Framework de Evaluación de Riesgos ICS/OT

Guía Práctica para Entornos Industriales

PROTISEC · 2026

Introducción

Este framework proporciona una metodología estructurada para evaluar riesgos de seguridad en sistemas de control industrial (ICS) y tecnología operacional (OT). Diseñado para:

- Directores de planta y responsables de operaciones
- Equipos de convergencia IT/OT
- CISOs con responsabilidad sobre infraestructura industrial
- Responsables de cumplimiento (NIS2, ISA/IEC 62443)

Los entornos industriales presentan desafíos únicos: protocolos legacy, restricciones de tiempo real, operaciones críticas para la seguridad y convergencia con redes IT. Una evaluación de seguridad IT genérica ignorará el 80% de los riesgos ICS/OT.

Este documento proporciona la metodología, checklists y matriz de scoring para identificar, priorizar y remediara brechas de seguridad ICS/OT — antes de que un incidente fuerce la conversación.

---

1. Metodología de Evaluación de Riesgos ICS/OT

1.1 Definición del Alcance

Antes de evaluar, define los límites:

Alcance físico: - ¿Qué instalaciones? (planta, subestación, almacén) - ¿Qué sistemas de control? (DCS, SCADA, PLC, RTU) - ¿Qué redes? (Niveles 0-5 del modelo Purdue)

Alcance operacional: - ¿Sistemas instrumentados de seguridad (SIS)? - ¿Sistemas de detección de incendios y gases? - ¿Sistemas de parada de emergencia?

Alcance regulatorio: - ¿Designación NIS2? (entidad esencial/importante) - ¿Requisito de cumplimiento ISA/IEC 62443? - ¿Regulaciones sectoriales? (energía, agua, transporte)

1.2 Fases de Evaluación

Fase 1: Descubrimiento de Activos (1-2 semanas) - Inventario de todos los dispositivos industriales (PLCs, RTUs, HMIs, estaciones de ingeniería) - Mapeo de topología de red (VLANs, firewalls, DMZs) - Identificación de protocolos en uso (Modbus, DNP3, OPC-UA, Profinet) - Documentación de versiones de firmware y niveles de parcheo

Fase 2: Modelado de Amenazas (1 semana) - Identificación de actores de amenaza (script kiddies → estados-nación) - Mapeo de superficies de ataque (HMIs expuestas a internet, acceso remoto, puertos USB) - Evaluación de capacidades del adversario (matriz MITRE ATT&CK ICS) - Consideración de amenazas internas (operadores, contratistas, empleados despedidos)

Fase 3: Evaluación de Vulnerabilidades (2-3 semanas) - Análisis a nivel de protocolo (Modbus en texto plano, sin autenticación) - Revisión de segmentación de red (redes planas, DMZs faltantes) - Auditoría de control de acceso (contraseñas por defecto, cuentas compartidas) - Evaluación de seguridad física (armarios sin cerrar, HMIs sin supervisión)

Fase 4: Scoring de Riesgos (1 semana) - Aplicar matriz de riesgo (probabilidad × impacto) - Priorizar por impacto en seguridad primero, luego operacional, luego financiero - Documentar decisiones de aceptación de riesgo

Fase 5: Hoja de Ruta de Remediación (1-2 semanas) - Victorias rápidas (cambio de contraseñas, segmentación de red) - Medio plazo (hardening de protocolos, despliegue de monitorización) - Largo plazo (implementación completa del modelo Purdue, certificación ISA 62443)

2. Referencia del Modelo Purdue

La Purdue Enterprise Reference Architecture (PERA) define 6 niveles para la segmentación de redes industriales:

Nivel 4 — Planificación Empresarial - ERP, MES, logística empresarial - Red corporativa IT - Conectado a internet

Nivel 3.5 — DMZ Industrial - Zona tampón entre IT y OT - Historiadores, servidores de monitorización, gestión de parches - **Punto de control crítico** — todo el tráfico IT↔OT pasa aquí

Nivel 3 — Gestión de Operaciones - Servidores HMI, estaciones de ingeniería - Sistemas de gestión de operaciones - Sin acceso directo a internet

Nivel 2 — Control Supervisorio - Servidores SCADA, controladores DCS - Monitorización y control en tiempo real - Acceso restringido

Nivel 1 — Control Básico - PLCs, RTUs, controladores independientes - Control directo de proceso - Crítico para la seguridad

Nivel 0 — Proceso Físico - Sensores, actuadores, variadores - Proceso de fabricación físico - Sin stack de red (analógico/eléctrico)

Reglas de Segmentación

1. **Sin conectividad directa Nivel 4 ↔ Niveles 0-2.** Todo el tráfico se enruta a través del DMZ Nivel 3.5.
2. **Gateways unidireccionales** para extracción de datos de Niveles 0-1 (diodos de datos).
3. **DMZ Industrial (Nivel 3.5)** aloja todos los servicios entre zonas (historiadores, jump hosts, servidores de parches).
4. **Sin HMIs expuestas a internet.** Acceso remoto vía VPN + jump host en DMZ.
5. **VLANs separadas por nivel** con reglas de firewall que restringen el movimiento lateral.

