OT-Knight
An RBJCS brand

CATÁLOGO DE FORMACIÓN



CIBERSEGURIDAD OT/ICS · SEGURIDAD FUNCIONAL · FORMACIÓN

# En OT e infraestructuras críticas, la ciberseguridad se convierte en una función de seguridad.

Conocimientos que vuelven a la planta. Programas especializados en ciberseguridad OT y seguridad funcional, de la sala de control a la dirección, impartidos por un formador autorizado ISA y PECB con experiencia real en planta.

| | | | | | |
|---|---|---|---|---|---|
| Talleres en planta | Cursos de varios días | Sesiones para directivos | Formatos de un día | Laboratorios prácticos | Itinerarios certificados |

**Formación autorizada ISA y PECB** · IEC 62443 · IEC 61511 · ISO/IEC 27001 · ISO 31000

PARA OPERADORES, EPC, INTEGRADORES Y FABRICANTES EN

Infraestructuras críticas · Petróleo y gas · Petroquímica · Energías renovables · BESS · Generación, transporte y distribución eléctrica

**information@ot-knight.com**
Bélgica · Europa · Oriente Medio

# Catálogo de formación

Conocimientos que vuelven a la planta.

Ocho programas especializados, adaptados a su equipo, activos y madurez. El contenido, la profundidad y los ejercicios pueden adaptarse a su equipo y contexto regulatorio: talleres en planta, cursos de varios días y sesiones para directivos, en inglés, francés o español.

**FORMATO DE UN DÍA** — T1 y T2 pueden impartirse como taller de un día en planta, con un ejercicio práctico condensado. Las duraciones son orientativas.

**ITINERARIOS CERTIFICADOS** — Formación autorizada ISA y PECB · materiales PECB en español; ISA en inglés

- **IC32** Uso de las normas ISA/IEC 62443 para proteger sus sistemas de control
- **IC33** Evaluación de la ciberseguridad de sistemas IACS nuevos o existentes
- **IC34** Diseño e implementación de ciberseguridad IACS
- **IC37** Operación y mantenimiento de ciberseguridad IACS
- **IC49** ISASecure ACSSA para evaluadores
- **PECB** Cursos NIS 2, ISO/IEC 27001 e ISO 31000

## T1 Seguridad funcional y ciberseguridad desde el diseño: aplicación práctica

3 DÍAS · OPCIÓN DE 1 DÍA

**IEC 61511 · IEC 62443 · ISO/IEC 27001 · ISA TR84.00.09 · ISASecure ACSSA, para propietarios de activos**

- Integre IEC 61511 e IEC 62443: evaluación de riesgos de ciberseguridad del SIS (IEC 61511, 8.2.4), requisitos de seguridad e impacto en la SRS
- Gobernanza conjunta: gestión del cambio, competencias, auditorías y pruebas periódicas junto con la verificación de ciberseguridad
- Taller: expediente combinado de seguridad funcional y ciberseguridad para una unidad de proceso
- ISA TR84.00.09 en la práctica: ciberamenazas capaces de anular capas de protección e independencia SIS/BPCS en el diseño de zonas
- Preparar una planta en operación para ISASecure ACSSA

## T2 Fundamentos de IEC 62443: el lenguaje de la ciberseguridad industrial

1 DÍA

**Fundamentos · Funciones · Panorama de normas**

- Estructura de la serie y responsabilidades: propietario de activos, proveedor de servicios, integrador y proveedor de productos
- Hoja de ruta: 2-1 (programa), 3-2 (riesgo), 3-3 (sistema) y 4-1/4-2 (producto)
- Esquemas ISASecure (CSA, SSA, SDLA, ACSSA)
- Elementos del programa de seguridad, zonas y conductos, niveles de seguridad SL-T, SL-C y SL-A, requisitos fundamentales FR 1–7
- Relación con ISO/IEC 27001 y NIST CSF 2.0

