					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P14					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, 8.1	
ISO/IEC 27002:2022	Controles 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
RGPD de la UE	Artículos 5(1)(e), 17, 32	
Directiva NIS2 de la UE	Artículo 21(2)(a-e)	
DORA de la UE	Artículos 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Propósito

1.1 El propósito de esta política es establecer los requisitos de la organización para la conservación y la eliminación segura de los datos en todas las fases del ciclo de vida de la información. Garantiza el cumplimiento de las obligaciones legales, regulatorias y contractuales aplicables, y evita la acumulación innecesaria o riesgosa de datos.

1.2 Esta política respalda la implantación de ISO/IEC 27001:2022 mediante la aplicación de controles sobre los plazos de conservación de datos y las prácticas de eliminación irreversible. Permite la documentación trazable de los registros, exige la conservación alineada con la sensibilidad de su clasificación y garantiza la preparación para auditorías, inspecciones regulatorias y requerimientos de exhibición documental en procedimientos judiciales.

1.3 Asimismo, tiene por objeto preservar la confidencialidad, integridad y disponibilidad de los datos, al tiempo que minimiza el riesgo para la organización, las ineficiencias operativas y la exposición a incumplimientos de privacidad derivados de una conservación o destrucción inadecuadas.

2. Alcance

2.1 Esta política se aplica a todos los activos de información físicos y digitales propiedad de la organización, tratados o conservados por esta, incluidos aquellos bajo el control de terceros, filiales o socios de externalización.

2.2 El alcance incluye, entre otros, los siguientes elementos:

2.2.1 Documentos, archivos y registros, tanto digitales como en papel

2.2.2 Bases de datos y archivos históricos

2.2.3 Correos electrónicos y registros de mensajería instantánea

2.2.4 Copias de seguridad, registros del sistema y trazas de auditoría

2.2.5 Código fuente, datos de aplicaciones y activos alojados en la nube

2.2.6 Medios extraíbles y hardware obsoleto que contenga datos

2.3 La política regula tanto los registros operativos como los conjuntos de datos regulados (por ejemplo, contenido financiero, jurídico, de recursos humanos, relacionado con clientes y relevante para auditoría), con independencia de su ubicación de almacenamiento o sistema.

2.4 Se aplica a todos los departamentos de la organización y a empleados, contratistas y proveedores que participen en la creación, almacenamiento, gestión o eliminación de datos.

3. Objetivos

3.1 Garantizar que los datos se conserven únicamente durante el tiempo necesario por motivos legales, contractuales u operativos, y que se eliminen de forma segura cuando dejen de ser necesarios.

3.2 Evitar la eliminación prematura, no autorizada o accidental de registros necesarios para operaciones en curso, cumplimiento normativo, litigios o fines de auditoría.

3.3 Establecer y aplicar calendarios de conservación coherentes basados en la clasificación de la información, el tipo de activo, la normativa aplicable y la exposición al riesgo.

3.4 Proteger la privacidad y la confidencialidad de los datos durante su período de conservación y en el momento de su eliminación, incluido el cumplimiento de los derechos del interesado (por ejemplo, la supresión conforme al artículo 17 del RGPD de la UE).

3.5 Garantizar que todos los métodos de eliminación de datos sean irreversibles, estén debidamente documentados y cumplan normas reconocidas como NIST SP 800-88.

3.6 Minimizar las ineficiencias operativas, los sobrecostes y la exposición jurídica causados por la conservación excesiva o por datos heredados no controlados.

3.7 Respaldar los objetivos de continuidad del negocio y recuperación ante desastres mediante una gobernanza integrada de la conservación de copias de seguridad y prácticas de archivado de datos defendibles.

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Aprueba esta política y garantiza una financiación, dotación de recursos e integración adecuadas en la gestión del riesgo empresarial y en los programas de cumplimiento.

4.1.2 Asume la responsabilidad global del cumplimiento legal y regulatorio relacionado con la conservación y la eliminación segura de datos.

4.2 Director de Seguridad de la Información (CISO)

4.2.1 Es el responsable de esta política y de definir y revisar la gobernanza de conservación y eliminación en alineación con el SGSI.

4.2.2 Garantiza que los requisitos de conservación y eliminación basados en la clasificación se implanten en las unidades de negocio y en los sistemas técnicos.

4.2.3 Supervisa el cumplimiento de la política y exige acciones correctivas cuando sea necesario.

[... 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 anualmente o cuando se cumpla cualquiera de las siguientes condiciones:

9.1.1 Cambios en leyes o reglamentos aplicables que afecten a la conservación de datos (por ejemplo, actualizaciones del RGPD de la UE, códigos tributarios o DORA de la UE)

9.1.2 Revisiones del marco de clasificación o de los procesos de la organización que afecten a las etapas del ciclo de vida de los datos

9.1.3 Introducción de nuevos sistemas de TI, plataformas de archivado o tecnologías de eliminación de medios

9.1.4 Hallazgos de auditoría interna o recomendaciones regulatorias que pongan de manifiesto deficiencias en las prácticas de conservación o eliminación

9.2 La revisión debe estar dirigida por el CISO y el Delegado de Protección de Datos (DPD), con aportaciones de Asesoría Jurídica, Cumplimiento, TI y las unidades de negocio.

