					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P15					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 6.1.3, 8	Tratamiento de riesgos, planificación y controles operativos de copias de seguridad
ISO/IEC 27002:2022	Controles 8.13, 5.28, 5.29	Gestión de copias de seguridad, eliminación segura y resiliencia
NIST SP 800-53 Rev.5	CP-9, CP-10, SI-12, MP-6	Requisitos de copia de seguridad del sistema, recuperación y saneamiento de soportes
RGPD de la UE	Artículo 32, considerando 49	Restauración y disponibilidad de datos personales, continuidad del negocio
Directiva NIS2 de la UE	Artículo 21(2)(c-e)	Controles de copias de seguridad y continuidad para la resiliencia
DORA de la UE	Artículos 10, 11	Requisitos del sector financiero para copias de seguridad, recuperación y pruebas
COBIT 2019	DSS01, DSS04, MEA03	Operaciones de copia de seguridad, continuidad y supervisión del cumplimiento

1. Propósito

1.1 El propósito de esta política es definir los requisitos obligatorios para la realización de copias de seguridad y la restauración de datos, sistemas y aplicaciones, con el fin de reforzar la resiliencia operativa, la integridad de los datos y la continuidad del negocio.

1.2 La política establece un marco normalizado para:

1.2.1 Proteger los datos de la organización frente a pérdidas derivadas de eliminación, corrupción, fallos o ciberataques.

1.2.2 Definir las expectativas de recuperación mediante parámetros claros de RTO (Recovery Time Objective) y RPO (Recovery Point Objective).

1.2.3 Integrar las operaciones de copia de seguridad con el SGSI y con los planes de continuidad del negocio y recuperación ante desastres (BCP/DRP).

1.2.4 Garantizar el cumplimiento de las leyes y reglamentos sectoriales aplicables en materia de disponibilidad y capacidad de recuperación.

1.3 Esta política aplica los controles de ISO/IEC 27001:2022 relacionados con la eliminación segura de datos (5.28), la resiliencia (5.29) y la copia de seguridad de la información (8.13), y se alinea con buenas prácticas de ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, el RGPD de la UE, DORA de la UE y la Directiva NIS2 de la UE.

2. Alcance

2.1 Esta política aplica a:

2.1.1 Todos los sistemas críticos para las operaciones de la organización y los sistemas incluidos en el alcance del Sistema de Gestión de la Seguridad de la Información (SGSI).

2.1.2 Todos los datos estructurados y no estructurados de la organización, incluidas bases de datos, archivos, correos electrónicos y configuraciones.

2.1.3 Todos los entornos: locales, en la nube, híbridos y de almacenamiento remoto o externo.

2.1.4 Todo el personal responsable de gestionar, ejecutar, verificar o restaurar procesos de copia de seguridad.

2.2 También aplica a:

2.2.1 Los soportes e infraestructuras de copia de seguridad, incluidas cintas físicas, dispositivos virtuales, instantáneas de disco y soluciones de copia de seguridad basadas en la nube.

2.2.2 Los proveedores externos contratados para alojar, gestionar o tratar copias de seguridad de la organización.

2.2.3 La copia de seguridad de registros, configuraciones, trazas de auditoría y documentación operativa crítica para la continuidad.

2.3 Los sistemas excluidos expresamente de la copia de seguridad deberán documentarse, someterse a una evaluación de riesgos y ser aceptados formalmente por el Responsable del SGSI y el propietario del sistema.

3. Objetivos

3.1 Garantizar que todos los sistemas y datos críticos dispongan de copias de seguridad fiables, con frecuencia, redundancia y controles de seguridad suficientes.

3.2 Proporcionar mecanismos de restauración que cumplan las expectativas definidas de RTO y RPO, en consonancia con los análisis de impacto en el negocio.

3.3 Mantener documentación completa de los procedimientos de copia de seguridad, calendarios de conservación, funciones y tecnologías.

3.4 Validar la eficacia de las operaciones de copia de seguridad mediante pruebas sistemáticas de restauración, registro de fallos y seguimiento de acciones correctivas.

