



CURSO/GUÍA PRÁCTICA CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS



Índice

¿QUÉ APRENDERÁ?	19
Introducción.	20
PARTE PRIMERA.	23
Fundamentos de la ciberseguridad OT en infraestructuras críticas	23
Capítulo 1: Infraestructuras críticas y particularidades de la ciberseguridad OT	23
1. Definición y tipología de infraestructuras críticas	23
a. Sectores estratégicos, energía, agua, transporte, salud, industria	23
b. Servicios esenciales y dependencias tecnológicas OT	24
c. Entornos regulados y no regulados en España y Latinoamérica	25
2. Diferencias estructurales entre entornos IT y entornos OT	26
a. Objetivos de seguridad, confidencialidad frente a disponibilidad y seguridad física	26
b. Tecnologías, protocolos y ciclos de vida de activos IT y OT	26
c. Restricciones de operación continua y limitaciones para intervenir en OT	27
3. Conceptos clave de ciberseguridad OT en infraestructuras críticas	28
a. Sistemas ICS, SCADA, DCS y sistemas ciberfísicos	28
b. IIoT, sensórica avanzada y conectividad industrial	29
c. Relación entre ciberseguridad OT, safety y fiabilidad operativa	29
4. Panorama actual de amenazas sobre infraestructuras críticas	30
a. Amenazas internas, externas y cadena de suministro	30
b. Tipologías de atacantes, delincuencia organizada, Estados, hacktivismo	31
c. Casuística de incidentes OT conocidos y tendencias recientes	32
5. Impacto de los incidentes de ciberseguridad OT	33
a. Impacto en la continuidad del servicio público y producción	33
b. Impacto económico, contractual y reputacional para el operador	33
c. Impacto en seguridad de las personas y medioambiente	34
6. Contexto internacional, España y Latinoamérica	35
a. Niveles de madurez en ciberseguridad OT por sectores	35
b. Brechas habituales, recursos, talento, presupuesto y gobernanza	35
c. Oportunidades de mejora y líneas estratégicas recomendadas	36
Capítulo 2: Arquitecturas OT y superficie de exposición en infraestructuras críticas	37
1. Componentes básicos de una arquitectura OT	37
a. PLC, RTU, IED, HMI y sistemas SCADA/DCS	37
b. Redes de campo, buses industriales y sensores	39
c. Sistemas auxiliares, historians, MES, interfaces con ERP	40
2. Capas de red y modelos de referencia en OT	41
a. Modelo Purdue y otras arquitecturas de referencia	41
b. Capas de planta, control, supervisión y negocio	42
c. Flujos de datos verticales y horizontales entre capas	43
3. Interconexión IT/OT y vectores de exposición	44
a. Integraciones con sistemas corporativos y nube	44

b. Accesos remotos de fabricantes, mantenedores y técnicos	45
c. Riesgos de túneles no controlados y soluciones improvisadas	45
4. Activos expuestos y Shadow OT	46
a. Equipos no inventariados y configuraciones heredadas	46
b. Sistemas obsoletos y sin soporte del fabricante	47
c. Dispositivos móviles, portátiles y medios extraíbles en planta	48
5. Cartografiado y modelado de la arquitectura OT.....	49
a. Descubrimiento pasivo y activo de activos OT	49
b. Herramientas de inventario, etiquetado y clasificación	49
c. Representación de zonas, conductos y dependencias críticas	50
6. Escenarios tipo de infraestructuras críticas	51
a. Plantas de generación y redes de transporte de energía	51
b. Redes de agua, saneamiento, transporte y logística	52
c. Salud, industria de procesos y manufactura discreta	52
PARTE SEGUNDA.....	54
Gobierno, riesgo y gestión de la ciberseguridad OT.....	54
Capítulo 3: Gobierno y estrategia de ciberseguridad OT en infraestructuras críticas.....	54
1. Estrategia de ciberseguridad OT alineada con la organización	54
a. Relación entre estrategia corporativa y estrategia OT	54
b. Integración de la ciberseguridad OT en la gestión del riesgo global	55
c. Prioridades, hoja de ruta y planes directores OT	56
2. Políticas y normas internas específicas para OT	56
a. Políticas de seguridad OT y estándares internos mínimos	56
b. Procedimientos operativos seguros en operación y mantenimiento	57
c. Gestión documental y control de versiones de políticas OT	58
3. Organización, roles y responsabilidades.....	58
a. Relación CISO, responsable OT y responsables de planta	58
b. Comités de riesgo, seguridad y continuidad de negocio	59
c. RACI de la ciberseguridad OT en la organización.....	59
4. Cultura de ciberseguridad en entornos OT	60
a. Concienciación y sensibilización de equipos de operación y mantenimiento	60
b. Gestión del cambio cultural entre perfiles IT y OT	61
c. Buenas prácticas de comunicación interna y reportes	61
5. Gestión de proveedores y contratos desde la perspectiva OT	62
a. Requisitos de seguridad OT en pliegos y contratos.....	62
b. Evaluación de proveedores críticos y servicios gestionados	62
c. Acuerdos de nivel de servicio (SLA) y métricas de seguridad OT.....	63
6. Indicadores para el gobierno de la ciberseguridad OT	63
a. Definición de KPI y KRI específicos de entornos OT	63
b. Cuadros de mando para dirección y responsables técnicos	64
c. Seguimiento y revisión periódica del nivel de madurez OT	64
Capítulo 4: Análisis y gestión de riesgos de ciberseguridad OT.....	66
1. Metodologías de análisis de riesgos aplicadas a OT	66
a. Enfoques cualitativos, semi-cuantitativos y cuantitativos	66

