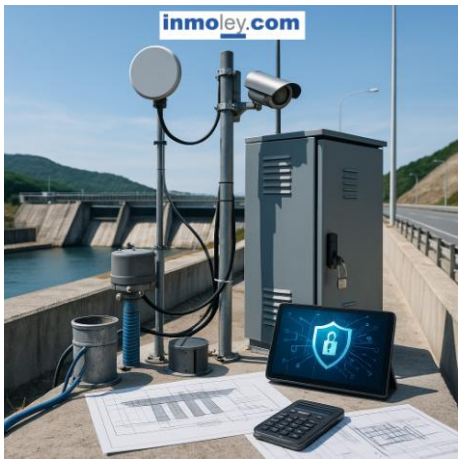
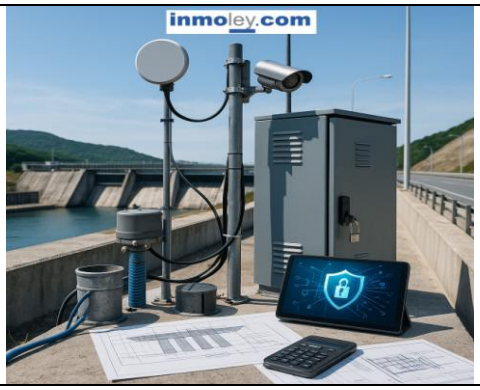
SISTEMA EDUCATIVO inmoley.com DE FORMACIÓN CONTINUA PARA PROFESIONALES INMOBILIARIOS. ©

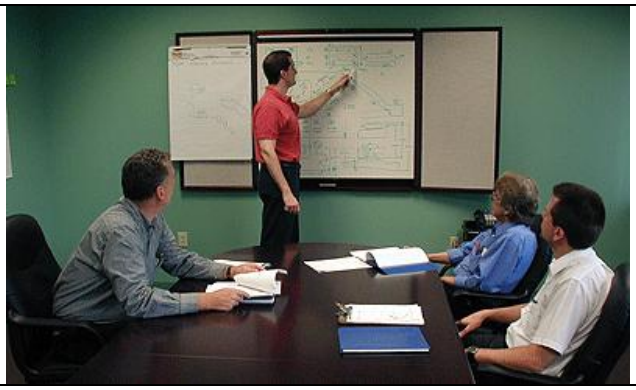
CURSO/GUÍA PRÁCTICA CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS



Índice

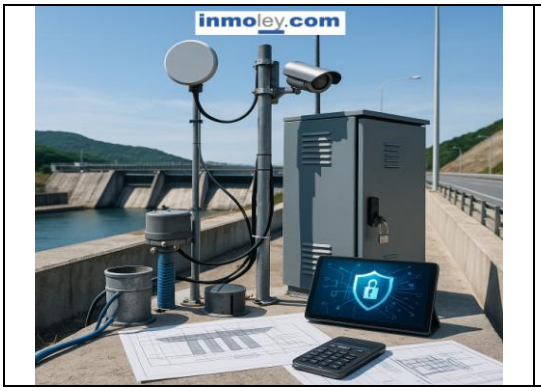
¿QUÉ APRENDERÁ?

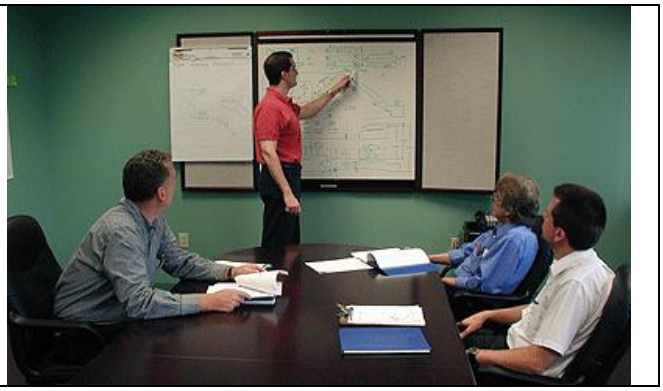




- Comprender el papel de las infraestructuras críticas y las particularidades de la ciberseguridad OT frente a la ciberseguridad IT
- Identificar arquitecturas OT reales, sus componentes clave (PLC, RTU, SCADA, redes de campo) y su superficie de exposición
- Diseñar y revisar segmentaciones de redes OT basadas en zonas y conductos, DMZ industrial y perímetros seguros IT/OT
- Aplicar técnicas de hardening específicas sobre PLC, RTU, sistemas SCADA, estaciones de ingeniería y comunicaciones de campo
- Implantar un modelo de gobierno, organización y responsabilidades claras para la ciberseguridad OT en la empresa
- Realizar análisis y gestión de riesgos de ciberseguridad OT, priorizando controles según criticidad de activos y procesos
- Definir y desplegar arquitecturas de monitorización OT, casos de uso de detección y su integración con el SOC corporativo
- Planificar y ejecutar la respuesta a incidentes OT, la recuperación segura y la continuidad operativa en entornos industriales
- Cumplir con los principales marcos normativos y contractuales aplicables a la ciberseguridad OT en España y Latinoamérica
- Preparar y superar auditorías técnicas y de gestión de ciberseguridad OT, generando evidencias y trazabilidad sólidas
- Utilizar checklists, formularios y plantillas prácticas para inventario, segmentación, hardening, riesgos y respuesta a incidentes OT
- Aprender de casos prácticos reales e hipotéticos para aplicar la ciberseguridad OT en sectores como energía, agua, transporte, salud e industria de procesos

Introducción.





CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS: LA DIFERENCIA ENTRE "FUNCIONAR" Y "SOBREVIVIR"

En los últimos años, la ciberseguridad ha dejado de ser un tema exclusivo del entorno corporativo IT para convertirse en un factor decisivo en la continuidad de negocio de cualquier operador de infraestructuras críticas. Plantas de generación, redes de agua, transporte, hospitales o instalaciones industriales dependen hoy de sistemas OT interconectados, donde un fallo o un ataque ya no se traduce solo en pérdida de datos, sino en paradas de producción, daños a equipos, impacto en la seguridad de las personas e incluso riesgo para el medioambiente. En este contexto, disponer de una estrategia sólida de ciberseguridad OT ya no es una opción: es una condición necesaria para seguir operando con garantías.

El problema al que se enfrenta el profesional del sector es conocido: abundan los documentos genéricos sobre ciberseguridad, pero escasean las guías que aterricen, con rigor técnico y enfoque práctico, lo que significa proteger redes industriales, PLC, RTU, sistemas SCADA o comunicaciones de campo en entornos reales. ¿Cómo segmentar correctamente una red OT sin provocar indisponibilidades? ¿Cómo aplicar hardening a PLC y estaciones de ingeniería sin romper la operación? ¿Cómo integrar la monitorización OT con el SOC corporativo sin ahogar a los equipos con falsas alarmas? ¿Qué exige realmente un regulador o un auditor cuando pone el foco en OT? Esta guía nace precisamente para responder a estas preguntas desde la perspectiva de quien está en primera línea, en plantas y centros de control.

La Guía Práctica de Ciberseguridad OT en Infraestructuras Críticas ofrece un recorrido completo, ordenado y accionable por todos los pilares que necesita un profesional para elevar el nivel de seguridad de sus sistemas industriales. Comienza fijando los fundamentos: qué son las infraestructuras críticas, qué particularidades tiene la ciberseguridad OT frente a la IT, cómo se estructura una arquitectura OT típica y cuál es su verdadera superficie de exposición. A partir de ahí, entra en profundidad en el gobierno y la gestión del riesgo OT, la segmentación de redes industriales, el diseño de DMZ y perímetros IT/OT

seguros, el hardening de PLC/RTU y sistemas SCADA, la monitorización continua y la respuesta a incidentes en entornos de operación.

La guía no se queda en la teoría. Incorpora capítulos específicos dedicados al cumplimiento normativo, a la auditoría técnica y de gestión, y culmina con una parte extensa de herramientas prácticas: checklists, formularios y plantillas listas para usar que cubren inventario de activos OT, análisis de riesgos, segmentación, hardening, monitorización, respuesta a incidentes, reporte a reguladores y clientes, así como lecciones aprendidas. Finalmente, una parte de casos prácticos sectoriales muestra, paso a paso, cómo aplicar estos conceptos en operadores de energía, agua, transporte, salud, petroquímica o redes renovables, entre otros, de forma que cada lector pueda reconocerse en situaciones muy próximas a su realidad diaria.

Para el profesional del sector, esta guía es mucho más que un texto de consulta: es una herramienta concreta para mejorar su forma de trabajar. Le ayuda a estructurar la gestión de la ciberseguridad OT, a priorizar inversiones, a justificar decisiones ante dirección y reguladores y a reducir la dependencia de soluciones improvisadas. Le proporciona un lenguaje común para alinear a los equipos de operación, mantenimiento, ciberseguridad, ingeniería y cumplimiento, facilitando la comunicación interna y acelerando la toma de decisiones en proyectos, auditorías o incidentes.

Desde la perspectiva de mejora de sus propias "estrategias de posicionamiento" como profesional, dominar los contenidos de esta guía supone avanzar varios pasos respecto a un enfoque puramente teórico: permite diseñar arquitecturas OT defensibles, definir requisitos claros a proveedores, liderar planes directores OT con criterio, preparar auditorías con tranquilidad y demostrar que se entiende la ciberseguridad no como un freno, sino como un habilitador de continuidad operativa, reputación y competitividad. En un mercado donde cada vez se valoran más los perfiles capaces de unir operación, seguridad y cumplimiento, contar con un dominio práctico de estas técnicas es un factor diferenciador real.

Adquirir esta guía práctica es, en definitiva, una inversión en conocimiento aplicado. No se trata solo de "saber más" sobre ciberseguridad, sino de disponer de un manual de trabajo que acompañe al profesional en el diseño de segmentaciones OT, en la definición de políticas de hardening, en la preparación de simulacros de incidentes o en la elaboración de informes ejecutivos para dirección y reguladores. Cada capítulo, cada checklist y cada formulario están pensados para ser utilizados en proyectos, comités, auditorías y planes de mejora, acortando curvas de aprendizaje y evitando errores que, en entornos críticos, pueden salir muy caros en términos de coste, reputación y seguridad.

En un entorno donde las amenazas evolucionan rápido, la regulación se vuelve más exigente y los incidentes OT empiezan a ocupar titulares, mantenerse actualizado y bien informado no es opcional: es parte de la responsabilidad profesional. Contar con una guía que combine fundamentos sólidos, enfoque OT, casos prácticos y herramientas listas para usar es una forma inteligente de

reforzar esa responsabilidad y de ganar confianza en la propia capacidad para tomar decisiones críticas.

Si su objetivo es llevar la ciberseguridad OT de su organización a un nivel superior, reducir la exposición al riesgo y consolidar su papel como referente interno en seguridad industrial, esta guía le ofrece un camino claro, ordenado y accionable. El siguiente paso está en sus manos: empezar a trabajar con ella y convertir sus contenidos en resultados tangibles sobre el terreno.