OT-Knight
An RBJCS brand

CATÁLOGO DE SERVICIOS



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

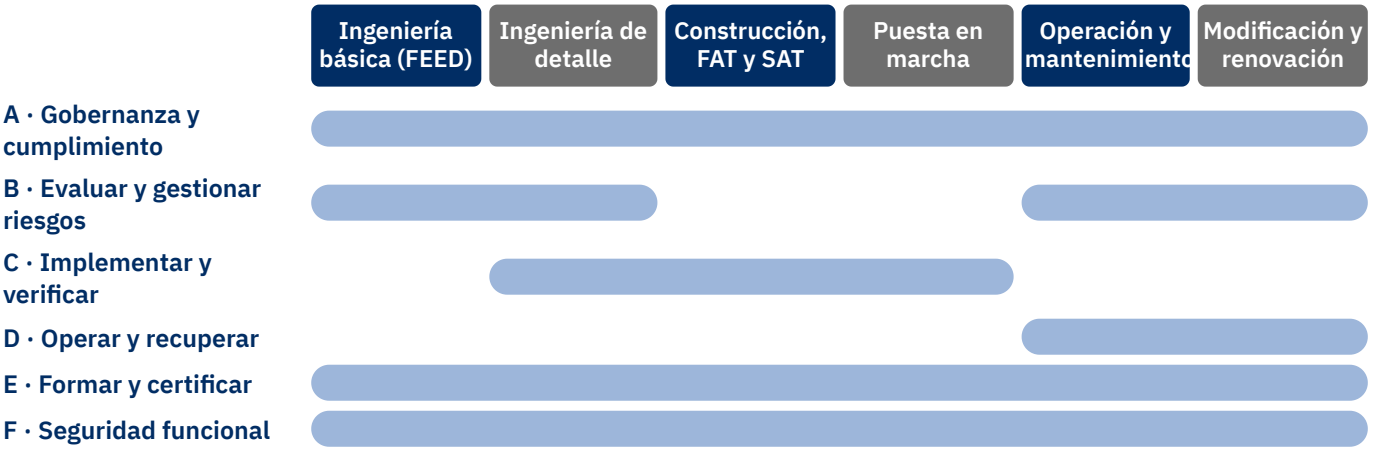
6 etapas, de FEED a la renovación

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 (servicio E).

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

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