Presentación de la asignatura: Seguridad Informática

Ciclo Formativo de Grado Medio – 2º SMR

---

1. ¿Qué es la Seguridad Informática?

- Conjunto de **técnicas, herramientas y procedimientos** para **proteger** los sistemas, redes y datos.
- Tres pilares básicos (**triángulo CIA**):
    - **Confidencialidad**: solo accede quien debe.
    - **Integridad**: la información no se altera.
    - **Disponibilidad**: los sistemas están accesibles cuando se necesitan.

En SMR: aprenderemos a **implantar medidas reales de protección** en ordenadores, servidores y redes.

---

2. Objetivos de la asignatura

- Conocer **amenazas y vulnerabilidades** comunes en sistemas informáticos.
- Aplicar **mecanismos de protección física y lógica** en equipos y redes.
- Configurar **copias de seguridad, cifrado y autenticación**.
- Gestionar **usuarios y permisos** en sistemas Windows y Linux.
- Detectar y mitigar **malware** y accesos no autorizados.
- Aprender a **documentar procedimientos de seguridad**.

3. Contenidos principales

Bloques de aprendizaje:

1. **Conceptos básicos de seguridad informática**
    - Amenazas, ataques y vulnerabilidades.
    - Principios de la ciberseguridad.
2. **Seguridad activa y pasiva**
    - Antivirus, antimalware, cortafuegos.
    - Backups, redundancia, RAID.
3. **Control de accesos**
    - Políticas de contraseñas.
    - Usuarios, grupos y permisos en Windows/Linux.
4. **Protección de datos y comunicaciones**
    - Cifrado simétrico y asimétrico.
    - SSL/TLS, VPN, Wi-Fi seguro.
5. **Planificación y recuperación ante incidentes**
    - Copias de seguridad (locales, en red, en la nube).
    - Restauración de sistemas.
    - Plan de contingencia.
6. **Normativa y legislación básica**
    - LOPDGDD y RGPD.
    - Normativa de uso seguro de sistemas.

Introducción a la Seguridad Informática

---

1. Concepto de Seguridad Informática

La seguridad informática es el **conjunto de políticas, procedimientos y tecnologías** destinadas a:

1. **Proteger los sistemas y la información** frente a accesos no autorizados.
2. **Garantizar continuidad del servicio** evitando interrupciones.
3. **Prevenir daños, pérdidas o modificaciones indebidas** en los datos.

No se trata solo de instalar un antivirus: la seguridad abarca **hardware, software, redes, usuarios y procedimientos**.

2. Principios básicos: Triángulo CIA

Toda estrategia de seguridad se apoya en tres pilares fundamentales:

- **Confidencialidad**
  La información solo debe ser accesible a personas autorizadas.
    - Ejemplo: cifrado de ficheros, contraseñas seguras.
- **Integridad**
  La información no debe ser modificada sin autorización.
    - Ejemplo: firmas digitales, sistemas de control de versiones.
- **Disponibilidad**
  La información y los sistemas deben estar disponibles cuando se necesiten.
    - Ejemplo: redundancia, copias de seguridad, UPS.

---

3. Amenazas y vulnerabilidades

3.1 Amenaza

Cualquier evento o acción que puede causar un daño:

- **Naturales**: apagones, incendios, inundaciones.
- **Accidentales**: borrado por error, pérdida de dispositivos.
- **Intencionadas**: malware, phishing, ataques de red.

3.2 Vulnerabilidad

Debilidad en un sistema que puede ser explotada por una amenaza.
Ejemplos:

- Sistema operativo sin actualizar.
- Contraseña débil.
- Puerto abierto sin protección.

Riesgo = Amenaza + Vulnerabilidad

---

4. Tipos de ataques informáticos

- **Malware**: virus, troyanos, ransomware, spyware.
- **Ingeniería social**: phishing, suplantación de identidad.
- **Ataques de red**: sniffing, denegación de servicio (DoS/DDoS), MITM (man-in-the-middle).
- **Acceso físico no autorizado**: robo de dispositivos, intrusiones.

---

5. Medidas de seguridad

5.1 Seguridad activa

- Antivirus y antimalware.
- Cortafuegos (firewalls).
- IDS/IPS (sistemas de detección y prevención de intrusos).
- Actualizaciones periódicas de software.

5.2 Seguridad pasiva

- Copias de seguridad.
- Sistemas redundantes (RAID, servidores espejo).
- Documentación de procedimientos.
- Planes de contingencia.

---

6. Seguridad en sistemas operativos

- **Gestión de usuarios y permisos**: mínimo privilegio, separación de roles.
- **Autenticación**: contraseñas robustas, autenticación multifactor.
- **Auditoría de eventos**: registros de accesos y modificaciones.

---

7. Normativa y legislación básica

- **LOPDGDD** (Ley Orgánica de Protección de Datos Personales y garantía de derechos digitales).
- **RGPD** (Reglamento General de Protección de Datos – UE).
- Normativas de seguridad en la empresa (ISO 27001, ENS en España).