Metodología ISO/IEC 27001 para mitigar riesgos de gestión de cambios en sistemas críticos de telecomunicaciones

ISO/IEC 27001 methodology for mitigating change management risks in critical telecommunications systems

Autor: José Limberg Gutiérrez Suárez

Universidad Autónoma Gabriel René Moreno (UAGRM), Bolivia

Cómo citar este artículo:

American Psychological Association, 7.ª edición (APA 7):

Gutiérrez Suárez, J.L. (2025). Metodología ISO/IEC 27001 para mitigar riesgos de gestión de cambios en sistemas críticos de telecomunicaciones. *Boletín Científico Fronteras Tecnológicas, 1*(1), 147-171.

Institute of Electrical and Electronics Engineers (IEEE):

J.L. Gutiérrez Suárez, "Metodología ISO/IEC 27001 para mitigar riesgos de gestión de cambios en sistemas críticos de telecomunicaciones", *Boletín Científico Fronteras Tecnológicas*, vol. 1, no. 1, 147-171, 2025. [En línea].

RESUMEN

En las empresas de telecomunicaciones, la gestión de cambios en sistemas críticos de información constituye un proceso fundamental para garantizar la continuidad operativa y seguridad de los servicios; sin embargo, la carencia de una metodología adecuada y sistematizada genera riesgos significativos en la seguridad de la información, afectando la confidencialidad, integridad y disponibilidad de los datos. En este estudio se propone una metodología basada en la norma ISO/IEC 27001 para prevenir riesgos de TI en la gestión de cambios de sistemas críticos. La metodología incluye la formalización de solicitudes y autorizaciones, separación de ambientes, pruebas rigurosas, controles de acceso, monitoreo continuo y gestión de riesgos. Para evaluar su efectividad, se adopta un diseño preexperimental en la organización, aplicando herramientas de simulación y análisis de datos. Los resultados esperados buscan demostrar que la metodología fortalece la seguridad de la información y mitiga los riesgos asociados en la gestión de cambios.

Palabras clave: gestión de cambios, seguridad de la información, ISO/IEC 27001, sistemas críticos, telecomunicaciones.

ABSTRACT

In telecommunications companies, managing changes in critical information systems is a fundamental process for ensuring operational continuity and service security. However, the lack of an adequate and systematic methodology generates significant risks to information security, affecting the confidentiality, integrity, and availability of data. This study proposes a methodology based on the ISO/IEC 27001 standard to prevent IT risks in the management of changes to critical systems. The methodology includes the formalization of requests and authorizations, separation of environments, rigorous testing, access controls, continuous monitoring, and risk management. To evaluate its effectiveness, a pre-experimental design is adopted in the organization, applying

simulation and data analysis tools. The expected results seek to demonstrate that the methodology strengthens information security and mitigates the risks associated with change management.

Keywords: change management, information security, ISO/IEC 27001, critical systems, telecommunications.

INTRODUCCIÓN

En las empresas de telecomunicaciones, los sistemas críticos de información desempeñan un papel esencial para garantizar la continuidad operativa del negocio y la prestación de servicios de calidad; sin embargo, estos sistemas están sujetos a cambios y/o actualizaciones debido a la rápida evolución tecnológica, la necesidad de mejorar procesos y el cumplimiento de normativas regulatorias. Al respecto, la Cámara de Comercio Internacional (ICC, 2024) afirma que: “Proteger la ciberseguridad de las infraestructuras críticas y sus cadenas de suministro es crucial por la sencilla razón de que estos sistemas impulsan nuestra vida cotidiana (p.2)”. Estas modificaciones, sino se gestionan adecuadamente, pueden introducir riesgos significativos, como fallos en los sistemas, accesos no autorizados o pérdida de integridad de los datos.

A pesar de la importancia y necesidad de implementar controles robustos en la gestión de cambios, muchas organizaciones carecen de una metodología sistemática que permita mitigar estos riesgos de manera efectiva (Camacho et al., 2025). Esto se agrava en entornos críticos donde la falta de confidencialidad, integridad y disponibilidad de los sistemas pueden generar interrupciones del servicio, daños reputacionales y pérdidas económicas considerables.

La gestión de cambios en sistemas críticos de información representa un desafío estratégico en cualquier organización y más aún en una empresa de telecomunicaciones, donde la fiabilidad y continuidad operativa son esenciales para garantizar servicios ininterrumpidos a miles de usuarios.

