					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P24					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**

1. Propósito

1.1 Esta política establece los requisitos de seguridad obligatorios para las actividades de desarrollo de software y sistemas dentro de la organización, incluidos los proyectos internos, el desarrollo externalizado y la integración de código de terceros.

1.2 El objetivo es garantizar que la seguridad se integre en todo el ciclo de vida del desarrollo de software (SDLC) y que las vulnerabilidades se identifiquen, mitiguen y prevengan antes del despliegue en producción.

1.3 Esta política respalda la aplicación de la cláusula 8.1 de ISO/IEC 27001:2022 y de los controles 8.25–8.28 del anexo A mediante la estandarización de la gobernanza del desarrollo seguro, las prácticas de validación de código y la supervisión del desarrollo realizado por terceros.

2. Alcance

2.1 Esta política se aplica a todos los elementos siguientes:

2.1.1 Software, aplicaciones, scripts, integraciones y herramientas de automatización desarrollados interna o externamente

2.1.2 Equipos de desarrollo, propietarios de producto, equipos DevOps, QA, arquitectos, responsables de proyecto y contratistas

2.1.3 Entornos del ciclo de vida del desarrollo de software (SDLC), incluidos los sistemas de desarrollo, pruebas, preproducción y puesta en producción

2.1.4 Componentes de código abierto y de terceros integrados en aplicaciones internas

2.1.5 Software desplegado en instalaciones propias y en entornos de nube privada, híbrida o pública

2.2 Todos los usuarios y entidades que participen en el desarrollo, las pruebas o el despliegue de sistemas en el contexto de la organización están sujetos a esta política, incluidos los proveedores de servicios gestionados y los proveedores de plataformas.

3. Objetivos

3.1 Integrar controles de seguridad en todas las fases del desarrollo de software, desde el diseño hasta el despliegue, garantizando una reducción proactiva y continua del riesgo.

3.2 Prevenir la introducción de vulnerabilidades explotables, como fallos de inyección, autenticación insegura y exposición a debilidades conocidas de terceros.

3.3 Establecer y aplicar prácticas de programación segura alineadas con OWASP, SANS CWE y guías específicas de cada marco tecnológico.

3.4 Garantizar que todo el código se someta a revisión por pares, análisis automatizado y validación de seguridad antes del despliegue.

3.5 Gestionar los riesgos de desarrollo derivados de actividades externalizadas, la inclusión de código de terceros y la reutilización de software de código abierto.

3.6 Proteger los entornos de desarrollo, pruebas y preproducción frente a accesos no autorizados y evitar el uso de datos de producción sin enmascaramiento o anonimización aprobados.

3.7 Promover la concienciación en seguridad entre desarrolladores, propietarios de producto y profesionales de aseguramiento de la calidad mediante formación basada en roles y actualizaciones continuas sobre amenazas emergentes.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es el responsable de esta política y garantiza que los requisitos de desarrollo seguro se apliquen en toda la organización.

4.1.2 Aprueba los estándares de programación segura y los acuerdos de desarrollo con terceros.

4.1.3 Valida las decisiones de tratamiento de riesgos relativas a vulnerabilidades no resueltas o aplazadas.

4.2 Responsable de Seguridad de Aplicaciones / Responsable de DevSecOps

4.2.1 Desarrolla, mantiene y promueve las directrices de programación segura.

4.2.2 Integra pruebas de seguridad estáticas y dinámicas en las canalizaciones de CI/CD.

4.2.3 Realiza revisiones de seguridad del código y define las acciones de remediación obligatorias.

[... 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 anualmente, o con mayor frecuencia, en respuesta a:

9.1.1 Revisiones significativas de las metodologías de desarrollo o de las herramientas DevOps

9.1.2 Incidentes materiales de seguridad derivados de vulnerabilidades en aplicaciones

9.1.3 Cambios en los requisitos reglamentarios relacionados con el software seguro (por ejemplo, RGPD de la UE, DORA de la UE)

9.1.4 Nuevos estándares del sector o inteligencia de amenazas (por ejemplo, OWASP Top 10, SLSA, MITRE CWE)

9.2 La revisión de la política debe estar dirigida por el Responsable de Seguridad de Aplicaciones en coordinación con el Director de Seguridad de la Información (CISO), los arquitectos de software, la dirección de QA y el área jurídica, cuando existan implicaciones derivadas del código de terceros.