3. Checklist Rápido ISA/IEC 62443

ISA/IEC 62443 es el estándar internacional para seguridad ICS. Usa este checklist para un análisis rápido de brechas:

Requisitos Fundacionales (Security Level 1)

SR 1 — Control de Identificación y Autenticación - [ ] IDs de usuario únicos para todos los operadores - [ ] Complejidad de contraseñas aplicada (mín 12 chars, sin por defecto) - [ ] Autenticación multi-factor para acceso remoto - [ ] Bloqueo de cuenta tras 5 intentos fallidos

SR 2 — Control de Uso - [ ] Control de acceso basado en roles (RBAC) implementado - [ ] Principio de mínimo privilegio (operadores ≠ ingenieros ≠ admins) - [ ] Timeout de sesión (15 min inactividad) - [ ] Sin cuentas compartidas

SR 3 — Integridad del Sistema - [ ] Anti-malware en todas las HMIs basadas en Windows - [ ] Whitelisting de aplicaciones (sin ejecutables no autorizados) - [ ] Monitorización de integridad de archivos en sistemas críticos - [ ] Secure boot donde esté soportado

SR 4 — Confidencialidad de Datos - [ ] Protocolos cifrados (OPC-UA modo seguro, no Modbus en texto plano) - [ ] TLS 1.2+ para acceso remoto - [ ] Sin credenciales en texto plano en archivos de configuración - [ ] Clasificación de datos (público, interno, confidencial, restringido)

SR 5 — Flujo de Datos Restringido - [ ] Segmentación de red según modelo Purdue - [ ] Reglas de firewall documentadas y revisadas trimestralmente - [ ] Sin acceso directo a internet desde Niveles 0-2 - [ ] DMZ Industrial (Nivel 3.5) aplicada

SR 6 — Respuesta Temporal a Eventos - [ ] Logging centralizado (SIEM o equivalente) - [ ] Alertas ante eventos de seguridad (logins fallidos, cambios de configuración) - [ ] Plan de respuesta a incidentes documentado y probado - [ ] Monitorización 24/7 para infraestructura crítica

SR 7 — Disponibilidad de Recursos - [ ] Controladores redundantes para procesos críticos - [ ] Sistema de alimentación ininterrumpida (UPS) para sistemas de control - [ ] Procedimientos de backup y restauración probados anualmente - [ ] Plan de recuperación ante desastres con RTO/RPO definidos

Requisitos Avanzados (Security Level 2-4)

- [ ] Sistema de gestión de seguridad (ISMS) establecido
- [ ] Evaluación de riesgos realizada según IEC 62443-3-2
- [ ] Niveles de seguridad asignados por zona y conducto
- [ ] Política de seguridad IACS documentada y aprobada
- [ ] Auditoría de terceros completada (organismo de certificación)

---

4. Evaluación de Segmentación IT/OT

Usa esta rúbrica de scoring para evaluar la madurez actual de segmentación:

Nivel 0 — Inexistente (0 puntos)

- Red plana: IT y OT en la misma VLAN
- Acceso directo a internet desde HMIs
- Sin firewall entre redes corporativa y de planta
- Cuentas compartidas, contraseñas por defecto

Nivel 1 — Básico (10-30 puntos)

- Alguna segmentación VLAN (IT vs OT)
- Firewall presente pero reglas no revisadas
- Acceso a internet restringido pero no bloqueado
- Política de contraseñas existe pero no se aplica

Nivel 2 — Definido (40-60 puntos)

- Modelo Purdue parcialmente implementado (DMZ Nivel 3.5 existe)
- Reglas de firewall documentadas y revisadas anualmente
- Acceso a internet bloqueado para Niveles 0-2

- RBAC implementado, MFA para acceso remoto

Nivel 3 — Gestionado (70-85 puntos)

- Modelo Purdue completo con gateways unidireccionales para Niveles 0-1
- DMZ Industrial aloja todos los servicios entre zonas
- Monitorización de red (IDS/IPS para protocolos OT)
- Revisiones de acceso trimestrales, tests de penetración anuales

Nivel 4 — Optimizado (90-100 puntos)

