ANEXO C. Propuesta de temario Formación Nivel 3 Módulos de Ciberseguridad en el sector ferroviario (Ciberseguridad en el diseño de proyectos aplicados al sector ferroviario, y Ciberseguridad en la operación y el mantenimiento aplicada al sector ferroviario)

.

1. Ciberseguridad en el diseño de proyectos aplicados al sector ferroviario.

1.1. Contexto de Ciberseguridad Industrial (proyectos).

- Contexto actual de ciberseguridad en infraestructuras críticas y transporte.
- Requisitos normativos y marcos de referencia (NIS2, PIC, CENELEC 50126/50128/50129/50701).
- Rol de la ciberseguridad en el ciclo de vida del proyecto ferroviario.

1.2. Conceptos de tecnologías de operación (perspectiva proyectos).

- Particularidades OT en entornos ferroviarios: disponibilidad, latencia, determinismo.
- Sistemas de automatización y control industrial aplicados al ferrocarril.
- Arquitecturas típicas ferroviarias (SCADA, enclavamientos, ATS/ATO/ATP, ERTMS/CBTC)

1.3. Redes industriales.

- Protocolos OT utilizados en entornos ferroviarios.
- Comunicaciones en sistemas de señalización y control.
- Vulnerabilidades de protocolos ICS/OT no autenticados.

1.4. Integración IT y OT.

- Riesgos y retos de la convergencia.
- Pasarelas, DMZ OT, segmentación y aislamiento.
- Modelos Zero Trust aplicados a OT ferroviario.

1.5. Modelo de activos ferroviarios según CENELEC 50701.

- Clasificación de activos y niveles de automatización.
- Diferencias entre zonas y conductos.
- Aplicación del modelo a señalización, telemandos, OCC y tren.

1.6. Modelos de Zonas y Conductos.

- Identificación de segmentos críticos.
- Requisitos de seguridad por zonas y conectores OT.

1.7. Vulnerabilidades y amenazas en un entorno industrial ferroviario.

- Amenazas sobre enclavamientos, balizas, sistemas de energía y telemetría.
- Casuística real en el sector ferroviario (incidentes internacionales).
- Amenazas dirigidas a operadores de transporte.

1.8. Threat Intelligence en el sector ferroviario.

- Grupos APT dirigidos al sector ferroviario.
- Técnicas MITRE ATT&CK for ICS aplicadas a sistemas ferroviarios.
- Tendencias de ataque emergentes (ransomware OT, laterales desde IT, sabotaje digital).

1.9. Metodología de diagnóstico de arquitectura de redes y sistemas y terceras partes.

- Validación de diseño desde un punto de vista de seguridad.
- Checklist de seguridad en proyectos ferroviarios.
- Evaluación de ciberseguridad de terceras partes, integradores y fabricantes.

1.10. Seguridad en la cadena de suministro (Supply Chain)

- Riesgos en firmware, componentes, PLCs y dispositivos.
- SBoM (Software Bill of Materials) en proyectos ferroviarios.
- Validación y certificación de componentes OT ferroviarios.

1.11. Ciberseguridad en el ciclo de vida de un proyecto de automatización industrial.

- Proceso de diseño, implantación, validación y aceptación.
- Pruebas FAT/SAT con criterios de ciberseguridad.

1.11.1. Ciberseguridad en la fase de diseño.

- Integración de requisitos de seguridad desde origen.
- Identificación de superficies de ataque en los planos y arquitecturas.
- Criterios de selección de equipamiento seguro.

1.11.2. Problemática Security–Safety en el diseño.

- Interacción entre SIL y ciberseguridad.
- Cómo compatibilizar requisitos de seguridad funcional y ciberseguridad.
- Riesgos de common cause failure.

1.11.3. Definición y defensa de requisitos de ciberseguridad.

- Cómo documentar requisitos según CENELEC 50701.
- Cómo negociarlos con fabricantes e integradores.

1.11.4. Ciberseguridad en la fase de aprovisionamiento y ejecución.

- Seguridad en instalación, parametrización e integración.
- Validación de dispositivos OT y redes industriales.

