					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P02					Título del documento: **Política P02 de funciones y responsabilidades de gobernanza**							
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 las normas y regulaciones aplicables

Norma/Regulación	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 5.3; Anexo A, Control 5	
ISO/IEC 27002:2022	Control 5	
NIST SP 800-53 Rev. 5	PL-1 a PL-4, PM-1 a PM-13	
RGPD de la UE	Artículos 5(1)(f), 24, 37	
Directiva NIS2 de la UE	Artículo 21(2)(a)	
DORA de la UE	Artículo 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Finalidad

1.1 Esta política define el modelo de gobernanza, las funciones organizativas y las responsabilidades necesarias para operar un Sistema de Gestión de la Seguridad de la Información (SGSI) eficaz.

1.2 Establece líneas claras de rendición de cuentas, autoridad para la toma de decisiones y vías de escalado para garantizar que la seguridad de la información quede integrada en todos los niveles de la organización y alineada con sus objetivos estratégicos.

1.3 Esta política implementa los requisitos de la cláusula 5.3 y del control A.5.2 de ISO/IEC 27001:2022, garantizando que las responsabilidades asociadas a las actividades de seguridad estén claramente asignadas, documentadas, comunicadas y revisadas periódicamente.

1.4 Esta política también proporciona una base para una gobernanza integrada con otras disciplinas, como la gestión de riesgos, el cumplimiento, las operaciones de TI y las funciones jurídicas.

2. Alcance

2.1 Esta política se aplica a todas las personas y entidades implicadas en la gobernanza, operación y supervisión de la seguridad de la información dentro del alcance del SGSI. Esto incluye:

2.1.1 Dirección ejecutiva, alta dirección y miembros del consejo de administración

2.1.2 Responsables del SGSI, CISO y propietarios de controles

2.1.3 Propietarios de procesos y de activos

2.1.4 Contratistas y proveedores de servicios externos con responsabilidades de seguridad delegadas

2.2 Abarca tanto funciones internas como externalizadas (por ejemplo, un SOC externalizado o administradores de plataformas en la nube) cuando las funciones de gobernanza estén formalmente asignadas o definidas contractualmente.

2.3 La política también se aplica a las unidades organizativas, departamentos y equipos de proyecto que gestionen o influyan en activos, sistemas o servicios relevantes para la seguridad.

3. Objetivos

3.1 Garantizar que las funciones y responsabilidades en materia de seguridad de la información estén formalmente definidas, asignadas, comunicadas y documentadas.

3.2 Mantener un modelo de gobernanza que garantice la segregación de funciones, elimine conflictos de interés y permita el escalado de cuestiones de seguridad no resueltas.

3.3 Garantizar que la responsabilidad y la autoridad sobre las decisiones de seguridad se distribuyan de forma coherente con el impacto en la organización y con su estructura organizativa.

3.4 Establecer un marco para gestionar delegaciones, cambios de función y la revisión de responsabilidades asignadas.

3.5 Proporcionar aseguramiento a las partes interesadas, incluidos reguladores, auditores y clientes, de que la seguridad de la información se gobierna de forma eficaz y de conformidad con las normas aplicables.

4. Funciones y responsabilidades

4.1 Dirección Ejecutiva (Alta Dirección)

4.1.1 Proporciona supervisión estratégica, asigna recursos y garantiza la alineación entre los objetivos del SGSI y los objetivos de la organización.

4.1.2 Aprueba la documentación principal del SGSI, incluida la Política de Seguridad de la Información, los planes de tratamiento de riesgos y las decisiones de remediación derivadas de auditorías.

4.1.3 Participa en las revisiones por la dirección del SGSI y eleva para aprobación al consejo de administración las decisiones que así lo requieran.

4.1.4 Promueve una cultura de seguridad y fomenta la adhesión de la organización a los principios de gobernanza de la seguridad.

4.2 Comité de Seguridad de la Información (ISSC)

4.2.1 Actúa como órgano transversal de gobernanza para la supervisión del SGSI.

4.2.2 Revisa la postura de riesgo, el desempeño de los controles, los hallazgos de auditoría y las iniciativas estratégicas de seguridad.

4.2.3 Facilita la coordinación entre departamentos (por ejemplo, TI, Jurídico, RR. HH., Riesgos, Cumplimiento y Operaciones).

4.2.4 Aprueba umbrales de escalado, asignaciones presupuestarias y cambios de política que requieran intervención ejecutiva.

[... 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 Calendario de revisión

9.1.1 Esta política deberá revisarse al menos una vez al año o cuando se produzca cualquiera de los siguientes supuestos:

9.1.1.1 Cambios en la estructura organizativa o en el equipo directivo

9.1.1.2 Ampliación o redefinición del alcance del SGSI

9.1.1.3 Cambios regulatorios que afecten a la asignación de funciones o a la supervisión

9.1.1.4 Hallazgos de auditoría significativos o incidentes que impliquen fallos de gobernanza

9.2 Proceso de revisión y aprobación

9.2.1 El Responsable del SGSI deberá iniciar y dirigir el proceso de revisión, incluida la recopilación de aportaciones de las partes interesadas y la retroalimentación de auditoría.

9.2.2 Las actualizaciones propuestas deberán ser revisadas por el ISSC y aprobadas formalmente por la Dirección Ejecutiva.

