					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P01S					Título del documento: **Política de Seguridad de la Información P01S**							
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 5.1, 5.2, 5.3, 6.1, 6.2, 8	Establece el compromiso de la dirección, los requisitos de la política, la asignación de funciones, la evaluación de riesgos y el control operativo
ISO/IEC 27002:2022	Controles 5.1–5	Establece la elaboración de políticas documentadas de seguridad de la información, la asignación de funciones, la segregación de funciones y las responsabilidades de la dirección
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Establece requisitos para el plan del programa de seguridad, la política de planificación de la seguridad, la evaluación y autorización, y el control de acceso
RGPD (UE) 2016/679	Artículo 5.2, artículo 32	Principio de responsabilidad proactiva y medidas de seguridad del tratamiento, especialmente en relación con las funciones documentadas
Directiva (UE) 2022/2555 NIS2	Artículo 21.2.a)	Exige medidas de gestión de riesgos, así como funciones y responsabilidades en materia de ciberseguridad
Reglamento (UE) 2022/2554 DORA	Artículo 9, artículo 10	Exige la asignación de funciones para la gestión del riesgo de las TIC y la continuidad del negocio
COBIT 2019	EDM03, APO13, DSS05	Garantiza la optimización del riesgo, la gestión de la seguridad y la gestión de los servicios de seguridad mediante una asignación clara de funciones

1. Finalidad

1.1 Esta política formaliza el compromiso de la organización con la protección de la información de clientes y de la propia organización mediante la definición clara de responsabilidades y de medidas prácticas de seguridad, adecuadas para organizaciones sin equipos de TI dedicados.

1.2 Garantiza que todos los empleados, contratistas y proveedores de servicios cumplan requisitos exigibles, permitiendo el pleno cumplimiento de los requisitos de certificación de ISO/IEC 27001.

1.3 Esta política permite a la organización generar confianza en los clientes al demostrar de forma clara cómo protegemos su información mediante responsabilidades definidas, procesos estructurados y una sólida rendición de cuentas.

2. Alcance

2.1 Esta política se aplica a todas las personas que acceden a los datos y sistemas de la organización o los gestionan, incluidas:

2.1.1 Propietarios de la empresa y directores generales

2.1.2 Empleados, contratistas y becarios

2.1.3 Proveedores externos de servicios de TI o consultores

2.2 Abarca todos los tipos de información, sistemas y servicios, incluidos:

2.2.1 Registros de la organización, datos de clientes, contraseñas y correos electrónicos

2.2.2 Equipos informáticos, como portátiles y teléfonos

2.2.3 Servicios en la nube utilizados para el almacenamiento de archivos, la comunicación o la gestión financiera

2.2.4 Documentos físicos almacenados en ubicaciones de oficina

2.3 La política se aplica en todos los entornos de trabajo —presenciales, remotos y en la nube— e incluye todos los dispositivos y programas utilizados para tratar o almacenar información de la organización.

3. Objetivos

3.1 Asignar una responsabilidad clara: garantizar que siempre exista una persona responsable de la seguridad de la información. Normalmente, será el Director General o la persona que este designe formalmente.

3.2 Proteger la información de clientes y de la organización: establecer salvaguardas fiables y coherentes para prevenir el uso indebido, la pérdida o el robo de datos sensibles, incluidos registros de clientes y datos financieros.

3.3 Respaldar la certificación ISO/IEC 27001: permitir que la organización demuestre el pleno cumplimiento de los requisitos de ISO/IEC 27001, con preparación para auditoría y aptitud para la certificación sin necesidad de una infraestructura compleja.

3.4 Integrar la seguridad en las operaciones de la organización: incorporar la seguridad de la información a las tareas y decisiones diarias en toda la organización.

3.5 Fomentar la concienciación y la cultura de seguridad: promover que cada empleado comprenda y mantenga las prácticas de seguridad, como el uso de contraseñas robustas y la notificación de actividades sospechosas.

4. Funciones y responsabilidades

4.1 Director General o propietario de la empresa

4.1.1 Asume la plena responsabilidad de la seguridad de la información.

4.1.2 Aprueba y mantiene esta política.

4.1.3 Garantiza que todas las tareas clave de seguridad se gestionen directamente o se deleguen por escrito.

4.1.4 Verifica que toda tarea de seguridad delegada (como la gestión de accesos o la respuesta a incidentes) se ejecute de forma eficaz.