b. Adaptación de metodologías IT al contexto OT	67
c. Frecuencia, alcance y actualización del análisis de riesgos	68
2. Identificación de amenazas y vulnerabilidades en OT	69
a. Amenazas específicas de OT, físicas, lógicas y mixtas	69
b. Vulnerabilidades técnicas de PLC/RTU, SCADA y redes de campo	70
c. Vulnerabilidades organizativas y de procesos en OT	71
3. Evaluación de impacto en infraestructuras críticas	71
a. Impacto sobre producción, servicio y seguridad física	71
b. Efectos en la cadena de suministro y ecosistema de socios	72
c. Criterios de cuantificación de impacto y escenarios de peor caso	73
4. Priorización y tratamiento del riesgo OT	74
a. Matrices de riesgo adaptadas a entornos industriales	74
b. Selección de controles técnicos, organizativos y físicos	75
c. Aceptación, mitigación, transferencia y evitación de riesgos	76
5. Riesgo de terceros y cadena de suministro OT	77
a. Dependencias de fabricantes, integradores y mantenedores	77
b. Riesgos de componentes y software de terceros	77
c. Estrategias de reducción de riesgo en la cadena OT	78
6. Planes directores de ciberseguridad OT	79
a. Objetivos, alcance y priorización de proyectos	79
b. Planificación temporal, presupuesto y recursos necesarios	79
c. Seguimiento, revisión y actualización del plan director OT	80
PARTE TERCERA.	81
Segmentación de redes OT y arquitecturas seguras	81
Capítulo 5: Segmentación de redes OT basada en zonas y conductos	81
1. Principios de segmentación en ciberseguridad OT	81
a. Defensa en profundidad y mínimo privilegio	81
b. Separación de dominios de seguridad y funciones	82
c. Reducción de la superficie de exposición OT	83
2. Zonas y conductos según ISA/IEC 62443	84
a. Conceptos de zona de seguridad y conducto de comunicación	84
b. Criterios para agrupar activos en zonas coherentes	84
c. Ejemplos prácticos de zonificación en plantas reales	86
3. Segmentación interna de la red OT	87
a. Diseño de VLAN y subredes para entornos industriales	87
b. Separación de redes de seguridad, control y supervisión	87
c. Segmentación de servicios auxiliares y redes técnicas	88
4. Controles de tráfico entre zonas y conductos	89
a. Listas de control de acceso y filtrado de tráfico	89
b. Uso adecuado de routers, switches gestionables y firewalls	89
c. Limitación de protocolos, puertos y servicios innecesarios	90
5. Integración de la segmentación en proyectos nuevos y existentes	91
a. Segmentación OT en proyectos greenfield	91
b. Re-segmentación de entornos legacy brownfield	91
c. Estrategias de transición minimizando paradas de planta	92

6. Errores típicos y buenas prácticas de segmentación OT	93
a. Problemas frecuentes detectados en auditorías de red OT	93
b. Patrones de diseño recomendados y patrones a evitar	93
c. Checklists básicos para revisar una segmentación OT	94
Capítulo 6: DMZ industrial, perímetros OT y conexiones seguras IT/OT	96
1. Concepto y funciones de la DMZ industrial	96
a. Rol de la DMZ en la protección de redes OT	96
b. Servicios permitidos y prohibidos en la DMZ industrial	97
c. Ejemplos de topologías DMZ en infraestructuras críticas	98
2. Arquitecturas de interconexión IT/OT	99
a. Topologías de referencia y variantes habituales	99
b. Separación de dominios corporativo, DMZ y OT	99
c. Evaluación de riesgos en cada punto de interconexión	100
3. Firewalls industriales y otros componentes de perímetro	101
a. Tipos de firewalls y capacidades avanzadas en entornos OT	101
b. Diodos de datos, proxies y pasarelas de aplicación	102
c. Diseño de reglas y políticas de filtrado en firewalls OT	102
4. Protección de accesos remotos a OT	103
a. Arquitecturas de acceso remoto para mantenimiento y soporte	103
b. VPN, autenticación fuerte y registro de sesiones	104
c. Saltos administrados y soluciones de acceso privilegiado	104
5. Monitorización del perímetro OT	105
a. Uso de SPAN/TAP para capturar tráfico	105
b. Sondas de monitorización específicas para redes OT	106
c. Integración de la visibilidad del perímetro en el SOC	106
6. Casos prácticos de rediseño de perímetros OT inseguros	107
a. Identificación de debilidades en diseños heredados	107
b. Propuesta de arquitecturas objetivo más seguras	108
c. Roadmap de implantación por fases en infraestructuras críticas	108
PARTE CUARTA.	110
Hardening de PLC/RTU y dispositivos industriales	110
Capítulo 7: Inventario, clasificación y políticas de hardening de activos OT	110
1. Inventario y clasificación de activos OT	110
a. Técnicas y herramientas para descubrir activos OT	110
b. Etiquetado y clasificación por función y ubicación	111
c. Asignación de propietarios funcionales y de seguridad	112
2. Criticidad de activos OT en infraestructuras críticas	113
a. Criterios para valorar la criticidad de cada activo	113
b. Activos de alta criticidad y activos de soporte	114
c. Matriz de criticidad y priorización de esfuerzos de hardening	115
3. Principios generales de hardening para dispositivos industriales	116
a. Reducción de superficie de ataque en PLC/RTU y SCADA	116
b. Desactivación de servicios y protocolos innecesarios	117
c. Gestión de contraseñas, cuentas y roles de usuario	117



4. Políticas de configuración segura OT	118
a. Configuraciones base (baselines) y parámetros obligatorios	118
b. Plantillas de configuración por tipo de dispositivo	119
c. Control de cambios y aprobación de nuevas configuraciones	120
5. Gestión de credenciales y secretos en entornos OT	120
a. Política de contraseñas y autenticación multifactor donde sea viable	120
b. Almacenamiento seguro de credenciales y llaves	121
c. Rotación de credenciales y revocación de accesos	122
6. Integración del hardening en el ciclo de vida de proyectos OT	122
a. Requisitos de hardening en fase de diseño y compra	122
b. Pruebas de aceptación de seguridad antes de la puesta en marcha	123
c. Revisión periódica del hardening durante la operación	124

Capítulo 8: Hardening técnico de PLC/RTU, sistemas SCADA y comunicaciones de campo 125