9.2.3 Cada versión debe registrarse en el Registro Documental del SGSI e incluir los siguientes metadatos:

9.2.3.1 ID y título de la política

9.2.3.2 Número de versión y resumen de cambios

9.2.3.3 Fecha de entrada en vigor y próxima fecha de revisión

9.2.3.4 Propietario de la política y aprobador

9.2.3.5 Nivel de clasificación del documento

9.2.3.6 Historial de conservación y archivo

10. Políticas relacionadas y vinculaciones

10.1 Esta política debe interpretarse conjuntamente con las siguientes políticas:

10.1.1 P1 – Política de Seguridad de la Información: establece el programa general de seguridad y define las responsabilidades de liderazgo en relación con la aprobación de políticas y la supervisión estratégica.

10.1.2 P5 – Política de Gestión de Cambios: garantiza que los cambios en estructuras de gobernanza, funciones o responsabilidades estén sujetos a aprobación documentada y revisión de riesgos.

10.1.3 P6 – Política de Gestión de Riesgos: identifica y trata los riesgos de gobernanza derivados de conflictos de funciones, tareas no asignadas o falta de escalado.

10.1.4 P7 – Política de incorporación y desvinculación: aplica los procesos de asignación y revocación de controles durante los cambios en el ciclo de vida del personal.

10.1.5 P33 – Política de Auditoría y Supervisión del Cumplimiento: respalda la revisión independiente de la eficacia de la gobernanza y aplica acciones correctivas frente al incumplimiento.

10.2 Estas políticas respaldan conjuntamente un marco de gobernanza del SGSI unificado y exigible.

11. Normas y marcos de referencia

11.1 Esta política se alinea con normas y marcos reconocidos internacionalmente para la gobernanza de la seguridad de la información y la rendición de cuentas de las funciones. Garantiza la trazabilidad respecto de requisitos regulatorios y de certificación, y respalda una estructura de SGSI sólida y auditables.

11.2 ISO/IEC 27001

11.2.1 Cláusula 5.3 – Funciones, responsabilidades y autoridades organizativas: esta política cumple el requisito de que las funciones relevantes para la seguridad de la información estén claramente asignadas, comunicadas y documentadas.

11.2.2 Cláusula 9.3 – Revisión por la dirección: esta política establece la supervisión ejecutiva de las funciones del SGSI y de su gobernanza mediante revisiones trimestrales y anuales.

11.2.3 Anexo A, Control 5.2 – Funciones y responsabilidades de seguridad de la información: define funciones en los niveles técnico, operativo y estratégico para garantizar la segregación de funciones, la titularidad del riesgo y una rendición de cuentas trazable.

11.3 ISO/IEC 27002:2022 – Control 5

11.3.1 Proporciona directrices de implantación para asignar responsabilidades de seguridad de la información en toda la organización. Esta política adopta dichas directrices al definir tipos de funciones, reglas de delegación, procedimientos de escalado y mecanismos de revisión.

11.4 NIST SP 800-53 Rev. 5

11.4.1 PL-1 a PL-4: establecen la necesidad de documentación formal de planificación, incluidas políticas que definan la gobernanza y asignen responsabilidades de seguridad.

11.4.2 PM-1 (Plan del programa de seguridad de la información) y PM-2 (Responsable superior de seguridad de la información): se reflejan en esta política mediante la asignación del CISO/Responsable del SGSI y de funciones formales de gobernanza.

11.4.3 PM-5 a PM-13: esta política satisface requisitos de documentación de funciones, funciones de riesgo a nivel corporativo, supervisión de la gestión de la configuración e integración con funciones de misión y de la organización.

11.5 RGPD de la UE (2016/679)

11.5.1 Artículo 5(1)(f): exige que los datos personales estén protegidos frente al tratamiento no autorizado o ilícito. Esta política garantiza que las personas responsables de la protección de datos estén claramente designadas y sujetas a supervisión.

11.5.2 Artículo 24: exige medidas organizativas adecuadas, incluidas estructuras de gobernanza.

11.5.3 Artículo 37: exige la designación de un Delegado de Protección de Datos (DPD), que debe reflejarse en el marco de gobernanza y en el registro de responsabilidades de la organización.

11.6 Directiva NIS2 de la UE (2022/2555)

11.6.1 Artículo 21(2)(a): exige que las entidades implanten políticas sobre análisis de riesgos y seguridad de los sistemas de información, incluidas responsabilidades específicas por función. Esta política define dichas funciones y sus mecanismos de gobernanza.

11.7 DORA de la UE (2022/2554)

11.7.1 Artículo 5 – Marco de gobernanza y control interno: exige la asignación formal de responsabilidades de gestión del riesgo de las TIC, funciones de toma de decisiones y canales de reporte. Esta política proporciona la base para la gobernanza de las funciones relacionadas con la seguridad en entornos TIC.

11.8 COBIT 2019

11.8.1 EDM01 – Establecimiento del marco de gobernanza asegurado: esta política garantiza que el SGSI disponga de una estructura de gobernanza claramente definida y alineada con las necesidades de la organización.

11.8.2 EDM02 – Entrega de beneficios asegurada: alinea las actividades de seguridad basadas en funciones con los objetivos estratégicos y operativos, garantizando la rendición de cuentas y resultados medibles.

11.8.3 APO01 – Marco de gestión de I&T gestionado y APO12 – Riesgo gestionado: esta política respalda la gestión estructurada de las funciones de seguridad de la información dentro de un marco más amplio de gobernanza de TI y riesgos.

11.8.4 MEA01 – Supervisar, evaluar y valorar el desempeño: incorpora mecanismos de revisión para verificar que las funciones de gobernanza sean eficaces, estén actualizadas y se apliquen.