3.5 Proteger los datos de copia de seguridad frente a accesos no autorizados, modificación o destrucción durante todo su ciclo de vida.

3.6 Permitir el cumplimiento de:

3.6.1 Los requisitos de control operativo y continuidad de ISO/IEC 27001.

3.6.2 Las familias CP y MP de NIST SP 800-53 para copia de seguridad y saneamiento.

3.6.3 El artículo 32 y el considerando 49 del RGPD de la UE en relación con la restauración del acceso a datos personales.

3.6.4 El artículo 10 de DORA de la UE y el artículo 21 de la Directiva NIS2 de la UE en materia de continuidad y resiliencia de las TIC.

3.7 Garantizar que los servicios de copia de seguridad prestados por terceros cumplan las obligaciones contractuales y regulatorias de seguridad, incluidos el cifrado, la eliminación y los protocolos de notificación.

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Aprueba esta política y garantiza que los sistemas críticos para las operaciones de la organización estén adecuadamente protegidos mediante prácticas aprobadas de copia de seguridad y restauración.

4.1.2 Asume la responsabilidad de asegurar que las operaciones de copia de seguridad cuenten con recursos suficientes y se revisen periódicamente para verificar el cumplimiento.

4.2 Director de Seguridad de la Información (CISO)

4.2.1 Es el responsable de esta política y garantiza su alineación con los marcos corporativos de seguridad de la información, gestión de riesgos y continuidad.

4.2.2 Supervisa la integración de los procedimientos de copia de seguridad en los planes BCP/DRP, la respuesta a incidentes y la planificación de la resiliencia.

4.2.3 Revisa las excepciones de copia de seguridad y evalúa las propuestas de aceptación del riesgo para exclusiones de sistemas críticos.

[... 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 deberá revisarse al menos una vez al año, o antes si se activa por:

9.1.1 Cambios en la estrategia de continuidad del negocio o recuperación ante desastres.

9.1.2 Nuevas obligaciones regulatorias o legales que afecten a la frecuencia de las copias de seguridad o a la conservación de datos.

9.1.3 Cambios en la arquitectura del sistema, las herramientas de copia de seguridad o los proveedores de servicios.

9.1.4 Incidentes significativos o hallazgos de auditoría relacionados con pérdida de datos o fallos de recuperación.

9.2 La revisión será coordinada por el Director de Seguridad de la Información en colaboración con:

9.2.1 Infraestructura y Operaciones de TI.

9.2.2 Auditoría Interna.

9.2.3 Delegado de Protección de Datos (DPD).

9.2.4 Los equipos de continuidad del negocio y recuperación ante desastres.

9.3 Los calendarios de copia de seguridad, las listas de inclusión de sistemas, la documentación de restauración y los registros de excepciones se revisarán en paralelo para garantizar:

9.3.1 La exactitud de la cobertura de copia de seguridad para todos los activos críticos.

9.3.2 El cumplimiento de los requisitos de RTO/RPO y conservación.

9.3.3 La integridad de los registros de pruebas y de los informes de incidentes.

9.3.4 La corrección de las deficiencias de control identificadas previamente.

9.4 Todas las actualizaciones deberán:

9.4.1 Estar sujetas a control de versiones y conservarse en el Repositorio Documental del SGSI.

9.4.2 Incluir un resumen de cambios y su justificación.

9.4.3 Ser aprobadas por la Alta Dirección.

9.4.4 Comunicarse a todo el personal técnico y de negocio afectado.

10. Políticas relacionadas e interdependencias

10.1 Esta política respalda e interactúa directamente con los siguientes documentos relacionados:

10.1.1 P6 - Política de Gestión de Riesgos: identifica la priorización basada en riesgos de la protección mediante copia de seguridad para sistemas y servicios.

10.1.2 P12 - Política de Gestión de Activos: garantiza que los sistemas susceptibles de copia de seguridad estén inventariados y vinculados al seguimiento del ciclo de vida y a su clasificación.