1. Configuración segura de PLC y RTU	125
a. Gestión de firmware, versiones y fuentes de confianza	125
b. Protección de programación y carga de lógica	126
c. Restricción de puertos, servicios y funciones de diagnóstico	127
2. Protección de sistemas SCADA/DCS y estaciones de ingeniería	128
a. Sistemas operativos endurecidos y reducción de servicios	128
b. Segmentación de estaciones de operación y de ingeniería	128
c. Copias de seguridad y recuperación segura de proyectos	129
3. Seguridad en protocolos industriales	130
a. Características de seguridad de Modbus, DNP3, IEC-104, OPC, etc.	130
b. Riesgos de protocolos sin cifrado ni autenticación	131
c. Estrategias de encapsulado y securización de protocolos legacy	131
4. Cifrado y autenticación en redes de campo	132
a. Opciones de cifrado a nivel de enlace, red y aplicación	132
b. Gestión de certificados y llaves criptográficas en OT	133
c. Limitaciones y consideraciones de rendimiento en planta	134
5. Gestión de vulnerabilidades y parches en sistemas OT	134
a. Fuentes de información de vulnerabilidades OT	134
b. Evaluación de impacto operativo de la aplicación de parches	135
c. Ventanas de mantenimiento, pruebas y reversión segura	136
6. Casos prácticos de hardening en plantas en servicio	136
a. Implantación progresiva de medidas en entornos legacy	136
b. Coordinación con operación para minimizar el impacto	137
c. Resultados medibles y lecciones aprendidas por fases	138

PARTE QUINTA. 139

Monitorización, detección y respuesta a incidentes OT	139
--	------------

Capítulo 9: Monitorización continua y detección de amenazas en redes OT 139

1. Arquitecturas de monitorización de ciberseguridad OT	139
a. NDR, IDS/IPS industriales y otras tecnologías específicas	139
b. Integración con SIEM y soluciones de logging centralizado	140
c. Modelos de SOC OT y SOC híbridos IT/OT	141

2. Detección basada en firmas y en comportamiento	141
a. Reglas de detección específicas para protocolos OT	141
b. Baselines de comportamiento normal en planta	142
c. Alarmado, correlación de eventos y umbrales	143
3. Casos de uso de detección en infraestructuras críticas	144
a. Detección de accesos remotos no autorizados	144
b. Detección de movimientos laterales y escaneos internos	144
c. Detección de modificaciones no autorizadas en lógicas de PLC	145
4. Integración de la monitorización OT en el SOC corporativo	146
a. Flujos de comunicación entre operación, mantenimiento y SOC	146
b. Procedimientos de escalado y coordinación en incidentes OT	146
c. Priorización de alertas OT en el contexto corporativo	147
5. Pruebas de intrusión y ejercicios de red teaming en OT	148
a. Alcance y limitaciones de las pruebas en entornos críticos	148
b. Enfoques de testeo “safe by design” para no afectar a la operación	148
c. Tratamiento de hallazgos y planes de mejora asociados	149
6. Métricas de eficacia y mejora continua de la monitorización	149
a. Indicadores de detección temprana y tiempo de respuesta	149
b. Calidad de las reglas y reducción de falsos positivos	150
c. Revisión periódica de casos de uso y cobertura OT	151
Capítulo 10: Respuesta a incidentes OT, recuperación y continuidad operativa	152
1. Marco de gestión de incidentes adaptado a OT	152
a. Fases de gestión de incidentes aplicadas a entornos OT	152
b. Integración con procesos corporativos de respuesta a incidentes	153
c. Clasificación y priorización de incidentes OT	154
2. Roles y coordinación durante un incidente OT	155
a. Responsabilidades de operación, mantenimiento y ciberseguridad	155
b. Coordinación con dirección, comunicación y relaciones externas	156
c. Participación de proveedores y autoridades competentes	156
3. Contención, erradicación y recuperación en OT	157
a. Estrategias de contención que minimicen el impacto operativo	157
b. Procedimientos de erradicación en sistemas industriales	158
c. Recuperación segura: restauración, validación y arranque	159
4. Continuidad de negocio y recuperación ante desastres OT	159
a. Análisis de impacto en el negocio aplicado a OT	159
b. Estrategias de redundancia y tolerancia a fallos en infraestructuras críticas	160
c. Planes de contingencia para pérdida parcial o total de sistemas OT	161
5. Ejercicios, simulacros y entrenamiento en incidentes OT	161
a. Diseños de simulacros técnicos y de mesa (table-top)	161
b. Formación específica para personal de planta y SOC	162
c. Evaluación de los ejercicios y mejora de procedimientos	163
6. Lecciones aprendidas y mejora de controles tras incidentes	163
a. Metodología de análisis post-incidente (post-mortem)	163
b. Incorporación de lecciones aprendidas a políticas y diseños	164
c. Comunicación interna y externa de resultados y cambios	164



PARTE SEXTA.166

Cumplimiento, auditoría y certificación en ciberseguridad OT166

Capítulo 11: Cumplimiento normativo y contractual en infraestructuras críticas166

1. Marcos normativos y regulatorios aplicables a OT166

- a. Normativa de infraestructuras críticas y servicios esenciales 166
- b. Normativa de ciberseguridad y protección de datos relevante 167
- c. Estándares de referencia: ISA/IEC 62443, ISO/IEC 27001, otros 168

2. Requisitos para operadores de infraestructuras críticas168

- a. Obligaciones de seguridad y notificación de incidentes..... 168
- b. Requisitos de gobernanza y de gestión del riesgo OT 169
- c. Plazos, registros y evidencias exigibles por las autoridades 170

3. Contratos de suministro, EPC y mantenimiento con requisitos OT170

- a. Cláusulas mínimas de ciberseguridad OT en contratos..... 170
- b. Niveles de servicio (SLA) y métricas de seguridad a exigir 171
- c. Responsabilidades, penalizaciones y gestión de incumplimientos 172

4. Relación con sistemas de gestión y certificaciones173

- a. Articulación con ISO/IEC 27001 y otros sistemas de gestión 173
- b. Integración con sistemas de gestión de continuidad y calidad 173
- c. Sinergias y solapamientos entre compliance IT y OT..... 174

5. Evidencias de cumplimiento y trazabilidad175

- a. Documentación técnica y organizativa necesaria 175
- b. Registros de actividad, cambios, auditorías y formación 175
- c. Herramientas para consolidar evidencias y generar informes 176