## T3 Desarrolle su programa de seguridad IEC 62443

3 DÍAS

**Para propietarios de activos y operadores**

- IEC 62443-2-1:2024 en sus 8 SPE: ORG, CM, NET, COMP, DATA, USER, EVENT, AVAIL
- Políticas y procedimientos prácticos para los equipos de operación
- Indicadores y mejora continua
- Análisis de deficiencias y hojas de ruta de madurez
- Gestión de proveedores de servicios con IEC 62443-2-4

## T4 Un ciberriesgo con sentido: gestión de ciberriesgos OT

3 DÍAS

**IEC 62443-3-2 · ISO/IEC 27005 · ISO 31000**

- Conecte ISO 31000, ISO/IEC 27005 e IEC 62443-3-2 en un único marco de riesgos
- Riesgos basados en consecuencias: vínculo con HAZOP y LOPA y calibración con la matriz corporativa
- ZCR 1 a ZCR 7: alcance del sistema (SuC), evaluaciones inicial y detallada, zonas y conductos, SL-T y especificación de requisitos de ciberseguridad (CRS)
- Caso práctico, del SuC a la CRS

## T5 Un SGSI, dos mundos: unificar IEC 62443 e ISO/IEC 27001

2 DÍAS

**SGSI · Correspondencia de controles · Programas de auditoría**

- Ampliar un SGSI de IT a OT
- Alcance, declaración de aplicabilidad y tratamiento de riesgos de los activos OT
- Relacionar los controles del Anexo A con los requisitos IEC 62443-2-1 y los SR de IEC 62443-3-3
- Un programa de auditoría que cubra ambas certificaciones

## T6 Seguridad desde la especificación hasta la planta: ciclo de vida de la ciberseguridad OT

3 DÍAS

**Para EPC, integradores, proveedores y equipos de proyecto de propietarios de activos**

- Capacidades IEC 62443-2-4 para integración y mantenimiento
- Prácticas de desarrollo seguro IEC 62443-4-1 (SM, SR, SD, SI, SVV, DM, SUM, SG) y requisitos de componentes 4-2 que contribuyen a las capacidades de sistema 3-3
- Fases desde FEED hasta la operación: diseño de detalle, FAT, SAT y entrega
- Entregables de ciberseguridad que deben figurar en los contratos: CRS, planos de zonas y conductos, bastionamiento, documentación

## T7 Confíe, pero verifique: aseguramiento OT, desde la evaluación de riesgos hasta el desmantelamiento

2-3 DÍAS

**Auditoría · Verificación · Pruebas seguras de ciberseguridad**

- Planificar el aseguramiento durante todo el ciclo de vida: qué verificar, cuándo, cómo y con qué independencia
- Definir FAT/SAT y pruebas seguras en planta: análisis de vulnerabilidades y alcance de pruebas de penetración
- Desmantelamiento seguro: eliminación segura de datos y retirada de credenciales
- Auditar programas de seguridad (IEC 62443-2-1 y 2-4) y verificar los niveles alcanzados (SL-A frente a SL-T)
- Documentar evidencias y hallazgos como los evaluadores ISASecure

## T8 Bastionamiento y pruebas prácticas para entornos ICS

2 DÍAS · LABORATORIOS PRÁCTICOS

**Impartido junto con un experto en pruebas de penetración OT · nivel inicial a intermedio**

- Un proceso de bastionamiento práctico e independiente del sistema operativo, vinculado a los requisitos IEC 62443
- Crear scripts y políticas de sistema propios; bastionamiento de red, físico y de usuarios
- Bastionamiento de HMI y servidores Windows, Linux, redes y PLC, aislados o en dominio, incluidos entornos restringidos para operadores
- Verificar los resultados con herramientas de seguridad, en laboratorios basados en escenarios reales

F

# Formación en seguridad funcional

Competencia IEC 61511 de la sala de control a la oficina de proyecto, adaptada a su planta y a sus procedimientos.

