					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P28					Título del documento: **Política de Desarrollo Externalizado**							
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**

Normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8.1	N/A
ISO/IEC 27002:2022	Controles 5.19-5.22, 8	N/A
RGPD de la UE	Artículos 28, 32	N/A
Directiva NIS2 de la UE	Artículos 21(2)(a), (h), 23	N/A
DORA de la UE	Artículos 28(1), (2)	N/A
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-10	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Propósito

1.1 Esta política define los controles obligatorios para la externalización del desarrollo de software o sistemas a proveedores externos, contratistas o agencias, garantizando la integración de prácticas seguras a lo largo de todo el ciclo de vida del desarrollo.

1.2 Su objetivo es prevenir vulnerabilidades de seguridad, pérdida de datos, exposición de la propiedad intelectual (PI) e incumplimientos normativos derivados de encargos de desarrollo externo.

1.3 La política establece requisitos de gobernanza de proveedores, estándares de programación segura, gestión de accesos, obligaciones de supervisión y procesos de baja al finalizar el contrato, con el fin de preservar la confidencialidad, integridad y disponibilidad del software desarrollado.

2. Alcance

2.1 Esta política se aplica a todas las unidades de la organización que contraten entidades externas para el desarrollo de software o sistemas, incluidos:

2.1.1 Aplicaciones web, aplicaciones móviles, sistemas embebidos, interfaces de programación de aplicaciones, scripts, flujos de trabajo de automatización o módulos de plataforma

2.1.2 Desarrollo a medida para plataformas internas, sistemas orientados al cliente o productos comerciales

2.1.3 Contrataciones con desarrolladores externos, profesionales autónomos, agencias o equipos offshore

2.2 La política también se aplica a cualquier entidad externa que acceda al código fuente, entornos de prueba o canalizaciones de CI/CD durante el desarrollo.

2.3 Los requisitos son exigibles con independencia del tipo de contrato, la metodología de desarrollo o la ubicación geográfica del proveedor externalizado.

3. Objetivos

3.1 Exigir prácticas de ciclo de vida de desarrollo seguro (SDLC) en todas las contrataciones externalizadas, desde la planificación hasta la validación posterior al despliegue.

3.2 Garantizar que todos los contratos con desarrolladores externos incluyan cláusulas obligatorias sobre protección de datos, programación segura y retención de la PI.

3.3 Definir requisitos de control de acceso, supervisión y auditoría para desarrolladores externos que interactúen con sistemas internos.

3.4 Proteger a la organización frente a riesgos de la cadena de suministro, incumplimientos legales y daños reputacionales relacionados con software desarrollado externamente.

3.5 Mantener el cumplimiento continuo de marcos de seguridad, incluidos ISO/IEC 27001, NIST, RGPD de la UE, Directiva NIS2 de la UE, DORA de la UE y COBIT 2019.

4. Funciones y responsabilidades

4.1 Alta Dirección

4.1.1 Aprueba los proyectos de desarrollo externalizado de alto riesgo y valida las excepciones a la política cuando estén justificadas.

4.1.2 Garantiza que las decisiones de externalización estén alineadas con los objetivos estratégicos y el apetito de riesgo de la organización.

4.2 Director de Seguridad de la Información (CISO)

4.2.1 Aprueba el alta de proveedores desde la perspectiva de seguridad.

4.2.2 Define los requisitos de controles de seguridad para las contrataciones externalizadas y revisa los informes de incidentes.

[... 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 o con mayor frecuencia en las siguientes circunstancias:

9.1.1 Introducción de nuevos modelos de externalización del desarrollo, proveedores o jurisdicciones

9.1.2 Actualizaciones de marcos regulatorios como el RGPD de la UE, la Directiva NIS2 de la UE o DORA de la UE

9.1.3 Tras un incidente de seguridad relacionado con código externalizado, accesos o entregables

9.1.4 Como resultado de hallazgos de auditoría interna o de mejoras del SGSI

9.2 El Director de Seguridad de la Información (CISO) es responsable de iniciar y coordinar la revisión de la política, en consulta con:

9.2.1.1 Asuntos Jurídicos y Compras (para la alineación de la aplicación contractual)

9.2.1.2 Responsables de Proyectos y Productos (para la viabilidad operativa)

9.2.1.3 Seguridad de la Información (para actualizaciones de amenazas y controles)

9.2.1.4 Alta Dirección (para la aprobación final)

9.3 Todas las actualizaciones de la política deben:

9.3.1.1 Estar sujetas a control de versiones y almacenarse en un repositorio documental designado

9.3.1.2 Comunicarse a las partes interesadas implicadas en actividades de desarrollo externalizado

9.3.1.3 Vincularse a cualquier actualización de políticas relacionadas o de documentación procedimental

9.4 Cada versión de la política debe ir acompañada de un registro de cambios para proporcionar trazabilidad de las modificaciones y aprobaciones.