6. Riesgos de incumplimiento y responsabilidad177

- a. Consecuencias legales, financieras y reputacionales 177
- b. Responsabilidades de la alta dirección y de los operadores 177
- c. Estrategias de reducción del riesgo de incumplimiento 178

Capítulo 12: Auditorías técnicas y de gestión de ciberseguridad OT179

1. Tipos de auditoría aplicables a ciberseguridad OT179

- a. Auditoría interna, auditoría externa y auditoría de certificación 179
- b. Auditorías técnicas, organizativas y mixtas 180
- c. Auditorías de proveedores críticos y de terceros 181

2. Planificación y alcance de auditorías en infraestructuras críticas182

- a. Definición de objetivos, alcance y criterios de éxito 182
- b. Selección de procesos, sistemas y emplazamientos a auditar 182
- c. Coordinación con operación y mantenimiento para minimizar impacto 183

3. Metodologías y herramientas de auditoría técnica OT184

- a. Revisión documental y entrevistas 184
- b. Pruebas técnicas, escaneos y verificaciones in situ 185
- c. Uso de herramientas específicas para redes y dispositivos OT 185

4. Evaluación de conformidad y detección de brechas.....186

- a. Criterios de conformidad frente a estándares y políticas internas 186
- b. Clasificación de hallazgos por criticidad y urgencia 187
- c. Priorización de acciones correctivas y preventivas 187

5. Informes de auditoría y planes de acción	188
a. Estructura de un informe de auditoría OT eficaz	188
b. Planes de acción, responsables y plazos	189
c. Seguimiento, cierre de hallazgos y verificación de eficacia	189
6. Integración de la auditoría OT en la mejora continua	190
a. Ciclo PDCA aplicado a ciberseguridad OT	190
b. Relación con revisiones de dirección y planes directores	191
c. Uso de resultados de auditoría para ajustar riesgos y controles.....	191
PARTE SÉPTIMA.	193
HERRAMIENTAS DE CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS. CHECKLISTS, FORMULARIOS Y PLANTILLAS PRÁCTICAS	193
Capítulo 13: Checklists de diagnóstico y madurez en ciberseguridad OT.....	193
CHECKLIST Nº 13.01 — Inventario y clasificación de activos OT	193
Sección 1. Identificación y alcance del expediente/proyecto	193
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	194
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	194
Sección 4. Riesgos, seguridad y cumplimiento normativo	195
Sección 5. Plazos, hitos y condicionantes.....	196
Sección 6. Costes, importes y garantías (si aplica)	196
Sección 7. Aprobaciones y firmas (RACI)	197
Sección 8. Evidencias y referencias	197
CHECKLIST Nº 13.02 — Madurez en gobierno y gestión de riesgos OT.....	199
Sección 1. Identificación y alcance del expediente/proyecto	199
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	199
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	200
Sección 4. Riesgos, seguridad y cumplimiento normativo	201
Sección 5. Plazos, hitos y condicionantes.....	201
Sección 6. Costes, importes y garantías (si aplica)	201
Sección 7. Aprobaciones y firmas (RACI)	202
Sección 8. Evidencias y referencias	202
CHECKLIST Nº 13.03 — Diseño de segmentación de redes OT	203
Sección 1. Identificación y alcance del expediente/proyecto	203
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	203
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	204
Sección 4. Riesgos, seguridad y cumplimiento normativo	204
Sección 5. Plazos, hitos y condicionantes.....	205
Sección 6. Costes, importes y garantías (si aplica)	205
Sección 7. Aprobaciones y firmas (RACI)	205
Sección 8. Evidencias y referencias	206
CHECKLIST Nº 13.04 — Hardening de PLC/RTU, SCADA y comunicaciones.....	206
Sección 1. Identificación y alcance del expediente/proyecto	206
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	207
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	207
Sección 4. Riesgos, seguridad y cumplimiento normativo	207
Sección 5. Plazos, hitos y condicionantes.....	208
Sección 6. Costes, importes y garantías (si aplica)	208
Sección 7. Aprobaciones y firmas (RACI)	209

Sección 8. Evidencias y referencias	209
CHECKLIST Nº 13.05 — Monitorización y detección de amenazas OT	209
Sección 1. Identificación y alcance del expediente/proyecto	210
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	210
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	210
Sección 4. Riesgos, seguridad y cumplimiento normativo	211
Sección 5. Plazos, hitos y condicionantes.....	211
Sección 6. Costes, importes y garantías (si aplica)	211
Sección 7. Aprobaciones y firmas (RACI)	212
Sección 8. Evidencias y referencias	212
CHECKLIST Nº 13.06 — Cumplimiento y auditoría de ciberseguridad OT	212
Sección 1. Identificación y alcance del expediente/proyecto	213
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	213
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	213
Sección 4. Riesgos, seguridad y cumplimiento normativo	214
Sección 5. Plazos, hitos y condicionantes.....	214
Sección 6. Costes, importes y garantías (si aplica)	215
Sección 7. Aprobaciones y firmas (RACI)	215
Sección 8. Evidencias y referencias	215
Capítulo 14: Formularios y plantillas para segmentación, hardening y respuesta a incidentes OT	216
FORMULARIO Nº 14.01 — Levantamiento de arquitecturas OT (redes, equipos y validación)...216	
Sección 1. Identificación y alcance del expediente/proyecto	216
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	217
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	217
Sección 4. Riesgos, seguridad y cumplimiento normativo	218
Sección 5. Plazos, hitos y condicionantes.....	218
Sección 6. Costes, importes y garantías (si aplica)	218
Sección 7. Aprobaciones y firmas (RACI)	219
Sección 8. Evidencias y referencias	219
FORMULARIO Nº 14.02 — Política de hardening OT y gestión de cambios de configuración.....219	
Sección 1. Identificación y alcance del expediente/proyecto	220
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	220
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	220
Sección 4. Riesgos, seguridad y cumplimiento normativo	221
Sección 5. Plazos, hitos y condicionantes.....	221
Sección 6. Costes, importes y garantías (si aplica)	221
Sección 7. Aprobaciones y firmas (RACI)	222
Sección 8. Evidencias y referencias	222
FORMULARIO Nº 14.03 — Análisis y registro de riesgos OT	222
Sección 1. Identificación y alcance del expediente/proyecto	223
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	223
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	223
Sección 4. Riesgos, seguridad y cumplimiento normativo	224
Sección 5. Plazos, hitos y condicionantes.....	224
Sección 6. Costes, importes y garantías (si aplica)	224
Sección 7. Aprobaciones y firmas (RACI)	225
Sección 8. Evidencias y referencias	225
FORMULARIO Nº 14.04 — Plan de respuesta a incidentes OT (fichas, listas de verificación y	

