OT-Knight
An RBJCS brand

CATÁLOGO DE SERVICIOS Y FORMACIÓN



CIBERSEGURIDAD OT/ICS · SEGURIDAD FUNCIONAL

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

Protegemos lo que mantiene su planta en marcha. Personas, procesos y tecnología, del primer diseño al último turno, con un socio responsable.

Ingeniería básica (FEED)	Ingeniería de detalle	Construcción, FAT y SAT	Puesta en marcha	Operación y mantenimiento	Modificación y renovación

Gestión de la ciberseguridad OT como servicio · durante todo el ciclo de vida

PARA OPERADORES 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

EL RETO

Su planta debe funcionar con seguridad, ciberseguridad, fiabilidad y productividad.

NIS 2 y el EU CRA endurecen la regulación, y los sistemas de control están más conectados que nunca. Integramos la ciberseguridad OT y la seguridad funcional en programas adaptados a la sala de control, las paradas programadas y el expediente de seguridad.

NUESTRA RESPUESTA

La seguridad es el punto de partida

IEC 62443 se une a IEC 61511 e ISA TR84.00.09. Las ciberamenazas a sus funciones de seguridad deben tratarse junto con los riesgos de proceso.

Gobernanza que funciona en OT

IEC 62443 e ISO/IEC 27001 en un único sistema de gestión, centrado en las personas que operan y mantienen sus activos.

Experiencia detrás del asesoramiento

Competencias certificadas y experiencia real en planta, con participación en el Comité Técnico ISASecure ACSSA.

80+ años de experiencia OT en campo

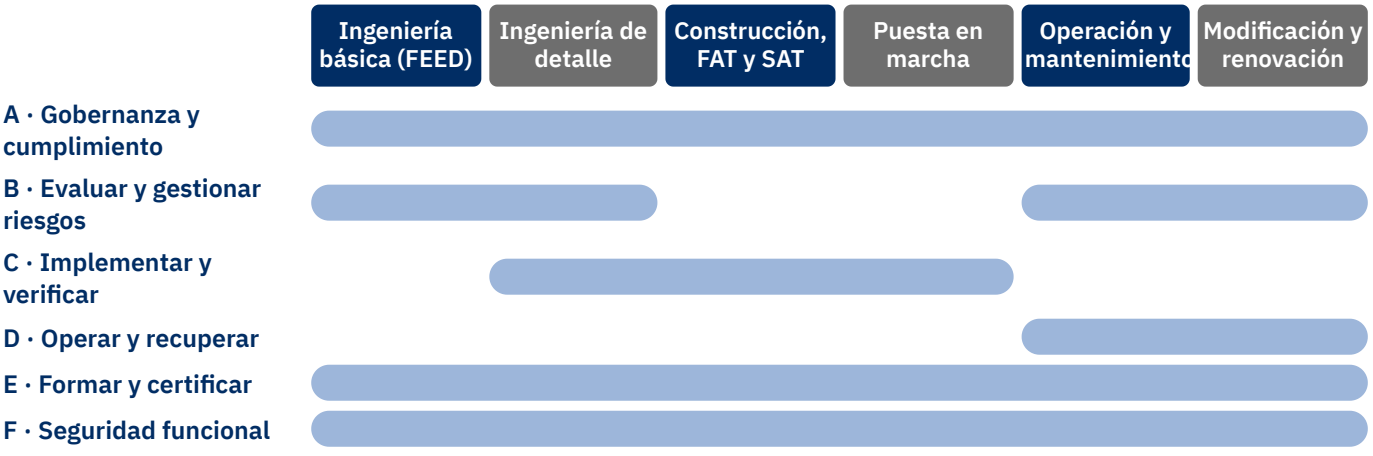
6 etapas, de FEED a la renovación

6 familias, un socio responsable

ML1–3 hoja de ruta ACSSA

Un socio responsable en cada etapa del ciclo de vida

Dónde interviene cada familia de servicios



Personas

Concienciación, competencias y funciones claras.

Procesos

Gobernanza, riesgos y procedimientos que funcionan en planta.

Tecnología

Arquitectura segura, controles y verificación en condiciones reales.

