					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P02S					Título del documento: **Política P02S 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**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 5	
ISO/IEC 27002:2022	Controles: 5.2, 5.3, 5	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
RGPD de la UE	Artículos 5(2), 32	

1. Propósito

1.1 Esta política establece cómo se asignan, delegan y gestionan las responsabilidades de gobernanza de la seguridad de la información en la organización, con el fin de garantizar el cumplimiento de ISO/IEC 27001:2022 y de otras obligaciones regulatorias aplicables.

1.2 Garantiza la rendición de cuentas en todos los niveles y respalda la eficacia operativa mediante la identificación clara de la persona responsable de cada función relacionada con la seguridad.

1.3 Esta política mejora la preparación para auditorías y refuerza la confianza de los clientes al demostrar una gobernanza formal de la seguridad, incluso en organizaciones con personal técnico limitado o con servicios de TI externalizados.

2. Alcance

2.1 Esta política se aplica a todas las personas que gestionen sistemas o datos de la organización, incluidos:

2.1.1 Propietarios de la empresa y directores generales

2.1.2 Empleados y contratistas

2.1.3 Proveedores externos de servicios de TI o consultores

2.2 Abarca todos los sistemas, entornos y servicios utilizados para tratar, transmitir o almacenar información de la organización o de clientes, incluidos:

2.2.1 Infraestructura de TI de oficina y dispositivos de trabajo remoto

2.2.2 Plataformas en la nube y servicios de correo electrónico

2.2.3 Registros físicos y unidades compartidas

2.3 El alcance incluye tanto las actividades internas como las externalizadas relacionadas con la gobernanza de la seguridad de la información.

3. Objetivos

3.1 Establecer una rendición de cuentas clara para todas las funciones relacionadas con la seguridad, incluidas la gestión de políticas, el control de acceso, la gestión de incidentes y la supervisión.

3.2 Permitir una segregación de funciones eficaz para reducir conflictos de interés o riesgos de fraude.

3.3 Garantizar que las tareas y funciones de seguridad estén claramente documentadas y se revisen periódicamente.

3.4 Facilitar la toma de decisiones informada, el escalado y la supervisión de los riesgos de TI y de seguridad.

3.5 Respaldar la certificación ISO/IEC 27001:2022 y generar confianza entre clientes, socios y auditores.

4. Funciones y responsabilidades

4.1 Director General / Propietario de la empresa

4.1.1 Es responsable último de la implantación y supervisión de esta política.

4.1.2 Aprueba todas las funciones de seguridad, responsabilidades y decisiones de delegación.

4.1.3 Supervisa el cumplimiento y adopta las decisiones finales sobre excepciones a la política y escalados.

4.2 Coordinador de Seguridad designado (si aplica)

4.2.1 Puede ser un miembro del personal o un consultor de confianza.

4.2.2 Esta función puede ser asumida por el Director General o por un proveedor externo en entornos de microempresa.

4.2.3 Presta apoyo en la aplicación diaria del control de acceso, la respuesta ante incidentes o las tareas básicas de seguridad técnica.

4.2.4 Informa directamente al Director General sobre cualquier problema o riesgo 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 Revisión anual

9.1.1 Esta política debe ser revisada por el Director General cada 12 meses para garantizar que sigue reflejando las obligaciones legales, las necesidades operativas y los requisitos de certificación de ISO/IEC 27001.

9.2 Revisiones intermedias

9.2.1 También deben realizarse revisiones cuando:

9.2.1.1 Se produzcan cambios organizativos significativos

9.2.1.2 Se incorpore un nuevo proveedor

9.2.1.3 Se produzca un incidente de seguridad grave

9.2.1.4 Se actualicen normativas como el RGPD de la UE, la Directiva NIS2 de la UE o DORA de la UE

9.3 Control de versiones y documentación

9.3.1 Todas las revisiones deben incluir:

9.3.1.1 Fecha de revisión

9.3.1.2 Resumen de los cambios, en su caso

9.3.1.3 Firma o aprobación documentada del Director General

9.3.1.4 Versiones anteriores archivadas como referencia de auditoría

9.4 Comunicación de cambios

9.4.1 Todas las actualizaciones de la política deben comunicarse sin demora al personal y a los proveedores por correo electrónico, portales internos o comunicaciones formales.

10. Políticas relacionadas y vínculos

10.1 Esta política debe implantarse junto con las siguientes políticas para pymes a fin de garantizar su plena eficacia:

10.1.1 P4S – Política de control de acceso: Define cómo se concede, gestiona y revoca el acceso, directamente vinculado a las funciones asignadas y a la supervisión.

10.1.2 P8S – Política de concienciación y formación en seguridad de la información: Refuerza las responsabilidades y expectativas específicas de cada función.

10.1.3 P17S – Política de protección de datos y privacidad: Describe las obligaciones legales en virtud del RGPD de la UE, que se asignan a las funciones definidas en esta política de gobernanza.

10.1.4 P30S – Política de respuesta ante incidentes: Exige responsabilidades definidas para la notificación, el escalado y la resolución de incidentes.

10.2 En conjunto, estas políticas permiten una aplicación coherente, la rendición de cuentas interna y el cumplimiento externo.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.3 – Funciones, responsabilidades y autoridades de la organización: Exige que las funciones se asignen claramente y cuenten con el apoyo de la alta dirección.

11.2 ISO/IEC 27002

11.2.1 Controles 5.2–5.4: Exigen una documentación clara de las funciones de seguridad de la información, la segregación de funciones y la supervisión por la dirección.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: Establece un programa general de seguridad de la información con responsabilidades definidas.

11.3.2 PL-1 a PL-4: Exigen controles de planificación, incluida la formulación de políticas y la asignación documentada de funciones.

11.3.3 CA-1: Exige funciones definidas de evaluación y autorización.

11.3.4 AC-1: Vincula el control de acceso basado en funciones con las responsabilidades de gobernanza asignadas.

11.4 RGPD de la UE

11.4.1 Artículo 5(2) – Responsabilidad proactiva: Exige que las organizaciones demuestren el cumplimiento mediante funciones y responsabilidades definidas.

11.4.2 Artículo 32 – Seguridad del tratamiento: Hace hincapié en la asignación clara de funciones para proteger los datos personales.

11.5 Directiva NIS de la UE

11.5.1 Artículo 21(2)(a): Exige estructuras de gobernanza que incluyan funciones formalizadas para la gestión del ciberriesgo y de los incidentes.

11.6 DORA de la UE

11.6.1 Artículos 9 y 10: Exigen que las entidades financieras asignen claramente y supervisen las responsabilidades relacionadas con las TIC y la seguridad.

11.7 COBIT 2019

11.7.1 EDM03 – Garantizar la optimización del riesgo: Exige funciones bien definidas y vías de escalado para la gestión del riesgo de seguridad.

11.7.2 APO13 – Gestionar la seguridad: Asigna responsabilidades estratégicas y operativas de seguridad a personas y funciones.

11.7.3 DSS05 – Gestionar los servicios de seguridad: Exige estructura y trazabilidad en las responsabilidades de los servicios de seguridad internos y externos.