					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P06					Título del documento: **Política de gestión de riesgos**							
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, 8.32, 10	Identificación y gestión de riesgos como elemento central, integración en la gestión de cambios, mejora continua
ISO/IEC 27005:2024	Metodología completa del ciclo de vida del riesgo	Proceso integral de gestión de riesgos conforme a la norma
ISO 31000:2018	Principios y marco de gestión de riesgos	Principios de gestión de riesgos adoptados en el marco
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Directrices y estructura para evaluaciones de riesgos, gobernanza de riesgos por niveles
RGPD de la UE	Artículos 24, 25, 32	Procesos y controles de riesgo para la protección de datos
Directiva NIS2 de la UE	Artículo 21(2)(a–d)	Obligaciones de evaluación de riesgos y seguridad
DORA de la UE	Artículos 5, 6	Gestión de riesgos de las TIC y resiliencia operativa
COBIT 2019	APO12, MEA	Estructura y supervisión de la gestión de riesgos

1. Finalidad

1.1 Esta política establece un marco unificado y formalizado para identificar, analizar, evaluar, tratar, supervisar y revisar los riesgos de seguridad de la información en toda la organización.

1.2 Garantiza la aplicación coherente de principios basados en el riesgo para proteger la confidencialidad, integridad y disponibilidad de los activos de información, en consonancia con la cláusula 6.1 de ISO/IEC 27001:2022 y con ISO 31000:2018.

1.3 La política integra la gestión de riesgos de seguridad de la información en los procesos de toma de decisiones de la organización para apoyar el cumplimiento de los objetivos estratégicos internos y de los requisitos reglamentarios externos.

2. Alcance

2.1 Esta política se aplica a todas las unidades organizativas, procesos de negocio, sistemas, personal y relaciones con terceros implicados en el tratamiento, desarrollo, almacenamiento o gestión de activos de información.

2.2 El alcance se extiende a los activos físicos, digitales y alojados en la nube, incluidos los datos estructurados y no estructurados, las aplicaciones, la infraestructura, las redes y los servicios.

2.3 Abarca los riesgos de seguridad de la información en los niveles estratégico, operativo, de proyecto y técnico, y es de obligado cumplimiento para todos los empleados, contratistas y proveedores de servicios que participen en actividades del Sistema de Gestión de la Seguridad de la Información (SGSI).

2.4 La gestión de riesgos debe aplicarse en los siguientes supuestos:

2.4.1 Implantación de nuevos proyectos o sistemas

2.4.1.1 Cambios significativos (p. ej., arquitectura, titularidad, procesos)

2.4.1.2 Proceso de incorporación de proveedores y acuerdos con terceros

2.4.1.3 Respuesta a incidentes y revisiones posteriores al incidente

2.4.1.4 Revisiones periódicas de riesgos de la organización o auditorías

3. Objetivos

3.1 Establecer y operar un proceso de gestión de riesgos repetible en toda la organización, basado en las metodologías ISO/IEC 27005 e ISO 31000.

3.2 Garantizar que los riesgos se identifiquen, analicen, evalúen y traten mediante métodos estructurados y trazables, incluida la asignación de responsables del riesgo y su vinculación con los controles.

3.3 Mantener un Registro de Riesgos centralizado y sujeto a control de versiones, así como un Plan de Tratamiento de Riesgos, que reflejen el estado actual de los riesgos, la cobertura de controles y el avance de la mitigación.

3.4 Alinear las decisiones sobre riesgos con los niveles documentados de apetito de riesgo y tolerancia al riesgo, y permitir decisiones de gobernanza fundamentadas sobre aceptación, mitigación, transferencia o evitación del riesgo.

3.5 Supervisar de forma continua las tendencias de riesgo y garantizar la eficacia de los tratamientos del riesgo, permitiendo ajustes proactivos en función de la evolución de las amenazas o de los cambios en la organización.

4. Funciones y responsabilidades

4.1 Alta dirección / Consejo de Administración

4.1.1 Aprueba el marco de gestión de riesgos y define el apetito de riesgo aceptable y los umbrales de tolerancia.

4.1.2 Autoriza las estrategias de tratamiento del riesgo para los riesgos residuales que superen la tolerancia.

4.1.3 Asigna recursos y supervisión para el funcionamiento eficaz del programa de gestión de riesgos.

4.2 Responsable del SGSI / Responsable de Riesgos

4.2.1 Es titular de esta política y mantiene su alineación con las normas ISO/IEC 27001 e ISO/IEC 27005.

4.2.2 Dirige el proceso corporativo de evaluación de riesgos y mantiene el Registro de Riesgos y el Plan de Tratamiento de Riesgos.

4.2.3 Garantiza revisiones periódicas y el escalado de los riesgos clave a la alta dirección o al comité de dirección del SGSI.

[... 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 y su marco asociado deberán revisarse anualmente, o bien:

9.1.1 Tras un evento de riesgo importante o un incidente de seguridad

9.1.2 Después de un cambio organizativo o técnico significativo

9.1.3 En respuesta a hallazgos de auditoría o nuevos requisitos reglamentarios

9.2 El Responsable del SGSI, el Responsable de Riesgos y el equipo de Cumplimiento son conjuntamente responsables de:

9.2.1 Iniciar el ciclo de revisión

9.2.2 Recopilar aportaciones de las unidades de negocio

9.2.3 Revisar procedimientos y umbrales según sea necesario

9.3 Todas las revisiones deberán:

9.3.1 Estar sujetas a control de versiones y quedar registradas

9.3.2 Ser aprobadas por la alta dirección

9.3.3 Comunicarse a las partes interesadas

9.3.4 Conservarse en el repositorio de auditoría durante un mínimo de 5 años

10. Políticas relacionadas e interrelaciones

10.1 Esta política es interdependiente con las siguientes políticas de seguridad de la información:

10.1.1 P1 – P01 Política de seguridad de la información: establece el modelo general de gobernanza de la seguridad bajo el cual opera esta política de riesgos.