4.1.5 Actúa como punto de contacto predeterminado para todos los asuntos internos y externos relacionados con la seguridad, incluidas auditorías y consultas de clientes.

4.1.6 Debe supervisar el avance respecto de estos objetivos durante la revisión anual. Siempre que sea posible, los objetivos deben ser medibles (por ejemplo, porcentaje de personal formado, número de incidentes notificados, etc.) y revisarse en función de los hallazgos de seguridad y de los cambios en el riesgo.

4.2 Empleado designado (si procede)

4.2.1 Puede asistir al Director General gestionando tareas diarias, como crear cuentas de usuario, retirar accesos a personas que dejan la organización o coordinarse con el proveedor de TI.

4.2.2 Debe estar designado formalmente y disponer de autoridad y herramientas suficientes para ejecutar las tareas.

4.2.3 Informa al Director General de cualquier incidencia.

[... 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 (DG) al menos una vez al año para garantizar el cumplimiento continuado de los requisitos de certificación de ISO/IEC 27001, de los cambios normativos y regulatorios (como el RGPD, la Directiva NIS2 y DORA) y de la evolución de las necesidades de la organización.

9.2 Revisiones extraordinarias

9.2.1 Deben realizarse revisiones adicionales siempre que se produzcan cambios significativos, como:

9.2.1.1 Incidentes de seguridad graves o violaciones de seguridad de los datos.

9.2.1.2 Introducción de nuevos procesos o tecnologías en la organización (por ejemplo, nuevo software, plataformas de trabajo remoto o servicios en la nube).

9.2.1.3 Cambios en los requisitos legales o regulatorios que afecten al tratamiento de la información.

9.3 Documentación de cambios

9.3.1 Todas las revisiones y cambios de la política deben documentarse formalmente, indicando claramente la fecha, la naturaleza de las revisiones y la aprobación del DG.

9.3.2 Debe mantenerse de forma segura un historial de versiones de la política para demostrar su evolución y el cumplimiento durante las auditorías.

9.4 Comunicación de actualizaciones

9.4.1 Todo cambio en esta política debe comunicarse con prontitud a todos los empleados, contratistas y terceros pertinentes.

9.4.2 Las versiones actualizadas de la política deben ser fácilmente accesibles para todo el personal afectado (por ejemplo, compartidas electrónicamente o expuestas físicamente en el lugar de trabajo).

10. Políticas relacionadas y vinculaciones

10.1 Esta política está estrechamente relacionada con otras políticas del conjunto de políticas para pymes de la organización, en concreto:

10.1.1 P2S – Política de funciones y responsabilidades de gobierno: aclara la asignación de funciones y responsabilidades de seguridad.

10.1.2 P4S – Política de control de acceso: define el tratamiento seguro del acceso a la información de la organización.

10.1.3 P8S – Política de concienciación y formación en seguridad de la información: proporciona directrices esenciales para la formación y la concienciación del personal.

10.1.4 P17S – Política de protección de datos y privacidad: garantiza el cumplimiento del RGPD y de otras leyes de protección de datos.

10.1.5 P30S – Política de respuesta a incidentes: describe las acciones detalladas requeridas en respuesta a incidentes de seguridad.

10.2 Estas políticas relacionadas proporcionan directrices operativas claras y deben aplicarse de forma conjunta para lograr el pleno cumplimiento de los requisitos de certificación de ISO/IEC 27001.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.1 – Liderazgo y compromiso: exige el compromiso de la alta dirección y su responsabilidad sobre la eficacia de la seguridad de la información dentro de la organización.

11.1.2 Cláusula 5.2 – Política de seguridad de la información: exige políticas claras y documentadas, alineadas con la estrategia de la organización y con los requisitos de cumplimiento.

11.1.3 Cláusula 5.3 – Funciones y responsabilidades organizativas: define una asignación clara de las responsabilidades de seguridad de la información en toda la organización, esencial para un gobierno eficaz y el cumplimiento en auditoría.

11.1.4 Cláusula 6.1 – Acciones para abordar riesgos y oportunidades: garantiza que los riesgos para la seguridad de la información se identifiquen, evalúen y traten de forma sistemática.

