					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P25S					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**

Alineada con normas y reglamentos

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusula 8	Controles operativos, incluida la seguridad de las aplicaciones
ISO/IEC 27002:2022	Controles 8.25–8.26	Diseño seguro, desarrollo, pruebas y revisión de código
NIST SP 800-53 Rev.5	SA-11, SI-10	Pruebas realizadas por desarrolladores/de aplicaciones, análisis de código y prevención de fallos
RGPD de la UE	Artículo 25	Protección de datos desde el diseño y por defecto
Directiva NIS2 de la UE	Artículo 21(2)(a), (e)	Medidas técnicas para proteger las aplicaciones y detectar riesgos
DORA de la UE	Artículos 9(2)(c), 10(2)(c)	Seguridad de las aplicaciones para la resiliencia operativa digital
COBIT 2019	BAI03	Gestionar la identificación y la construcción o adquisición segura de soluciones de software

1. Propósito

1.1 Esta política define los controles mínimos obligatorios de seguridad de las aplicaciones exigidos para todas las soluciones de software y sistemas utilizados por la organización, con independencia de que se desarrollen internamente o se adquieran a proveedores externos.

1.2 Garantiza que las aplicaciones se diseñen, implanten y mantengan de forma que protejan los datos de clientes, empleados y de la organización frente al acceso no autorizado, el uso indebido, la alteración o la destrucción.

1.3 Esta política respalda los esfuerzos de la organización para obtener y mantener la certificación ISO/IEC 27001, cumplir las obligaciones del RGPD de la UE y de la Directiva NIS2 de la UE, y reducir los riesgos operativos asociados a despliegues de software inseguros.

1.4 Ayuda a establecer un enfoque coherente y auditable de la seguridad de las aplicaciones para pymes mediante la definición de una lista uniforme de verificación de controles y prácticas de seguridad, adaptada a entornos con recursos técnicos internos limitados.

2. Alcance

2.1 Esta política aplica a todas las aplicaciones, sistemas, herramientas y plataformas que:

2.1.1 Se desarrollen internamente, se personalicen o se automaticen mediante scripts para uso interno

2.1.2 Se adquieran como software comercial, SaaS o sistemas basados en la nube

2.1.3 Traten, almacenen o transmitan datos personales, registros de la organización o información operativa sensible

2.1.4 Sean accesibles por empleados, contratistas, clientes o socios a través de redes internas, Internet o plataformas móviles

2.2 La política aplica a:

2.2.1 Desarrolladores (internos o contratados)

2.2.2 Proveedores de software y proveedores de servicios en la nube

2.2.3 Personal de soporte de TI o administradores responsables del despliegue y del soporte

2.2.4 Propietarios de aplicaciones y usuarios de negocio que participen en la aprobación y supervisión del sistema

3. Objetivos

3.1 Garantizar que todas las aplicaciones utilizadas por la organización incorporen controles de seguridad integrados y verificables que mitiguen vulnerabilidades habituales de software.

3.2 Proteger la confidencialidad, integridad y disponibilidad de los datos tratados por las aplicaciones, con independencia de dónde estén alojadas.

3.3 Exigir pruebas, revisión y validación formales de la seguridad de las aplicaciones antes de aprobar cualquier aplicación nueva o actualización significativa para su uso en producción.

3.4 Permitir una gestión coherente y segura de las credenciales de usuario, los datos de sesión y los derechos de acceso en todos los sistemas críticos para las operaciones de la organización.

3.5 Exigir funcionalidades de registro de auditoría, capacidad de auditoría y funciones de trazabilidad en todas las aplicaciones para apoyar la detección y respuesta ante actividades sospechosas.

3.6 Reducir los riesgos legales y de cumplimiento garantizando que las aplicaciones cumplan los requisitos regulatorios de seguridad que resulten aplicables.

4. Funciones y responsabilidades

4.1 Director General (DG)

4.1.1 Mantiene la responsabilidad global sobre la seguridad de las aplicaciones en toda la organización.

4.1.2 Aprueba esta política y garantiza que todas las adquisiciones o proyectos de desarrollo cumplan sus requisitos.

4.1.3 Garantiza que los proveedores y prestadores de servicios queden obligados contractualmente al cumplimiento de los requisitos de seguridad de las aplicaciones.

4.1.4 Revisa y aprueba excepciones al riesgo cuando no pueda alcanzarse el cumplimiento total debido a restricciones de la organización.

4.2 Propietario de la aplicación (si se designa)

4.2.1 Identifica las necesidades de seguridad específicas de la aplicación durante la selección del sistema o el inicio del proyecto.

4.2.2 Verifica que se incluyan controles clave como la protección del inicio de sesión, el cifrado y los registros de actividad.