coordinación)	225
Sección 1. Identificación y alcance del expediente/proyecto	226
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	226
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	226
Sección 4. Riesgos, seguridad y cumplimiento normativo	227
Sección 5. Plazos, hitos y condicionantes.....	227
Sección 6. Costes, importes y garantías (si aplica)	227
Sección 7. Aprobaciones y firmas (RACI)	228
Sección 8. Evidencias y referencias	228
FORMULARIO Nº 14.05 — Reporte de incidentes OT a dirección, reguladores y clientes	229
Sección 1. Identificación y alcance del expediente/proyecto	229
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	229
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	230
Sección 4. Riesgos, seguridad y cumplimiento normativo	230
Sección 5. Plazos, hitos y condicionantes.....	230
Sección 6. Costes, importes y garantías (si aplica)	231
Sección 7. Aprobaciones y firmas (RACI)	231
Sección 8. Evidencias y referencias	231
FORMULARIO Nº 14.06 — Lecciones aprendidas y cierre de incidentes OT	232
Sección 1. Identificación y alcance del expediente/proyecto	232
Sección 2. Datos del activo/terreno/inmueble (y/o del contrato/licencia)	232
Sección 3. Requisitos y verificaciones técnicas/urbanísticas/financieras	233
Sección 4. Riesgos, seguridad y cumplimiento normativo	233
Sección 5. Plazos, hitos y condicionantes.....	233
Sección 6. Costes, importes y garantías (si aplica)	234
Sección 7. Aprobaciones y firmas (RACI)	234
Sección 8. Evidencias y referencias	234
PARTE OCTAVA.	235
PRÁCTICA DE CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS.....	235
Capítulo 15: Casos prácticos de Ciberseguridad OT en infraestructuras críticas.	235
Caso práctico 1. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Implantación básica de segmentación OT en una planta de tratamiento de agua	235
Causa del Problema	235
Soluciones Propuestas.....	237
1. Fase 0: diagnóstico detallado OT y análisis de riesgos específico	237
2. Diseño formal de arquitectura OT basada en zonas y conductos.....	237
3. Implantación técnica de la segmentación en la planta	238
4. Creación de una DMZ industrial y perímetro IT/OT controlado	239
5. Gestión segura y centralizada de accesos remotos de proveedores	239
6. Gobierno, procedimientos y formación específica para personal de planta	240
Consecuencias Previstas.....	241
Resultados de las Medidas Adoptadas.....	242
Lecciones Aprendidas	243
Caso práctico 2. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Implantación de hardening en PLC y estaciones de ingeniería tras un incidente de malware	245
Causa del Problema	245
Soluciones Propuestas.....	246
1. Definición de política corporativa de hardening OT y baselines de configuración segura	246

2. Hardening específico de PLC y RTU en la subestación	247
3. Hardening de estaciones de ingeniería y control de dispositivos USB.....	248
4. Gestión de credenciales y secretos en entorno OT	249
5. Estrategia de copias de seguridad, pruebas de restauración y plan de recuperación OT	249
Consecuencias Previstas.....	250
Resultados de las Medidas Adoptadas.....	251
Lecciones Aprendidas.....	253
Caso práctico 3. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Despliegue de monitorización OT y coordinación con el SOC corporativo.....	255
Causa del Problema	255
Soluciones Propuestas.....	256
1. Programa de visibilidad OT y cartografiado mediante monitorización pasiva	256
2. Arquitectura de monitorización OT con sondas NDR industriales y consolidación de logs.....	257
3. Definición de casos de uso de detección OT y correlación con el SOC	258
4. Organización y procedimientos de coordinación entre SOC y operación OT	258
5. Ejercicios de simulación y mejora continua de la monitorización OT.....	259
Consecuencias Previstas.....	260
Resultados de las Medidas Adoptadas.....	261
Lecciones Aprendidas.....	262
Caso práctico 4. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Diseño y despliegue de un plan de respuesta a incidentes OT en una planta petroquímica	265
Causa del Problema	265
Soluciones Propuestas.....	266
1. Definición de un marco de gestión de incidentes específico para OT	266
2. Creación de un equipo de respuesta a incidentes OT (OT-IRT) y definición de roles	267
3. Desarrollo de playbooks específicos para escenarios OT de alto impacto	268
4. Integración del plan de respuesta OT con continuidad de negocio y recuperación de desastres.....	269
5. Programa de formación, simulacros y ejercicios combinados OT–IT–safety.....	270
6. Ajuste contractual con proveedores OT y requisitos de notificación de incidentes.....	270
Consecuencias Previstas.....	271
Resultados de las Medidas Adoptadas.....	272
Lecciones Aprendidas.....	274
Caso práctico 5. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Programa de cumplimiento y auditoría OT en una red metropolitana de transporte ferroviario	276
Causa del Problema	276
Soluciones Propuestas.....	277
1. Marco de cumplimiento OT y alineamiento con estándares de referencia.....	277
2. Programa de “gap analysis” OT y plan director de mejora por líneas y centros.....	278
3. Auditorías técnicas OT periódicas y metodología homogénea.....	279
4. Sistema de indicadores de cumplimiento OT (KPI/KRI) y cuadro de mando ejecutivo.....	280
5. Integración del cumplimiento OT en contratos y procesos de compra	281
6. Programa de concienciación OT y alineamiento cultural.....	281
Consecuencias Previstas.....	282
Resultados de las Medidas Adoptadas.....	283
Lecciones Aprendidas.....	285
Caso práctico 6. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Rediseño integral de perímetros OT y DMZ industrial en un operador de transporte eléctrico	287
Causa del Problema	287
Soluciones Propuestas.....	288
1. Revisión detallada de la arquitectura actual y definición del modelo objetivo IT/OT/DMZ.....	288

