					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P26					Título del documento: **Política de seguridad de proveedores y terceros**							
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 8	Planificación y control operacional: requiere controles formales sobre los servicios de terceros que afectan al SGSI
ISO/IEC 27002:2022	Controles 5.19–5.22	Políticas y procedimientos para las relaciones con proveedores; gestión del riesgo de proveedores; gestión de la prestación de servicios de proveedores; supervisión y revisión de proveedores
NIST SP 800-53 Rev. 5	SA-9, SA-10, CA-3, PS-7	Servicios de sistemas externos; gestión de la configuración del desarrollador; interconexiones de sistemas; seguridad del personal de terceros
RGPD de la UE	Artículos 28, 32, 33	Obligaciones del encargado del tratamiento, seguridad del tratamiento, notificación de violaciones de seguridad de los datos personales
Directiva NIS2 de la UE	Artículo 21(2)(e–f)	Gestión de proveedores basada en riesgos y supervisión de la seguridad
DORA de la UE	Artículos 28, 30	Riesgo de terceros de las TIC, supervisión de terceros proveedores críticos de servicios de TIC
COBIT 2019	BAI05, DSS02, MEA03	Gestionar la habilitación del cambio organizativo; gestionar solicitudes de servicio e incidentes; supervisar, evaluar y valorar el cumplimiento

1. Propósito

1.1 Esta política define los requisitos de seguridad de la información para establecer, gestionar y mantener relaciones seguras con terceros proveedores y prestadores de servicios.

1.2 Garantiza que todos los proveedores con acceso a los datos, sistemas o infraestructuras de la organización estén sujetos a controles de seguridad rigurosos, salvaguardas contractuales y supervisión continua durante todo el ciclo de vida del servicio.

1.3 La política respalda los controles 5.19 a 5.22 del anexo A de ISO/IEC 27001 mediante la integración de requisitos de seguridad en los procesos de adquisición, alta, diligencia debida, gestión contractual, supervisión del servicio y terminación.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los terceros proveedores, contratistas, proveedores de servicios en la nube y organizaciones de servicios que traten o accedan a activos de información de la organización

2.1.2 Todas las funciones internas implicadas en la evaluación de proveedores, alta, contratación, gestión de riesgos, supervisión o terminación

2.1.3 Todas las relaciones con proveedores que incluyan acceso a datos sensibles, integración con servicios de producción o soporte a funciones críticas para las operaciones de la organización

2.2 Abarca tanto a los proveedores directos como a sus subcontratistas, cuando resulte aplicable, e incluye software de terceros, infraestructura, soporte y servicios gestionados.

3. Objetivos

3.1 Asegurar que los riesgos de seguridad asociados a los proveedores se identifiquen, evalúen y mitiguen de forma coherente durante todo el ciclo de vida de la relación.

3.2 Integrar requisitos de seguridad normalizados en todos los contratos con proveedores, incluidas las obligaciones de notificación de violaciones de seguridad, las cláusulas de derecho de auditoría y las responsabilidades en materia de protección de datos.

3.3 Exigir una diligencia debida formal y evaluaciones de riesgos documentadas antes de contratar nuevos proveedores o renovar acuerdos de servicio de alto riesgo.

3.4 Establecer mecanismos de monitorización continua del cumplimiento por parte de los proveedores, incluidas revisiones del desempeño, auditorías y escalado de incidentes.

3.5 Gestionar los cambios en los servicios de los proveedores y aplicar una baja segura, así como la devolución o destrucción de datos durante la terminación.

3.6 Alinear los controles de seguridad de terceros con las obligaciones regulatorias y contractuales aplicables, incluidas las derivadas del RGPD de la UE, la Directiva NIS2 de la UE, DORA de la UE e ISO/IEC 27001.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es responsable de esta política y garantiza su alineación con la estrategia global del SGSI, la gestión de riesgos y el cumplimiento.

4.1.2 Aprueba los niveles de clasificación de proveedores, los resultados de las revisiones de seguridad y las excepciones de alto riesgo.

4.1.3 Participa en el escalado de incidentes graves relacionados con proveedores y en las negociaciones contractuales de servicios críticos.

4.2 Adquisiciones y diligencia debida de proveedores

4.2.1 Garantiza que todos los contratos nuevos y renovados con proveedores incorporen cláusulas aprobadas de seguridad y protección de datos.

4.2.2 Mantiene el registro centralizado de proveedores y coordina con Recursos Humanos y Asuntos Jurídicos la documentación de riesgos de terceros.

4.2.3 Inicia los procesos de alta y garantiza su alineación con las evaluaciones de seguridad previas a la contratación.

[... 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 deberá revisarse al menos una vez al año, o antes en caso de:

9.1.1 Cambios materiales en la estrategia de adquisiciones o en el ecosistema de proveedores

9.1.2 Actualizaciones de los marcos legales o regulatorios (p. ej., DORA de la UE, RGPD de la UE)

9.1.3 Incidentes graves de terceros, violaciones de seguridad de los datos o hallazgos de auditoría

9.1.4 Hallazgos procedentes de evaluaciones de riesgos o de entidades externas de certificación

9.2 El proceso de revisión es responsabilidad conjunta del CISO y de las funciones de Adquisiciones, Recursos Humanos, Asuntos Jurídicos y Gestión de Riesgos.

