					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P06S					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, cuando corresponda

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 6.1, 6.1.3	
ISO/IEC 27002:2022	5.4, 5.25	
Directiva NIS2 de la UE	Artículo 21(2)(a–d)	
DORA de la UE	Artículo 5	
COBIT 2019	APO12, MEA01	

1. Propósito

1.1 Esta política establece cómo la organización identifica, evalúa y gestiona los riesgos relacionados con la seguridad de la información, las operaciones, la tecnología y los servicios prestados por terceros.

1.2 Garantiza que la gestión de riesgos forme parte integrante de la planificación, la ejecución de proyectos, la selección de proveedores y la respuesta a incidentes, en alineación con ISO 27001, ISO 31000 y los requisitos reglamentarios aplicables.

1.3 La política respalda la toma de decisiones informada, la protección de los activos de información y la resiliencia de las operaciones críticas de la organización.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los departamentos, sistemas y usuarios de la organización

2.1.2 Toda la información, los servicios y los activos gestionados internamente o a través de terceros

2.1.3 Las actividades relacionadas con la gestión de riesgos, incluidas las revisiones de proyectos, las actualizaciones de sistemas, la externalización y el cumplimiento normativo

2.2 Incluye todos los tipos de riesgos, tales como:

2.2.1 Amenazas de ciberseguridad y vulnerabilidades de los sistemas

2.2.2 Interrupciones operativas e indisponibilidad de los servicios

2.2.3 Exposiciones legales, de cumplimiento o reputacionales

2.2.4 Riesgos de terceros y de la cadena de suministro

2.3 Todos los empleados, contratistas y proveedores de servicios deben cumplir esta política al identificar o comunicar riesgos.

3. Objetivos

3.1 Integrar procedimientos de evaluación de riesgos sencillos y repetibles en las operaciones habituales de la organización.

3.2 Identificar y priorizar los riesgos que puedan afectar a la confidencialidad, integridad y disponibilidad o al cumplimiento legal.

3.3 Asignar responsables y definir acciones de tratamiento del riesgo para todos los riesgos significativos.

3.4 Mantener un Registro de Riesgos preciso y actualizado para respaldar la preparación para auditorías y la supervisión de riesgos.

3.5 Garantizar la participación de la dirección en la aprobación de la tolerancia al riesgo y de los principales planes de tratamiento.

4. Funciones y responsabilidades

4.1 Director General

4.1.1 Establece el apetito de riesgo de la organización y respalda el marco de gestión de riesgos.

4.1.2 Aprueba las decisiones clave de tratamiento del riesgo y los recursos necesarios.

4.1.3 Revisa trimestralmente los principales riesgos con el Coordinador de Riesgos.

4.2 Coordinador de Riesgos (o responsable del SGSI)

4.2.1 Facilita las evaluaciones de riesgos y mantiene el Registro de Riesgos.

4.2.2 Garantiza que la valoración del riesgo, la asignación de responsables y las acciones de tratamiento del riesgo queden documentadas.

4.2.3 Organiza al menos una revisión formal de riesgos al año.

[... 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 Revisión anual de la política

9.1.1 Esta política debe revisarse al menos una vez al año por el Director General y el Coordinador de Riesgos para garantizar su vigencia e integridad.

9.2 Desencadenantes de actualización

9.2.1 Debe realizarse una revisión y actualización anticipadas si:

9.2.1.1 Un incidente grave o un hallazgo de auditoría pone de manifiesto deficiencias en la gestión del riesgo

9.2.1.2 Se introducen nuevas unidades de negocio, tecnologías o alianzas

9.2.1.3 Cambia un requisito reglamentario o contractual

9.3 Control de versiones

9.3.1 Todas las actualizaciones de esta política deben versionarse con los siguientes metadatos:

9.3.1.1 Número de versión y fecha de entrada en vigor

9.3.1.2 Resumen de cambios

9.3.1.3 Aprobador (Director General)

9.3.1.4 Versiones anteriores archivadas a efectos de auditoría

9.4 Comunicación y concienciación

9.4.1 Las versiones actualizadas de la política y los principales planes de tratamiento del riesgo deben comunicarse al personal afectado. La formación anual de actualización debe incluir principios básicos de concienciación sobre riesgos.

10. Políticas relacionadas y vinculaciones

10.1 Esta política funciona de forma coordinada con otras para garantizar una gobernanza integral de la seguridad:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: define quién rinde cuentas sobre la titularidad de los riesgos y la toma de decisiones.

10.1.2 P5S – Política de gestión de cambios: exige una evaluación de riesgos antes de implantar cambios técnicos o de proceso.

10.1.3 P17S – Política de protección de datos y privacidad: aborda el riesgo reglamentario asociado al tratamiento de datos personales.

10.1.4 P30S – Política de respuesta a incidentes: garantiza que el tratamiento del riesgo continúe durante y después de los incidentes de seguridad.

10.1.5 P33S – Política de continuidad de negocio: identifica riesgos residuales y medidas de recuperación para los servicios críticos.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:

11.1.1 La cláusula 6.1 establece un proceso formal de gestión de riesgos y de planificación del tratamiento.

11.1.2 La cláusula 6.1.3 exige que las organizaciones conserven planes de tratamiento y aprobaciones documentados.

11.2 ISO/IEC 27002:

11.2.1 Los controles 5.4 y 5.25 proporcionan orientación para la implantación sobre la asignación de responsables de riesgos, la priorización y la gestión del ciclo de vida.

11.3 NIST SP 800-53 Rev.:

11.3.1 RA-1 a RA-7 definen la evaluación de riesgos, las estrategias de respuesta, la documentación y los mecanismos de revisión.

11.4 PM-9 exige una supervisión coherente, a nivel directivo, de los riesgos de la organización.

11.5 Directiva NIS2 de la UE

11.5.1 El artículo 21(2)(a–d) impone controles obligatorios de evaluación de riesgos, mitigación y gobernanza a las entidades esenciales e importantes.

11.6 DORA de la UE

11.6.1 El artículo 5 exige que las entidades reguladas definan y gestionen marcos de gestión del riesgo de las TIC, incluida la identificación, clasificación y respuesta.

11.7 COBIT 2019

11.7.1 APO12 – Gestionar el riesgo: integra el riesgo en la planificación estratégica y operativa.

11.7.2 MEA01 – Supervisar, evaluar y valorar: garantiza la eficacia y el cumplimiento de los procesos y acciones de gestión de riesgos.