A Gobernanza y cumplimiento

Un sistema de gestión para IT y OT, y un enfoque de cumplimiento adaptado a las jurisdicciones en las que opera.

A1

Sistema unificado de gestión de la ciberseguridad

IEC 62443 integrada con ISO/IEC 27001

Un sistema de gestión para la IT corporativa y el OT de planta, concebido desde OT para que los controles funcionen en la sala de control.

QUÉ OBTIENE

- Sistema de gestión y declaración de aplicabilidad conjuntos (SPE de IEC 62443-2-1 + Anexo A de ISO/IEC 27001)
- Procedimientos OT prácticos para operadores y mantenimiento
- Preparación para ISO/IEC 27001 e ISASecure ACSSA

A2

NIS 2 — aplicación nacional

Cumplimiento en toda la planta, OT incluido, por país

Base común del grupo adaptada a los requisitos nacionales de NIS 2. Le ayudamos a gestionar la aplicación local de NIS 2 en cualquier jurisdicción, por ejemplo, en España.

QUÉ OBTIENE

- Clasificación de entidades y alcance por planta y país
- Base común del grupo adaptada a los requisitos nacionales
- Evidencias para los supervisores y notificación de incidentes

A3

Programa de seguridad durante el ciclo de vida

Para entidades SEVESO o COMAH

Un plan de gestión de seguridad funcional y ciberseguridad alineado con IEC 62443 e IEC 61511: quién hace qué en cada hito del proyecto.

QUÉ OBTIENE

- FS/CSMP con actividades por fase e hito
- Entrega EPC a operación y criterios de aceptación
- Indicadores de rendimiento y gestión del cambio

A4

Certificación ISASecure ACSSA

Acompañamiento de ML1 a ML3

ACSSA es la certificación ISASecure para propietarios de activos y operadores que implementan IEC 62443. Le guiamos durante todo el recorrido, con la experiencia de nuestra participación en el Comité Técnico ACSSA.

QUÉ OBTIENE

- Elegibilidad, alcance y división en zonas
- Análisis de deficiencias frente a IEC 62443-2-1, -3-2, -2-4 y -3-3
- Auditoría de prueba y apoyo hasta la certificación

A5

Seguridad de la cadena de suministro

Los mismos requisitos para cada proveedor

EPC, integradores, OEM y proveedores de servicios con los mismos requisitos de seguridad, de la licitación a la entrega.

QUÉ OBTIENE

- Requisitos IEC 62443-2-4 en licitaciones y contratos
- Evaluaciones de proveedores y registro de terceros
- Requisitos de conformidad CRA para productos adquiridos

A6

Reglamento europeo de Ciberresiliencia

EU CRA · Para fabricantes e integradores

Combinamos las normas horizontales EN 40000, las verticales e IEC 62443-4-1 / -4-2: un único conjunto de evidencias para todas.

QUÉ OBTIENE

- Clasificación de productos y vía de conformidad
- Evaluación de riesgos y desarrollo seguro
- Gestión de vulnerabilidades, notificación, expediente técnico

B Evaluar y gestionar riesgos

Conozca sus riesgos antes de invertir: un lenguaje común, de la dirección a la sala de control.

B1 Marco de gestión de riesgos

ISO 31000, IEC 62443 (2-1 y 3-2) e ISO/IEC 27005 integradas con su matriz de riesgos HSE.

ENTREGABLES · criterios y metodología de riesgos, registro de riesgos y proceso de tratamiento

B2 Análisis de riesgos IEC 62443-3-2

Sistema bajo consideración, zonas y conductos, evaluación de riesgos de alto nivel y detallada, y nivel de seguridad objetivo por zona.

ENTREGABLES · modelo de zonas y conductos, SL-T, informe de riesgos, CRS

B3 Ciberseguridad y seguridad funcional

Ciberamenazas al SIS y las funciones de seguridad evaluadas según IEC 61511 e ISA TR84.00.09, e incorporadas a HAZOP y LOPA.

ENTREGABLES · evaluación de riesgos del SIS, interfaz BPCS/SIS, aportes a la SRS

B4 Análisis de deficiencias

Su situación frente a IEC 62443, ISO/IEC 27001, los requisitos nacionales de NIS 2, el CRA o los criterios ACSSA.

