Ciberseguridad (36 horas)

Competencia

Implementar medidas de seguridad informática y protocolos de protección de datos en entornos digitales.

Unidad 1: Fundamentos de Seguridad (6 horas)

- **Conceptos esenciales** (2h)
  - Amenazas actuales
  - Casos reales documentados
- **Seguridad en Google Workspace** (2h)
  - Configuraciones de seguridad
  - Permisos y accesos
- **Gestión de contraseñas** (2h)
  - Bitwarden configuración
  - Google Authenticator para 2FA

Unidad 2: Análisis y Detección (10 horas)

- **Chrome DevTools para seguridad** (4h)
  - Análisis de sitios web
  - Detección de vulnerabilidades web
  - Console y Network analysis
- **Nmap fundamentals** (4h)
  - Escaneo de redes
  - Scripts NSE básicos
  - Laboratorio: 10 escenarios
- **Wireshark esencial** (2h)
  - Captura de tráfico
  - Filtros y análisis

Unidad 3: Protección y Hardening (10 horas)

- **Seguridad en Chrome y navegadores** (4h)
  - Configuraciones avanzadas
  - Extensiones de seguridad
  - Navegación segura
- **Google Advanced Protection** (2h)
  - Configuración para cuentas
  - Políticas de seguridad
- **Backup y recuperación con Google** (4h)
  - Google Takeout
  - Drive para backups seguros

    - Plan de contingencia
    - Ejercicios de recuperación

Unidad 4: Proyecto de Seguridad Integral (10 horas)

- **Auditoría de seguridad** (4h)
    - Checklist con Google Forms
    - Análisis de vulnerabilidades
    - Evaluación de riesgos
- **Implementación de mejoras** (4h)
    - Hardening de cuentas Google
    - Configuración de alertas
    - Documentación de políticas
- **Reporte y presentación** (2h)
    - Informe en Docs
    - Dashboard en Sheets