					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P24S					Título del documento: **Política de Desarrollo Seguro**							
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**

Aviso legal (derechos de autor y restricciones de uso)

(C) 2025 Clarysec LLC. All rights reserved.

Este documento es propiedad intelectual de Clarysec LLC. Ninguna parte de este documento podrá copiarse, reutilizarse, distribuirse ni modificarse con fines comerciales o de implantación sin autorización previa y expresa por escrito.

El uso no autorizado está estrictamente prohibido y puede dar lugar a acciones legales.

Para cuestiones de licenciamiento, contacte con: info@clarysec.com

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	Controles de seguridad relevantes para las prácticas operativas, incluido el desarrollo seguro
ISO/IEC 27002:2022	Controles 8.25–8.27	Cubre el ciclo de vida de desarrollo seguro, las pruebas y las responsabilidades de seguridad de los desarrolladores externos
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Aborda el ciclo de vida de desarrollo de software seguro, el control de acceso y la gestión de vulnerabilidades en el desarrollo
RGPD de la UE	Artículo 25	Exige privacidad desde el diseño y por defecto en el desarrollo de software
Directiva NIS2 de la UE	Artículo 21(2)(a), (e), (h)	Exige políticas de desarrollo seguro, supervisión del uso de código abierto y documentación de las medidas de mitigación
DORA de la UE	Artículos 6(7), 9(1)(c), 10(2)(c)	Seguridad del ciclo de vida para sistemas TIC críticos en el sector financiero
COBIT 2019	BAI	Marco para una gestión del desarrollo seguro estructurada, trazable y resiliente

1. Propósito

1.1 Esta política garantiza que todo software, script y herramienta web creada o modificada por la organización o por sus socios externos se desarrolle de forma segura, minimizando el riesgo de vulnerabilidades, accesos no autorizados a los datos o interrupciones operativas.

1.2 Define reglas obligatorias de desarrollo seguro y prácticas de programación que deben seguir todos los desarrolladores internos, contratistas y proveedores, con independencia del tamaño o la complejidad del proyecto.

1.3 Esta política tiene por objeto proteger los datos de los clientes, prevenir brechas de seguridad y garantizar que el software desarrollado o personalizado por o para la organización pueda superar auditorías de seguridad, cumplir los requisitos legales aplicables (p. ej., RGPD de la UE, Directiva NIS2 de la UE, DORA de la UE) y respaldar la certificación ISO/IEC 27001.

2. Alcance

2.1 Esta política se aplica a todas las personas y entidades que participen en el desarrollo, la personalización, el despliegue o la gestión de los siguientes elementos en nombre de la organización:

2.1.1 Sitios web, aplicaciones o herramientas de automatización

2.1.2 Scripts o software desarrollados internamente

2.1.3 Código creado por desarrolladores externos o trabajadores autónomos

2.1.4 Complementos, bibliotecas y componentes de software integrados en sistemas de producción

2.2 Cubre todos los entornos utilizados en actividades de desarrollo, incluidos:

2.2.1 Entornos de desarrollo y pruebas

2.2.2 Entornos de preproducción y preproducción avanzada

2.2.3 Sistemas de producción utilizados para ejecutar código desarrollado a medida

2.3 La política también regula el tratamiento de datos durante el desarrollo y el despliegue, especialmente cualquier uso de datos de producción en sistemas no productivos.

3. Objetivos

3.1 Prevenir la introducción de fallos de seguridad o vulnerabilidades en software personalizado o desarrollado por terceros.

3.2 Garantizar que las prácticas de programación segura y la prevención de vulnerabilidades se integren en cada fase del ciclo de vida del desarrollo de software.

3.3 Reducir los riesgos asociados al uso de componentes de código abierto o de terceros, exigiendo su validación y seguimiento adecuados.

3.4 Exigir la revisión formal del código y las pruebas de seguridad de las aplicaciones antes de su liberación.

3.5 Controlar el acceso a los entornos de desarrollo y garantizar su separación de los sistemas de producción en explotación.

3.6 Cumplir los requisitos obligatorios establecidos por normas y reglamentos internacionales (p. ej., ISO/IEC 27001, RGPD de la UE, DORA de la UE, Directiva NIS2 de la UE).

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Aprueba esta política y asume su titularidad.

