					Introduzca aquí la denominación de la entidad jurídica registrada							
Número de documento: P05					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**

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

Alineación con normas y reglamentos aplicables

Norma/Reglamento	Cláusula/Artículo	Comentario
ISO/IEC 27001:2022	Cláusulas 6.1, 5.15	Aborda las acciones sobre riesgos, el control de acceso y la gestión de cambios
ISO/IEC 27002:2022	Control 8	Implementa un proceso estructurado de gestión de cambios
NIST SP 800-53 Rev.5	CM-2 a CM-14	Controles de gestión de la configuración
RGPD de la UE	Artículos 32(1)(b–d), 25; Considerando 78	Establece medidas técnicas y organizativas para la seguridad de sistemas y datos durante los cambios
Directiva NIS2 de la UE	Artículo 21(2)(a, b, d, e)	Exige la gestión de riesgos asociados a los cambios en las TIC
DORA de la UE	Artículos 5, 8, 12	Regula el riesgo operativo y de TIC, así como la notificación de incidentes
COBIT 2019	BAI06, BAI02, BAI03, DSS01, MEA01, MEA03	Establece requisitos estructurados de rendimiento, cumplimiento y gestión de cambios de TI

1. Propósito

1.1. Esta política establece un marco formal para iniciar, evaluar, aprobar, implantar y revisar cambios en los sistemas de información, la infraestructura, las aplicaciones y los procesos relacionados de la organización.

1.2. Garantiza que todos los cambios se ejecuten de forma controlada y auditable, minimizando el riesgo de interrupciones, incidentes de seguridad o incumplimiento normativo.

1.3. Da soporte al control 8.32 del anexo A de ISO/IEC 27001:2022 mediante la aplicación de prácticas de gestión de cambios seguras, documentadas y alineadas con el riesgo.

1.4. Esta política también garantiza la trazabilidad de las decisiones sobre cambios y promueve la resiliencia operativa durante modificaciones planificadas o de emergencia.

2. Alcance

2.1. Esta política se aplica a todos los cambios que afecten a sistemas, datos y entornos dentro del alcance del SGSI, incluidos:

2.1.1. Infraestructura de TI (local, en la nube o híbrida)

2.1.2. Entornos de producción, preproducción y recuperación ante desastres

2.1.3. Aplicaciones empresariales, servicios, interfaces de programación de aplicaciones e integraciones

2.1.4. Ajustes de configuración, aplicación de parches, versiones de software y migraciones de sistemas

2.1.5. Correcciones de emergencia y cambios planificados o basados en proyectos

2.2. Regula los cambios iniciados por:

2.2.1. Personal interno (operaciones de TI, desarrolladores y propietarios de sistemas)

2.2.2. Proveedores externos, proveedores de servicios gestionados (MSP) y contratistas

2.2.3. Equipos de proyecto durante la implantación de sistemas, actualizaciones o transiciones de servicio

2.3. Esta política no se aplica a:

2.3.1. Entornos temporales de prueba y desarrollo sin acceso a datos de producción

2.3.2. Configuraciones personales de usuario (cubiertas por la Política de uso aceptable)

2.3.3. Cambios en sistemas fuera del perímetro de control de la organización, salvo que afecten a activos integrados o a obligaciones de cumplimiento

3. Objetivos

3.1. Garantizar que todos los cambios se revisen, aprueben, prueben y documenten antes de su ejecución.

3.2. Mantener la disponibilidad de los sistemas, la integridad de los datos y la continuidad del servicio durante y después de las actividades de cambio.

3.3. Exigir clasificaciones de cambios definidas, planes de reversión y evaluaciones de riesgos para todos los tipos de cambios.

3.4. Permitir la toma de decisiones transparente y el escalado mediante una gobernanza estructurada.

3.5. Dar soporte a la preparación para auditorías mediante registros de cambios trazables y revisiones posteriores a la implantación.

3.6. Aplicar la segregación de funciones y reducir el riesgo de cambios no autorizados o en conflicto en sistemas críticos.