.

.

2. Ciberseguridad en la operación y el mantenimiento aplicada al sector ferroviario.

2.1. Contexto de Ciberseguridad Industrial (operación)

- Diferencias entre proyectos y operación.
- Garantía de continuidad operacional.
- Gestión de cambios y mantenimiento seguro.

2.2. Conceptos de tecnologías de operación.

- Arquitecturas OT en operación cotidiana.
- Estructura y funciones del material móvil, instalaciones fijas y OCC.

2.3. Sistemas de automatización y control industrial.

- Particularidades ferroviarias en sistemas de control.

- Protocolos y dispositivos habituales.

2.4. Redes industriales e integración IT/OT.
- Comunicaciones tren–tierra.
- Redes de señalización y control descentralizado.

2.5. Modelo de activos ferroviarios según CENELEC 50701.
- Identificación de activos críticos en operación.

2.6. Modelo de Zonas y Conductos.
- Aplicación práctica a una operación ferroviaria.

2.7. Vulnerabilidades y amenazas en operación.
- Error humano, configuraciones erróneas y accesos inseguros.
- Amenazas internas e internas intencionadas.

2.8. Modelo de amenazas y vulnerabilidades en el sector ferroviario (error humano)
- Casos reales de fallos de configuración y errores de operación.
- Buenas prácticas para reducir el impacto del factor humano.

2.9. Diagnóstico de arquitectura de redes, sistemas y terceras partes.
- Evaluación continuada de exposición y riesgos.

2.10. Caso de uso práctico — Arquitectura ERTMS.
- Identificación de riesgos por cadena el ámbito de automatización.
- Medidas básicas de protección por cada nivel y subsistema.

2.11. Gestión de la ciberseguridad en un entorno de automatización industrial.
- Política, procesos y roles implicados.
- Integración con sistemas corporativos.

2.11.1. Análisis de riesgos de ciberseguridad en un entorno ferroviario.
- Metodologías recomendadas (CENELEC, MAGERIT adaptado, IEC 62443-3-2).
- Cuantificación y criterios de aceptación.

2.11.2. Ciberseguridad en la fase de operación.
- Supervisión, actualizaciones, gestión de vulnerabilidades.
- Monitorización y SOC OT ferroviario.

2.11.3. Ciberseguridad en la fase de mantenimiento.
- Mantenimiento predictivo y problemas de seguridad asociados.
- Control de acceso de mantenedores.
- Gestión de portátiles de mantenimiento y herramientas OT.

IA aplicada al sector ferroviario y a los entornos OT.

3.

3.1. Introducción a la IA en el sector ferroviario.

Tipos de IA utilizada: predicción, detección de anomalías, planificación, visión artificial.

- Aplicación en sistemas OCC, ERTMS, vigilancia, mantenimiento, energía.
-

3.2. Riesgos de seguridad y vulnerabilidades de la IA en OT ferroviario.

Model poisoning, data poisoning, manipulación de telemetría.

- *Engaño a modelos de detección y visión artificial.*
- Dependencia operativa de IA en sistemas de seguridad.
-

3.3. IA adversaria en entornos ferroviarios.

Deepfakes para ingeniería social o manipulación operativa.

- Ataques adversarios en sensores y modelos vision-based.
-

3.4. IA en el ciclo de vida de proyectos ferroviarios.

Uso de IA para documentación, código o configuraciones → validación humana obligatoria.

- Impacto en FAT/SAT y en la certificación ferroviaria.
- Consideraciones de Safety cuando la IA afecta a funciones críticas.
-

3.5. Uso seguro de IA generativa por personal técnico.

Buenas prácticas para evitar exfiltración de datos.

- Qué no se puede introducir nunca en una IA pública.
- IA en diagnóstico y troubleshooting.
-

3.6. IA y marcos normativos.

Relación con CENELEC 50701 (aunque indirecta).

- Relación con ENS:
- M.6, M.10 → configuración segura.
    - M.15 → monitorización de uso.
    - M.17 → gestión de incidentes derivados de IA.