

Seguridad y Alta Disponibilidad

Propuesta Didáctica – 2.º ASIR

2.1 Contextualización




Módulo: Seguridad y Alta Disponibilidad

Nivel: 2.º ASIR




 Enfoque práctico:

Diseño, despliegue y mejora de sistemas **seguros y resilientes**.

2.2 Objetivos de Aprendizaje

- Identificar los **cinco pilares** de la seguridad de datos.
- Implementar medidas técnicas:
 Cifrado,  Backups,  Autenticación.
- Comprender marcos legales: **RGPD, ENS**.
- Desarrollar una **cultura de seguridad profesional**.

2.3 Metodología

-  Teoría aplicada
-  Laboratorio técnico:
 - TLS, AES, roles, cifrado en BD
 - Simulación de ataques y recuperación
-  Análisis real de vulnerabilidades

2.4 Atención a la Diversidad

- **Escalabilidad de retos:**
 - Nivel básico: backups, cifrado de archivos.
 - Nivel avanzado: gestión de certificados, automatización.
- **Soporte visual:**

Diagramas de capas, auditorías, flujos.

2.5 Diseño Universal para el Aprendizaje (DUA)

- **Representación:** flujogramas, comparativas, alertas reales.
- **Acción:**
Laboratorios: Wazuh, GPG, cifrado de roles, simulaciones.
- **Motivación:**
Casos reales, errores comunes y su prevención.

2.6 Actividad Principal

“Protege tus datos: construye y defiende tu sistema”

Tu misión es construir un sistema **seguro**, simular un **ataque** y **mejorarlo**. Trabajarás en grupo como un verdadero equipo de seguridad.

Fase 1: Diseña tu sistema

- Define qué datos hay y clasifícalos
- Elige medidas de protección:
 - ¿Qué cifras?
 - ¿Qué roles acceden a qué?
 - ¿Se hacen backups?

Fase 2: Simula un ataque

- Introduce errores intencionales (rol de admin, sin contraseña)
- Ataca: accede sin permiso
- Detecta los fallos
- Corrige:
 - Añade validación
 - Protege campos
 - Establece roles y logs

✅ Fase 3: Comprueba y defiende

- Verifica que tu sistema responde correctamente
- Analiza los **logs y mensajes del sistema**
- Expón:
 - Qué has aprendido
 - Qué medidas evitaron o mitigaron los errores
 - Qué harías diferente la próxima vez

🎤 Entrega final:

Documentación del proceso

2.7 Evaluación

 Evaluación mediante **rúbrica ponderada**:


- Calidad técnica: **90 %**
- Documentación y argumentación: **10 %**

 Criterios:

- Aplicación de técnicas de cifrado y autenticación
- Eficacia frente a ataques simulados
- Claridad y alineación con estándares (ENS, RGPD)

2.8 Conclusión Didáctica

- La **seguridad no es una función**, es un proceso continuo.
- El alumnado desarrolla competencias:
 - Técnicas
 - Éticas
 - Estratégicas

 Preparación real para roles en:

 Seguridad |  Administración |  Sistemas distribuidos