2. Diseño e implantación de una DMZ industrial específica para OT.....	289
3. Introducción de diodos de datos y mecanismos unidireccionales para telemedida	290
4. Reordenación de accesos remotos y despliegue de un bastión OT con PAM	291
5. Refuerzo de la monitorización del perímetro OT y la DMZ industrial.....	292
6. Formalización de la gestión de cambios en el perímetro OT y DMZ industrial.....	293
Consecuencias Previstas.....	294
Resultados de las Medidas Adoptadas.....	295
Lecciones Aprendidas.....	296
Caso práctico 7. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Programa corporativo de inventario y hardening de activos OT en un operador del ciclo integral del agua.....	299
Causa del Problema	299
Soluciones Propuestas.....	300
1. Proyecto de inventario OT híbrido (pasivo, activo controlado y conocimiento de planta)	300
2. Clasificación de activos y matriz corporativa de criticidad OT	301
3. Política corporativa de hardening OT y baselines por familia tecnológica	302
4. Implantación del hardening por oleadas, priorizando activos críticos	303
5. Gestión centralizada de credenciales OT y eliminación de cuentas genéricas	304
6. Integración de inventario, criticidad y hardening en el ciclo de vida de proyectos OT	304
Consecuencias Previstas.....	305
Resultados de las Medidas Adoptadas.....	306
Lecciones Aprendidas.....	308
Caso práctico 8. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Protección de protocolos industriales y comunicaciones de campo en una red de oleoductos	310
Causa del Problema	310
Soluciones Propuestas.....	312
1. Segmentación lógica de redes de campo y clasificación de enlaces según criticidad	312
2. Securitización de protocolos industriales mediante túneles cifrados y pasarelas OT	313
3. Cifrado y autenticación en radioenlaces y redes celulares M2M	314
4. Gestión de vulnerabilidades y parches en equipos de comunicaciones y SCADA	315
5. Laboratorio de pruebas y banco de configuración de comunicaciones OT	315
6. Programa de formación y procedimientos para operación y mantenimiento sobre las nuevas medidas	316
Consecuencias Previstas.....	317
Resultados de las Medidas Adoptadas.....	318
Lecciones Aprendidas.....	320
Caso práctico 9. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Monitorización avanzada y detección de amenazas OT en un gran complejo hospitalario	322
Causa del Problema	322
Soluciones Propuestas.....	324
1. Diseño de una arquitectura de monitorización OT hospitalaria basada en NDR y logging centralizado.....	324
2. Definición de casos de uso de detección OT orientados a la seguridad de pacientes	325
3. Integración de la monitorización OT en el SOC corporativo y creación de un "SOC híbrido" IT/OT con foco sanitario	326
4. Securitización y monitorización de accesos remotos de proveedores OT	326
5. Programa de simulacros de incidentes OT centrados en impacto clínico	327
6. Mejora continua, métricas y extensión progresiva a hospitales asociados	328
Consecuencias Previstas.....	329
Lecciones Aprendidas.....	332
Caso práctico 10. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Gestión de un ataque de ransomware con impacto potencial en sistemas OT de un aeropuerto internacional	334

Causa del Problema	334
Soluciones Propuestas.....	336
1. Marco integrado de respuesta a incidentes IT/OT específico para aeropuerto	336
2. Arquitectura de recuperación OT: backups inmutables, imágenes “golden” y segmentación de dominios	337
3. Refuerzo de segmentación y controles de tráfico entre IT, OT y sistemas aeroportuarios críticos ..	338
4. Plan de continuidad operativa OT por escenarios: BHS, combustible e iluminación de pistas	339
5. Programa de simulacros de ciberincidentes OT con participación de compañías aéreas y autoridades	340
6. Refuerzo contractual y de soporte OT con proveedores aeroportuarios críticos.....	341
Consecuencias Previstas.....	342
Resultados de las Medidas Adoptadas.....	343
Lecciones Aprendidas.....	345

Caso práctico 11. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Implantación de un programa de cumplimiento y certificación OT en una central de ciclo combinado.....348

Causa del Problema	348
Soluciones Propuestas.....	349
1. Elaboración de un mapa integral de requisitos normativos y contractuales OT	349
2. Diseño de un Sistema de Gestión de Ciberseguridad OT (SGC-OT) integrado con el SGSI	350
3. Programa de auditorías técnicas y de gestión OT, orientadas a certificación	351
4. Gobierno de evidencias y sistema de trazabilidad OT	352
5. Programa de formación y concienciación en cumplimiento OT para personal de planta y corporativo	353
6. Hoja de ruta para la certificación y alineamiento con fabricantes OT	354
Consecuencias Previstas.....	355
Resultados de las Medidas Adoptadas.....	356
Lecciones Aprendidas.....	358

Caso práctico 12. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Programa corporativo de auditorías OT en un grupo energético multisede.....360

Causa del Problema	360
--------------------------	-----

Soluciones Propuestas362

1. Definición del marco corporativo de auditorías OT	362
2. Desarrollo de metodología y checklists homogéneos basados en riesgos.....	363
3. Ejecución de auditorías piloto integrales y ajuste del modelo	364
4. Implantación de una herramienta GRC para trazabilidad de hallazgos y planes de acción OT.....	365
5. Programa de capacitación y esquema de cualificación de auditores OT internos	366
6. Alineamiento con reguladores y aseguradoras sobre el nuevo programa de auditorías OT	367
Consecuencias Previstas.....	368
Resultados de las Medidas Adoptadas.....	369
Lecciones Aprendidas.....	370

Caso práctico 13. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Diseño e implantación de checklists de diagnóstico y madurez OT en una red metropolitana de transporte373

