					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P25					Título del documento: **Política de Requisitos de Seguridad de las Aplicaciones**							
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	Cláusula 8	—
ISO/IEC 27002:2022	Controles 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
RGPD de la UE	Artículos 25, 32	—
Directiva NIS2 de la UE	Artículos 21(2)(f), 23	—
DORA de la UE	Artículos 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Propósito

1.1 Esta política define los requisitos obligatorios de seguridad en la capa de aplicación para el software desarrollado, adquirido, integrado o desplegado por la organización. Garantiza que todas las aplicaciones se diseñen, implementen y mantengan de conformidad con los principios de desarrollo seguro, las obligaciones reglamentarias y el apetito de riesgo de la organización.

1.2 La política exige la incorporación de la seguridad a lo largo de todo el ciclo de vida de la aplicación, abarcando la autenticación de usuarios, la gestión de datos, la protección de interfaces y la interacción segura con interfaces de programación de aplicaciones y servicios.

1.3 Mediante la adopción de esta política, la organización pretende prevenir la introducción de vulnerabilidades de software, proteger los datos sensibles y garantizar la trazabilidad y la resiliencia frente a la explotación y el uso indebido.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Aplicaciones desarrolladas internamente o adquiridas externamente, incluidas las soluciones SaaS y las herramientas desarrolladas a medida.

2.1.2 Aplicaciones que dan soporte a operaciones críticas de la organización, al acceso de clientes o al tratamiento de datos regulados.

2.1.3 Equipos de desarrollo, DevOps, QA, producto y seguridad.

2.1.4 Terceros desarrolladores, proveedores de software y socios de integración con acceso a aplicaciones de la organización o a interfaces de programación de aplicaciones.

2.2 Se aplica a todos los entornos: desarrollo, pruebas, preproducción, producción y recuperación ante desastres, con independencia de si están alojados en instalaciones propias, en centros de datos privados o en entornos de nube pública.

3. Objetivos

3.1 Definir requisitos base de seguridad, funcionales y no funcionales, que deben cumplir todas las aplicaciones, con independencia del método de desarrollo o de la pila tecnológica utilizada.

3.2 Garantizar la integración de protecciones en la capa de aplicación, incluidas la validación de entradas, la codificación de salidas, la gestión de errores y la seguridad de las sesiones.

3.3 Exigir la implementación segura de mecanismos de autenticación, autorización y control de acceso alineados con las políticas de gestión de identidades y accesos de la organización.

3.4 Exigir la interacción segura con interfaces de programación de aplicaciones, interfaces web y componentes de terceros mediante el uso de hardware, protocolos y controles de seguridad aprobados.

3.5 Permitir la detección temprana y la mitigación de vulnerabilidades mediante análisis estático y dinámico, revisión de código y modelado de amenazas.

3.6 Proteger los datos sensibles de conformidad con los requisitos reglamentarios, aplicando cifrado, clasificación y reglas de conservación de datos.

3.7 Garantizar la validación continua de la postura de seguridad de las aplicaciones tras el despliegue, mediante pruebas, supervisión y preparación para auditorías.

4. Funciones y responsabilidades

4.1 Director de Seguridad de la Información (CISO)

4.1.1 Es el responsable de esta política y garantiza su alineación con la estrategia de seguridad de la información y la postura de riesgo de la organización.

4.1.2 Aprueba los requisitos de seguridad de las aplicaciones y exige controles obligatorios en las funciones de desarrollo y adquisición.

4.2 Responsable de Seguridad de Aplicaciones / Responsable de DevSecOps

4.2.1 Define los controles de seguridad de referencia y las metodologías de prueba para los componentes de las aplicaciones.

4.2.2 Supervisa la integración segura de herramientas como SAST, DAST, IAST y SCA en el proceso de entrega de software.

4.2.3 Mantiene la Lista de Verificación de Requisitos de Seguridad de las Aplicaciones y los criterios de validación.

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

9.1.1 Divulgaciones de vulnerabilidades críticas que afecten a marcos de trabajo o dependencias de uso común.

9.1.2 Actualizaciones de las obligaciones reglamentarias en materia de seguridad de aplicaciones, por ejemplo, la Directiva NIS2 de la UE y DORA de la UE.

9.1.3 Cambios importantes en las prácticas de desarrollo de software, el conjunto de herramientas o la arquitectura de nube de la organización.

9.1.4 Hallazgos de auditorías internas o pruebas de penetración externas.

9.2 La revisión deberá estar dirigida por el Responsable de Seguridad de Aplicaciones, en coordinación con el CISO, Ingeniería DevOps, Asuntos Jurídicos, Adquisiciones y los responsables de QA.

