					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P15S					Título del documento: **Política de Copias de Seguridad y Restauración**							
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	cláusula 8	Controles de copia de seguridad conforme a los requisitos del SGSI
ISO/IEC 27002:2022	controles 5.29, 8	Buenas prácticas para copias de seguridad e integración con la continuidad del negocio
NIST SP 800-53 Rev. 5	CP-9, MP-6	Copias de seguridad y protección de soportes
Directiva NIS2 de la UE	artículo 21(2)(c)	Resiliencia y continuidad mediante copias de seguridad
DORA de la UE	artículo 10(1)	Continuidad de las TIC: copias de seguridad para organizaciones del sector financiero
COBIT 2019	BAI04.05, DSS04	Documentación y prueba de copias de seguridad, y control de procesos
RGPD de la UE	artículos 5(1)(f), 32(1)(c)	Integridad, disponibilidad y restauración oportuna de los datos

1. Propósito

1.1 Esta política define cómo la organización realiza y gestiona las copias de seguridad para garantizar la continuidad del negocio, proteger frente a la pérdida de datos y posibilitar una recuperación oportuna ante incidentes.

1.2 Establece requisitos obligatorios sobre cómo deben realizarse, almacenarse y restaurarse las copias de seguridad de sistemas y datos, en particular en pymes sin una infraestructura de TI compleja.

1.3 Esta política respalda la preparación para auditorías y la certificación ISO/IEC 27001 al garantizar que los controles esenciales de copia de seguridad estén implantados, se apliquen de forma consistente y se revisen periódicamente.

1.4 La capacidad de la organización para recuperarse de fallos técnicos, eliminaciones accidentales o incidentes de ciberseguridad depende del cumplimiento estricto de esta política.

2. Alcance

2.1 Esta política se aplica a todos los sistemas y datos de la organización, incluidos:

2.1.1 Registros financieros, información de clientes y datos de Recursos Humanos

2.1.2 Equipos de sobremesa, portátiles, servidores y aplicaciones en la nube utilizados en las operaciones de la organización

2.1.3 Soportes de copia de seguridad, como unidades USB, almacenamiento externo o copias de seguridad en la nube

2.2 También se aplica a todas las personas con responsabilidad en la ejecución o gestión de los procesos de copia de seguridad, incluidos:

2.2.1 El Director General (DG) o la persona responsable designada

2.2.2 Proveedores externos de soporte de TI o consultores

2.2.3 Todos los empleados responsables de almacenar datos en ubicaciones aprobadas

3. Objetivos

3.1 Garantizar que todos los datos y sistemas críticos para las operaciones de la organización se sometan a copias de seguridad seguras con una periodicidad adecuada en función del riesgo y de las necesidades operativas.

3.2 Garantizar que los datos puedan recuperarse de forma oportuna y completa tras interrupciones.

3.3 Prevenir el acceso no autorizado, la manipulación o la pérdida de los datos de copia de seguridad mediante controles de almacenamiento eficaces.

3.4 Asignar de forma clara las funciones y responsabilidades para implantar y probar los procedimientos de copia de seguridad, y exigir su cumplimiento.

3.5 Respaldar el cumplimiento de ISO/IEC 27001, del RGPD de la UE y de otras obligaciones reglamentarias mediante prácticas de copia de seguridad estructuradas y documentadas.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba esta política y garantiza su aplicación.

4.1.2 Asigna recursos y designa responsables para las actividades de copia de seguridad y restauración.

4.1.3 Revisa los fallos de copia de seguridad, los incidentes y las desviaciones de la política.

4.1.4 Dirige las revisiones anuales de la política y garantiza la preparación para auditorías.

4.2 Proveedor externo de soporte de TI (si procede)

4.2.1 Implanta y gestiona soluciones de copia de seguridad, ya sean locales o en la nube.

4.2.2 Supervisa la correcta ejecución de las copias de seguridad y programa pruebas de restauración.

4.2.3 Informa directamente al DG de fallos e incidentes.

4.2.4 Garantiza el cifrado, las restricciones de acceso y el tratamiento adecuado de los soportes de copia de seguridad.

[... 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 por el DG. Los desencadenantes de revisiones extraordinarias incluyen:

9.1.1 Cambios importantes en sistemas o métodos de almacenamiento.

9.1.2 Introducción de nuevas plataformas en la nube o de TI.

9.1.3 Cambios legales o reglamentarios que afecten a la recuperación de datos.

9.1.4 Hallazgos de auditoría o incidentes.

9.2 El DG es responsable de iniciar la revisión, aprobar los cambios y comunicar las actualizaciones.

9.3 Las versiones de la política deben controlarse y archivarse. Las versiones sustituidas deben mantenerse con acceso restringido para evitar confusiones durante auditorías o eventos de recuperación de la organización.

10. Políticas relacionadas y vinculaciones

10.1 Esta política está alineada con las siguientes políticas para pymes y depende de ellas:

10.1.1 P14S – Política de Conservación y Eliminación de Datos: define durante cuánto tiempo deben conservarse los datos de copia de seguridad y cómo deben eliminarse de forma segura.

10.1.2 P13S – Política de Clasificación y Etiquetado de Datos: ayuda a priorizar qué datos deben incluirse en las copias de seguridad según sus niveles de clasificación.

10.1.3 P30S – Política de Respuesta a Incidentes: establece los procedimientos aplicables si las copias de seguridad fallan o si se requiere recuperación de datos tras una brecha de seguridad o una indisponibilidad del servicio.

10.1.4 P2S – Política de Funciones y Responsabilidades de Gobernanza: asigna autoridad clara para la supervisión de las copias de seguridad y la aplicación de la política.

10.1.5 P17S – Política de Protección de Datos y Privacidad: garantiza que la gestión de copias de seguridad con datos personales esté alineada con los requisitos legales y de privacidad.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 cláusula 8.1: planificación operativa y control de los sistemas de copia de seguridad como parte del SGSI.

11.2 ISO/IEC 27002

11.2.1 control 8.13: establece buenas prácticas para la programación, supervisión y restauración de copias de seguridad.

11.2.2 anexo A, control 5.29: integración de las copias de seguridad con la continuidad del negocio y la preparación para la restauración.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CP-9 (planificación de contingencias): define estrategias estructuradas de copia de seguridad para la resiliencia de la organización.

11.3.2 MP-6 (protección de soportes): exige la gestión y destrucción seguras de los soportes de copia de seguridad.

11.4 RGPD de la UE

11.4.1 artículo 5(1)(f): exige la integridad y disponibilidad de los datos personales.

11.4.2 artículo 32(1)(c): exige la capacidad de restaurar el acceso a los datos personales de forma oportuna.

11.5 Directiva NIS2 de la UE

11.5.1 artículo 21(2)(c): exige copias de seguridad y recuperación como parte de la planificación de resiliencia y continuidad.

11.6 DORA de la UE

11.6.1 artículo 10(1): las organizaciones del sector financiero deben garantizar copias de seguridad como parte de las medidas de continuidad de las TIC.

11.7 COBIT 2019

11.7.1 BAI04.05: exige estrategias de copia de seguridad documentadas.

11.7.2 DSS04.07: hace hincapié en las pruebas periódicas y el control de los procesos de copia de seguridad y recuperación de datos.