					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P28S					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**

Alineación con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 5.1, 6.1, 8	Controles del SGSI aplicables y relacionados con proveedores
ISO/IEC 27002:2022	Controles 5.19, 5.20, 8.25–8.27	Controles sobre proveedores y ciclo de vida del desarrollo seguro
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-11, SA-15, SR-3	Requisitos de adquisición, cadena de suministro, desarrollo seguro y acuerdos con proveedores
RGPD de la UE	Artículo 28	Requisitos contractuales y de protección de datos para el tratamiento por terceros
Directiva NIS2 de la UE	Artículo 21(2)(a), (h)	Controles de seguridad de la cadena de suministro y del desarrollo seguro de aplicaciones
DORA de la UE	Artículo 10	Gestión del riesgo de terceros de las TIC, incluido el desarrollo externalizado
COBIT 2019	BAI03, DSS05	Requisitos para el desarrollo externalizado y los proveedores externos de servicios de TI

1. Propósito

1.1 Esta política garantiza que todo desarrollo de software externalizado, ya sea realizado por autónomos, agencias o proveedores externos, se lleve a cabo de forma segura, bajo control contractual y en conformidad con los requisitos legales, regulatorios y de auditoría aplicables.

1.2 Protege a la organización frente a riesgos relacionados con código inseguro, titularidad no definida, exposición de datos y una gestión inadecuada de proveedores, mediante la aplicación de estándares de desarrollo exigibles y la supervisión de proveedores, incluso en ausencia de un departamento de TI dedicado.

1.3 Esta política respalda la certificación ISO/IEC 27001:2022 al establecer expectativas de desarrollo claramente definidas, una responsabilidad proactiva y controles documentados sobre las actividades de desarrollo realizadas por terceros.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Todos los desarrolladores externalizados, incluidos autónomos y agencias de desarrollo.

2.1.2 Cualquier trabajo de desarrollo que implique herramientas internas, sitios web expuestos públicamente, aplicaciones de software o automatización de procesos de la organización.

2.1.3 El personal responsable de seleccionar, gestionar o supervisar a desarrolladores externos.

2.1.4 Cualquier integración de sistemas de terceros, scripting o desarrollo que interactúe con datos o sistemas de la empresa.

2.2 También incluye a cualquier tercero o plataforma con acceso a credenciales de la empresa, repositorios de datos, repositorios de código fuente, entornos de preproducción o sistemas de producción.

3. Objetivos

3.1 Garantizar que todo desarrollo externalizado cumpla los principios de programación segura y que los desarrolladores estén obligados contractualmente a seguir estándares documentados y cláusulas de confidencialidad.

3.2 Establecer la titularidad de todos los entregables —código, activos, credenciales y documentación—, asegurando la transferencia íntegra de derechos a la empresa y una entrega final trazable al cierre del proyecto.

3.3 Prevenir riesgos habituales del desarrollo, incluidos la reutilización de código propietario, los ataques a la cadena de suministro a través de bibliotecas, el uso de frameworks sin soporte y el acceso administrativo no validado.

3.4 Exigir documentación previa al inicio para cada proyecto externalizado, incluidos contratos, acuerdos de confidencialidad y requisitos mínimos de seguridad.

3.5 Proteger los datos de clientes, los sistemas y los procesos internos mediante la aplicación de una supervisión robusta del desarrollo, pruebas posteriores a la entrega y gestión segura del acceso a los sistemas.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba todas las relaciones con proveedores y firma los acuerdos de desarrollo.

4.1.2 Garantiza que todo desarrollo externalizado cumpla esta política.

4.1.3 Elimina el acceso a los sistemas de la empresa tras la finalización del proyecto.

4.1.4 Revisa la documentación y los resultados posteriores a la entrega.

4.2 Responsable del Proyecto (normalmente un empleado interno o coordinador designado)

4.2.1 Gestiona la coordinación diaria con el desarrollador externo.

4.2.2 Verifica que se cumplan los requisitos funcionales y que los entregables hayan sido probados.

4.2.3 Garantiza la entrega segura del código y de las credenciales.

4.2.4 Notifica al DG cualquier problema o incidente relacionado con el desarrollo.

[... 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. La revisión garantiza que siga cumpliendo:

9.1.1.1 Los requisitos de certificación ISO/IEC 27001.

9.1.1.2 Los cambios en las obligaciones legales (por ejemplo, artículo 28 del RGPD de la UE, artículo 10 de DORA de la UE).

9.1.1.3 Las prácticas actuales de desarrollo propias de una pyme y los riesgos de terceros.

9.2 Revisiones intermedias

9.2.1 También deben realizarse revisiones de la política cuando:

9.2.1.1 Se incorpore un nuevo proveedor o plataforma de desarrollo externalizado.

9.2.1.2 Se produzca un incidente significativo relacionado con el desarrollo externalizado.

9.2.1.3 Existan cambios materiales en las herramientas, plataformas o entornos utilizados.

9.3 Proceso de revisión

9.3.1 El DG es responsable de:

9.3.1.1 Verificar que los contratos, los acuerdos de confidencialidad y los procesos de control de acceso sigan siendo eficaces.

