					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P35S					Título del documento: **Política de seguridad de IoT/OT - PYME**							
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	Cláusulas 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controles 5.23, 5	
NIST SP 800-53 Rev. 5	SI-7, CM-7, AC-6, PE-20, SC-7	
RGPD de la UE	Artículo 32	
Directiva NIS2 de la UE	Artículo 21(2)(a), (d), (f)	
DORA de la UE	Artículo 9(2), 10(1)	

1. Propósito

1.1. Esta política establece los requisitos obligatorios para el uso y la gestión seguros de dispositivos de Internet de las Cosas (IoT) y de Tecnología Operativa (OT) dentro de la organización. Estos dispositivos pueden incluir sensores inteligentes, cámaras de seguridad, máquinas de producción, controladores de climatización o cualquier sistema industrial conectado a la red.

1.2. El propósito de esta política es:

1.2.1. Proteger las operaciones físicas y digitales frente a interrupciones o manipulaciones a través de dispositivos conectados insuficientemente protegidos

1.2.2. Exigir el despliegue, la supervisión y el mantenimiento seguros de los sistemas IoT y OT

1.2.3. Garantizar el cumplimiento de ISO/IEC 27001:2022, la Directiva NIS2 de la UE y los marcos regulatorios relacionados

1.2.4. Proporcionar controles prácticos y exigibles para pymes que operan en entornos de oficina, almacén o producción

2. Alcance

2.1. Esta política se aplica a todas las personas que participen en la planificación, instalación, configuración, uso, soporte o retirada de dispositivos IoT u OT. Esto incluye:

2.1.1. Empleados, contratistas o becarios con acceso físico o remoto a los dispositivos

2.1.2. Proveedores externos o técnicos de servicio que instalen o mantengan sistemas conectados

2.1.3. Directores generales o personal responsable de supervisar las políticas de seguridad

2.2. La política cubre:

2.2.1. Dispositivos IoT como cerraduras inteligentes, sistemas de videovigilancia, contadores inteligentes o impresoras

2.2.2. Sistemas OT, incluidos los controladores lógicos programables (PLC), paneles SCADA o pasarelas industriales

2.2.3. El hardware de soporte, las aplicaciones de gestión y las redes de comunicaciones utilizadas por estos sistemas

2.3. Esta política se aplica en todas las ubicaciones de trabajo: entornos de oficina, emplazamientos remotos, áreas de producción y plataformas en la nube que interactúen con estos dispositivos.

3. Objetivos

3.1. Despliegue seguro: garantizar que todos los sistemas IoT/OT estén configurados de forma segura antes de su incorporación al entorno operativo.

3.2. Limitar la exposición: impedir el acceso no autorizado, el uso indebido o la toma de control de dispositivos conectados mediante la aplicación de controles de acceso robustos y segmentación de red.

3.3. Supervisión continua: mantener visibilidad sobre las operaciones de IoT/OT mediante el registro de actividad y la supervisión de comportamientos inusuales.

3.4. Responsabilidad de proveedores: garantizar que los proveedores externos apliquen prácticas seguras de instalación, configuración y mantenimiento.

3.5. Cumplimiento normativo: demostrar la plena alineación con las normas aplicables, como ISO 27001, el RGPD de la UE (si se recopilan datos personales) y NIS2 para la resiliencia de infraestructuras críticas.

4. Funciones y responsabilidades

4.1. Director General (DG)

4.1.1. Asume la responsabilidad global sobre la seguridad de los sistemas IoT y OT

4.1.2. Aprueba esta política y garantiza su aplicación en todas las áreas de trabajo

4.1.3. Verifica que los proveedores y contratistas apliquen prácticas seguras de instalación y mantenimiento

4.1.4. Autoriza el acceso a la red de cualquier sistema IoT/OT

4.2. Empleado designado o Responsable de Operaciones (si se asigna)

4.2.1. Supervisa el inventario, la ubicación y la configuración de los dispositivos IoT/OT

4.2.2. Registra la ubicación de cada dispositivo, su asignación de red y su documentación de soporte

4.2.3. Garantiza que cualquier cambio (por ejemplo, actualizaciones de firmware o sustituciones de dispositivos) quede documentado

[... 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. Revisión anual

9.1.1. Esta política debe revisarse al menos una vez al año por el DG

9.1.2. La revisión debe evaluar si la política sigue siendo eficaz, si cubre los tipos actuales de dispositivos y si se alinea con nuevos riesgos o tecnologías