Causa del Problema	373
Soluciones Propuestas.....	375
1. Definición de un modelo de madurez OT específico para transporte metropolitano	375
2. Desarrollo de checklists de inventario y clasificación de activos OT por línea y centro	376
3. Checklists de diagnóstico rápido de controles técnicos y organizativos OT	377
4. Herramienta ligera para consolidación de resultados y evidencias.....	378
5. Programa de despliegue por fases y red de “facilitadores OT”	379
6. Integración con el plan director de ciberseguridad OT y la planificación de inversiones	380
Consecuencias Previstas.....	381
Resultados de las Medidas Adoptadas.....	382

Lecciones Aprendidas	383
Caso práctico 14. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Estandarización de formularios y plantillas OT para segmentación, hardening y respuesta a incidentes en un operador eléctrico regional	386
Causa del Problema	386
Soluciones Propuestas.....	388
1. Catálogo corporativo de formularios para levantamiento y revisión de arquitecturas OT	388
2. Plantillas de políticas de hardening y formularios de gestión de cambios OT	389
3. Formularios estructurados de análisis y registro de riesgos OT	390
4. Plantillas operativas para planes y fichas de respuesta a incidentes OT	391
5. Formularios de reporte ejecutivo a dirección, reguladores y clientes críticos	392
6. Integración de formularios y plantillas en herramientas corporativas y en el ciclo de vida OT	392
Consecuencias Previstas.....	393
Resultados de las Medidas Adoptadas.....	394
Lecciones Aprendidas	395
Caso práctico 15. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Gestión del riesgo de terceros y de la cadena de suministro OT en un complejo petroquímico.....	398
Causa del Problema	398
Soluciones Propuestas.....	400
1. Marco corporativo de gestión de riesgo de terceros OT	400
2. Centralización y securización de accesos remotos OT de terceros.....	401
3. Inventario de componentes de terceros, SBOM OT y gestión de vulnerabilidades asociadas	402
4. Revisión contractual y pliegos OT con requisitos explícitos de ciberseguridad de terceros.....	403
5. Programa de homologación y auditoría de proveedores OT críticos	404
6. Sensibilización interna y cambios en procesos de planta relativos a terceros	405
Consecuencias Previstas.....	406
Resultados de las Medidas Adoptadas.....	407
Lecciones Aprendidas	409
Caso práctico 16. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Implantación de un plan integral de respuesta a incidentes OT en una empresa de agua y saneamiento	412
Causa del Problema	412
Soluciones Propuestas.....	414
1. Diseño de un marco de gestión de incidentes específico para OT integrado con el proceso corporativo	414
2. Desarrollo de playbooks específicos por escenarios OT críticos	415
3. Refuerzo de capacidades técnicas de detección, análisis y recuperación OT	416
4. Simulacros y ejercicios de mesa OT-IT con foco en seguridad del agua y continuidad del servicio .	417
5. Integración del plan de respuesta OT con los planes de continuidad, calidad del agua y comunicación externa	418
6. Sistema de lecciones aprendidas y mejora continua tras incidentes y simulacros OT	419
Consecuencias Previstas.....	419
Resultados de las Medidas Adoptadas.....	421
Lecciones Aprendidas	422
Caso práctico 17. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Planificación segura de pruebas de intrusión y ejercicios de red teaming en una red de transporte de gas natural	425
Causa del Problema	425
Soluciones Propuestas.....	426
1. Definición de un marco de pruebas de seguridad OT "safe by design"	426
2. Creación de un laboratorio OT representativo y uso de gemelos digitales para pruebas ofensivas .	427
3. Diseño de una metodología de red teaming OT combinando ejercicios técnicos y de mesa	428

4. Integración de hallazgos de red teaming OT en el análisis de riesgos y el plan director	429
5. Participación de reguladores y aseguradoras en la definición y supervisión de ejercicios	430
6. Programa de formación y cambio cultural sobre pruebas de seguridad OT	431
Consecuencias Previstas	432
Resultados de las Medidas Adoptadas	433
Lecciones Aprendidas	434
Caso práctico 18. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Integración de la monitorización OT en el SOC corporativo de una red hospitalaria	437
Causa del Problema	437
Soluciones Propuestas	439
1. Diseño de una arquitectura de monitorización OT multisede específica para entornos hospitalarios	439
2. Integración de OT en el SOC corporativo mediante la creación de una célula OT	440
3. Definición de casos de uso de detección específicos para entornos OT hospitalarios	441
4. Gestión de logs y evidencias OT con criterios de privacidad y cumplimiento sanitario	442
5. Procedimientos de coordinación entre SOC OT, ingeniería y mantenimiento hospitalario	443
6. Despliegue gradual, indicadores de eficacia y extensión a la red	443
Consecuencias Previstas	444
Resultados de las Medidas Adoptadas	445
Lecciones Aprendidas	447
Caso práctico 19. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Gestión integral de vulnerabilidades y parches OT en una red de generación renovable distribuida	449
Causa del Problema	449
Soluciones Propuestas	451
1. Marco corporativo de gestión de vulnerabilidades OT específico para renovables	451
2. Inventario detallado de versiones de firmware y software OT y clasificación según criticidad y "parcheabilidad"	452
3. Laboratorio OT renovable para pruebas de parches y cambios de configuración	453
4. Estrategia de mitigación compensatoria para activos OT que no se pueden parchear	454
5. Coordinación estructurada con fabricantes e integradores OT y revisión de contratos	454
6. Automatización ligera del seguimiento, KPIs de vulnerabilidades OT y priorización de despliegues	455
Consecuencias Previstas	456
Resultados de las Medidas Adoptadas	457
Lecciones Aprendidas	459
Caso práctico 20. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Programa de cumplimiento OT y auditorías integradas en un operador de transporte eléctrico	462
Causa del Problema	462
Soluciones Propuestas	464
1. Mapa de requisitos de ciberseguridad OT y marco de controles unificado	464
2. Organización y roles de cumplimiento OT: comité, responsables y RACI	465
3. Sistema corporativo de gestión de evidencias OT y trazabilidad	466
4. Programa de auditorías internas OT por capas y guías de auditoría	467
5. Integración con certificaciones (ISO/IEC 27001 e ISA/IEC 62443) y alineamiento con el regulador	468
6. Sistema de seguimiento de hallazgos, planes de acción y métricas de cumplimiento OT	469
Consecuencias Previstas	470
Resultados de las Medidas Adoptadas	470
Lecciones Aprendidas	472
Caso práctico 21. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Implantación de checklists de diagnóstico y madurez OT en un grupo industrial multisectorial	475
Causa del Problema	475
Soluciones Propuestas	477

