



# Formación: Taller Práctico de Ciberseguridad OT

Identificador  
Versión  
Fecha  
Generado  
URL de control

SRV-FORM-003  
v1.0  
2026-02-20  
202602241122  
<https://docs.fortiseg.eu/SRV-FORM-003.pdf>



Versión online

## Fortiseg Technology

Fortiseg Technology es una empresa especializada en **ciberseguridad aplicada a entornos críticos** y en el cumplimiento normativo en materia de seguridad de la información.

Nuestro enfoque combina **experiencia técnica, conocimiento normativo y orientación a resultados**, ayudando a entidades públicas y privadas a proteger sus sistemas y garantizar la confianza digital.

## Formación: Taller Práctico de Ciberseguridad OT

### Información General

|                         |                                                         |
|-------------------------|---------------------------------------------------------|
| <b>Duración</b>         | 4 horas (1 sesión)                                      |
| <b>Modalidad</b>        | Presencial (recomendado) / Online                       |
| <b>Nivel</b>            | Práctico-aplicado                                       |
| <b>Requisito previo</b> | Recomendable haber cursado los módulos NIS2 e IEC 62443 |
| <b>Certificado</b>      | Certificado de asistencia Fortiseg Technology           |

### Audiencia

- Equipos técnicos de OT, IT y mantenimiento de la organización
- Responsables de ciberseguridad industrial
- Ingenieros de automatización y SCADA
- Mandos intermedios con responsabilidad sobre infraestructuras OT
- Idealmente: asistentes de los dos módulos anteriores (NIS2 + IEC 62443)

### Beneficios Esperados

- **Mapear la arquitectura OT real** de la organización con criterios de seguridad
- **Identificar vulnerabilidades concretas** en la propia infraestructura
- **Obtener un informe de gaps** personalizado con priorización de acciones
- **Definir una hoja de ruta realista** de ciberseguridad OT a 12-24 meses
- **Alinear equipos IT y OT** en una visión común de seguridad

## Temario

### Bloque 1 — Descubrimiento de activos (1h)

#### 1. Inventario de activos OT

- Metodología de inventario: qué información capturar
- Clasificación: PLCs, RTUs, HMIs, historians, gateways, switches industriales
- Ejercicio: los asistentes completan el inventario de su propia planta
- Identificación de activos críticos y dependencias

#### 2. Mapeo de la arquitectura de red OT

- Diagrama de red actual: documentar lo que existe
- Identificación de conexiones IT-OT
- Puntos de acceso remoto (VPN, TeamViewer, escritorios remotos)
- Conexiones a terceros (integradores, fabricantes, SCADA cloud)

### Bloque 2 — Análisis de vulnerabilidades (1h)

#### 3. Evaluación de la superficie de ataque

- Revisión de protocolos en uso y sus riesgos
- Sistemas sin parchear: cómo evaluar el riesgo real
- Credenciales por defecto y gestión de accesos
- Dispositivos legacy sin soporte del fabricante

#### 4. Checklist de gaps NIS2 + IEC 62443

- Ejercicio guiado con checklist de ~40 controles
- Los asistentes evalúan su estado actual (Sí/No/Parcial)
- Identificación de los 10 gaps más críticos
- Comparación con niveles SL objetivo definidos en el módulo anterior

### Bloque 3 — Priorización y hoja de ruta (1h 30min)

#### 5. Matriz de riesgo aplicada

- Priorización de gaps por impacto y facilidad de implementación
- Quick wins: acciones que se pueden ejecutar en <30 días
- Medio plazo: proyectos de 3-6 meses
- Largo plazo: inversiones de 6-24 meses

#### 6. Diseño de la arquitectura objetivo

- Segmentación de red propuesta (zonas y conductos)
- Controles de acceso recomendados
- Estrategia de monitorización OT
- Plan de respuesta a incidentes OT

#### 7. Caso práctico: escenario de incidente

- Simulación tabletop de un ciberincidente OT
- Roles y responsabilidades durante un incidente
- Comunicación interna y notificación (plazos NIS2)
- Lecciones aprendidas y mejora continua

## Bloque 4 — Plan de acción y cierre (30min)

### **8. Entregable: informe preliminar de gaps**

- Resumen de hallazgos del taller
- Top 10 acciones priorizadas
- Estimación de esfuerzo y recursos
- Propuesta de siguientes pasos

### **9. Debate final y compromisos**

- Revisión de la hoja de ruta con la dirección
- Asignación de responsables por acción
- Calendario propuesto de implementación
- Turno de preguntas