9.3.1.2 Confirmar que los proveedores y autónomos actuales estén alineados con la política.

9.3.1.3 Revisar los términos en función de la retroalimentación de los usuarios procedente de proyectos o incidentes anteriores.

9.4 Control de versiones y comunicación

9.4.1 Todos los cambios deben:

9.4.1.1 Registrarse con la fecha, el motivo y la descripción del cambio.

9.4.1.2 Ser aprobados por el DG y añadirse al historial de versiones.

9.4.1.3 Comunicarse a todo el personal o responsables de proyecto que trabajen con desarrolladores externos.

9.4.1.4 Redistribuirse a todos los proveedores y terceros afectados cuando sea necesario.

10. Políticas relacionadas y vinculaciones

10.1 Esta política respalda directamente y depende de la implantación de las siguientes políticas alineadas con pymes:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: aclara quién es responsable de la aprobación de proveedores, el control de acceso y la aceptación del riesgo al utilizar desarrolladores externalizados.

10.1.2 P4S – Política de control de acceso: define la creación, restricción y terminación adecuadas de cuentas de usuario y del acceso administrativo utilizados durante el desarrollo externalizado.

10.1.3 P8S – Política de concienciación y formación en seguridad de la información: garantiza que el personal interno comprenda cómo coordinarse de forma segura con desarrolladores externos, incluido el manejo de credenciales y archivos de proyecto.

10.1.4 P17S – Política de protección de datos y privacidad: establece requisitos legales y de seguridad para el tratamiento de datos personales que puedan ser tratados por desarrolladores externalizados conforme al RGPD de la UE.

10.1.5 P24S – Política de desarrollo seguro: especifica cómo el desarrollo interno y externo debe seguir prácticas de programación segura y validación de bibliotecas y frameworks.

10.1.6 P30S – Política de respuesta a incidentes: es obligatoria cuando el desarrollo externalizado da lugar a incidentes de seguridad o vulnerabilidades, y guía la investigación coordinada y la remediación.

10.2 Estas políticas deben implantarse en paralelo para garantizar que el desarrollo externalizado no genere riesgos no gestionados ni incumpla las obligaciones de cumplimiento de una pyme.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1: las organizaciones deben evaluar y tratar los riesgos de seguridad de la información asociados a los proveedores.

11.1.2 Cláusula 8.1: exige planificación y control operacional, incluidos los servicios de terceros como el desarrollo externalizado.

11.2 ISO/IEC 27002

11.2.1 Control 5.19: recomienda evaluar la capacidad de los proveedores para cumplir los requisitos de seguridad de la información.

11.2.2 Control 5.20: fomenta la supervisión y revisión periódicas de los servicios de terceros.

11.2.3 Controles 8.25–8.27: describen prácticas del ciclo de vida del desarrollo seguro aplicables al desarrollo externalizado.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-4: exige que las estrategias de adquisición incluyan medidas de seguridad de la información.

11.3.2 SA-9: aborda el desarrollo de sistemas externos y los riesgos de la cadena de suministro.

11.3.3 SA-11: define prácticas de desarrollo seguro, incluidas la revisión de código y la remediación de fallos.

11.3.4 SA-15: fomenta el uso de herramientas automatizadas para la detección de fallos y el aseguramiento del software.

11.3.5 SR-3: exige que los acuerdos con proveedores incluyan requisitos de ciberseguridad.

11.4 Reglamento General de Protección de Datos de la UE (RGPD)

11.4.1 Artículo 28: exige contratos con encargados del tratamiento externos para garantizar salvaguardas adecuadas de protección de datos, aplicable directamente a desarrolladores que traten o accedan a datos personales.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(a), (h): exige controles de seguridad de la cadena de suministro y prácticas de desarrollo seguro de software para proveedores de servicios digitales incluidos en el ámbito de aplicación, incluidas las pymes cuando corresponda.

11.6 DORA de la UE

11.6.1 Artículo 10: exige la gestión del riesgo de terceros de las TIC, incluidos acuerdos de desarrollo, obligaciones de seguridad y controles de riesgo relacionados con proveedores externos.

11.7 COBIT 2019

11.7.1 BAI03 – Gestionar la identificación y construcción de soluciones: garantiza que el desarrollo externalizado cumpla los requisitos de la organización y las expectativas de seguridad.

11.7.2 DSS05 – Gestionar los servicios de seguridad: exige que los servicios externos de seguridad y los proveedores de desarrollo operen bajo reglas de seguridad aplicadas y supervisión.