10. Políticas relacionadas y vinculaciones

10.1 Esta política respalda y se complementa con los siguientes documentos relacionados:

10.1.1 P1 - Política de Seguridad de la Información: Establece los principios de seguridad a nivel organizativo aplicables a contextos de desarrollo interno y de terceros.

10.1.2 P5 - Política de Gestión de Cambios: Garantiza que todos los cambios de despliegue relacionados con bases de código externalizadas sean revisados y aprobados antes de su implantación.

10.1.3 P13 - Política de Clasificación y Etiquetado de Datos: Determina cómo se identifican los datos sensibles antes de exponerse a proveedores de desarrollo o repositorios.

10.1.4 P18 - Política de Controles Criptográficos: Orienta sobre cómo deben gestionarse las claves, secretos y credenciales sensibles durante el desarrollo y la entrega.

10.1.5 P24 - Política de Desarrollo Seguro: Define los requisitos de referencia para las prácticas de desarrollo de software internas y externas.

10.1.6 P30 - Política de Respuesta a Incidentes: Regula cómo se escalan, investigan y resuelven las brechas o incidentes de seguridad relacionados con el desarrollo externalizado.

10.1.7 P33 - Política de Supervisión de Auditoría y Cumplimiento: Proporciona requisitos para revisar las actividades de desarrollo externalizado durante auditorías o revisiones de cumplimiento.

11. Normas y marcos de referencia

11.1 Esta política está alineada con marcos y normativas de seguridad reconocidos internacionalmente para garantizar la externalización segura del desarrollo de software y las prácticas de gestión de proveedores.

11.2 ISO/IEC 27001

11.2.1 Cláusula 8.1 - Planificación y control operacional: Exige controles de proceso para el desarrollo seguro y la entrega por terceros.

11.3 ISO/IEC 27002:2022 - controles 5.19 a 5.21, 8.

11.3.1 Anexo A control 5.19 - Gestión de las relaciones con los proveedores: Requiere acuerdos formales con cláusulas de seguridad y cumplimiento.

11.3.2 Anexo A control 5.20 - Tratamiento de la seguridad de la información en los acuerdos con proveedores: Garantiza la incorporación de controles específicos de desarrollo en los contratos.

11.3.3 Anexo A control 5.21 - Gestión de la prestación de servicios de los proveedores: Incluye la supervisión de entregables y riesgos de desarrollo de terceros.

11.3.4 Anexo A control 8.27 - Desarrollo externalizado: Exige requisitos de seguridad definidos y control de acceso sobre el software desarrollado externamente.

11.3.5 Estos controles establecen requisitos estructurados para seleccionar, contratar y supervisar a desarrolladores externalizados, incluidas prácticas de desarrollo seguro, gestión del código y validación del desempeño.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SA-4 - Proceso de adquisición: Requiere que los requisitos de desarrollo seguro se definan en el momento de la adquisición.

11.4.2 SA-9 - Servicios de sistemas externos: Regula cómo los desarrolladores externos interactúan de forma segura con servicios internos.

11.4.3 SA-10 - Gestión de configuraciones del desarrollador: Se alinea con las obligaciones de control de versiones, acceso al código y seguimiento de cambios para equipos externos.

11.5 RGPD de la UE (2016/679)

11.5.1 Artículo 28 - Obligaciones del encargado del tratamiento: Requiere que los contratos con desarrolladores externos especifiquen requisitos de seguridad, control y auditoría para el tratamiento de datos personales.

11.5.2 Artículo 32 - Seguridad del tratamiento: Exige salvaguardas apropiadas (por ejemplo, cifrado, control de acceso) al desarrollar sistemas que tratan datos personales.

11.6 Directiva NIS2 de la UE (2022/2555)

11.6.1 Artículos 21(2)(a), (h), 23: Exigen la aplicación de prácticas de desarrollo seguro en las relaciones con terceros y en las cadenas de suministro digitales, con supervisión y verificación técnica.

11.7 DORA de la UE (2022/2554)

11.7.1 Artículos 28(1), (2): Exigen que las entidades financieras gestionen el riesgo de terceros de las TIC mediante controles contractuales y supervisión del desarrollo seguro, especialmente en desarrollos externalizados críticos.

11.8 COBIT 2019

11.8.1 APO10 - Gestionar proveedores: Establece requisitos estructurados para la evaluación de proveedores, contratos y supervisión del desempeño.

11.8.2 BAI03 - Gestionar la construcción de soluciones: Se corresponde directamente con procesos de SDLC seguro, revisiones de código y validación del desarrollo.

11.8.3 DSS05 - Gestionar los servicios de seguridad: Se alinea con la supervisión y protección de sistemas desarrollados externamente o por terceros.