9.3 Todas las revisiones de la política deben documentarse en el registro de control documental del SGSI, estar sujetas a control de versiones y comunicarse a las partes interesadas pertinentes a través de los canales de gobernanza de proveedores y de los programas de concienciación para empleados.

9.4 Las versiones sustituidas deben archivarse durante un período mínimo de tres años para garantizar la trazabilidad y el cumplimiento legal.

10. Políticas relacionadas y vinculaciones

10.1 P1 – Política de Seguridad de la Información. Establece el compromiso general de proteger todas las operaciones de la organización, incluida la dependencia de terceros proveedores y prestadores de servicios externos.

10.2 P6 – Política de Gestión de Riesgos. Orienta la identificación, evaluación y mitigación de los riesgos asociados a las relaciones con terceros, incluidos los riesgos heredados o sistémicos de los ecosistemas de proveedores.

10.3 P17 – Política de Protección de Datos y Privacidad. Se aplica a todos los proveedores que traten datos personales y exige condiciones contractuales adecuadas, salvaguardas para las transferencias y principios de privacidad desde el diseño.

10.4 P4 – Política de Control de Acceso. Regula cómo el personal de terceros obtiene acceso a los sistemas de la organización, aplicando permisos basados en roles, control de sesiones y procedimientos de revocación.

10.5 P22 – Política de Registro de Eventos y Supervisión. Exige que el acceso de proveedores a los sistemas sea supervisado, registrado y revisado, en particular en entornos donde se realicen actividades privilegiadas o centradas en datos.

10.6 P30 – Política de Respuesta a Incidentes. Define los procedimientos de escalado y los requisitos de notificación de violaciones de seguridad para eventos de seguridad originados en proveedores o investigaciones conjuntas que involucren sistemas de terceros.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001: cláusula 8.1 – Planificación y control operacional: requiere controles formales sobre los servicios de terceros que afectan al SGSI.

11.2 ISO/IEC 27002:2022 – controles 5.19 a 5.22:

11.2.1 Control 5.19 del anexo A – Políticas y procedimientos para las relaciones con proveedores: exige controles para gestionar las interacciones con proveedores.

11.2.2 Control 5.20 del anexo A – Gestión del riesgo de proveedores: se centra en la identificación, evaluación y supervisión continua de la postura de seguridad de los proveedores.

11.2.3 Control 5.21 del anexo A – Gestión de la prestación de servicios de proveedores: exige la alineación del desempeño y la seguridad con las expectativas contractuales.

11.2.4 Control 5.22 del anexo A – Supervisión y revisión de proveedores: refuerza la necesidad de validación continua y reevaluación del cumplimiento de terceros.

11.3 NIST SP 800-53 Rev. 5:

11.3.1 SA-9 – Servicios de sistemas externos: define los requisitos de seguridad y riesgo para sistemas operados por entidades externas.

11.3.2 SA-10 – Gestión de la configuración del desarrollador: aplica cuando terceros entregan software o entornos.

11.3.3 CA-3 – Interconexiones de sistemas: exige supervisión y acuerdo sobre los flujos de datos entre sistemas de distintas entidades.

11.3.4 PS-7 – Seguridad del personal de terceros: garantiza que los contratistas y el personal del proveedor sean objeto de verificación y supervisión adecuadas.

11.4 RGPD de la UE (2016/679):

11.4.1 Artículo 28 – Obligaciones del encargado del tratamiento: requiere acuerdos por escrito con los encargados del tratamiento de datos, incluidas medidas técnicas y organizativas (MTO).

11.4.2 Artículo 32 – Seguridad del tratamiento: exige salvaguardas adecuadas tanto por parte de responsables como de encargados.

11.4.3 Artículo 33 – Notificación de una violación de la seguridad de los datos personales: requiere notificación rápida por parte de los proveedores en caso de violación de seguridad.

11.5 Directiva NIS2 de la UE (2022/2555):

11.5.1 Artículo 21(2)(e–f): exige gestión de proveedores basada en riesgos y supervisión de la seguridad, especialmente en las cadenas de suministro digitales de entidades esenciales e importantes.

11.6 DORA de la UE (2022/2554):

11.6.1 Artículo 28 – Riesgo de terceros de las TIC: impone obligaciones de evaluación de riesgos, condiciones contractuales de seguridad y estrategias de salida para proveedores de servicios financieros.

11.6.2 Artículo 30 – Supervisión de terceros proveedores críticos de servicios de TIC: establece expectativas reforzadas de supervisión y control supervisor sobre proveedores clave.

11.7 COBIT 2019:

11.7.1 BAI05 – Gestionar la habilitación del cambio organizativo: garantiza que las transiciones de proveedores se gobiernen de forma segura.

11.7.2 DSS02 – Gestionar solicitudes de servicio e incidentes: aplica a incidencias notificadas por proveedores y a la integración de la gestión de incidentes.

11.7.3 MEA03 – Supervisar, evaluar y valorar el cumplimiento: refuerza la medición del desempeño de los proveedores y la supervisión del cumplimiento.