



Formación: IEC 62443 Aplicada a Entornos OT

Identificador	SRV-FORM-102
Versión	v1.1
Fecha	2026-02-23
Generado	202602241122
URL de control	https://docs.fortiseg.eu/SRV-FORM-102.pdf



Versión online

Formación: IEC 62443 Aplicada a Entornos OT

Información General

Duración	4 horas (1 sesión)
Modalidad	Presencial / Online
Nivel	Intermedio
Certificado	Certificado de asistencia Fortiseg Technology

Audiencia

- Ingenieros de automatización y control (SCADA, PLC, DCS)
- Responsables de ciberseguridad industrial / OT
- Responsables de sistemas de información con entornos OT
- Integradores de sistemas y proveedores de tecnología OT
- Personal técnico de mantenimiento de infraestructuras críticas

Beneficios Esperados

- **Dominar el estándar de referencia** en ciberseguridad industrial a nivel mundial
- **Aplicar el modelo de zonas y conductos** a la propia infraestructura OT
- **Asignar niveles de seguridad** (Security Levels) de forma práctica
- **Entender los roles** de propietario, integrador y fabricante según IEC 62443
- **Priorizar inversiones** en seguridad OT con criterios técnicos sólidos

Temario

Bloque 1 — Fundamentos de seguridad OT (45min)

1. IT vs OT: diferencias fundamentales

- Prioridades invertidas: disponibilidad > confidencialidad
- Ciclos de vida de 15-25 años vs 3-5 años
- Protocolos industriales: Modbus, OPC UA, Profinet, DNP3
- Por qué los enfoques IT no funcionan directamente en OT

2. Panorama de amenazas OT

- Casos reales: Stuxnet, Triton/Trisis, Colonial Pipeline, Oldsmar
- Vectores de ataque más comunes en plantas industriales
- El mito del air gap

Bloque 2 — Estructura de IEC 62443 (1h)

3. Visión general del estándar

- Las 4 partes: General, Políticas, Sistema, Componente
- Documentos clave: 62443-2-1, 62443-3-2, 62443-3-3, 62443-4-2
- Relación con otros marcos (NIST CSF, ISO 27001, NIS2)

4. Los tres roles

- Propietario del activo (Asset Owner)
- Integrador de sistemas (System Integrator)
- Fabricante de componentes (Product Supplier)
- Responsabilidades de cada uno según el estándar

5. Security Levels (SL)

- SL 0 a SL 4: qué significa cada nivel
- SL-T (Target) vs SL-A (Achieved) vs SL-C (Capability)
- Cómo determinar el SL adecuado para cada zona

Bloque 3 — Zonas y conductos (1h 15min)

6. Modelo de zonas y conductos

- Definición y criterios de segmentación
- Modelo Purdue simplificado: niveles 0-5
- DMZ industrial: función y diseño
- Ejemplos aplicados a plantas de agua y desalación

7. Ejercicio guiado: segmentación de una planta tipo

- Diagrama de red OT proporcionado
- Identificación de zonas y conductos
- Asignación de SL-T por zona
- Discusión de soluciones de segmentación (firewalls industriales, data diodes, jump servers)

Bloque 4 — Evaluación y hoja de ruta (1h)

8. Evaluación de riesgos según 62443-3-2

- Identificación de amenazas por zona
- Evaluación de riesgo: impacto × probabilidad
- Requisitos de seguridad derivados (SR/RE)

9. Medidas de protección clave

- Foundational Requirements (FR1-FR7)
- Controles prioritarios para entornos legacy
- Gestión de parches en sistemas que no se pueden parar
- Monitorización OT: qué vigilar y con qué herramientas

10. Plan de acción y cierre

- Quick wins en seguridad OT
- Cómo vender internamente un proyecto de seguridad OT
- Turno de preguntas y debate