					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P26S					Título del documento: **Política de seguridad de proveedores y terceros - PYME**							
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**

1. Finalidad

1.1 Esta política establece los requisitos de seguridad obligatorios para la contratación, gestión y finalización de las relaciones con terceros y proveedores que acceden a los datos, sistemas o servicios de la organización, o influyen en ellos.

1.2 Garantiza que los proveedores externos, incluidos los proveedores de soporte de TI, operadores de servicios en la nube, desarrolladores de software y contratistas de procesos de negocio, gestionen los activos de la empresa de forma segura y en cumplimiento de las leyes y normas aplicables.

1.3 Esta política reduce riesgos como la fuga de datos, los cambios no autorizados en los sistemas, las sanciones regulatorias o las interrupciones de las operaciones de la organización causadas por acuerdos con terceros inseguros o deficientemente gestionados.

2. Alcance

2.1 Esta política aplica a todos los terceros que:

2.1.1 Proporcionen software, infraestructura, servicios de alojamiento o servicios en la nube

2.1.2 Accedan a sistemas, dispositivos o aplicaciones internos, o los gestionen

2.1.3 Manejen datos, documentos o copias de seguridad de la empresa

2.1.4 Den soporte a las operaciones de la organización, a Recursos Humanos, a finanzas o a servicios de atención al cliente

2.2 También aplica a:

2.2.1 El personal interno implicado en la selección, contratación o supervisión de proveedores

2.2.2 Cualquier persona que gestione el alta de proveedores, contratos, accesos o revisiones

2.2.3 Cualquier sistema o proceso que dependa de componentes o servicios de terceros

3. Objetivos

3.1 Garantizar que todos los proveedores cumplan expectativas de seguridad claramente definidas.

3.2 Exigir que los contratos con proveedores incluyan obligaciones exigibles en materia de seguridad, privacidad y respuesta a incidentes.

3.3 Evaluar y documentar los riesgos de los proveedores antes de la firma de acuerdos o de la concesión de acceso.

3.4 Aplicar revisiones periódicas a los proveedores de alto riesgo o críticos para confirmar el cumplimiento.

3.5 Establecer un proceso formal para excepciones, gestión de incidentes y actualización de contratos.

3.6 Dar soporte al cumplimiento de las obligaciones de ISO/IEC 27001:2022, RGPD de la UE, Directiva NIS2 de la UE y DORA de la UE relacionadas con la gobernanza de proveedores.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Ostenta la responsabilidad final sobre la selección de proveedores y el cumplimiento de la seguridad

4.1.2 Aprueba contratos, excepciones y escalados relacionados con proveedores

4.1.3 Supervisa la respuesta a incidentes y la toma de decisiones cuando los proveedores incumplen sus obligaciones

4.2 Proveedor externo de TI o responsable interno de seguridad

4.2.1 Evalúa el acceso técnico solicitado por los proveedores

4.2.2 Implementa reglas de control de acceso, revisa registros y verifica la gestión segura de los datos

4.2.3 Revisa evidencias de controles de seguridad, certificaciones o resultados de auditoría, cuando corresponda

[... 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 debe revisarse al menos una vez al año por el Director General, con la participación del proveedor de TI o del responsable de proveedores.

9.2 La política también debe revisarse:

9.2.1 Tras cualquier cambio significativo en las obligaciones legales, regulatorias o contractuales

9.2.2 Después de un incidente de seguridad relacionado con un proveedor o de un hallazgo de auditoría

9.2.3 Al incorporar nuevas categorías de proveedores (por ejemplo, plataformas SaaS críticas)

9.3 Todas las actualizaciones deben:

9.3.1 Documentarse con historial de versiones y justificación

9.3.2 Ser aprobadas por el Director General

9.3.3 Comunicarse al personal interno pertinente y a los responsables de proveedores

9.3.4 Conservarse junto con las versiones anteriores conforme a la P14S – Política de conservación y eliminación de datos

10. Políticas relacionadas y vinculaciones

10.1 La eficacia de esta política depende de la coordinación con las siguientes políticas de seguridad de la información para pymes:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: asigna la responsabilidad final de la supervisión de proveedores y de la ejecución contractual.

10.1.2 P4S – Política de control de acceso: proporciona las reglas de restricción de acceso que deben aplicarse cuando se conceda a proveedores acceso a sistemas.

10.1.3 P17S – Política de protección de datos y privacidad: garantiza que los proveedores que tratan datos personales cumplan los principios de protección de datos y los requisitos legales.

10.1.4 P14S – Política de conservación y eliminación de datos: aplica a cualquier dato o registro compartido con proveedores o almacenado por estos, y regula la eliminación segura tras la finalización del contrato.

10.1.5 P30S – Política de respuesta a incidentes: define cómo responder cuando un proveedor cause o esté implicado en un incidente de seguridad, incluidos los procedimientos de escalado y gestión de evidencias.

10.2 Estas políticas funcionan conjuntamente para garantizar que el riesgo de proveedores se controle durante todo el ciclo de vida contractual.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1: requiere la implantación de controles operativos, incluidos los aplicados a las relaciones con terceros y proveedores.

11.2 ISO/IEC 27002

11.2.1 Control 5.19: garantiza que las medidas de seguridad de los proveedores estén alineadas con los requisitos de la organización.

11.2.2 Control 5.20: exige acuerdos formales que contemplen condiciones de seguridad, responsabilidades y obligaciones en caso de brecha de seguridad.

11.2.3 Control 5.21: gestiona los cambios en los servicios de los proveedores que puedan afectar a la postura de seguridad.

11.2.4 Control 5.22: exige la supervisión y revisión de los servicios de los proveedores y de su cumplimiento.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-9: regula la adquisición de sistemas y servicios externos, y exige evaluaciones de riesgos y expectativas definidas.

11.3.2 SA-10: regula la configuración y los procedimientos de cambio relacionados con sistemas gestionados por terceros.

11.3.3 CA-3: exige acuerdos de interconexión para sistemas que involucren entidades externas.

11.3.4 PS-7: especifica la verificación y la responsabilidad respecto del personal externo.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 28: exige contratos de encargo del tratamiento con proveedores que actúen como encargados del tratamiento.

11.4.2 Artículo 32: exige medidas técnicas y organizativas apropiadas para todos los encargados del tratamiento.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(a), (b), (i): exige la gestión de riesgos de la cadena de suministro de TIC y controles sobre terceros.

11.5.2 Artículo 23(1): exige la supervisión documentada de servicios de terceros para entidades esenciales e importantes.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 5(1): exige un marco de gestión del riesgo de las TIC que cubra a todos los proveedores críticos externos.

11.6.2 Artículo 5(2): establece controles contractuales y operativos para las dependencias de servicios TIC.

11.6.3 Artículo 28(1), (2): establece reglas de supervisión para el riesgo de terceros TIC en el sector financiero.

11.7 COBIT 2019

11.7.1 APO10 – «Gestionar los proveedores» define controles de aprovisionamiento y expectativas de gestión de relaciones.

11.7.2 APO12 – «Gestionar el riesgo» integra el riesgo de proveedores en la gobernanza de riesgos de la organización.

11.7.3 DSS05 – «Gestionar los servicios de seguridad» aplica a proveedores externos de servicios y proveedores de servicios gestionados.