4. Funciones y responsabilidades

4.1. Alta dirección

4.1.1. Respalda la Política de gestión de cambios y garantiza su alineación con los objetivos estratégicos y las obligaciones regulatorias.

4.1.2. Aprueba programas de cambio de alto impacto o transversales como parte de la supervisión de la gobernanza.

4.1.3. Asigna los recursos y el presupuesto necesarios para las herramientas de control de cambios y la formación del personal.

4.2. Comité Asesor de Cambios (CAB)

4.2.1. Revisa y autoriza los cambios estándar y mayores, garantizando una evaluación adecuada del riesgo, el impacto y las dependencias.

4.2.2. Valida los planes de reversión, los resultados de las pruebas, las comunicaciones a las partes interesadas y la planificación.

4.2.3. Está compuesto por propietarios de sistemas, representantes de seguridad, operaciones de TI, responsables de negocio y representantes de cumplimiento.

4.2.4. Puede delegar decisiones sobre cambios de bajo riesgo o de emergencia en condiciones documentadas.

[... 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. Desencadenantes y frecuencia de revisión

9.1.1. Esta política debe revisarse anualmente o cuando se produzca alguno de los siguientes supuestos:

9.1.1.1. Cambios significativos de TI o de infraestructura

9.1.1.2. Incidentes significativos relacionados con cambios fallidos o no autorizados

9.1.1.3. Actualizaciones regulatorias o nuevas obligaciones legales relacionadas con los cambios

9.1.1.4. Implantación de nuevas herramientas o plataformas de CMS

9.2. Proceso de revisión de la Política de gestión de cambios

9.2.1. El Responsable de cambios dirigirá el proceso de revisión en colaboración con:

9.2.1.1. TI, Seguridad y Operaciones

9.2.1.2. Auditoría interna y Riesgos

9.2.1.3. Representantes del CAB

9.2.2. Las actualizaciones deben ser revisadas y aprobadas por la alta dirección y el Comité Directivo del SGSI.

9.2.3. Las versiones reemitidas deben registrarse en el Registro documental y comunicarse a las partes afectadas, con nuevo acuse de recibo cuando sea necesario.

9.3. Control documental y gestión de versiones

9.3.1. Todas las versiones deben incluir:

9.3.1.1. ID de la política, título y nivel de clasificación

9.3.1.2. Propietario e historial de revisiones

9.3.1.3. Registro de cambios y fecha de entrada en vigor

9.3.1.4. Autoridad de aprobación

9.3.2. Las versiones archivadas deben conservarse de acuerdo con la Política de conservación documental (mínimo 3 años).

10. Políticas relacionadas y vinculaciones

10.1. Esta política está directamente vinculada con y respalda la aplicación de:

10.1.1. P1 – Política de seguridad de la información: establece el requisito de controles formales de seguridad y de rendición de cuentas a nivel de proceso, incluida la gobernanza de la gestión de cambios.

10.1.2. P2 – Política de funciones y responsabilidades de gobernanza: define las autoridades de aprobación y la segregación de funciones relevantes para la autorización y supervisión de cambios.

10.1.3. P4 – Política de control de acceso: garantiza que los permisos de acceso de quienes implantan y revisan cambios sigan el principio de mínimo privilegio.

10.1.4. P6 – Política de gestión de riesgos: garantiza que todos los cambios estén sujetos a una evaluación de riesgos adecuada y a estrategias de mitigación.

10.1.5. P33 – Política de supervisión de auditoría y cumplimiento: regula la validación y la revisión de auditoría de los registros de gestión de cambios y de las vulneraciones.

10.2. Estas políticas permiten conjuntamente un ciclo de vida de gestión de cambios sólido, trazable y seguro dentro del marco del SGSI.

11. Normas y marcos de referencia

11.1. ISO/IEC 27001:2022

11.1.1. Cláusula 6.1 – Acciones para abordar riesgos y oportunidades: esta política respalda la identificación, evaluación y control de los riesgos relacionados con el cambio.