4.1.2 Garantiza que todo desarrollo de software, interno o externalizado, cumpla esta política.

4.1.3 Revisa y firma los contratos de desarrollo o de servicios que incluyan cláusulas de desarrollo seguro.

4.1.4 Verifica el cumplimiento de los proveedores mediante revisiones periódicas o solicitando evidencias de seguridad.

4.2 Desarrollador interno o responsable de la aplicación

4.2.1 Sigue prácticas seguras de programación y despliegue.

4.2.2 Aplica la lista de verificación de desarrollo seguro a cada proyecto.

4.2.3 Valida la seguridad de cualquier componente de código abierto o de terceros utilizado.

4.2.4 Informa de inmediato al Director General de cualquier vulnerabilidad detectada.

[... 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 ser revisada por el Director General al menos una vez al año para:

9.1.1 Verificar el cumplimiento continuado de ISO/IEC 27001, RGPD de la UE, Directiva NIS2 de la UE y DORA de la UE

9.1.2 Reflejar amenazas actualizadas o cambios en las mejores prácticas de desarrollo seguro

9.1.3 Garantizar la compatibilidad con nuevas herramientas, plataformas o relaciones con proveedores

9.2 Las revisiones intermedias deben activarse por:

9.2.1 Cualquier incidente de seguridad del software notificado

9.2.2 La introducción de un nuevo marco de desarrollo o plataforma de alojamiento

9.2.3 Un cambio en los socios externos de desarrollo

9.2.4 Actualizaciones regulatorias que afecten a las obligaciones de software o seguridad

9.3 Todos los cambios en esta política deben:

9.3.1 Documentarse con la fecha, el resumen del cambio y la aprobación del Director General

9.3.2 Comunicarse con claridad a todo el personal de desarrollo interno y externo

9.3.3 Conservarse como parte del control de versiones de políticas y del historial de versiones de la organización

9.4 Las versiones actualizadas deben estar fácilmente accesibles, ya sea mediante plataformas internas, documentación impresa o servicios en la nube accesibles para los proveedores.

10. Políticas relacionadas y vinculaciones

10.1 Esta política respalda y depende de la implantación satisfactoria de varias otras políticas para pymes:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: establece la responsabilidad proactiva para asignar y verificar controles de seguridad del desarrollo en proyectos y proveedores.

10.1.2 P4S – Política de control de acceso: proporciona reglas básicas para limitar el acceso a entornos de desarrollo y repositorios de código, incluida la segregación de funciones.

10.1.3 P8S – Política de concienciación y formación en seguridad de la información: garantiza que los desarrolladores internos y contratistas comprendan las prácticas de programación segura y las responsabilidades de seguridad asociadas.

10.1.4 P17S – Política de protección de datos y privacidad: aclara cómo deben manejarse los datos personales durante los procesos de desarrollo, pruebas y registro de eventos para cumplir el RGPD de la UE.

10.1.5 P30S – Política de respuesta a incidentes: define cómo deben notificarse, evaluarse y remediarse los incidentes de seguridad relacionados con el desarrollo, incluidas las exposiciones relacionadas con el código.

10.2 Todas estas políticas actúan conjuntamente para garantizar que el desarrollo seguro sea viable y verificable, incluso en una pyme o en una organización con capacidad técnica limitada.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 8.1 exige la implantación de controles operativos, incluido el desarrollo seguro, alineados con los objetivos de negocio y la postura de riesgo.

11.2 ISO/IEC 27002

11.2.1 El control 8.25 recomienda integrar la seguridad en todo el ciclo de vida del software, incluido el control del código fuente, el control de versiones y el acceso de los desarrolladores.

11.2.2 El control 8.26 especifica métodos para las pruebas de aplicaciones y la verificación de la funcionalidad de seguridad antes de la puesta en producción.

11.2.3 El control 8.27 exige que los desarrolladores externos se adhieran a los mismos estándares de desarrollo y que sus responsabilidades de seguridad estén claramente definidas.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 a SA-15 definen procesos de desarrollo seguro, incluido el control de acceso de los desarrolladores, las pruebas, el modelado de amenazas y la documentación.

11.3.2 SI-10 exige que los desarrolladores identifiquen y mitiguen debilidades comunes del software y utilicen herramientas automatizadas cuando corresponda.

11.4 RGPD de la UE (2016/679)

11.4.1 El artículo 25, «privacidad desde el diseño y por defecto», exige integrar protecciones de seguridad y privacidad durante el diseño y desarrollo del software, especialmente cuando se traten datos personales.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 El artículo 21(2)(a), (e) y (h) exige políticas de desarrollo seguro, supervisión del uso de código abierto y mitigación documentada de los riesgos relacionados con las aplicaciones en entidades esenciales e importantes.

11.6 DORA de la UE (2022/2554)

11.6.1 Los artículos 6(7), 9(1)(c) y 10(2)(c) imponen obligaciones de seguridad del ciclo de vida de desarrollo para entidades del sector financiero, incluidas las pymes, en particular para sistemas TIC críticos.

11.7 COBIT 2019

11.7.1 BAI03, «Gestionar la identificación y construcción de soluciones», respalda la implantación de controles de desarrollo estructurados que hacen hincapié en la seguridad, la trazabilidad y la resiliencia, adaptados a las limitaciones de las pymes.