- Arquitectura Zero Trust para ICS (micro-segmentación)
- Monitorización continua con detección de anomalías (basada en ML)
- Reporting automatizado de cumplimiento (ISA 62443)
- Respuesta a incidentes probada trimestralmente con escenarios específicos OT

Instrucciones de Scoring

1. Puntúa cada categoría (físico, red, control de acceso, monitorización, respuesta a incidentes)
2. Calcula la media ponderada (segmentación de red = 30%, control de acceso = 25%, monitorización = 20%, respuesta a incidentes = 15%, físico = 10%)
3. Mapea a nivel de madurez
4. Identifica brechas y prioriza remediación

---

5. Matriz de Scoring de Riesgos

Probabilidad (1-5)

1 — Rara - El ataque requiere acceso físico + conocimiento interno - Sin vulnerabilidades conocidas en sistemas desplegados - Red completamente segmentada, sin exposición a internet

2 — Improbable - Existe vulnerabilidad pero requiere exploit complejo - Segmentación parcial (algunos activos expuestos a internet) - Monitorización básica en marcha

3 — Posible - Vulnerabilidad conocida con exploit público - Red plana, conectividad directa IT↔OT - Sin monitorización ni alertas

4 — Probable - Vulnerabilidad activamente explotada (lista CISA KEV) - HMIs o estaciones de ingeniería expuestas a internet - Credenciales por defecto en uso

5 — Casi Segura - Indicadores de compromiso activo (malware, acceso no autorizado) - Sin segmentación, sin monitorización, sin control de acceso - Incidentes similares recientes en el sector

Impacto (1-5)

1 — Negligible - Sin impacto en seguridad - Sin paradas de producción - Impacto financiero < 10K€

2 — Menor - Incidente menor de seguridad (primeros auxilios) - Parada de producción < 4 horas - Impacto financiero 10K-100K€

3 — Moderado - Lesión con pérdida de jornada laboral - Parada de producción 4-24 horas - Impacto financiero 100K-1M€ - Notificación regulatoria requerida

4 — Mayor - Lesión grave o vertido medioambiental - Parada de producción 1-7 días - Impacto financiero 1M-10M€ - Reporting de incidente NIS2 activado

5 — Catastrófico - Fatalidad o desastre medioambiental mayor - Parada de producción > 7 días - Impacto financiero > 10M€ - Responsabilidad penal, pérdida de licencia de operación

Puntuación de Riesgo = Probabilidad × Impacto

1-4 — Riesgo Bajo - Aceptar o monitorizar - Incluir en próximo ciclo presupuestario

5-9 — Riesgo Medio - Mitigar en 6 meses - Asignar responsable, trackear en registro de riesgos

10-15 — Riesgo Alto - Mitigar en 30 días - Escalar a CISO/director de planta

16-25 — Riesgo Crítico - Acción inmediata requerida - Considerar parada hasta remediación - Notificación a dirección ejecutiva

---

6. Vulnerabilidades Comunes ICS/OT

Vulnerabilidades de Protocolo

Modbus TCP (sin autenticación) - Riesgo: Cualquiera en la red puede leer/escribir registros - Impacto: Cambios de control no autorizados, disrupción de proceso - Remediación: Desplegar gateways de seguridad Modbus, segmentación de red

OPC Classic (DA/HDA, basado en DCOM) - Riesgo: Vulnerabilidades DCOM, sin cifrado - Impacto: Movimiento lateral, exfiltración de datos - Remediación: Migrar a OPC-UA modo seguro

Profinet / EtherNet/IP (sin autenticación) - Riesgo: Dispositivos rogue pueden inyectar comandos - Impacto: Bypass de sistemas de seguridad, daño a equipos - Remediación: Seguridad de puertos, 802.1X, control de acceso a red

Vulnerabilidades de Red

Redes planas IT/OT - Riesgo: Compromiso de IT corporativa → planta - Impacto: Ransomware se propaga de IT a OT - Remediación: Segmentación modelo Purdue, DMZ industrial

HMIs expuestas a internet - Riesgo: Vector de ataque directo desde internet - Impacto: Toma de control remota de procesos industriales - Remediación: Eliminar acceso a internet, VPN + jump host

Redes inalámbricas (Wi-Fi, Zigbee) - Riesgo: Escucha, puntos de acceso rogue - Impacto: Control no autorizado, robo de datos - Remediación: WPA3-Enterprise, segmentación de red, monitorización

Vulnerabilidades de Control de Acceso

Credenciales por defecto - Riesgo: Compromiso trivial - Impacto: Control total del sistema - Remediación: Auditoría de contraseñas, cambiar todas las por defecto, MFA

Cuentas compartidas - Riesgo: Sin trazabilidad, no se pueden rastrear acciones - Impacto: Amenaza interna, fallo de cumplimiento - Remediación: IDs de usuario únicos, RBAC