ENTREGABLES · informe de deficiencias, puntuación de madurez, hoja de ruta adaptada a sus paradas programadas

C Implementar y verificar

Subsane las deficiencias. Después, demuéstrelo.

C1 Requisitos y especificaciones

Requisitos IEC 62443-3-3 en su SL-T, convertidos en la base de diseño que rige las entregas EPC y de proveedores.

ENTREGABLES · TRS (especificación de requisitos técnicos), segmentación, acceso remoto y recuperación

C2 Gestión de la ciberseguridad OT como servicio

Su función de ciberseguridad OT, desde los objetivos y proyectos hasta las auditorías.

ENTREGABLES · responsable designado, dirección de proyectos, selección de herramientas, pliegos de condiciones, auditorías, asesoramiento a demanda

C3 Proyectos de subsanación de deficiencias

Segmentación, interfaz IT/OT, acceso remoto, bastionamiento, cuentas, copias de seguridad y monitorización.

ENTREGABLES · alcance, selección de proveedores, supervisión, evidencias de cierre

C4 Aseguramiento y verificación

Verificación de SL, FAT y SAT de ciberseguridad, evaluaciones OT, pruebas de penetración y auditorías, considerando las condiciones reales de la planta.

ENTREGABLES · protocolos de prueba, informes de pruebas presenciadas, registro de hallazgos

Gestión de la ciberseguridad OT como servicio a su lado durante todo el ciclo de vida

- Un responsable de ciberseguridad OT designado
- Proyectos de ciberseguridad dirigidos
- Herramientas OT seleccionadas con usted
- Preparación de auditorías internas y externas
- Objetivos clave identificados y supervisados
- Subsanación de deficiencias
- Pliegos de condiciones y prescripciones técnicas
- Respuestas a demanda a consultas puntuales

D Operar y recuperar

Seguridad cada día. Preparados para los días difíciles.

D1 Evaluación de la postura operativa

Más allá de los documentos: arquitectura, acceso remoto, cuentas, copias de seguridad, medios extraíbles y prácticas diarias de su planta.

ENTREGABLES · puntuación por SPE de IEC 62443-2-1 y FR de IEC 62443-3-3, principales riesgos, plan de acción de 90 días

D2 Respuesta a incidentes OT

Planes y procedimientos alineados con la respuesta de emergencia de la planta y las obligaciones regulatorias de notificación.

ENTREGABLES · plan de respuesta, procedimientos por escenarios, matriz de escalado, ejercicios de mesa

D3 Continuidad y recuperación ante desastres

Requisitos de disponibilidad IEC 62443 (AVAIL) combinados con ISO 22301, ISO/IEC 27031 y prácticas NIST.

ENTREGABLES · análisis de impacto OT, RTO/RPO, procedimientos y pruebas de restauración

D4 Monitorización OT, NDR, EDR y SOC

Definimos los requisitos de monitorización, seleccionamos proveedores y gestionamos su rendimiento, con independencia de cualquier proveedor de SOC.

ENTREGABLES · alcance del trabajo, marco de indicadores, selección de proveedores

E Formar y certificar

Las personas son el primer control: desarrollamos las competencias detrás de cada control.

E1 Formación certificada ISA y PECB

Cursos ISA/IEC 62443 IC32, IC33, IC34, IC37 e IC49, y cursos PECB NIS 2, ISO/IEC 27001 e ISO 31000. Impartidos por nuestro ISA Qualified Instructor y PECB Certified Trainer, en su empresa o en sesiones abiertas.

E2 Concienciación y competencias

Sesiones adaptadas a operadores, técnicos, ingenieros, contratistas y órganos de dirección, incluida la formación prevista por NIS 2, basadas en la experiencia real en planta.



«La seguridad funcional y la ciberseguridad no son simplemente análogas: se encuentran literalmente en el mismo controlador».

Por eso, cada proyecto de OT-Knight integra la ciberseguridad en su expediente de seguridad.

F Seguridad funcional

Alineada con el ciclo de vida IEC 61511: segura desde el diseño y en operación.

