					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P14S					Título del documento: **Política de conservación y eliminación de datos**							
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 6.1.3, 8	Cubre el tratamiento de riesgos, los controles operativos y los requisitos de conservación
ISO/IEC 27002:2022	Control 5	Proporciona orientación sobre períodos de conservación y métodos de destrucción segura
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12	Conservación de registros de auditoría, sanitización de soportes y límites y aplicación de la conservación de datos
Directiva NIS2 de la UE	Artículo 21(2)(a)	Exige una política de gestión del ciclo de vida adecuada al riesgo
DORA de la UE	Artículo 5(1)	Gestión del riesgo de las TIC: disponibilidad y eliminación de datos
COBIT 2019	BAI03.04, DSS01	Controles del ciclo de vida de la información y eliminación segura
RGPD de la UE	Artículo 5(1)(e), 17	Los datos no deben conservarse más tiempo del necesario; derecho de supresión

1. Propósito

1.1 El propósito de esta política es establecer reglas exigibles para la conservación y la eliminación segura de la información en un entorno de pyme. Garantiza que los registros se conserven únicamente durante el tiempo exigido por la ley, por una obligación contractual o por una necesidad organizativa, y que posteriormente se destruyan de forma segura.

1.2 Esta política tiene por objeto reducir el riesgo asociado a la información, gestionar la exposición legal y limitar el almacenamiento de datos redundantes u obsoletos. Contribuye a garantizar el cumplimiento de ISO/IEC 27001 y de marcos de privacidad como el RGPD de la UE, minimizando la conservación no autorizada de información personal o sensible.

1.3 Un marco de conservación y eliminación bien estructurado reduce los costes operativos, mejora el rendimiento de los sistemas y refuerza la preparación para auditorías. Para las pymes con capacidad de TI limitada, proporciona una forma práctica de gestionar de manera responsable los activos de información digitales y físicos.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los registros, archivos, registros de eventos, comunicaciones y conjuntos de datos creados, recopilados, tratados o almacenados por la organización

2.1.2 Todos los empleados, contratistas y terceros que gestionen datos de la organización

2.1.3 Todos los formatos de datos (p. ej., papel, electrónico, imagen, audio o registro de eventos) y todos los soportes de almacenamiento (p. ej., unidades locales, servicios en la nube, servidores de correo electrónico, copias de seguridad)

2.2 El alcance incluye:

2.2.1 Documentos de la organización (p. ej., facturas, contratos, informes de proyecto)

2.2.2 Registros operativos (p. ej., registros de eventos, historial de acceso, instantáneas de copias de seguridad)

2.2.3 Datos personales (p. ej., expedientes de RR. HH., comunicaciones con clientes, registros de soporte)

2.2.4 Datos alojados internamente, externamente o en sistemas híbridos

2.2.5 Datos archivados y copias de seguridad, tanto activos como inactivos

2.3 El alcance abarca todas las etapas del ciclo de vida de los datos, desde su creación hasta su eliminación autorizada.

3. Objetivos

3.1 Definir reglas de conservación coherentes basadas en criterios legales, operativos y regulatorios.

3.2 Evitar la eliminación prematura de registros críticos y eliminar la acumulación innecesaria de datos.

3.3 Garantizar la eliminación segura e irreversible de los datos cuando su conservación deje de ser necesaria.

3.4 Asignar la responsabilidad de aplicar las decisiones de conservación y eliminación dentro de las limitaciones de personal propias de una pyme.

3.5 Proporcionar documentación apta para auditoría que demuestre diligencia debida conforme a ISO 27001, RGPD, NIS2 y otros marcos de referencia.

3.6 Promover la gestión segura del ciclo de vida de los datos sin imponer una carga técnica innecesaria al personal no especialista.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba esta política y asume su titularidad.

4.1.2 Garantiza que los procedimientos de conservación y eliminación se implanten de forma coherente con el riesgo legal y organizativo.

4.1.3 Autoriza excepciones y retenciones legales cuando sea necesario.

4.1.4 Inicia revisiones de la política y aprueba actualizaciones basadas en cambios organizativos o regulatorios.

4.2 Responsable designado de los datos

4.2.1 Se asigna para cada categoría de datos (p. ej., financiera, recursos humanos, registros de clientes).

4.2.2 Clasifica los registros y determina la conservación aplicable con base en la política y en el asesoramiento jurídico.

4.2.3 Autoriza la eliminación cuando se hayan cumplido los requisitos de conservación.

4.2.4 Da soporte a las revisiones internas proporcionando contexto sobre la lógica de conservación y los eventos de eliminación.

[... 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 cuando se produzca cualquiera de las siguientes circunstancias:

9.1.1 Cambios en la legislación aplicable (p. ej., privacidad de datos, información financiera)

9.1.2 Adopción de nuevos sistemas o procesos que afecten al ciclo de vida de los datos

9.1.3 Hallazgos de auditoría o incidentes que revelen deficiencias en las prácticas de conservación

9.2 Las revisiones deben garantizar que el Registro de Conservación siga siendo completo y refleje todas las categorías principales de registros.

9.3 Las actualizaciones de la política deben ser aprobadas por el DG y comunicadas al personal afectado. La versión más reciente debe estar accesible y sujeta a control de versiones.

10. Políticas relacionadas y vinculaciones

10.1 P2S – Política de funciones y responsabilidades de gobernanza: Define la titularidad de la política y la autoridad para las excepciones.

10.2 P13S – Política de clasificación y etiquetado de datos: Determina cómo se alinean las reglas de conservación con la clasificación de los datos.

10.3 P12S – Política de gestión de activos: Regula los soportes de almacenamiento que contienen datos sujetos a conservación y eliminación.

10.4 P17S – Política de Protección de Datos y Privacidad: Garantiza la minimización de datos y respalda el tratamiento lícito conforme al RGPD.

10.5 P30S – Política de Respuesta a Incidentes: Se activa cuando los fallos de eliminación o conservación dan lugar a una posible exposición de datos.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1.3: Exige el tratamiento de los riesgos relacionados con la información, incluidos los riesgos de conservación.

11.1.2 Cláusula 8.1: Define controles operativos del ciclo de vida.

11.2 ISO/IEC 27002

11.2.1 Control 5.33: Proporciona orientación para establecer períodos de conservación y métodos de destrucción segura.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Exige la conservación de registros de auditoría.

11.3.2 MP-6: Define procedimientos de sanitización de soportes.

11.3.3 SI-12: Aborda los límites de conservación de datos y su aplicación.

11.4 RGPD de la UE

11.4.1 Artículo 5(1)(e): Los datos no deben conservarse más tiempo del necesario.

11.4.2 Artículo 17: El derecho de supresión se aplica cuando los datos ya no se conservan lícitamente.

11.5 Directiva NIS2 de la UE

11.5.1 Artículo 21(2)(a): Exige políticas organizativas adecuadas al riesgo, incluida la gestión del ciclo de vida.

11.6 DORA de la UE

11.6.1 Artículo 5(1): La gestión del riesgo de las TIC incluye la disponibilidad y la eliminación de datos.

11.7 COBIT 2019

11.7.1 BAI03.04: Exige controles del ciclo de vida de la información.

11.7.2 DSS01.06: Exige procedimientos de eliminación segura como parte de la protección de los activos de información.