9.2. Actualizaciones por eventos desencadenantes

9.2.1. Las actualizaciones de la política también deben iniciarse cuando:

9.2.2. Se introduzcan nuevos tipos de sistemas IoT u OT

9.2.3. Los proveedores emitan boletines de seguridad o avisos de fin de vida útil

9.2.4. Un incidente o una auditoría identifique deficiencias en los controles de IoT/OT

9.2.5. Nuevas leyes o normas impongan requisitos adicionales

9.3. Documentación y control de versiones

9.3.1. Todas las actualizaciones deben documentarse, incluida la fecha, el número de versión y el resumen de cambios

9.3.2. El DG debe conservar las versiones históricas de la política con fines de auditoría

9.4. Comunicación de cambios

9.4.1. Toda actualización de la política debe comunicarse a todo el personal y proveedores pertinentes

9.4.2. Las versiones actualizadas deben estar accesibles a través de unidades compartidas o materiales impresos en los lugares de instalación o centros de control

10. Políticas relacionadas y vinculaciones

10.1. Esta política debe implantarse en alineación con las siguientes políticas relacionadas de la pyme:

10.1.1. P4S – Política de Control de Acceso: aplica controles de inicio de sesión a nivel de dispositivo, uso de contraseñas robustas y procedimientos de acceso autorizado para plataformas IoT y OT

10.1.2. P9S – Política de Trabajo Remoto: impide el uso de acceso remoto a paneles de IoT/OT a través de canales inseguros o no aprobados

10.1.3. P17S – Política de Protección de Datos y Privacidad: aplica si los dispositivos IoT (por ejemplo, cámaras de seguridad) tratan o graban datos personales, garantizando el cumplimiento del RGPD de la UE

10.1.4. P30S – Política de Respuesta a Incidentes: define los procedimientos para detectar, notificar y resolver incidentes de IoT u OT, incluida la sospecha de manipulación o fallo operativo

10.1.5. P36S – Política de Redes Sociales y Comunicaciones Externas: garantiza que no se comparta externamente información de dispositivos o del diseño de red salvo aprobación previa

10.2. Cada política relacionada refuerza la aplicación y el uso práctico de esta política al proporcionar orientación procedimental específica.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001

11.1.1. Cláusula 6.1 – Identificación de riesgos y tratamiento de riesgos: requiere que los riesgos relacionados con los sistemas IoT y OT se evalúen y mitiguen de forma sistemática

11.1.2. Cláusula 8.1 – Planificación y control operacional: garantiza el control operacional seguro sobre los dispositivos conectados

11.2. ISO/IEC 27002

11.2.1. Control 5.23 – Seguridad de la información para el uso de Tecnología Operativa (OT): define el uso seguro de la OT en entornos físicos y digitales

11.2.2. Control 5.31 – Configuración segura de los sistemas de información: requiere configuraciones seguras para dispositivos IoT/OT y evitar valores predeterminados inseguros

11.3. NIST SP 800-53 Rev. 5

11.3.1. SI-7 – Integridad del software, firmware e información: requiere la validación de la integridad del firmware y de las actualizaciones

11.3.2. CM-7 – Funcionalidad mínima: los dispositivos no deben tener habilitadas funciones no utilizadas o inseguras

11.3.3. AC-6 – Mínimo privilegio: el acceso a los dispositivos debe limitarse únicamente a usuarios autorizados

11.3.4. PE-20 – Supervisión de activos: supervisión física y operativa de los activos IoT y OT

11.3.5. SC-7 – Protección del perímetro: segmentación y control de las comunicaciones de red para sistemas conectados

11.4. RGPD de la UE (2016/679)

11.4.1. Artículo 32 – Seguridad del tratamiento: si se capturan datos personales (por ejemplo, mediante cámaras de videovigilancia), la organización debe implantar medidas técnicas y organizativas apropiadas para proteger dicho tratamiento

11.5. Directiva NIS2 de la UE (2022/2555)

11.5.1. Artículo 21(2)(a) – Medidas de gestión de riesgos

11.5.2. Artículo 21(2)(d) – Configuración y uso seguros de dispositivos

11.5.3. Artículo 21(2)(f) – Seguridad de la cadena de suministro y de los sistemas

11.6. DORA de la UE (2022/2554)

11.6.1. Artículo 9(2) – Alcance de la gestión del riesgo de las TIC: incluye dispositivos industriales y embebidos utilizados en entornos operativos

11.6.2. Artículo 10(1) – Continuidad de las TIC: requiere que las configuraciones de los dispositivos respalden la resiliencia y las operaciones de recuperación

11.7. COBIT 2019

11.7.1. DSS01 – Gestionar las operaciones: aplica a la supervisión de las operaciones tecnológicas, incluidos los dispositivos físicos

11.7.2. DSS05 – Gestionar los servicios de seguridad: garantiza que los sistemas conectados se supervisen y protejan adecuadamente

11.7.3. APO13 – Gestionar la seguridad: refuerza las políticas para proteger los activos operativos en pymes