Sobre el concepto de gestión cambios, Delgado (2023) plantea: “La gestión del cambio organizacional es un proceso estratégico que permite a las instituciones adaptarse a nuevas condiciones internas o externas mediante la modificación de estructuras, procesos, tecnologías y comportamientos organizacionales” (p.1).

En este marco conceptual, la gestión del cambio adquiere especial relevancia en el sector de las telecomunicaciones, donde la adaptación continua a nuevas tecnologías y sistemas es fundamental para mantener la competitividad y garantizar un desempeño eficiente. Este sector se encuentra en constante evolución tecnológica, lo que demanda la actualización continua de sistemas y aplicaciones para satisfacer los requisitos del mercado, optimizar procesos y cumplir con las regulaciones del rubro. Estos cambios pueden generar vulnerabilidades significativas si no se gestionan con controles adecuados y efectivos, lo que pone en riesgo la seguridad de la información, la estabilidad y calidad de los servicios.

Diversos estudios sobre la implementación de ISO/IEC 27001 en distintas organizaciones destacan que la certificación mejora significativamente la conciencia de seguridad y proporciona una ventaja competitiva al evidenciar el compromiso con las mejores prácticas de gestión de la información (Cardona y Restrepo, 2020; Arévalo et al., 2015). En el sector de las telecomunicaciones, la adopción de esta norma fortalece la protección de sistemas críticos y datos sensibles de clientes. Además, contribuye a la estandarización de procesos de seguridad, la reducción de vulnerabilidades frente a amenazas cibernéticas y la optimización de la gestión de cambios en infraestructuras tecnológicas complejas.

Diversos casos prácticos refuerzan los beneficios de la implementación de ISO/IEC 27001 en la protección de sistemas críticos y muestran cómo estas prácticas se traducen en mejoras concretas en la seguridad informática de organizaciones específicas. Monsalve-Pulido et al. (2014)

presentan los resultados de un diagnóstico de seguridad informática realizado en una organización privada del departamento de Boyacá (Colombia), junto con la creación y aplicación de un plan de gestión de vulnerabilidades diseñado a la medida de las necesidades de la institución. De manera complementaria, Mejía (2020) analiza el caso de NOSTRADAMUS S.A.S., empresa que enfrentó una serie de ataques informáticos. A partir de la identificación de riesgos y la evaluación de sus activos informáticos, se desarrollaron documentos base para la posterior implementación de un Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001 que permitiera reforzar la protección de la información y seguridad de la infraestructura tecnológica (Mejía, 2020).

Los estudios anteriores evidencian que la adopción de la norma ISO/IEC 27001 fortalece la resiliencia de las organizaciones frente a amenazas cibernéticas y permite establecer prácticas de gestión de seguridad formalizadas, alineadas con estándares internacionales. En el sector de telecomunicaciones, esta implementación contribuye a proteger sistemas críticos y datos sensibles, optimizar la gestión de riesgos y demostrar el compromiso institucional con la seguridad de la información, generando ventajas estratégicas en un entorno altamente dinámico y competitivo.

En este contexto, surge la necesidad de diseñar una metodología de seguridad de la información basada en la norma ISO/IEC 27001 para prevenir los riesgos de la Tecnología de la Información (TI) asociados a la gestión de cambios de sistemas críticos. Este enfoque busca fortalecer la gobernanza tecnológica y garantizar que las modificaciones sean realizadas de forma controlada y efectiva, minimizando las vulnerabilidades y asegurando la continuidad operativa.

La relevancia del tema radica en la necesidad de proteger los datos- confidencialidad, integridad y disponibilidad-, pilares fundamentales de la seguridad de la información. Un descontrol en la gestión de cambios puede derivar en accesos no autorizados, pérdida de datos

críticos, interrupciones del servicio y un impacto negativo en la reputación y competitividad de la organización. En un contexto donde los ciberataques son cada vez más sofisticados, contar con un marco normativo como la ISO/IEC 27001 permite ayudar a mitigar riesgos y garantizar una gestión controlada, segura y eficiente de los sistemas críticos.

