					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P12					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**

1. Propósito

1.1 Esta política establece los requisitos organizativos obligatorios para identificar, clasificar, gestionar y proteger los activos de información a lo largo de su ciclo de vida. Da soporte a la gobernanza corporativa de los activos de hardware, software, datos, servicios en la nube e información intangible, incluidos los entornos móviles, remotos y gestionados por terceros.

1.2 El propósito de esta política es garantizar la visibilidad completa del entorno de activos de información de la organización, permitiendo la aplicación eficaz de controles de seguridad, la asignación de responsables, la alineación con los requisitos de cumplimiento y la retirada o eliminación responsable de los activos.

1.3 Esta política se alinea con el control A.5.9 del Anexo A de ISO/IEC 27001:2022 al exigir el mantenimiento de un inventario centralizado de la información y de otros activos asociados. Asimismo, garantiza la rendición de cuentas proactiva al vincular cada activo con un propietario y aplicar medidas de protección basadas en su clasificación, según su sensibilidad para la organización y los requisitos regulatorios aplicables.

2. Alcance

2.1 Esta política es de aplicación a todos los empleados, contratistas, terceros y proveedores de servicios que gestionen, utilicen, accedan, almacenen o traten activos de información propiedad de la organización o bajo su control.

2.2 El alcance incluye todas las categorías de activos, entre otras:

2.2.1 Activos físicos: portátiles, equipos de sobremesa, dispositivos móviles, soportes extraíbles, impresoras y equipos de red

2.2.2 Activos digitales: software, aplicaciones, imágenes de sistema, bases de datos, copias de seguridad y claves de cifrado

2.2.3 Activos de información: datos estructurados y no estructurados, informes, correos electrónicos y propiedad intelectual

2.2.4 Activos en la nube y virtuales: entornos IaaS, SaaS y PaaS, máquinas virtuales y contenedores

2.2.5 Activos lógicos: nombres de dominio, licencias, cuentas de usuario y configuraciones base

2.3 Esta política también regula los activos utilizados en entornos de trabajo remoto, híbrido o externalizado, garantizando su protección y visibilidad incluso cuando no estén ubicados físicamente en las instalaciones de la organización.

3. Objetivos

3.1 Mantener un inventario completo, exacto y actualizado de todos los activos de información de la organización, con atributos definidos de propiedad, clasificación y ubicación.

3.2 Asignar propietarios de activos responsables de la clasificación, el tratamiento y la protección de los activos bajo su control, de conformidad con las políticas de gobernanza de datos y seguridad.

3.3 Aplicar una clasificación y un etiquetado adecuados a todos los activos en función de su sensibilidad, criticidad y requisitos regulatorios.

3.4 Proteger los activos de acuerdo con su clasificación y la exposición al riesgo asociada, incluidos su almacenamiento, acceso, transmisión y eliminación.

3.5 Exigir procedimientos de devolución de activos y eliminación segura durante la baja de empleados, la finalización de contratos o el fin del ciclo de vida del activo.

3.6 Apoyar el cumplimiento de marcos como ISO/IEC 27001, el RGPD, la Directiva NIS2, DORA y COBIT 2019 mediante una gestión estructurada de activos y trazabilidad a efectos de auditoría.

4. Funciones y responsabilidades

4.1 Alta dirección

4.1.1 Aprueba la Política de Gestión de Activos y garantiza la asignación de recursos para su plena implantación.

4.1.2 Asume la responsabilidad última de asegurar que los activos de la organización estén protegidos y gestionados de conformidad con las obligaciones regulatorias y contractuales.

4.2 Director de Seguridad de la Información (CISO)

4.2.1 Es el responsable de la Política de Gestión de Activos y garantiza su integración con el Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización.

4.2.2 Revisa las excepciones y desviaciones de esta política y exige estrategias de mitigación basadas en el riesgo.

4.2.3 Supervisa las auditorías periódicas de la clasificación de activos, la integridad del inventario y el cumplimiento del ciclo de vida de los activos.

[... 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, o en respuesta a:

9.1.1 Cambios en obligaciones legales o regulatorias que afecten a la clasificación de activos o a los requisitos de inventario

9.1.2 La incorporación de nuevas categorías de activos o plataformas de gestión (por ejemplo, CMDB nativas de la nube)

9.1.3 Hallazgos de auditoría interna o incidentes de seguridad relacionados con una gestión inadecuada de activos

9.1.4 Reestructuraciones organizativas que afecten a la propiedad o a los controles del ciclo de vida

9.2 El proceso de revisión será iniciado por el Responsable de Activos de TI y coordinado con el Director de Seguridad de la Información, Compras, Asesoría Jurídica y los responsables de departamento afectados.