9.3 Cualquier revisión debe registrarse en el registro de control documental del SGSI, mantenerse sujeta a control de versiones y comunicarse a los equipos afectados mediante notas de versión o formación obligatoria.

9.4 Las versiones anteriores deben conservarse en el repositorio de archivo para garantizar la trazabilidad jurídica y de auditoría.

10. Políticas relacionadas y vinculaciones

10.1 P1 – Política de Seguridad de la Información. Establece el mandato estratégico para integrar la seguridad en todos los sistemas de información, del que el desarrollo seguro constituye un control operativo fundamental.

10.2 P4 – Política de Control de Acceso. Define las medidas de control para restringir el acceso a los entornos de desarrollo, repositorios, herramientas de compilación y canalizaciones de CI/CD.

10.3 P5 – Política de Gestión de Cambios. Garantiza que los cambios de código, las versiones y los despliegues estén sujetos a la aprobación adecuada, a la planificación de la reversión y a la verificación posterior al despliegue.

10.4 P12 – Política de Gestión de Activos. Respalda el inventario de entornos de desarrollo, repositorios de código fuente y sistemas de compilación como activos gestionados sujetos a clasificación y protección.

10.5 P22 – Política de Registro de Eventos y Supervisión. Aplica a las canalizaciones de desarrollo, garantizando que los procesos de compilación, las promociones de código y los eventos de despliegue se registren, supervisen y analicen para detectar anomalías de seguridad.

10.6 P30 – Política de Respuesta a Incidentes. Proporciona el marco para analizar y responder a fallos de seguridad detectados después del despliegue o durante las pruebas de seguridad de aplicaciones.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Planificación y control operacional: exige la integración de procesos y controles de desarrollo seguro en las operaciones.

11.2 ISO/IEC 27002:2022 – Controles 8.25–8.28

11.2.1 Control 8.25 del anexo A – Ciclo de vida de desarrollo seguro: exige la inclusión formal de la seguridad en el diseño y desarrollo de software.

11.2.2 Control 8.26 del anexo A – Requisitos de seguridad de las aplicaciones: exige la definición de prácticas de programación segura y de criterios de aceptación de seguridad.

11.2.3 Control 8.27 del anexo A – Arquitectura segura de sistemas y principios de ingeniería: exige la aplicación de principios de diseño seguro y la mitigación de debilidades conocidas.

11.2.4 Control 8.28 del anexo A – Codificación segura: exige la aplicación de prácticas de codificación segura a lo largo del desarrollo del software.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 a SA-15: establecen prácticas estructuradas de desarrollo seguro de aplicaciones, incluidos requisitos de diseño, integridad del código y pruebas.

11.3.2 SI-10 – Validación de entradas de información: aborda controles de programación segura.

11.3.3 SR-3 – Protección de la cadena de suministro: exige la evaluación de software de terceros, componentes y proveedores de desarrollo.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 25 – Protección de datos desde el diseño y por defecto: exige integrar la seguridad y la privacidad en el desarrollo de sistemas.

11.4.2 Artículo 32 – Seguridad del tratamiento: respalda medidas técnicas como la validación de entradas, los controles de acceso y el despliegue seguro.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(e–f): exige prácticas de desarrollo de software que incluyan la gestión de vulnerabilidades, la seguridad del código y la notificación de incidentes.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 9 – Gestión del riesgo de las TIC: exige prácticas de desarrollo seguro para entidades financieras, incluidos controles de calidad del software y remediación de defectos.

11.6.2 Artículo 10 – Continuidad del negocio y pruebas: promueve pruebas y validación rigurosas de los sistemas TIC, incluidas las aplicaciones.

11.7 COBIT 2019

11.7.1 BAI03 – Gestionar la identificación y construcción de soluciones: rige el diseño, el desarrollo y la integración de la seguridad en nuevas soluciones.

11.7.2 BAI07 – Gestionar la aceptación del cambio y la transición: garantiza el despliegue seguro y la evaluación posterior al despliegue.

11.7.3 DSS05 – Gestionar los servicios de seguridad: aplica la validación de seguridad al software y a la prestación de servicios.