					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P35					Título del documento: **Política de seguridad de IoT/OT**							
Versión: 1.0		Fecha de entrada en vigor: 01.01.2025			Propietario del documento:							
X	Política		Norma		Procedimiento		Formulario		Registro		Otro	

Historial de revisiones				
Número de revisión	**Fecha de revisión**	**Cambios**	**Revisado por**	**Propietario del proceso**

Aprobaciones			
Nombre	**Cargo**	**Fecha**	**Firma**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	
ISO/IEC 27002:2022	Controles 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev. 5	SC-7, SI-4, CM-2, AC-6, PL-8	
RGPD de la UE	Artículos 5, 25, 32	
Directiva NIS2 de la UE	Artículos 21, 23	
DORA de la UE	Artículos 9, 10	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Propósito

1.1 Esta política establece los requisitos obligatorios de seguridad de la información para el despliegue, la operación, la supervisión y la retirada de sistemas de Internet de las Cosas (IoT) y de Tecnología Operativa (OT) dentro de la organización.

1.2 Garantiza que dichos sistemas se integren en el sistema global de gestión de la ciberseguridad de la organización y estén protegidos frente a incidentes de seguridad, uso indebido o sabotaje operativo.

1.3 Esta política tiene por objeto implantar controles técnicos, organizativos y procedimentales robustos para proteger los sistemas IoT/OT que interactúan con infraestructuras físicas, procesos de producción y entornos críticos para la seguridad.

1.4 Da soporte al cumplimiento de las obligaciones regulatorias y contractuales en materia de ciberseguridad, seguridad física, control ambiental y continuidad.

2. Alcance

2.1 Esta política se aplica a todos los sistemas IoT y OT, ya sean propiedad de la organización, arrendados o proporcionados por terceros, utilizados en los entornos operativos, administrativos o de producción.

2.2 Los sistemas incluidos comprenden, entre otros:

2.2.1 Dispositivos IoT como sensores ambientales, sistemas de control de acceso, iluminación inteligente, equipos de videovigilancia y dispositivos vestibles

2.2.2 Plataformas OT como PLC, SCADA, DCS, paneles HMI, interfaces MES y controladores de campo

2.2.3 Redes de control industrial o activos conectados a la nube que supervisan operaciones físicas

2.3 La política cubre:

2.3.1 Todos los entornos (local, edge y en la nube gestionada)

2.3.2 Todas las partes interesadas (usuarios internos, integradores, proveedores externos y contratistas)

2.3.3 Todas las fases del ciclo de vida (diseño, adquisición, despliegue, operación y retirada)

3. Objetivos

3.1 Proteger la infraestructura IoT y OT frente a amenazas internas y externas de ciberseguridad, incluidas la denegación de servicio, el acceso no autorizado, la propagación de ransomware y la manipulación del firmware.

3.2 Garantizar que las plataformas IoT/OT no se conviertan en vectores de ataque entre TI y OT ni comprometan sistemas críticos para la seguridad.

3.3 Aplicar los principios de seguridad desde el diseño y de defensa en profundidad a lo largo del ciclo de vida de estas tecnologías.

3.4 Permitir la integración fiable, segura y auditable de las plataformas IoT y OT en el Centro de Operaciones de Seguridad (SOC) de la organización y en los planes de respuesta a incidentes.

3.5 Garantizar que todos los despliegues estén alineados con los controles de ISO/IEC 27001 y con las guías sectoriales aplicables (p. ej., IEC 62443, ISO/IEC 27019, NIST SP 800-82).

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO) / Responsable de Seguridad de la Información

4.1.1 Define las políticas y los estándares técnicos de ciberseguridad para IoT/OT

4.1.2 Supervisa las evaluaciones de riesgos, la validación de controles y la coordinación interdepartamental

4.2 Ingenieros de OT / Responsables de instalaciones y planta

4.2.1 Validan las configuraciones de los sistemas OT y hacen cumplir esta política en las áreas de producción

4.2.2 Mantienen las salvaguardas físicas y lógicas necesarias para preservar la integridad y la seguridad de los entornos OT

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Requisitos de revisión y actualización

9.1 Esta política debe revisarse al menos una vez al año y actualizarse en función de:

9.1.1 Cambios en la arquitectura, los proveedores o las plataformas de sistemas OT o IoT

9.1.2 Actualizaciones regulatorias significativas (p. ej., revisiones de DORA, NIS2 o directivas sectoriales)

9.1.3 La aparición de nuevas vulnerabilidades o patrones de amenaza en sistemas de control

9.1.4 Hallazgos de auditorías internas o externas, pruebas de penetración o ejercicios de red team

9.2 El CISO, el Responsable de Seguridad de OT y los responsables de departamento pertinentes son responsables de iniciar conjuntamente el proceso de revisión.

9.3 Deben activarse revisiones intermedias tras:

9.3.1 Cualquier incidente relacionado con IoT/OT que dé lugar a un fallo del sistema o a pérdida de datos

9.3.2 La incorporación significativa de nuevos equipos, software de supervisión o plataformas de firmware

9.3.3 La integración de computación inteligente en el edge o de automatización mejorada con IA a nivel de campo

9.4 Todos los cambios en la política deben:

9.4.1 Documentarse en el historial de versiones y en el Registro de Cambios de Políticas

9.4.2 Comunicarse a todos los usuarios, proveedores y operadores de TI/OT afectados

9.4.3 Ser aprobados nuevamente por la Dirección Ejecutiva

10. Políticas relacionadas y vinculaciones

10.1 Esta política opera conjuntamente con las siguientes políticas de seguridad de la información y está respaldada por ellas:

10.1.1 P1 – Política de Seguridad de la Información: Establece los principios fundamentales de seguridad que se extienden a la protección de los sistemas IoT y OT.