Sin timeout de sesión - Riesgo: Estaciones desatendidas = acceso abierto - Impacto: Cambios de control no autorizados - Remediación: Timeout de 15 minutos, bloqueos de pantalla

Vulnerabilidades de Seguridad Física

Armarios de control sin cerrar - Riesgo: Acceso físico = fin del juego - Impacto: Malware por USB, manipulación de hardware - Remediación: Armarios cerrados, logs de acceso

HMIs sin supervisión - Riesgo: Acceso físico no autorizado - Impacto: Manipulación de proceso - Remediación: Control de acceso, CCTV, modo kiosko

Sin gestión de visitantes - Riesgo: Contratistas, vendors sin monitorizar - Impacto: Introducción de malware, espionaje - Remediación: Logs de visitantes, acceso escoltado, escaneo de dispositivos

---

7. Priorización de Remediación

Victorias Rápidas (0-30 días)

1. **Cambiar todas las contraseñas por defecto** (PLCs, HMIs, dispositivos de red)
2. **Bloquear acceso a internet** para sistemas de Niveles 0-2
3. **Deshabilitar servicios no usados** (FTP, Telnet, SMBv1)
4. **Parchear HMIs Windows** (solo actualizaciones de seguridad críticas)
5. **Implementar segmentación de red** (VLANs, reglas básicas de firewall)

Medio Plazo (1-6 meses)

1. **Desplegar DMZ industrial** (Nivel 3.5)
2. **Implementar RBAC** (control de acceso basado en roles)
3. **Activar logging y monitorización** (integración SIEM)
4. **Migrar a protocolos seguros** (OPC-UA, seguridad Modbus)
5. **Formación a operadores** (phishing, higiene USB, reporting de incidentes)

Largo Plazo (6-18 meses)

1. **Implementación completa del modelo Purdue** (gateways unidireccionales)
2. **Desplegar IDS/IPS específico OT** (monitorización consciente de protocolos)
3. **Certificación ISA/IEC 62443** (Security Level 1-2)
4. **Testing de respuesta a incidentes** (escenarios específicos OT)
5. **Monitorización continua de cumplimiento** (reporting automatizado)

Framework de Priorización

Seguridad primero: Cualquier riesgo con impacto en seguridad (lesiones, vertidos medioambientales) = prioridad crítica.

Regulatorio segundo: Entidades esenciales NIS2 tienen deadlines de cumplimiento 2025-2026. ISA 62443 puede ser requerido contractualmente.

Operacional tercero: Riesgo de parada de producción. Calcular coste por hora de parada vs. coste de remediación.

Financiero cuarto: Pérdida financiera directa (ransomware, robo, fraude).

---

8. Próximos Pasos

Este framework proporciona la metodología para evaluar riesgos de seguridad ICS/OT. La ejecución requiere:

1. **Inventario de activos** — no puedes proteger lo que no puedes ver
2. **Modelado de amenazas** — entender tus adversarios específicos
3. **Análisis de brechas** — comparar estado actual con requisitos ISA 62443
4. **Scoring de riesgos** — priorizar por impacto en seguridad y operacional
5. **Hoja de ruta de remediación** — victorias rápidas primero, luego mejora sistemática

Cómo Puede Ayudar PROTISEC

PROTISEC está especializado en seguridad ICS/OT para infraestructura crítica:

- **Evaluación ISA/IEC 62443** — análisis completo de brechas, determinación de Security Level
- **Implementación modelo Purdue** — diseño de segmentación de red, DMZ industrial
- **Detección de anomalías OT** — monitorización basada en IA para desviaciones de protocolo
- **Respuesta a incidentes** — playbooks específicos ICS, contención sin impacto en producción
- **Cumplimiento** — NIS2, ISO 27001, regulaciones sectoriales

Contacta para una evaluación técnica gratuita de 30 minutos: - Web: protisec.com/contacto - WhatsApp: +34 XXX XXX XXX - Email: contacto@protisec.com

---

Sobre PROTISEC

PROTISEC es una firma boutique de ciberseguridad especializada en seguridad ICS/OT, MLSecOps y cumplimiento regulatorio (NIS2, ISO 27001, RGPD). Trabajamos con operadores de infraestructura crítica, manufactura y compañías energéticas en España y la UE.

Nuestro equipo combina 30+ años de experiencia en automatización industrial con prácticas modernas de ciberseguridad. Entendemos que en entornos OT, la disponibilidad y la seguridad van primero — la seguridad debe habilitar las operaciones, no disrumpirlas.

Certificaciones: ISO 27001 Lead Implementer, ISA/IEC 62443 Cybersecurity Expert, DPO Certificado AEPD