9.3 Las revisiones extraordinarias también podrán activarse por:

9.3.1 Adquisición o desinversión de unidades de negocio

9.3.2 Cambios de proveedor que afecten a activos gestionados por terceros

9.3.3 Renovaciones tecnológicas que impliquen retirada o aprovisionamiento masivo

9.4 Todas las revisiones de esta política deben:

9.4.1 Estar sujetas a control de versiones y almacenarse en el repositorio del SGSI

9.4.2 Ser aprobadas por la alta dirección

9.4.3 Incluir un resumen de los cambios y su justificación

9.4.4 Comunicarse a todas las partes interesadas afectadas, incluidos los procedimientos actualizados o la formación sobre sistemas, cuando resulte aplicable

10. Políticas relacionadas y vinculaciones

10.1 Esta política opera conjuntamente con las siguientes políticas relacionadas y da soporte a su aplicación:

10.1.1 P4 - Política de Control de Acceso: garantiza que la visibilidad de los activos esté alineada con los derechos de acceso y los mecanismos de control en los sistemas y entornos de datos.

10.1.2 P7 - Política de Incorporación y Cese: regula el aprovisionamiento oportuno y la devolución de activos físicos y lógicos durante las transiciones del personal.

10.1.3 P13 - Política de Clasificación y Etiquetado de Datos: establece reglas obligatorias de clasificación para los activos, que determinan los procedimientos de etiquetado, tratamiento y eliminación.

10.1.4 P14 - Política de Conservación y Eliminación de Datos: define los plazos y métodos de eliminación segura para los activos físicos y digitales que contienen información.

10.1.5 P22 - Política de Registro de Eventos y Monitorización: permite la trazabilidad del acceso y uso de los activos mediante el registro de eventos del sistema, la visibilidad de endpoints y la analítica de comportamiento.

10.1.6 P30 - Política de Respuesta a Incidentes: da soporte a la contención e investigación rápidas de brechas de seguridad relacionadas con activos, como portátiles perdidos o soportes de almacenamiento sin trazabilidad.

10.2 Estas políticas conforman una estructura de gobernanza coherente que garantiza que los activos se gestionen de forma segura, se inventaríen con exactitud y se traten adecuadamente a lo largo de su ciclo de vida.

11. Normas y marcos de referencia

11.1 Esta política está alineada con normas internacionales reconocidas de seguridad de la información y marcos regulatorios que exigen una gestión robusta de los activos a lo largo de todo su ciclo de vida.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 8.1: exige que las organizaciones planifiquen, implanten y controlen los procesos necesarios para cumplir los requisitos de seguridad de la información, incluidos los relativos a la gestión del ciclo de vida de los activos.

11.3 ISO/IEC 27002:2022 - controles 5.9 a 5.11

11.3.1 Control 5.9 - Inventario de la información y otros activos asociados: exige un inventario actualizado y completo de todos los activos relevantes para el tratamiento de la información.

11.3.2 Control 5.10 - Uso aceptable de la información y otros activos asociados: se apoya en reglas de uso, propiedad y procesos de devolución.

11.3.3 Control 5.11 - Devolución de activos: se implanta mediante procedimientos formales de entrega y retirada.

11.3.4 Estos controles establecen requisitos estructurados para identificar, etiquetar, mantener y realizar el seguimiento de los activos de la organización, con responsabilidades correspondientes para propietarios y custodios a lo largo del ciclo de vida.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 CM-8 - Inventario de componentes del sistema: reflejado mediante gestión centralizada de activos, visibilidad en tiempo real y vinculación con configuraciones operativas.

11.4.2 RA-3 - Evaluación de riesgos: los inventarios de activos sirven como elementos fundacionales para el modelado de amenazas y la evaluación de riesgos.

11.4.3 MP-6 - Saneamiento de soportes: aplicado mediante métodos de eliminación segura definidos en los controles del ciclo de vida de los activos y en la Política de Eliminación de Datos.

11.5 RGPD de la UE (2016/679):

11.5.1 Artículo 30 - Registros de actividades de tratamiento: exige que las organizaciones documenten los sistemas, dispositivos y repositorios que almacenan o tratan datos personales.

11.5.2 Artículo 32 - Seguridad del tratamiento: se alinea con la evaluación de riesgos basada en activos y las salvaguardas adaptadas a activos clasificados e infraestructuras críticas.

11.6 Directiva NIS2 de la UE (2022/2555):

11.6.1 Artículo 21(2)(a, b): exige visibilidad e inventario de activos como base para el análisis de riesgos, la protección y la respuesta a incidentes de ciberseguridad.

11.6.2 Artículo 21(3): refuerza la necesidad de una gobernanza estructurada de los activos como parte de la cultura de seguridad de la organización.

11.7 DORA de la UE (2022/2554):

11.7.1 Artículo 5 - Gobernanza de las TIC y control interno: exige que las entidades financieras controlen los activos TIC con requisitos claros de inventario, propiedad y protección.

11.7.2 Artículo 9 - Marco de gestión del riesgo de las TIC: establece que los procesos de gestión de activos deben respaldar la mitigación de amenazas, la planificación de la continuidad y la resiliencia del servicio.

11.8 COBIT 2019:

11.8.1 BAI09 - Gestionar activos: alineado directamente con la identificación, clasificación, uso y eliminación estructurados de los activos de la organización.

11.8.2 DSS01 - Operaciones gestionadas: apoya la implantación de controles que garanticen la protección de activos y una gobernanza operativa continua.

11.8.3 MEA03 - Supervisar, evaluar y valorar el cumplimiento: garantiza la auditoría periódica de los controles de gestión de activos y de su eficacia para la alineación regulatoria.