10.1.3 P13 - Política de Clasificación y Etiquetado de Datos: orienta qué categorías de datos requieren copia de seguridad, incluido el etiquetado de metadatos para su priorización.

10.1.4 P14 - Política de Conservación y Eliminación de Datos: coordina la conservación de copias de seguridad con los límites regulatorios de conservación y la eliminación adecuada de soportes caducados.

10.1.5 P16 - Política de Enmascaramiento y Seudonimización de Datos: respalda la minimización de datos durante la copia de seguridad de conjuntos de datos sensibles.

10.1.6 P30 - Política de Respuesta a Incidentes: se activa durante fallos de copia de seguridad, incidencias de restauración o compromiso de repositorios de datos de copia de seguridad.

10.2 Estas políticas interrelacionadas forman un marco coherente que garantiza que la gobernanza de las copias de seguridad esté integrada en el SGSI general de la organización y en su estrategia de resiliencia operativa.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:

11.1.1 Cláusula 6.1.3 - Plan de tratamiento de riesgos: respalda la priorización de copias de seguridad basada en riesgos y la planificación de la restauración.

11.1.2 Cláusula 8.1 - Planificación y control operacional: integra controles de recuperación y continuidad como parte de las salvaguardas operativas.

11.1.3 Anexo A control 5.28 - Eliminación segura o reutilización de equipos: aborda el saneamiento seguro de soportes de copia de seguridad.

11.1.4 Anexo A control 5.29 - Seguridad de la información durante interrupciones: garantiza capacidades de restauración durante incidentes o desastres.

11.1.5 Anexo A control 8.13 - Copia de seguridad de la información: se aborda directamente mediante operaciones de copia de seguridad programadas, probadas y seguras.

11.2 ISO/IEC 27002:2022 - Controles 8.13, 5.28, 5.29: estos controles refuerzan el requisito de copias de seguridad periódicas, validación de integridad y planificación de la restauración en todos los entornos de TI.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - Copia de seguridad del sistema: establece procedimientos integrales de copia de seguridad, incluido el almacenamiento externo y las pruebas de restauración.

11.3.2 CP-10 - Recuperación y restauración del sistema: exige procedimientos validados para restauración total o parcial alineados con los objetivos de recuperación.

11.3.3 MP-6 - Saneamiento de soportes: garantiza el manejo seguro de soportes de copia de seguridad obsoletos.

11.3.4 SI-12 - Procedimientos de manejo de la información: refuerza las responsabilidades de copia de seguridad y recuperación para datos sensibles.

11.4 RGPD de la UE (2016/679):

11.4.1 Artículo 32 - Seguridad del tratamiento: exige capacidades de restauración y salvaguardas de disponibilidad de datos, especialmente para datos personales.

11.4.2 Considerando 49: respalda medidas de continuidad del negocio y recuperación ante desastres, incluida la copia de seguridad segura como parte de la resiliencia de la organización.

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

11.5.1 Artículo 21(2)(c-e): exige medidas técnicas y organizativas, incluidos controles de copia de seguridad y continuidad, para garantizar la resiliencia del servicio.

11.6 DORA de la UE (2022/2554):

11.6.1 Artículo 10 - Continuidad del negocio de las TIC: exige que las entidades financieras dispongan de copia de seguridad completa de datos, recuperación y planificación de continuidad.

11.6.2 Artículo 11 - Pruebas de los planes de continuidad del negocio de las TIC: enfatiza la validación de la capacidad de recuperación mediante pruebas periódicas.

11.7 COBIT 2019:

11.7.1 DSS01 - Operaciones gestionadas: respalda la prestación fiable de servicios mediante la disponibilidad protegida de los datos.

11.7.2 DSS04 - Continuidad gestionada: define controles estratégicos y operativos de continuidad, incluidas copias de seguridad verificadas.

11.7.3 MEA03 - Supervisar, evaluar y valorar el cumplimiento: exige la revisión periódica de las medidas de continuidad, incluida la eficacia de los controles de copia de seguridad.