F1 Gestión de la seguridad funcional y planificación del ciclo de vida

Creamos y gestionamos el sistema que mantiene seguro su SIS durante toda su vida útil: un sistema permanente para una planta en operación, o un plan de seguridad funcional dentro de un proyecto de inversión. Listo para evaluación y con una entrega limpia a operación.

- Planificación del ciclo de vida y validación
- Gestión de competencias
- Gestión del cambio
- Funciones de propietario, contratistas y proveedores
- Planificación de verificación y FSA
- Control documental

F2 Evaluaciones de seguridad funcional

FSA independientes en cada etapa del ciclo de vida, del análisis de peligros y riesgos y la SRS a la puesta en marcha, la operación y las modificaciones, además de auditorías que comprueban que se siguen sus procedimientos.

ENTREGABLES · informes FSA, auditorías de seguridad funcional, registro de hallazgos

F3 Requisitos de seguridad (SRS)

Redactamos o revisamos la SRS de cada función instrumentada de seguridad: estado seguro, puntos de disparo, tiempos de respuesta, SIL objetivo, reglas de by-pass y rearme, requisitos de proof test.

ENTREGABLES · SRS, lista de SIF, comentarios de revisión

F4 Verificación SIL

PFD, tolerancia a fallos de hardware, restricciones de arquitectura y capacidad sistemática frente a cada SIL objetivo: un cálculo independiente que puede defender en una evaluación.

ENTREGABLES · informe de verificación SIL, recomendaciones

F5 Apoyo a operación y mantenimiento

Procedimientos de proof test y optimización de intervalos, seguimiento de demandas y fallos, gestión de by-pass y revisión de modificaciones del SIS en operación.

ENTREGABLES · procedimientos de proof test, revisiones del desempeño del SIS, revisiones MoC

F6 Certifique su FSMS

Le guiamos en la elección del organismo de certificación y durante todo el proceso. Hemos liderado un sistema de gestión de seguridad funcional hasta la certificación exida: conocemos el camino de primera mano.

+ Seguridad y ciberseguridad, unidas

Un SIS necesita su propia evaluación de riesgos de ciberseguridad según IEC 61511. La realizamos junto con nuestro trabajo de seguridad funcional (véase B3) y formamos a sus equipos en ambos ámbitos (páginas 7–9).

Con usted a lo largo del ciclo de vida de seguridad IEC 61511

Del análisis de peligros a la retirada de servicio

Análisis de peligros y riesgos	Asignación de SIL y SRS	Diseño e ingeniería	Instalación, FAT y validación	Operación y mantenimiento	Modificación y retirada

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

Un camino claro. Un siguiente paso práctico.

1 **Descubrir**
Su planta, obligaciones y prioridades

2 **Evaluar**
Riesgos, deficiencias y madurez, verificados en planta

3 **Planificar**
Hoja de ruta adaptada a sus paradas programadas

4 **Implementar**
Especificar, gestionar y subsanar las deficiencias

5 **Verificar y mantener**
Probar, auditar, formar y seguir mejorando

PARA OPERACIONES CRÍTICAS

- Infraestructuras críticas
- Petróleo y gas
- Petroquímica
- Energías renovables
- BESS
- Generación eléctrica
- Transporte de electricidad
- Distribución

DÓNDE TRABAJAMOS

Proyectos en **Europa y Oriente Medio**, incluidos programas NIS 2 en varios países. Con sede en Bruselas, Bélgica.

Idiomas de trabajo: English · Français · Español.

COMPETENCIAS CERTIFICADAS

Miembro del Comité Técnico ISASecure ACSSA

ISA/IEC 62443 Cybersecurity Expert (ISA) · ISASecure ACSSA for Evaluators Specialist · Qualified ISA Instructor · PECB ISO/IEC 27001 Senior Lead Implementer · PECB ISO/IEC 27001 Senior Lead Auditor · PECB NIS 2 Directive Senior Lead Implementer · PECB ISO 31000 Senior Lead Risk Manager · TÜV SÜD · RISKNOWLOGY Certified Competency

Protejamos su planta juntos.

Háblenos sobre su planta, sus obligaciones y su próximo proyecto. Le propondremos un alcance claro y un primer paso práctico.

information@ot-knight.com

Bruselas, Bélgica · Europa y Oriente Medio