



Shaping your present  
and future together

## CASO DE ÉXITO ASSESSMENT DE CIBERSEGURIDAD INDUSTRIAL



Scan this code to follow ROUE and receive  
standards, best practices and case studies



Caso de Éxito

# Assessment de Ciberseguridad Industrial

Alineado al estándar internacional ISA/IEC 62443

**Cliente:** Grupo industrial diversificado con operación multi-negocio **(caso anonimizado por confidencialidad)**

**Relevancia:** Experiencia directamente aplicable a entornos de proceso continuo y manufactura pesada con activos OT críticos (DCS, SCADA, PLCs).

Grupo industrial mexicano diversificado, estructurado como holding con múltiples unidades de negocio en sectores estratégicos, con presencia internacional y un portafolio de plantas productivas. Sus operaciones dependen de manera crítica de la continuidad de procesos industriales y de una amplia base de activos de tecnología operativa (OT).

Aunque cada unidad de negocio opera en una industria distinta, todas comparten un denominador común: ambientes productivos de alto valor donde una interrupción no planificada tiene impacto operativo, financiero y de seguridad física.



## Reto de negocio

La organización enfrentaba limitaciones para gestionar su riesgo cibernético industrial de forma efectiva y consistente entre sus distintas unidades de negocio:

- **Falta de visibilidad ejecutiva** del nivel de riesgo en entornos OT críticos.
- **Exposición creciente** a incidentes con potencial impacto directo en la operación y la producción.
- **Ausencia de un marco estructurado** y homologado, alineado a estándares internacionales.
- **Dificultad para priorizar inversiones** en ciberseguridad con base en el impacto real al negocio.

En entornos de proceso, un incidente OT no se traduce únicamente en sistemas de TI fuera de servicio: puede significar **paros de producción, riesgos de seguridad para el personal y pérdidas financieras por hora de inactividad.**

## Nuestro enfoque metodológico (ISA/IEC 62443)

Roue ejecuta un assessment estructurado en cinco fases, diseñado para realizarse sin afectar la operación. El resultado son hallazgos priorizados por criticidad y recomendaciones accionables que sirven como base para definir la hoja de ruta de inversión.

### Fase 1 - Planeación y alcance:

Reunión de arranque con el personal técnico y los responsables del sitio; confirmación de áreas, procesos, activos y ventanas de trabajo; revisión de la información disponible (diagramas de red, inventarios, topologías de automatización) y definición de los criterios de ejecución bajo el principio de no afectación operativa.

### Fase 2 - Levantamiento técnico en sitio

Recorrido técnico por las áreas en alcance y entrevistas con el personal operativo; identificación de los activos industriales relevantes (PLCs, HMIs, SCADA, estaciones de ingeniería, servidores OT, switches industriales) y su relación con procesos, líneas y funciones; validación de los puntos de comunicación y de las dependencias críticas entre activos.

### Fase 3 - Definición de zonas y conduits

Agrupación de activos según criticidad, función operacional, nivel Purdue y dependencia de proceso; identificación de los flujos de comunicación entre zonas; y análisis de la exposición entre redes OT, redes IT, sistemas corporativos y accesos remotos.

### Fase 4 - Evaluación de riesgos OT

Identificación de vectores potenciales de ataque y de debilidades de arquitectura y exposición; evaluación del impacto sobre la disponibilidad del proceso, la seguridad operacional y la integridad de los sistemas; priorización de riesgos según criticidad operativa; y evaluación del estado actual de los controles frente a los Foundational Requirements (FR) de la norma.

### Fase 5 - Consolidación y entrega

Consolidación y clasificación de los hallazgos técnicos por criticidad; definición de recomendaciones técnicas y de quick wins, que constituyen la base de la hoja de ruta priorizada.

## Alcance del proyecto

El assessment se ejecutó sobre una planta productiva representativa por cada unidad de negocio, abarcando deliberadamente entornos OT estructuralmente distintos entre sí.

- Múltiples industrias, un mismo marco. Roue aplicó un enfoque homologado ISA/IEC 62443 a procesos productivos diferentes, demostrando capacidad para evaluar entornos OT heterogéneos con un criterio consistente.
- Comparabilidad ejecutiva. Al usar la misma metodología y los mismos criterios de madurez, la dirección obtuvo una lectura comparable del riesgo entre unidades de negocio.
- Base escalable. El alcance inicial fue diseñado como punto de partida replicable hacia el resto de las plantas y operaciones del grupo.

[Mándanos un mensaje aquí](#)



## Entregable central: hoja de ruta priorizada

El objetivo principal del proyecto fue traducir los hallazgos en una **hoja de ruta (roadmap) de iniciativas de Ciberseguridad OT a 24–36 meses**, priorizando lo más relevante de acuerdo con los riesgos identificados durante el análisis.

| Horizonte                            | Enfoque de las iniciativas                                                                                 |
|--------------------------------------|------------------------------------------------------------------------------------------------------------|
| Quick wins<br>(0–6 meses)            | Acciones de alto impacto y baja complejidad para reducir la exposición más crítica de forma temprana.      |
| Corto–mediano<br>plazo (6–18 meses)  | Iniciativas de segmentación, control y fortalecimiento de la arquitectura OT prioritaria.                  |
| Mediano–largo<br>plazo (18–36 meses) | Consolidación del programa, gobierno de ciberseguridad industrial y escalamiento al resto de la operación. |

De esta forma, la organización pasó de un escenario de incertidumbre a contar con **un plan claro, secuenciado y defendible para invertir en ciberseguridad industrial**.

## Valor para el negocio

- **Protección de la continuidad operativa** en los activos críticos de cada unidad de negocio.
- **Reducción de riesgos** con impacto financiero y operativo directo.
- **Priorización eficiente** de las inversiones en ciberseguridad, con base en riesgo e impacto al negocio.
- **Fortalecimiento del cumplimiento** y del gobierno corporativo frente a estándares internacionales.
- **Visibilidad ejecutiva del riesgo** para una toma de decisiones informada a nivel dirección.
- **Base escalable** para una estrategia de ciberseguridad industrial a nivel de todo el grupo.

## Por qué Roue

- **Especialización en convergencia IT/OT.** No somos una firma de TI que “también atiende OT”: la seguridad de entornos industriales es nuestro foco central.
- **Independencia de fabricante.** Nuestras recomendaciones responden al riesgo del cliente, no a la venta de una tecnología específica.
- **Experiencia en industria pesada y multi-planta.** Capacidad probada para evaluar entornos OT diversos bajo un mismo marco y consolidarlos en una estrategia única.
- **Orientación a la decisión.** Entregamos claridad ejecutiva y hojas de ruta accionables, no diagnósticos que terminan archivados.



Shaping your present  
and future together

### Transforma la visibilidad de riesgo en decisiones estratégicas

Esta misma metodología, aplicada a tu planta, te da claridad ejecutiva sobre tu exposición real, tus prioridades y el plan de inversión recomendado para los próximos meses.

Agenda un Assessment de Ciberseguridad Industrial con Roue.

[www.roue.com.mx](http://www.roue.com.mx)

**Mádanos un mensaje aquí**