					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P12S					Título del documento: **Política de Gestión de Activos**							
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 cuando corresponda

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	Requisitos de gestión de activos
ISO/IEC 27002:2022	Control 5	Controles de gestión de activos
NIST SP 800-53 Rev.5	CM-8	Inventario de componentes del sistema
Directiva NIS2 de la UE	Artículo 21(2)(a)	Seguimiento de activos para la protección de redes y sistemas de información
DORA de la UE	Artículo 5(8)	Requisitos de inventario de activos de TIC
COBIT 2019	BAI	Ciclo de vida de la gestión de activos de TI
RGPD de la UE	Artículo 30	Inventario de actividades de tratamiento de datos

1. Propósito

1.1 Esta política establece cómo la organización identifica, registra, protege y retira sus activos de información, incluidos tanto los componentes físicos como los digitales.

1.2 El objetivo es reducir los riesgos operativos y de seguridad mediante el mantenimiento de la visibilidad, la asignación clara de responsabilidades y la gestión segura de todos los activos de la organización a lo largo de su ciclo de vida.

1.3 Un inventario de activos fiable respalda el cumplimiento normativo, la respuesta a incidentes, la planificación de la continuidad y la gestión de riesgos.

1.4 Esta política también respalda la certificación conforme a ISO/IEC 27001 y demuestra la alineación con obligaciones legales, financieras y de ciberseguridad en marcos como el RGPD de la UE, la Directiva NIS2 de la UE y DORA de la UE.

1.5 Para las pymes, un enfoque de gestión de activos sencillo pero sistemático es esencial para evitar dispositivos no gestionados, la pérdida de datos o hallazgos de auditoría, especialmente cuando se opera con recursos técnicos limitados.

2. Alcance

2.1 Esta política se aplica a todos los activos que sean propiedad de la organización, estén arrendados o sean gestionados de cualquier otra forma por esta, incluidos los utilizados en:

2.1.1 Trabajo en oficina

2.1.2 Modalidades remotas o híbridas

2.1.3 Operaciones sobre el terreno o móviles

2.1.4 Entornos en la nube y externalizados

2.2 Los tipos de activos cubiertos incluyen, entre otros:

2.2.1 Hardware: portátiles, equipos de sobremesa, monitores, teléfonos, tabletas, unidades USB, routers, impresoras, soportes de copia de seguridad

2.2.2 Software: aplicaciones instaladas, herramientas SaaS, sistemas operativos, herramientas antivirus, licencias

2.2.3 Activos de datos: repositorios de datos de la organización, hojas de cálculo, registros de clientes, código fuente

2.2.4 Credenciales y servicios digitales: nombres de dominio, certificados digitales, claves API, cuentas de correo electrónico, accesos a servicios en la nube

2.2.5 Dispositivos de acceso: llaves, tarjetas inteligentes, dispositivos de proximidad, tokens biométricos

2.3 Todos los empleados, contratistas y proveedores externos que manejen activos de la organización están dentro del alcance de esta política.

2.4 La política también regula tanto los activos a corto plazo (por ejemplo, portátiles específicos para proyectos) como los activos a largo plazo, así como los activos compartidos utilizados por varios miembros del personal.

3. Objetivos

3.1 Establecer y mantener un inventario completo y exacto de todos los activos relevantes, actualizado de forma continua.

3.2 Garantizar que cada activo tenga un propietario designado responsable de su uso, almacenamiento y devolución.

3.3 Clasificar los activos en función de su sensibilidad, impacto para la organización o relevancia regulatoria, permitiendo niveles de protección diferenciados.

3.4 Definir procedimientos claros para la entrega, reasignación, mantenimiento, notificación de pérdidas y retirada de activos.

3.5 Garantizar que los activos se gestionen de forma segura durante todo su ciclo de vida y que la información que almacenen esté protegida o se elimine de forma segura en el momento de su disposición final.

3.6 Reducir la probabilidad de incidentes de seguridad causados por recursos de la organización no registrados, no devueltos o utilizados de forma indebida.