9.3 El Calendario Maestro de Conservación de Datos (MDRS) y el Registro de Eliminación deben revisarse en paralelo para garantizar que:

9.3.1 Los calendarios sigan siendo precisos y reflejen las necesidades operativas, jurídicas y regulatorias

9.3.2 La documentación de eliminación sea completa y auditable

9.3.3 Los registros de retención legal se validen y se liberen cuando corresponda

9.4 Cualquier actualización de la política debe:

9.4.1 Estar formalmente versionada y conservarse en el Repositorio Documental del SGSI

9.4.2 Incluir un historial de versiones y la justificación del cambio

9.4.3 Estar aprobada por la Alta Dirección

9.4.4 Comunicarse al personal pertinente con materiales actualizados de formación u orientación

9.5 Cuando se produzcan cambios significativos en la política, los empleados afectados deben completar formación específica en un plazo de 30 días desde su publicación para garantizar el cumplimiento continuado.

9.6 Políticas relacionadas y vinculaciones

10. Políticas relacionadas y vinculaciones

10.1.1 P4 - Política de Control de Acceso: garantiza que solo las personas autorizadas accedan a los datos durante su período de conservación y que los datos caducados queden restringidos hasta su eliminación.

10.1.2 P12 - Política de Gestión de Activos: identifica qué activos contienen datos que requieren eliminación programada y realiza el seguimiento de su ciclo de vida desde la adquisición hasta la destrucción.

10.1.3 P13 - Política de Clasificación y Etiquetado de la Información: guía las decisiones de clasificación que influyen directamente en el tiempo de conservación de los datos y en el método de eliminación requerido.

10.1.4 P15 - Política de Copias de Seguridad y Restauración: define los períodos de conservación y los procedimientos de eliminación para los medios de copia de seguridad y los activos de datos replicados.

10.1.5 P18 - Política de Controles Criptográficos: respalda el borrado criptográfico para la eliminación y exige el cifrado durante el almacenamiento de los datos hasta su destrucción.

10.1.6 P30 - Política de Respuesta a Incidentes: se activa en los casos en que una eliminación inadecuada dé lugar a una posible pérdida de datos, brecha de seguridad o incumplimiento regulatorio.

10.2 Cada política vinculada desempeña un papel en la aplicación de un modelo coherente de gobierno del dato en materia de clasificación, control del ciclo de vida, acceso y preparación para auditorías.

11. Normas y marcos de referencia

11.1 Esta política se alinea con normas y marcos regulatorios reconocidos internacionalmente que definen prácticas seguras, conformes y eficientes para el ciclo de vida de los datos.

11.2 ISO/IEC 27001:

11.2.1 Cláusula 6.1.3 - Plan de tratamiento de riesgos: respalda la mitigación de los riesgos asociados a la conservación excesiva, las brechas de seguridad de los datos o los fallos en la eliminación.

11.2.2 Cláusula 8.1 - Planificación y control operacionales: establece controles del ciclo de vida que regulan el almacenamiento, el archivado y la destrucción.

11.3 ISO/IEC 27002:2022 - Controles 5.10, 5.12, 5.30, 5: proporcionan orientación práctica sobre el uso aceptable de los datos, la justificación de la conservación, la eliminación controlada y la gestión defendible de registros, alineadas con la tolerancia al riesgo de la organización.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Conservación de registros de auditoría: garantiza un almacenamiento suficiente de registros de auditoría y evidencias de cumplimiento.

11.4.2 MP-6 - Saneamiento de medios: exige métodos de destrucción segura y documentada para medios físicos y electrónicos.

11.4.3 SI-12 - Manejo de la información: exige un tratamiento adecuado de los datos alineado con los controles de conservación y eliminación.

11.4.4 PL-2 - Plan de seguridad y privacidad del sistema: exige documentación específica por sistema sobre la gestión del ciclo de vida de los datos y las disposiciones de eliminación segura.

11.5 RGPD de la UE (2016/679):

11.5.1 Artículo 5(1)(e) - Minimización de datos y limitación del plazo de conservación: exige que los datos no se conserven más tiempo del necesario.

11.5.2 Artículo 17 - Derecho de supresión ("derecho al olvido"): exige la eliminación pronta y permanente de los datos personales ante una solicitud válida.

11.5.3 Artículo 32 - Seguridad del tratamiento: refuerza la protección de los datos durante su conservación y exige la destrucción segura de los registros caducados.

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

11.6.1 Artículo 21(2)(a-e): exige que las entidades adopten políticas y medidas técnicas para el manejo seguro de los datos, incluidas las limitaciones de almacenamiento y los métodos de eliminación.

11.7 DORA de la UE (2022/2554):

11.7.1 Artículo 5 - Gobernanza y control: exige una gestión estructurada del riesgo de las TIC, incluida la gestión segura del ciclo de vida de la información.

11.7.2 Artículo 9 - Marco de gestión del riesgo de las TIC: exige políticas de conservación de datos, destrucción y cumplimiento legal y regulatorio de las operaciones digitales.

11.8 COBIT 2019:

11.8.1 DSS01 - Operaciones gestionadas: respalda el seguimiento de la conservación y la coherencia entre sistemas de datos.

11.8.2 DSS05 - Gestionar los servicios de seguridad: garantiza la protección de los datos almacenados y archivados hasta su eliminación segura.

11.8.3 MEA03 - Supervisar, evaluar y valorar el cumplimiento: permite auditar la aplicación de la conservación, los procedimientos de eliminación y el cumplimiento regulatorio.