Proyecto: Ciberdefensores en red

2.º CFGS ASIR – Seguridad y Alta Disponibilidad

🎯 Enunciado de la actividad principal

El alumnado trabajará en equipos simulando un **Centro de Operaciones de Seguridad (SOC)** con el objetivo de **diseñar, desplegar y defender** una infraestructura de red **ante ciberataques simulados**, en un entorno virtualizado.

⚙️ Entorno y herramientas

- **TryHackMe**: escenarios reales de ataque/detección
- **VirtualBox / Proxmox**: para montar:
  - estaciones de trabajo
  - cortafuegos
  - servidores con vulnerabilidades
  - sistemas de monitorización

🧪 Fases del proyecto

1. Diseño de infraestructura segura

- Creación de red segmentada (DMZ, intranet, etc.)
- Configuración de firewalls, ACLs, monitorización, usuarios

2. Implementación defensiva

- Hardening de servicios
- Configuración de alertas, backups y reglas de red

3. Simulación de ciberataques

- Ataques tipo:
  - Ransomware
  - Escaneo de puertos
  - Escalada de privilegios
- Detección, respuesta y recuperación

4. Evaluación y defensa final

- Informe técnico del incidente
- Análisis de resiliencia y medidas adoptadas
- Presentación y defensa técnica del equipo

✅ Resultado final

- Red segura operativa bajo ataque simulado
- Documentación técnica del incidente
- Defensa oral justificada
- Desarrollo real de competencias profesionales