4.2.3 Participa en las revisiones previas al despliegue y confirma que los controles de seguridad satisfacen las necesidades de la organización.

[... 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 por año natural para:

9.1.1 Reflejar cambios en los requisitos regulatorios (p. ej., RGPD de la UE, Directiva NIS2 de la UE, DORA de la UE)

9.1.2 Incorporar amenazas nuevas o emergentes y técnicas de ataque

9.1.3 Actualizar el lenguaje y los requisitos para reflejar cambios en plataformas, proveedores o métodos de desarrollo

9.2 También deben realizarse revisiones intermedias cuando:

9.2.1 Se introduzcan nuevas aplicaciones

9.2.2 Las aplicaciones existentes se sometan a actualizaciones significativas o integraciones

9.2.3 Se produzca un incidente o una brecha de seguridad relacionada con una aplicación

9.2.4 Se identifiquen nuevos riesgos a partir de avisos externos o alertas del sector

9.3 Todas las actualizaciones de esta política deben:

9.3.1 Ser aprobadas por el Director General

9.3.2 Documentarse con el historial de versiones y el motivo del cambio

9.3.3 Comunicarse a todos los empleados, desarrolladores y proveedores implicados en la gestión de aplicaciones

9.3.4 Almacenarse de forma segura como referencia para auditoría y cumplimiento

10. Políticas relacionadas y vinculaciones

10.1 Esta política se apoya directamente en las siguientes políticas de seguridad alineadas con pymes y contribuye a su aplicación:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: asigna la responsabilidad de aprobar aplicaciones, aplicar la política y gestionar proveedores.

10.1.2 P4S – Política de control de acceso: garantiza que el acceso a las aplicaciones se alinee con los principios de mínimo privilegio y control de sesiones.

10.1.3 P8S – Política de concienciación y formación en seguridad de la información: garantiza que los usuarios y desarrolladores reciban formación para reconocer y notificar amenazas relacionadas con las aplicaciones.

10.1.4 P17S – Política de protección de datos y privacidad: proporciona salvaguardas de privacidad de los datos que deben aplicarse en cualquier aplicación que trate datos personales.

10.1.5 P14S – Política de conservación y eliminación de datos: regula cómo deben conservarse, archivarse y destruirse de forma segura los registros, copias de seguridad y datos sensibles generados por las aplicaciones.

10.1.6 P30S – Política de respuesta a incidentes: describe los pasos para identificar, notificar y contener eventos de seguridad relacionados con aplicaciones.

10.2 En conjunto, estas políticas garantizan que la seguridad de las aplicaciones esté plenamente integrada en el Sistema de Gestión de la Seguridad de la Información (SGSI) de la organización y en condiciones de superar auditorías.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 La cláusula 8.1 exige que las organizaciones establezcan controles operativos para abordar los riesgos de seguridad de la información, incluidos los relacionados con aplicaciones y sistemas de software.

11.2 ISO/IEC 27002

11.2.1 El control 8.25 recomienda implantar prácticas de diseño seguro, desarrollo seguro y revisión de código en todas las aplicaciones, incluidas las proporcionadas por proveedores.

11.2.2 El control 8.26 recomienda realizar pruebas formales de los controles de seguridad de las aplicaciones, especialmente en ámbitos relacionados con el control de acceso, la validación de entradas y la gestión de sesiones.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 especifica requisitos para pruebas realizadas por desarrolladores, análisis de código y análisis dinámico de aplicaciones antes del despliegue.

11.3.2 SI-10 aborda la detección y prevención de defectos comunes de software, con énfasis en la concienciación de los desarrolladores y las salvaguardas técnicas.

11.4 RGPD de la UE (2016/679)

11.4.1 El artículo 25, «protección de datos desde el diseño y por defecto», exige integrar la privacidad y la seguridad en el diseño esencial de las aplicaciones que tratan datos personales.

11.5 Directiva NIS2 de la UE (2022/2555)

11.5.1 El artículo 21(2)(a) y (e) exige que las entidades esenciales e importantes implanten medidas técnicas para proteger las aplicaciones y detectar riesgos relacionados con el software.

11.6 DORA de la UE (2022/2554)

11.6.1 Los artículos 9(2)(c) y 10(2)(c) exigen que las pymes del sector financiero integren controles de seguridad a nivel de aplicación y realicen evaluaciones periódicas para mantener la resiliencia operativa digital.

11.7 COBIT 2019

11.7.1 BAI03, «Gestionar la identificación y construcción de soluciones», orienta el desarrollo o la adquisición de software seguro alineado con el riesgo, el cumplimiento y los requisitos de la organización, incluso en entornos pyme con recursos limitados.