## T9 Concienciación en seguridad funcional: por qué importa el SIS

MEDIO DÍA A 1 DÍA

**Para operadores, equipos de mantenimiento, contratistas y directivos**

- Qué hace un sistema instrumentado de seguridad y en qué se diferencia del sistema de control
- Por qué los by-pass, los forzados y los cambios sin revisar ponen en riesgo la protección
- El ciclo de vida de seguridad IEC 61511 en palabras sencillas, y quién es responsable de cada etapa
- Qué debe hacer cada rol, y qué nunca debe hacer, en torno a una SIF

## T10 IEC 61511 en la práctica: del análisis de peligros a la SRS

3 DÍAS

**Para ingenieros, especialistas en seguridad de procesos y equipos de proyecto**

- El ciclo de vida de seguridad y cómo se enlazan sus fases: análisis de peligros y riesgos, asignación, SRS, diseño, validación, operación
- Redacción de la SRS: estado seguro, puntos de disparo, tiempos de respuesta, reglas de by-pass y rearme, requisitos de proof test
- Determinación del SIL objetivo con HAZOP y LOPA, y calibración con la matriz de riesgo corporativa
- Taller: de un escenario de peligro a una SRS completa para una SIF

## T11 Verificación SIL: demostrar que el diseño cumple su objetivo

2 DÍAS

**Para ingenieros de diseño de SIS, EPC y proveedores**

- Cálculo de la PFD para arquitecturas típicas, y los datos y supuestos que lo sustentan
- Fijar el intervalo de proof test y documentar de qué depende el resultado
- Tolerancia a fallos de hardware, restricciones de arquitectura y capacidad sistemática
- Taller: verificar una SIF y defender el resultado en una evaluación

## T12 Operar el SIS: proof test, by-pass y gestión del cambio

2 DÍAS

**Para equipos de operación, mantenimiento e ingeniería**

- Redacción y ejecución de procedimientos de proof test, y optimización de los intervalos
- Seguimiento de demandas y fallos, y uso de los datos para revisar los supuestos de diseño
- Gestión de by-pass y reglas operativas de la SRS
- Revisión de las modificaciones del SIS bajo gestión del cambio

## T13 Gestión de la seguridad funcional: operar el sistema FSM

2 DÍAS

**Para directivos, responsables de seguridad funcional y propietarios de proyecto**

- El plan de seguridad funcional, los planes de ciclo de vida y validación, y las funciones de propietario, contratistas y proveedores
- Evaluaciones y auditorías de seguridad funcional: qué buscan los evaluadores en cada etapa
- Gestión de competencias, actividades de verificación y control documental
- Preparar su sistema FSM para la evaluación y para la certificación del FSMS

## Coaching en proyectos reales

trabajamos junto a su equipo en sus propios proyectos

Ayudamos a su equipo a desarrollar la competencia que exige IEC 61511, sobre el trabajo que tiene entre manos. También: T1, seguridad funcional y ciberseguridad OT en un solo curso (3 días o taller de un día).

CÓMO TRABAJAMOS

## Competencias detrás de cada control

**1 — Descubrir**
Su equipo, su planta y sus objetivos de aprendizaje

**2 — Adaptar**
Contenido, profundidad y ejercicios adaptados

**3 — Impartir**
En su empresa o en sesiones abiertas, en EN, FR o ES

**4 — Practicar**
Casos prácticos, talleres y laboratorios

**5 — Certificar**
Exámenes certificados y seguimiento

### A QUIÉN FORMAMOS

- Operadores
- Técnicos
- Ingenieros
- Equipos de proyecto
- EPC e integradores
- Fabricantes
- Directivos
- Órganos de dirección

### DÓNDE FORMAMOS

Sesiones en planta y abiertas en **Europa y Oriente Medio**, en su empresa o a través de nuestro proveedor de formación autorizado. Con sede en Bruselas, Bélgica.

Idiomas de trabajo: English · Français · Español.

### COMPETENCIAS CERTIFICADAS

Miembro del Comité Técnico ISASecure ACSSA

# Desarrollemos las competencias de su equipo.

Háblenos sobre su equipo, su planta y sus objetivos. Le propondremos un programa adaptado y una primera sesión práctica.

information@ot-knight.com

Bruselas, Bélgica · Europa y Oriente Medio



*En OT e infraestructuras críticas, la ciberseguridad se convierte en una función de seguridad.*