11.1.5 Cláusula 8.1 – Planificación y control operativos: exige que la organización planifique e implante los procesos necesarios para cumplir los objetivos de seguridad de la información y gestionar eficazmente los riesgos asociados.

11.2 Controles 5.1–5 de ISO/IEC 27002:2022

11.2.1 Control 5.1 del Anexo A – Políticas de seguridad de la información: establece la elaboración y comunicación de políticas documentadas de seguridad de la información.

11.2.2 Control 5.2 del Anexo A – Funciones de seguridad de la información: aclara y asigna formalmente las funciones y responsabilidades de seguridad de la información a las partes pertinentes.

11.2.3 Control 5.3 del Anexo A – Segregación de funciones: exige una separación clara de funciones para reducir conflictos de intereses y riesgos de fraude en la gestión de información sensible.

11.2.4 Control 5.4 del Anexo A – Responsabilidades de la dirección: exige que la dirección demuestre su compromiso con la seguridad de la información mediante supervisión activa y asignación de recursos.

11.2.5 Refuerza la necesidad de contar con políticas, funciones, responsabilidades y estructuras de gobierno de la seguridad de la información claramente documentadas, garantizando una gestión coherente y trazabilidad de auditoría en toda la organización.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Plan del programa de seguridad de la información: exige estrategias y políticas documentadas de gobierno de la seguridad de la información, proporcionando un marco para una implantación y gestión coherentes.

11.3.2 PL-1 – Política de planificación de la seguridad: exige una política de planificación de la seguridad de alcance organizativo para orientar la operación segura y la alineación estratégica de las actividades de seguridad de la información.

11.3.3 CA-1 – Política de evaluación y autorización de la seguridad: exige funciones de evaluación y autorización claramente definidas para asegurar la eficacia continuada y el cumplimiento de los requisitos de seguridad de la información.

11.3.4 AC-1 – Política de control de acceso: exige que las organizaciones definan, documenten y apliquen claramente las prácticas y responsabilidades de gestión de accesos.

11.4 RGPD (UE) 2016/679

11.4.1 Artículo 5.2 – Principio de responsabilidad proactiva: exige que las organizaciones demuestren el cumplimiento de los principios de protección de datos, incluidas funciones y políticas documentadas para las responsabilidades de protección de datos.

11.4.2 Artículo 32 – Seguridad del tratamiento: exige la implantación de medidas técnicas y organizativas apropiadas, incluidas responsabilidades de seguridad claramente definidas, para proteger los datos personales frente a violaciones de seguridad y accesos no autorizados.

11.5 Directiva (UE) 2022/2555 NIS2

11.5.1 Artículo 21.2.a) – Medidas de gestión de riesgos: exige mecanismos claros de gobierno, incluidas funciones y responsabilidades definidas para la seguridad de la información, esenciales para gestionar eficazmente los riesgos de ciberseguridad.

11.6 Reglamento (UE) 2022/2554 DORA

11.6.1 Artículo 9 – Gestión del riesgo de las TIC: exige que las organizaciones asignen claramente las funciones y responsabilidades relacionadas con la gestión del riesgo de las TIC, reforzando la resiliencia y la preparación para la continuidad del negocio.

11.6.2 Artículo 10 – Continuidad operativa de las TIC: exige una responsabilidad clara y funciones estructuradas para mantener la resiliencia y la continuidad de las TIC, garantizando que las organizaciones puedan responder de forma fiable a las interrupciones.

11.7 COBIT 2019

11.7.1 EDM03 – Garantizar la optimización del riesgo: subraya la necesidad de responsabilidades y funciones claramente definidas en la gestión de los riesgos de la organización, proporcionando un gobierno sólido y una supervisión eficaz de los riesgos de seguridad de la información.

11.7.2 APO13 – Gestionar la seguridad: exige que las organizaciones establezcan y comuniquen claramente las responsabilidades de gestión de la seguridad, garantizando la alineación con los objetivos de la organización y los requisitos regulatorios.

11.7.3 DSS05 – Gestionar los servicios de seguridad: requiere funciones estructuradas y responsabilidades claras en la gestión de los servicios de seguridad, permitiendo una implantación coherente y la verificación del cumplimiento.