3.7 Respaldar el cumplimiento de la legislación aplicable (por ejemplo, el principio de responsabilidad proactiva del RGPD de la UE) y de los estándares de certificación en ciberseguridad.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Es responsable de esta política y de garantizar que las prácticas de gestión de activos se implanten y cumplan en toda la organización.

4.1.2 Revisa y aprueba las actualizaciones del inventario de activos y autoriza la retirada o transferencia de activos cuando sea necesario.

4.1.3 Debe ser informado de cualquier pérdida, robo o uso indebido significativo de activos.

4.2 Responsable de TI o custodio de activos designado

4.2.1 Mantiene el inventario de activos (por ejemplo, en una hoja de cálculo, un sistema de tickets o una herramienta ligera de seguimiento de activos).

4.2.2 Asigna la titularidad de los activos y registra los cambios de estado (por ejemplo, nuevo, en uso, en reparación, retirado).

4.2.3 Verifica que todos los activos entregados estén documentados y vinculados a una persona o unidad de negocio.

4.2.4 Garantiza que las etiquetas de clasificación se apliquen y se respeten (por ejemplo, Interno, Confidencial).

4.2.5 Coordina la recuperación, sanitización y desactivación de activos durante la baja o la retirada.

4.2.6 Informa al DG de cualquier discrepancia de activos no resuelta.

[... 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 siempre que:

9.1.1 Se introduzcan nuevos tipos de tecnología o activos

9.1.2 Cambien los procedimientos de seguimiento de activos (por ejemplo, adopción de nuevas herramientas o plataformas)

9.1.3 Nuevas obligaciones regulatorias afecten a la trazabilidad o eliminación de activos

9.1.4 Un incidente o una auditoría identifiquen una deficiencia en las prácticas actuales de gestión de activos

9.2 Las revisiones deben contar con la participación del DG y del Responsable de TI e incluir actualizaciones de los procedimientos de gestión de activos, las plantillas de inventario y las directrices de clasificación.

9.3 Todas las actualizaciones deben documentarse y comunicarse al personal afectado. Debe conservarse un registro de cambios sujeto a control de versiones.

10. Políticas relacionadas y vinculaciones

10.1 P2S – Política de funciones y responsabilidades de gobernanza: asigna la responsabilidad proactiva sobre la titularidad de las políticas y las operaciones de TI.

10.2 P4S – Política de control de acceso: vincula el uso de activos (por ejemplo, portátiles, dispositivos móviles) con los derechos de acceso de los usuarios y la gestión de identidades.

10.3 P7S – Política de incorporación y cese: garantiza que la entrega y recuperación de activos se integren en los procesos del ciclo de vida del personal.

10.4 P13S – Política de clasificación y etiquetado de datos: establece las reglas para determinar si un activo debe clasificarse como Interno o Confidencial.

10.5 P30S – Política de respuesta a incidentes: orienta los procedimientos de respuesta si un evento relacionado con activos da lugar a una brecha de seguridad o privacidad.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1: exige controles operativos para gestionar los activos y protegerlos durante su uso.

11.2 ISO/IEC 27002

11.2.1 Control 5.9: detalla cómo identificar, asignar titularidad, clasificar y gestionar activos de forma segura.

11.3 NIST SP 800-53 Rev

11.3.1 CM-8: exige que las organizaciones elaboren y mantengan un inventario de componentes del sistema, incluidos hardware, software y activos virtuales.

11.4 RGPD de la UE

11.4.1 Artículo 30: exige documentar las actividades de tratamiento de datos, lo que depende de conocer dónde se almacenan los datos y en qué activos.

11.5 Directiva NIS de la UE

11.5.1 Artículo 21(2)(a): exige medidas técnicas y organizativas, incluido el seguimiento de activos, para proteger las redes y los sistemas de información.

11.6 DORA de la UE

11.6.1 Artículo 5(8): las entidades financieras deben mantener inventarios detallados de activos de TIC como parte de la gestión del riesgo de las TIC.

11.7 COBIT 2019

11.7.1 BAI09: especifica que los activos de TI deben gestionarse a lo largo de su ciclo de vida, desde su adquisición hasta su retirada, con titularidad y controles claros.