10.1.2 P2 – Política de funciones y responsabilidades de gobernanza: define los responsables y los niveles de gobernanza referenciados en la matriz de escalado de riesgos.

10.1.3 P5 – P05 Política de gestión de cambios: activa la reevaluación de riesgos ante cambios en la infraestructura y en la organización.

10.1.4 P13 – Política de clasificación y etiquetado de datos: respalda la evaluación de impacto durante la identificación de riesgos.

10.1.5 P33 – Política de supervisión de auditoría y cumplimiento: valida el cumplimiento de políticas, incluida la integridad del Registro de Riesgos y la evidencia de los tratamientos.

11. Normas y marcos de referencia

11.1 Esta política está expresamente alineada con las siguientes normas y marcos para garantizar que cumple las mejores prácticas internacionales y las expectativas regulatorias en materia de gestión de riesgos de seguridad de la información:

11.2 ISO/IEC 27001:

11.2.1 Cláusula 6.1: establece los requisitos para identificar riesgos y oportunidades, incluido el ciclo de vida completo de las evaluaciones y los tratamientos de riesgos de seguridad de la información. Esta política operacionaliza las cláusulas 6.1.2 y 6.1.3 mediante un marco estructurado que exige protocolos documentados para la identificación, análisis, evaluación, tratamiento y aceptación del riesgo residual.

11.2.2 Cláusula 8.32: la integración del enfoque basado en el riesgo en los procesos de gestión de cambios garantiza que todos los cambios organizativos significativos activen reevaluaciones formales del riesgo.

11.2.3 Cláusula 10: la mejora continua se integra mediante revisiones periódicas de la política, análisis de tendencias de riesgo y actualizaciones de la SoA impulsadas por el conocimiento obtenido de los riesgos.

11.3 ISO/IEC 27005:

11.3.1 Proporciona directrices especializadas y detalladas sobre la gestión de riesgos de seguridad de la información. Esta política implanta el modelo completo del proceso de riesgo de ISO/IEC 27005: establecimiento del contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo, supervisión y revisión del riesgo.

11.4 ISO 31000:

11.4.1 Esta política integra principios de ISO 31000 como el compromiso del liderazgo, la integración con la toma de decisiones y la mejora continua. Garantiza que la gestión de riesgos se integre en la cultura y en las operaciones de la organización.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Se alinea con la guía de NIST para la realización de evaluaciones de riesgos, incluida la identificación de amenazas, el análisis de vulnerabilidades, la estimación de la probabilidad y la determinación del impacto. La estructura de esta política refleja las etapas de evaluación de riesgos definidas por NIST y las adapta tanto a procesos técnicos como de negocio.

11.6 NIST SP 800-39:

11.6.1 Respalda la gobernanza de riesgos a nivel corporativo, haciendo hincapié en la gestión de riesgos por niveles en la organización, la misión o proceso de negocio y el sistema de información. La política garantiza que la titularidad del riesgo esté claramente definida en todos los niveles e incluye estrategias de tratamiento a nivel organizativo.

11.7 RGPD de la UE:

11.7.1 Artículo 24: exige la implantación de medidas técnicas y organizativas apropiadas para garantizar que los riesgos de protección de datos se gestionen adecuadamente; este requisito se aborda mediante el proceso estructurado de riesgos de esta política.

11.7.2 Artículo 25: la «protección de datos desde el diseño y por defecto» se alinea con la integración del tratamiento del riesgo en los diseños de sistemas y procesos.

11.7.3 Artículo 32: exige un enfoque basado en el riesgo para las medidas de seguridad, que se cumple mediante evaluaciones de riesgos basadas en el impacto y la selección de controles.

11.8 Directiva NIS2 de la UE:

11.8.1 Artículo 21(2)(a–d): exige que las entidades realicen evaluaciones de riesgos, implanten políticas sobre análisis de riesgos y garanticen medidas de seguridad proporcionadas. Esta política satisface dichas obligaciones mediante la aplicación continua del ciclo de vida del riesgo y una gobernanza documentada.

11.9 DORA de la UE:

11.9.1 Artículo 5: exige un marco documentado de gestión de riesgos de las TIC, plenamente cubierto por la arquitectura de esta política, incluida su correspondencia con la SoA y los KRI.

11.9.2 Artículo 6: exige la integración de la gestión de riesgos en las estrategias de resiliencia operativa, abordada mediante matrices de escalado y seguimiento de activos críticos.

11.10 COBIT 2019:

11.10.1 APO12 – Gestionar los riesgos: corresponde directamente al establecimiento por parte de la organización de un enfoque estructurado de gestión de riesgos, la asignación de funciones, el seguimiento de los tratamientos y la garantía de rendición de cuentas a nivel del Consejo.

11.10.2 MEA01 – Supervisar, evaluar y valorar el desempeño y la conformidad: se refleja en el énfasis de esta política en el análisis de tendencias, la supervisión de KRI y la integración de la retroalimentación de auditoría en ciclos de mejora continua.