11.1.2. Cláusula 5.15 – Control de acceso: garantiza que el acceso durante los cambios esté controlado y sea trazable.

11.1.3. Control 8.32 del anexo A – Gestión de cambios: esta política implanta plenamente el requisito de gestionar los cambios en instalaciones y sistemas de tratamiento de la información de forma planificada y controlada.

11.2. ISO/IEC 27002:2022 – Control 8

11.2.1. Refuerza la implantación de un proceso estructurado de gestión de cambios que incluye clasificación del cambio, aprobación, pruebas, reversión y documentación.

11.3. NIST SP 800-53 Rev.5

11.3.1. Familia CM (CM-1 a CM-14): esta política está estrechamente alineada con los controles de gestión de la configuración, incluidas las configuraciones de referencia (CM-2), el control de cambios de configuración (CM-3), el análisis de impacto en la seguridad (CM-4) y las restricciones de acceso (CM-5).

11.3.2. Familia AU (AU-2, AU-6, AU-12): los mecanismos de registro y auditoría a los que se hace referencia en esta política respaldan la trazabilidad de eventos y la revisión del cumplimiento para las actividades relacionadas con cambios.

11.3.3. RA-3, RA-5: las evaluaciones de riesgos derivadas de cambios y los análisis de vulnerabilidades están integrados en el proceso de evaluación del cambio.

11.3.4. PM-11 (Definición de misión/proceso de negocio): garantiza que la continuidad del negocio y los objetivos operativos se preserven durante los cambios.

11.4. RGPD de la UE (2016/679)

11.4.1. Artículo 32(1)(b–d): esta política respalda el requisito de adoptar medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos, especialmente durante los cambios de sistema.

11.4.2. Artículo 25 – Protección de datos desde el diseño y por defecto: garantiza que los cambios que afecten a datos personales integren la privacidad y la seguridad en el diseño y el despliegue.

11.4.3. Considerando 78: exige que los responsables del tratamiento implanten mecanismos, como políticas de control de cambios, para garantizar la confidencialidad, integridad y resiliencia continuas de los sistemas de tratamiento.

11.5. Directiva NIS2 de la UE (2022/2555)

11.5.1. Artículo 21(2)(a, b, d, e): exige medidas técnicas y organizativas para gestionar los riesgos de TIC, incluidos los derivados de cambios del sistema, actualizaciones de software y modificaciones de infraestructura.

11.6. DORA de la UE (2022/2554)

11.6.1. Artículo 5 – Marco de gobernanza y control interno: esta política aplica principios de gestión del riesgo operativo vinculados a cambios y actualizaciones de TIC.

11.6.2. Artículo 8 – Marco de gestión de riesgos de TIC: exige que las entidades financieras gestionen todos los cambios que afecten a los sistemas TIC mediante procesos estructurados de gestión de cambios, reflejados en los requisitos de clasificación, pruebas, reversión y documentación de esta política.

11.6.3. Artículo 12 – Notificación de incidentes: garantiza que los cambios fallidos que den lugar a interrupciones de TIC sean trazables, documentados y notificados cuando corresponda.

11.7. COBIT 2019

11.7.1. BAI06 – Cambios de TI gestionados: esta política cumple directamente los objetivos de BAI06 al establecer flujos de trabajo estructurados para la aprobación de cambios, la evaluación de impacto, la comunicación y las pruebas.

11.7.2. BAI02 – Definición de requisitos gestionada y BAI03 – Identificación y construcción de soluciones gestionadas: garantizan que los cambios impulsados por el negocio se revisen y se implanten de forma segura.

11.7.3. DSS01 – Operaciones gestionadas: respalda la integridad continua del sistema durante la ejecución de cambios.

11.7.4. MEA01 y MEA03 – Supervisar, evaluar y valorar el rendimiento y el cumplimiento: permite la supervisión continua de la eficacia y aplicación de la política de gestión de cambios.