9.3 Todas las revisiones deberán quedar sujetas a control de versiones en el Registro de Control Documental del SGSI y distribuirse a todos los equipos de desarrollo y producto afectados.

9.4 Las versiones sustituidas deberán archivarse durante un periodo no inferior a tres años para garantizar la trazabilidad, la capacidad de auditoría y el apoyo a las investigaciones de brechas de seguridad.

10. Políticas relacionadas y vinculaciones

10.1 P1 – Política de Seguridad de la Información. Establece la base para proteger los sistemas y los datos, en cuyo marco se exigen controles a nivel de aplicación para prevenir accesos no autorizados, fuga de datos y explotación.

10.2 P4 – Política de Control de Acceso. Define los estándares de gestión de identidad y sesiones que deben aplicar todas las aplicaciones, incluida la autenticación robusta, el principio de mínimo privilegio y los requisitos de revisión de accesos.

10.3 P5 – Política de Gestión de Cambios. Regula la promoción de código y configuraciones de aplicaciones a entornos de producción, garantizando que los cambios no autorizados o no probados se bloqueen.

10.4 P17 – Política de Protección de Datos y Privacidad. Exige que las aplicaciones implementen privacidad desde el diseño y garanticen el tratamiento lícito, el cifrado y la conservación de datos personales y sensibles en todos los entornos.

10.5 P24 – Política de Desarrollo Seguro. Proporciona el marco general para incorporar la seguridad al SDLC, del que esta política define los requisitos concretos y los controles técnicos que deben implantarse en la capa de aplicación.

10.6 P30 – Política de Respuesta a Incidentes. Exige una gestión estructurada de los incidentes de seguridad de aplicaciones, incluidas las vulnerabilidades identificadas tras el despliegue o durante pruebas de penetración, y establece los procedimientos de escalado, contención y recuperación.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001:2022

11.1.1 Cláusula 8.1 – Planificación y control operacional: exige que la seguridad de las aplicaciones se incorpore a los procesos y sistemas para garantizar la confidencialidad, integridad y disponibilidad.

11.2 ISO/IEC 27002:2022

11.2.1 Controles 8.25–8.26: detallan las expectativas para la seguridad en la capa de aplicación, incluidas las prácticas de programación segura, el modelado de amenazas, los controles arquitectónicos y la validación de software de terceros.

11.2.2 Anexo A, control 8.25 – Ciclo de vida de desarrollo seguro: exige la integración de la seguridad en todo el ciclo de vida de la aplicación.

11.2.3 Anexo A, control 8.26 – Requisitos de seguridad de las aplicaciones: exige la definición y aplicación de controles técnicos para proteger las aplicaciones frente al uso indebido y el compromiso.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Pruebas y evaluación de seguridad de desarrolladores: exige pruebas estáticas, dinámicas y de penetración durante el desarrollo.

11.3.2 SA-15 – Proceso, estándares y herramientas de desarrollo: establece estándares formales para el desarrollo seguro de aplicaciones.

11.3.3 SI-10 – Validación de entradas de información: exige mecanismos de control para prevenir ataques de inyección y de análisis sintáctico.

11.4 RGPD de la UE (2016/679)

11.4.1 Artículo 25 – Protección de datos desde el diseño y por defecto: exige la integración de la protección de datos y la privacidad en la lógica de la aplicación y en los flujos de trabajo.

11.4.2 Artículo 32 – Seguridad del tratamiento: exige medidas técnicas apropiadas, como validación de entradas, cifrado y controles seguros de acceso.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 Artículo 21(2)(f): exige la gestión de vulnerabilidades y prácticas seguras del ciclo de vida de las aplicaciones para entidades esenciales e importantes.

11.5.2 Artículo 23 – Notificación de incidentes de seguridad: exige capacidades de registro y supervisión en la capa de aplicación para detectar y notificar incidentes significativos.

11.6 DORA de la UE (2022/2554)

11.6.1 Artículo 9 – Gestión del riesgo de las TIC: obliga a las entidades financieras a garantizar que las aplicaciones sean seguras, estén probadas y sean resilientes frente a amenazas cibernéticas.

11.6.2 Artículo 11 – Pruebas de herramientas TIC: fomenta las pruebas de penetración periódicas y los ejercicios de red team sobre aplicaciones y servicios críticos.

11.7 COBIT 2019

11.7.1 BAI03 – Gestionar la identificación y construcción de soluciones: establece requisitos de diseño y control durante el desarrollo de aplicaciones.

11.7.2 BAI09 – Gestionar aplicaciones: hace hincapié en el mantenimiento seguro, la supervisión y la mejora de las aplicaciones en explotación.

11.7.3 DSS05 – Gestionar los servicios de seguridad: vincula la protección de las aplicaciones con las operaciones y controles generales de seguridad de la organización.