					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P05S					Título del documento: **Política de gestión de cambios**							
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 6.1, 8	
ISO/IEC 27002:2022	control 8	
NIST SP 800-53 Rev. 5	CM-2 a CM-5, CM-11	
Directiva NIS2 de la UE	artículo 21(2)(b)	
DORA de la UE	artículos 6(9), 8(4)(b)	
COBIT 2019	BAI06, DSS	

1. Propósito

1.1 Esta política garantiza que todos los cambios en los sistemas de información, las configuraciones, las aplicaciones de la organización y los servicios en la nube se planifiquen, se evalúen desde la perspectiva del riesgo, se prueben y se aprueben antes de su implantación.

1.2 El objetivo es reducir las interrupciones operativas, los riesgos de seguridad y las caídas del servicio mediante el establecimiento de un proceso simplificado, pero exigible, aplicable incluso a pequeñas empresas con recursos limitados.

1.3 Esta política respalda la certificación ISO/IEC 27001:2022 al formalizar la forma en que se gestionan y documentan los cambios técnicos y operativos.

2. Alcance

2.1 Esta política se aplica a:

2.1.1 Empleados y responsables de departamento que propongan o ejecuten cambios

2.1.2 Proveedores externos de servicios de TI que gestionen sistemas o software

2.1.3 El Director General, que asume la responsabilidad general sobre la aprobación de cambios

2.2 Abarca cambios en:

2.2.1 Software (actualizaciones, parches, nuevas aplicaciones)

2.2.2 Hardware (sustituciones, ampliaciones)

2.2.3 Configuraciones de red y de cortafuegos

2.2.4 Servicios en la nube, permisos de acceso de usuarios e integraciones con proveedores

2.2.5 Cambios críticos en procesos de la organización que involucren sistemas de información

2.3 Tanto los cambios planificados como los cambios de emergencia están dentro del alcance de esta política.

3. Objetivos

3.1 Garantizar que todos los cambios de TI y en los sistemas de la organización estén autorizados, documentados y puedan revertirse en caso de incidencia.

3.2 Evitar tiempos de inactividad no planificados, pérdida de datos o incidentes de seguridad causados por cambios no controlados.

3.3 Definir procedimientos sencillos y repetibles para la solicitud, aprobación, prueba y reversión de cambios.

3.4 Mantener un Registro de Cambios auditable que respalde la trazabilidad operativa y el cumplimiento normativo.

3.5 Permitir la toma de decisiones basada en el riesgo para cambios significativos o sensibles.

4. Funciones y responsabilidades

4.1 Director General

4.1.1 Asume la responsabilidad última sobre todos los cambios importantes.

4.1.2 Revisa y aprueba los cambios no rutinarios, críticos o de alto riesgo.

4.1.3 Revisa el Registro de Cambios trimestralmente o tras incidentes graves.

4.2 Soporte de TI o proveedor externo de TI

4.2.1 Implementa cambios, incluidas actualizaciones de configuración, aplicación de parches y migraciones de sistemas.

4.2.2 Mantiene un Registro de Cambios básico con las fechas, los tipos de cambio, los resultados y los aprobadores.

4.2.3 Prueba los cambios antes de su implantación y aplica los pasos de reversión cuando sea necesario.

4.2.4 Notifica a los usuarios afectados antes y después de los cambios importantes.

[... 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 revisarse anualmente por el Director General o por el responsable de TI designado para garantizar su alineación con los sistemas, flujos de trabajo y requisitos regulatorios vigentes.

9.2 Revisiones intermedias

9.2.1 Las revisiones también deben activarse por:

9.2.1.1 Incidentes de seguridad causados por una gestión deficiente de cambios

9.2.1.2 Introducción de nuevos sistemas de TI

9.2.1.3 Cambios en normas relevantes como ISO, NIS2 o DORA

9.3 Documentación de actualizaciones

9.3.1 Los cambios en esta política deben estar sujetos a control de versiones y ser aprobados por el Director General. Cada versión debe registrar la fecha, el resumen de cambios y el aprobador.

9.4 Comunicación de la política

9.4.1 Cualquier actualización debe comunicarse a todos los empleados y proveedores externos afectados. La documentación debe actualizarse en todas las ubicaciones de referencia (p. ej., portal del personal o unidades compartidas).

10. Políticas relacionadas y vinculaciones

10.1 Esta política está estrechamente relacionada con las siguientes políticas para pymes:

10.1.1 P2S – Política de funciones y responsabilidades de gobernanza: define la autoridad de aprobación de cambios.

10.1.2 P4S – Política de control de acceso: garantiza que las modificaciones de acceso derivadas de cambios se documenten e implanten correctamente.

10.1.3 P7S – Política de incorporación y baja: coordina los cambios relacionados con transiciones de funciones y aprovisionamiento de accesos.

10.1.4 P15S – Política de copia de seguridad y restauración: garantiza que los pasos de reversión y recuperación puedan ejecutarse si un cambio falla.

10.1.5 P30S – Política de respuesta a incidentes: regula cómo los cambios fallidos o no autorizados se tratan como incidentes de seguridad.

11. Normas y marcos de referencia

11.1 ISO/IEC 27001

11.1.1 cláusula 6.1 – La planificación basada en el riesgo debe incluir las actividades de cambio.

11.1.2 cláusula 8.1 – Los controles operativos deben aplicarse de forma consistente a las actividades relacionadas con cambios para garantizar la integridad del servicio.

11.2 ISO/IEC 27002

11.2.1 control 8.32 – Proporciona orientación para procesos seguros de gestión de cambios, incluidos la documentación, las pruebas y la aprobación.

11.3 NIST SP 800-53 Rev. 5

11.3.1 CM-2 – Configuración de referencia del sistema antes del cambio.

11.3.2 CM-3 – Control de cambios de configuración.

11.3.3 CM-4 – Análisis del impacto en la seguridad.

11.3.4 CM-5 – Aprobación y documentación de cambios.

11.3.5 CM-11 – Auditoría y supervisión de cambios.

11.4 Directiva NIS2 de la UE

11.4.1 artículo 21(2)(b) – Exige procedimientos formales para medidas de seguridad técnicas y organizativas, incluida la gestión de cambios.

11.5 DORA de la UE

11.5.1 artículos 6(9) y 8(4)(b) – Exigen que las entidades financieras mantengan la gestión de cambios y de la configuración para los sistemas TIC.

11.6 COBIT 2019

11.6.1 BAI06 – Gestionar cambios: hace hincapié en la planificación, la evaluación de riesgos y la capacidad de reversión.

11.6.2 DSS01 – Gestionar operaciones: garantiza la integridad operativa durante transiciones y cambios técnicos.