de servicio
- Escuchas de red
- Spoofing
- Fuerza bruta
- Elevación de privilegios



Protección contra el malware

Políticas de seguridad:

Conjunto de normas y procedimientos recomendados para garantizar un cierto grado de seguridad

Objetivos a proteger:

- Navegación por Internet
- Correo electrónico
- Aplicaciones
- Dispositivos
- Soportes de almacenamiento

Protección contra el malware



Antivirus:

- ◆ Software para prevenir, detectar y eliminar virus, software malicioso y otros ataques en el sistema.
- ◆ Reside en la memoria y analiza constantemente los archivos ejecutados, los correos entrantes, las páginas visitadas, las memorias USB conectadas, etc.
- ◆ Actualizan continuamente sus definiciones de virus para incluir nuevas definiciones que van apareciendo (necesitan conexión a internet)
- ◆ Ante una amenaza se puede:
 - Omitir el aviso
 - Desinfectar el archivo
 - Moverlo a la cuarentena
 - Eliminarlo





Protección contra el malware

Síntomas de una infección

- Ralentización del equipo
- Desaparición de carpetas o archivos
- Movimiento automático del ratón, menús o ventanas
- Fallo de dispositivos o aplicaciones
- Secuestro de la página de inicio del navegador y cambio del buscador predeterminado
- Aparición de barras de herramientas extrañas en el navegador
- Redireccionamientos no deseados
- Envío de correos o mensajes a los contactos de una lista
- Aumento de la actividad en el equipo y del tráfico en la red



Protección contra el malware

Pasos a seguir en caso de infección

- Restaurar el sistema a un estado anterior (Windows)
- Actualizar la base de datos del antivirus y realizar un análisis completo del sistema
- Arrancar el equipo con un live CD o Live USB
- Ejecutar utilidades de desinfección específicas para eliminar amenazas concretas

En el peor de los casos

- Formatear el equipo
- Reinstalar el sistema operativo y las aplicaciones
- Restaurar la copia de seguridad de los datos si la hubiera



Navegación segura

- ◆ Buenas prácticas de navegación
 - ◆ Proteger la privacidad de la red con un proxy
 - ◆ Navegación privada
 - ◆ Navegación anónima
- 



Navegación segura

Buenas prácticas de navegación

- Configurar el navegador adecuadamente
- No acceder a sitios web de dudosa reputación y evitar enlaces sospechosos
- Aceptar únicamente las cookies deseadas
- Proteger los datos personales
- Descargar las aplicaciones de sitios web oficiales
- Revisar el correo electrónico
- Actualizar el sistema operativo y sus aplicaciones



Privacidad de la información

- 
- ◆ Información privada es toda aquella información protegida por la Ley Orgánica de Protección de Datos
 - ◆ La gran cantidad de datos personales que circula por la red representa una amenaza a la privacidad de los individuos



Privacidad de la información

Amenazas a la privacidad

- Sistemas operativos
- Contraseñas
- Registro de visitas web
- Sesiones del navegador
- Cookies
- Formularios
- Redes sociales
- Google



Protección de conexiones en red

- 
- **Cortafuegos**
 - **Redes privadas virtuales**
 - **Certificados SSL/TLS**



Seguridad en las comunicaciones inalámbricas

Seguridad en Bluetooth

- Bluejacking
- Bluesnarfing
- Bluebugging



Seguridad en las comunicaciones inalámbricas

Seguridad en redes wifi

- Personalizar la contraseña de acceso
- Cambiar el SSID
- Revisar el cifrado
- Desactivar el acceso por WPS
- Filtrar las MAC
- Actualizar el firmware
- Comprobar el historial
- Utilizar software de auditoría