					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P41					Título del documento: **Política de gestión del riesgo de dependencia de proveedores**							
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 Reforzar las prácticas de seguridad de la cadena de suministro de la organización mediante el establecimiento de un proceso para identificar y gestionar las dependencias críticas de proveedores y prestadores de servicios, de conformidad con lo exigido por el artículo 21(3) de la Directiva NIS2 de la UE y por las evaluaciones de riesgos de la cadena de suministro a escala de la Unión.

1.2 Garantizar que los riesgos derivados de la concentración o de la dependencia de un único proveedor se comprendan y mitiguen, y que cualquier riesgo sectorial específico de la cadena de suministro, según lo señalado por las autoridades conforme al artículo 22 de la Directiva NIS2 de la UE, se incorpore a nuestra gestión de riesgos y a la planificación de la continuidad del negocio.

2. Alcance

2.1 Esta política se aplica a todos los proveedores esenciales y prestadores de servicios de los que la organización depende para sus operaciones críticas, en particular aquellos de la cadena de suministro de TIC (hardware, software, servicios en la nube, telecomunicaciones y servicios gestionados).

2.2 Abarca las funciones internas, incluidas Compras y diligencia debida de proveedores, Gestión de proveedores, Gestión de riesgos y las áreas operativas pertinentes. También involucra a dichos proveedores en la medida necesaria para recabar información sobre riesgos. Se consideran «proveedores críticos» aquellos cuyo fallo o compromiso pueda afectar de forma significativa a nuestra capacidad para prestar servicios o cumplir obligaciones legales.

3. Objetivos

3.1 Obtener visibilidad sobre las dependencias de la cadena de suministro, en particular mediante la identificación de puntos únicos de fallo o de un alto riesgo de concentración en nuestra base de proveedores (por ejemplo, la dependencia de un único proveedor de servicios en la nube para todos los servicios).

3.2 Implantar medidas para reducir y gestionar los riesgos relacionados con proveedores, como la diversificación, los planes de contingencia o la exigencia de controles reforzados al proveedor, fortaleciendo así la resiliencia frente a fallos de proveedores o ataques originados en la cadena de suministro.

3.3 Alinearse con los requisitos de la Directiva NIS2 de la UE mediante la integración, en las decisiones de riesgo de la organización, de los resultados de cualquier evaluación coordinada de riesgos de seguridad de cadenas de suministro críticas conforme al artículo 22, y garantizar que nuestro propio enfoque del riesgo de la cadena de suministro esté documentado y sea demostrable.

4. Funciones y responsabilidades

4.1 Oficina de Gestión de Proveedores (VMO): es responsable del registro de dependencias de proveedores y coordina las evaluaciones de riesgos. Garantiza que, durante el alta y posteriormente con carácter periódico, cada proveedor clave sea evaluado en cuanto a criticidad y nivel de dependencia.

4.2 Gestión de riesgos (Comité de Riesgos Empresariales): revisa el riesgo de concentración y los análisis de dependencia, y respalda las estrategias de tratamiento del riesgo (por ejemplo, aprobar la incorporación de un proveedor alternativo o mantener inventario adicional de componentes críticos). Incorpora el riesgo de la cadena de suministro al Registro de Riesgos corporativo e informa a la Alta Dirección.

[... Las secciones 4.3–8 no están incluidas en esta vista previa. Adquiera el documento completo para acceder al contenido íntegro. ...]

9. Supervisión y auditoría

9.1 El registro de dependencias y las evaluaciones de riesgos serán objeto de auditoría interna con periodicidad anual. La función de auditoría interna verificará que todos los proveedores críticos estén

incluidos, que sus calificaciones de riesgo estén actualizadas y que existan planes de mitigación implantados y en ejecución. También comprobará que se hayan considerado debidamente las aportaciones de evaluaciones externas de riesgos (informes del artículo 22, etc.).