1. Definición de un modelo de madurez OT corporativo, sencillo y comparable	477
2. Desarrollo de checklists de inventario y clasificación de activos OT	478
3. Checklists de diagnóstico de madurez OT por dimensión	479
4. Checklists de diseño mínimo de segmentación y hardening OT	480
5. Integración de checklists en una herramienta ligera y cuadros de mando corporativos	481
6. Programa piloto, formación y vínculo con el plan director OT	482
Consecuencias Previstas	483
Resultados de las Medidas Adoptadas	483
Lecciones Aprendidas	485

Caso práctico 22. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Estandarización de formularios OT para gestión de cambios y análisis de riesgos en una red ferroviaria metropolitana

.....	488
Causa del Problema	488
Soluciones Propuestas	490
1. Diseño de un catálogo corporativo de formularios OT y su ciclo de vida	490
2. Rediseño del formulario de gestión de cambios OT (F-OT-GC-01) con integración de ciberseguridad	491
3. Plantilla unificada de análisis de riesgos OT (F-OT-AR-01) para proyectos y cambios mayores	492
4. Formulario de incidentes OT (F-OT-IN-01) adaptado a entornos ferroviarios	493
5. Digitalización de formularios OT y flujos de aprobación integrados	494
6. Programa de formación y acompañamiento en el uso de formularios OT	495
Consecuencias Previstas	496
Resultados de las Medidas Adoptadas	497
Lecciones Aprendidas	498

Caso práctico 23. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Estandarización de plantillas de respuesta a incidentes OT en un operador aeroportuario multinacional

.....	501
Causa del Problema	501
Soluciones Propuestas	503
1. Diseño de un conjunto de plantillas de incidentes OT por tipo de sistema crítico	503
2. Desarrollo de listas de verificación por fases de respuesta (detección, contención, recuperación) para sistemas OT críticos	504
3. Plantillas de coordinación OT–operaciones–SOC y activación de escalados	505
4. Formatos de reporte post-incidente a dirección y reguladores	506
5. Integración de las plantillas OT en el Proceso Corporativo de Gestión de Incidentes y en el SGSI	507
6. Programa de simulacros OT centrados en el uso de plantillas y lecciones aprendidas	508
Consecuencias Previstas	509
Resultados de las Medidas Adoptadas	509
Lecciones Aprendidas	511

Caso práctico 24. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Diseño de plantillas ejecutivas de reporte OT para dirección, reguladores y clientes en un operador de agua y saneamiento

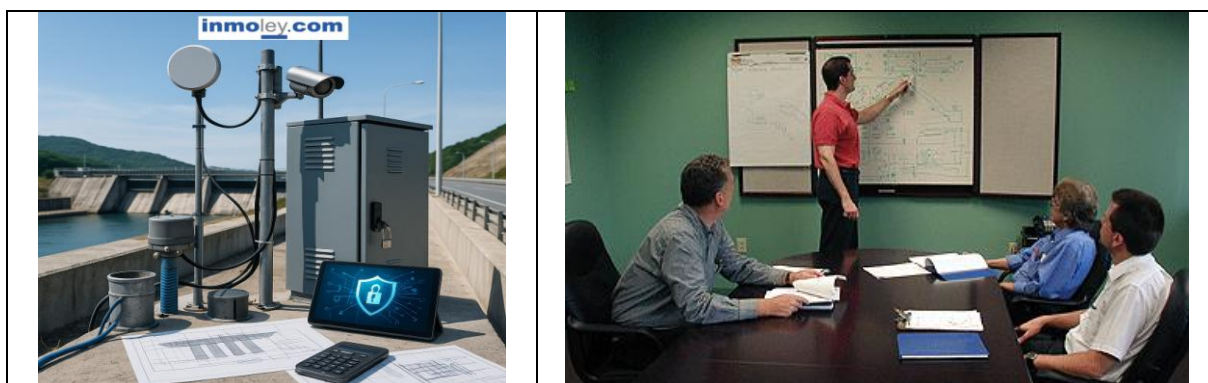
.....	513
Causa del Problema	513
Soluciones Propuestas	515
1. Definición de un modelo de información OT para dirección (plantilla ejecutiva estándar)	515
2. Diseño de plantillas específicas de reporte OT a reguladores (España y Latinoamérica)	516
3. Plantillas de comunicación técnica hacia grandes clientes y actores clave	517
4. Integración de métricas OT en cuadros de mando corporativos y plantillas periódicas	518
5. Flujo de trabajo y responsabilidades para la generación y aprobación de informes OT	519
6. Programa de formación y simulacros de reporte OT	519
Consecuencias Previstas	520
Resultados de las Medidas Adoptadas	521



Caso práctico 25. "CIBERSEGURIDAD OT EN INFRAESTRUCTURAS CRÍTICAS." Transformación integral de la ciberseguridad OT en un holding energético iberoamericano.....525

Causa del Problema	525
Soluciones Propuestas.....	527
1. Modelo de gobierno y arquitectura de referencia OT común para el holding	527
2. Programa de segmentación OT y DMZ industrial multicapa priorizado por criticidad	528
3. Hardening sistemático de PLC/RTU/IED y estaciones de ingeniería	529
4. SOC híbrido IT/OT con capacidades avanzadas para infraestructuras críticas	530
5. Gestión integrada de riesgos, cumplimiento y cadena de suministro OT	531
6. Capacidad de recuperación OT y pruebas de crisis ciber-físicas.....	532
7. Programa de cambio cultural, formación y KPIs OT.....	533
Consecuencias Previstas.....	534
Resultados de las Medidas Adoptadas.....	535
Lecciones Aprendidas	537

¿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.

