Universidad de Navarra

Security in IoT (MIT)
Guía docente 2026-27

PRESENTACIÓN

Breve descripción:

- **Titulación**: Máster Universitario en Ingeniería de Telecomunicación
- **Módulo/Materia**: Tecnología de Telecomunicación / Teoría de la Señal y la Comunicación
- **ECTS**: 5
- **Curso, semestre**: 1º, 2
- **Carácter**: Obligatoria
- **Profesorado**:
- Figueroa Lorenzo, Santiago / Invitado
- Vidal Cassanya, Gerard / Invitado
- Flores, José Luis / Invitado
- **Idioma**:

RESULTADOS DE APRENDIZAJE

- RA2 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
- RA5 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
- RA6 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería de telecomunicación.
- RA20 - Capacidad para diseñar sistemas de radionavegación y de posicionamiento, así como los sistemas radar.
- RA22 - Capacidad para realizar la planificación, toma de decisiones y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, los procedimientos de seguridad, el escalado y el mantenimiento, así como gestionar y asegurar la calidad en el proceso de desarrollo.

PROGRAMA

Tema 1. Fundamentos de la ciberseguridad industrial

- Conceptos básicos de ciberseguridad aplicados a entornos industriales e IoT.
- Diferencias entre entornos IT y OT: requisitos operacionales, de disponibilidad y de seguridad.
- Amenazas y superficie de ataque en redes industriales y sistemas de control.

Tema 2. Ciberseguridad en redes de control

- Terminología y conceptos de redes de control industrial y ciberseguridad OT.
- El modelo Purdue y las arquitecturas industriales segmentadas.
- La familia de estándares IEC 62443 (partes 2-1, 3-2 y 3-3): gestión de la ciberseguridad, análisis de riesgos, niveles de seguridad y requisitos técnicos de protección.
- Evaluación de la madurez de ciberseguridad de una planta industrial.
- Contramedidas y tecnologías de protección en redes OT, con casos reales de distintos sectores.

Universidad de Navarra

Tema 3. Ciberseguridad en producto

- Desarrollo seguro de producto a lo largo de su ciclo de vida (IEC 62443-4-1).
- Requisitos técnicos de seguridad para componentes industriales (IEC 62443-4-2).
- Gestión de vulnerabilidades, hardening, autenticación y control de acceso, integridad de firmware, actualizaciones seguras y cadena de suministro.
- Marco regulatorio europeo: el Cyber Resilience Act (CRA) y las obligaciones de fabricantes y desarrolladores.

Tema 4. Protección de una arquitectura industrial: laboratorio práctico

- Despliegue de una infraestructura ICS virtualizada (caso de uso: planta de tratamiento de agua) y sus niveles según el modelo Purdue.
- Segmentación de red y zonas de seguridad: firewalls, listas de control de acceso (ACL) y VLANs.
- Monitorización y respuesta a incidentes: monitorización de tráfico y eventos, gestión de logs y threat hunting.
- Inteligencia de amenazas y plataformas de intercambio de información.
- Validación mediante escenarios de ataque: explotación del protocolo Modbus y, en su caso, ataques sobre Active Directory.

Tema 5. Seguridad en el ciclo de vida del desarrollo de software

- Etapas del ciclo de vida del software (IEEE 12207) y su alineación con IEC 62443-4-1 y DevSecOps.
- Integración de la seguridad en pipelines CI/CD con enfoque shift-left: modelado de amenazas, análisis estático de código (SAST), análisis de composición de software (SCA) y análisis de vulnerabilidades en contenedores.
- Gestión de defectos de seguridad: detección temprana, centralización de hallazgos y priorización de la remediación.

ACTIVIDADES FORMATIVAS

- **Clases teóricas (20 horas)**
- **Prácticas de laboratorio (30 horas)**

EVALUACIÓN

CONVOCATORIA ORDINARIA

- Prácticas laboratorio: 50%
- Examen final: 50%

CONVOCATORIA EXTRAORDINARIA

- Prácticas laboratorio: 50%
- Examen final: 50%

HORARIOS DE ATENCIÓN

Dra.....(mail@unav.es)

- Despacho..... Edificio. Planta .....
- Horario de tutoria:

Universidad de Navarra

BIBLIOGRAFÍA Y RECURSOS