9.2 La eficacia de las medidas de diversificación y contingencia se probará periódicamente. Por ejemplo, podrá realizarse una simulación planificada en la que se asuma el fallo de un proveedor principal, con el fin de poner a prueba nuestros planes de continuidad y medidas alternativas (de forma similar a un simulacro de recuperación ante desastres, pero aplicado a la indisponibilidad de un proveedor). Los resultados de estas pruebas se documentarán y cualquier deficiencia se corregirá.

9.3 Métricas: la función de Gestión de riesgos realizará el seguimiento de métricas como «% de servicios críticos con al menos un proveedor o solución alternativos disponibles» o «las 5 principales dependencias de proveedores y su tendencia de riesgo». Estas métricas se incluirán en los cuadros de mando de riesgos dirigidos a la dirección. Una tendencia descendente del riesgo de dependencia a lo largo del tiempo es un objetivo; si las métricas muestran un aumento de la dependencia, la dirección deberá analizarlo.

10. Revisión y mantenimiento

10.1 Esta política será revisada al menos anualmente por los equipos de Gestión de proveedores y Gestión de riesgos. La revisión incorporará cualquier cambio en el panorama de proveedores (por ejemplo, si un nuevo proveedor pasa a ser crítico o si otro se retira progresivamente) y cualquier nuevo requisito normativo sobre externalización o riesgo de terceros.

10.2 Si las autoridades sectoriales emiten orientaciones actualizadas o si un incidente revela deficiencias (por ejemplo, si una indisponibilidad de un proveedor tiene un impacto mayor del previsto, lo que indicaría que nuestra evaluación de riesgos valoró incorrectamente la dependencia), la política se actualizará para perfeccionar los criterios o las estrategias de mitigación.

10.3 Las versiones revisadas de la política deberán ser aprobadas por la Alta Dirección. Los cambios significativos se comunicarán a todos los departamentos pertinentes, y los materiales de formación se actualizarán en consecuencia para reflejar los nuevos procedimientos o estándares.

11. Políticas relacionadas y vinculaciones

11.1 P01 – Política de Seguridad de la Información. Asigna la responsabilidad proactiva sobre la gobernanza de la dependencia de proveedores.

11.2 P02 – Política de funciones y responsabilidades de gobernanza. Aclara la titularidad de las decisiones sobre riesgo de proveedores.

11.3 P06 – Política de gestión de riesgos. Incorpora el riesgo de concentración en los registros de riesgos corporativos.

11.4 P26 – Política de Seguridad de Terceros y Proveedores. Establece la seguridad base; P41 añade controles de dependencia y concentración.

11.5 P27 – Política de Uso de la Nube. Aplica criterios de dependencia a la adopción de servicios en la nube y a los planes de salida.

11.6 P28 – Política de Desarrollo Externalizado. Cubre los riesgos de dependencia en la ingeniería externalizada.

11.7 P32 – Política de Continuidad del Negocio y Recuperación ante Desastres. Planifica escenarios de indisponibilidad o sustitución de proveedores.

11.8 P37 – Política de Cumplimiento Legal y Normativo. Garantiza que los contratos y obligaciones reflejen controles de dependencia.

12. Referencias

12.1 Directiva NIS2 (UE 2022/2555), artículo 21(3) (exige considerar las vulnerabilidades específicas de cada proveedor directo o prestador de servicios y la calidad de su ciberseguridad, incluidos los resultados de las evaluaciones coordinadas de riesgos de la cadena de suministro)

12.2 Directiva NIS2, artículo 22(1) (evaluaciones coordinadas de riesgos de seguridad de cadenas de suministro críticas a escala de la Unión; informa a las entidades sobre riesgos sectoriales de proveedores)

12.3 Reglamento de Ejecución (UE) 2024/2690 de la Comisión, anexo, sección 5 (requisitos de seguridad de la cadena de suministro para las entidades, incluidos criterios para la selección de proveedores, la diversificación y las obligaciones contractuales)

12.4 Buenas prácticas de ENISA para la ciberseguridad de la cadena de suministro (2022): recomendaciones sobre la identificación de proveedores críticos y la gestión de los riesgos relacionados

12.5 ISO/IEC 27001:2022 / ISO/IEC 27002:2022