10.1.2 P3 – Política de Uso Aceptable: Define restricciones sobre el uso personal y no autorizado de dispositivos, también en entornos operativos.

10.1.3 P6 – Política de Gestión de Riesgos: Orienta la evaluación, aceptación y mitigación de riesgos relacionados con sistemas embebidos y de control.

10.1.4 P12 – Política de Gestión de Activos: Garantiza que todos los sistemas IoT y OT estén formalmente inventariados y tengan propietarios responsables asignados.

10.1.5 P20 – Política de Protección de Endpoints / Malware: Se aplica a controladores conectados, pasarelas inteligentes y sistemas edge en producción.

10.1.6 P22 – Política de Registro y Supervisión: Se extiende a los procedimientos de captura y revisión de registros para entornos OT.

10.1.7 P30 – Política de Respuesta a Incidentes: Regula directamente cómo deben escalarse y gestionarse las brechas, anomalías o fallos del sistema en IoT/OT.

10.1.8 P33 – Política de Auditoría y Supervisión del Cumplimiento: Proporciona mecanismos de aseguramiento para validar el cumplimiento continuado de esta política.

11. Normas y marcos de referencia

11.1 Esta política está alineada con normas reconocidas internacionalmente y marcos regulatorios que garantizan la seguridad, la resiliencia y el cumplimiento de los sistemas de Internet de las Cosas (IoT) y de Tecnología Operativa (OT) en entornos industriales, de producción y corporativos.

11.2 ISO/IEC 27002:2022 – Controles 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Control 5.7 – Inteligencia de amenazas: Orienta la supervisión de entornos OT y la identificación de vulnerabilidades específicas de IoT.

11.2.2 Control 5.23 – Seguridad de la información para el uso de servicios en la nube: Se aplica cuando los dispositivos IoT interactúan con plataformas en la nube para telemetría, control o analítica.

11.2.3 Control 5.27 – Arquitectura segura de sistemas y principios de ingeniería: Rige los principios de seguridad desde el diseño para sistemas embebidos y redes de control.

11.2.4 Control 5.31 – Seguridad en los procesos de desarrollo y soporte: Exige la validación de software y firmware, controles de parcheado y requisitos a proveedores en despliegues OT.

11.2.5 Control 5.36 – Cumplimiento de requisitos legales y contractuales: Garantiza que los activos OT cumplan los mandatos de seguridad, medioambientales y regulatorios.

11.2.6 Estos controles establecen conjuntamente buenas prácticas para proteger los sistemas IoT/OT a lo largo de su ciclo de vida, incluido el diseño de la arquitectura, el despliegue seguro, el parcheado, la detección de anomalías y el cumplimiento de requisitos sectoriales.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-7 – Protección del perímetro: Garantiza que las redes OT estén segmentadas y protegidas frente a accesos no autorizados.

11.3.2 SI-4 – Supervisión del sistema: Requiere la implantación de mecanismos de supervisión continua y detección de anomalías en entornos ICS.

11.3.3 CM-2 – Configuración de referencia: Establece el control de configuraciones y el endurecimiento de dispositivos en plataformas IoT/OT.

11.3.4 AC-6 – Mínimo privilegio: Se aplica al acceso de usuarios y al servicio remoto prestado por proveedores sobre sistemas de control embebidos.

11.3.5 PL-8 – Arquitecturas de seguridad y privacidad: Rige la planificación de la integración segura de sistemas, especialmente en proyectos de modernización de OT.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 5 – Principios relativos al tratamiento de datos personales: Se aplica a plataformas IoT que tratan datos basados en sensores o datos conductuales vinculados a personas.

11.4.2 Artículo 25 – Protección de datos desde el diseño y por defecto: Exige salvaguardas de privacidad integradas en el diseño del producto IoT y en el firmware.

11.4.3 Artículo 32 – Seguridad del tratamiento: Exige cifrado, control de acceso y comunicaciones seguras para las transmisiones de datos de dispositivos inteligentes.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículos 21 y 23: Imponen obligaciones de seguridad a las entidades esenciales e importantes que utilizan sistemas OT. Estas incluyen la evaluación de riesgos, la notificación de incidentes y la validación de la cadena de suministro de proveedores IoT/OT y de la integridad del firmware.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 9 – Gestión del riesgo de las TIC: Requiere la integración segura de sistemas embebidos y tecnologías OT en el programa de gobierno del riesgo de las TIC.

11.6.2 Artículo 10 – Requisitos de seguridad de las TIC: Exige medidas de protección para plataformas OT interconectadas utilizadas en entornos financieros y de servicios críticos.

11.7 COBIT 2019

11.7.1 DSS05.01 – Protección frente a malware: Incluye la detección y respuesta ante amenazas específicas de ICS y campañas de malware dirigidas a IoT.

11.7.2 BAI09.01 – Establecer y mantener requisitos de seguridad: Se corresponde con el aprovisionamiento y la operación seguros de infraestructuras inteligentes o embebidas.

11.7.3 APO13.02 – Establecer y mantener un plan de seguridad de la información: Requiere la inclusión de los sistemas OT y sus vulnerabilidades en la estrategia de ciberseguridad de toda la organización.