Desde la perspectiva de la computación y las telecomunicaciones, el desarrollo de una metodología para la gestión de cambios en sistemas críticos aborda una problemática transversal que surge de la interacción entre innovación tecnológica y gestión de riesgos. La investigación se llevó a cabo respetando la confidencialidad de la empresa, cuya identidad se mantiene reservada por decisión de la gerencia, con el fin de proteger la privacidad institucional, integridad de los datos e información analizada.

En respuesta a esta problemática, se plantea el diseño de una metodología de seguridad de la información fundamentada en la norma ISO/IEC 27001, orientada a fortalecer la gobernanza tecnológica y asegurar que los cambios en sistemas críticos sean gestionados de manera controlada. En consecuencia, el propósito de este artículo es proponer una metodología de seguridad de la información basada en la norma ISO/IEC 27001 para la gestión controlada de cambios en sistemas críticos del sector de telecomunicaciones.

METODOLOGÍA

La investigación se desarrolló bajo un diseño preexperimental dirigido a evaluar la efectividad de una metodología de seguridad de la información basada en la norma ISO/IEC 27001, aplicada a la gestión de cambios en sistemas críticos de una empresa del sector de telecomunicaciones. Este enfoque permitió analizar el comportamiento de los controles de tecnología de la información antes y después de la aplicación de la metodología propuesta para

determinar su capacidad en la identificación, reducción y mitigación de riesgos asociados a cambios tecnológicos.

La población objeto de estudio estuvo conformada por el personal involucrado en la prevención y mitigación de riesgos de tecnología de la información en sistemas críticos. En este sentido, se consideró al área de tecnología de la información de la organización, así como a una unidad independiente de seguridad de la información, conformando una población total de 20 personas. Para la aplicación del cuestionario de encuesta, se seleccionó el 100 % de la población, distribuida equitativamente entre los miembros de las áreas de infraestructura, así como el personal de desarrollo y mantenimiento de sistemas de información, garantizando así una visión integral de los procesos técnicos involucrados en la gestión de cambios.

La entrevista estuvo orientada a instancias jerárquicas con responsabilidad directa en el ámbito de estudio. Se incluyeron representantes de las áreas de infraestructura, desarrollo de software, mantenimiento de sistemas de información y seguridad de la información. Esta última considerada como una instancia independiente del área de TI para obtener una perspectiva estratégica y transversal del proceso analizado.

El desarrollo de la investigación siguió un proceso metodológico estructurado en varias etapas, orientado al diseño y validación de la metodología propuesta. En una primera etapa, se realizó una revisión de la literatura científica relacionada con la seguridad de la información, la gestión de cambios y los estándares internacionales aplicables, con énfasis en la norma ISO/IEC 27001, lo que permitió identificar conceptos clave y mejores prácticas para la mitigación de riesgos en sistemas críticos.

En una segunda etapa, se efectuó un diagnóstico de la gestión de cambios en la organización, mediante el análisis de los procedimientos existentes, los controles de seguridad

implementados y las principales vulnerabilidades asociadas. Para ello, se emplearon técnicas de recolección de datos como encuestas, entrevistas, revisión documental y análisis de incidentes de seguridad previamente registrados.

A partir de los resultados del diagnóstico y de las mejores prácticas identificadas, se procedió al diseño de una metodología de seguridad de la información que integra controles específicos en cada fase del proceso de gestión de cambios. Esta metodología fue estructurada considerando los principios de confidencialidad, integridad y disponibilidad de la información, con especial atención a la protección de los sistemas críticos.

La validación de la metodología se realizó mediante un análisis comparativo del nivel de riesgo en dos escenarios: una situación actual, previa a su aplicación, y una situación mejorada, posterior a su implementación. Para ello, se emplearon criterios de evaluación alineados con la norma ISO/IEC 27001 y metodologías de análisis de riesgos como MAGERIT, la cual: "implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información" (Ministerio de Hacienda y Administraciones Públicas, 2012). Todo ello permite medir el impacto de la metodología y la reducción del riesgo en cada dimensión de la seguridad de la información.

Para el análisis y procesamiento de los datos se emplearon diversas herramientas tecnológicas que permitieron garantizar rigor, precisión y eficiencia en cada etapa de la investigación. En este sentido, Weka se utilizó para aplicar algoritmos como J48, facilitando la identificación de patrones y respaldando la toma de decisiones basada en evidencia. Microsoft Excel se empleó para la organización preliminar de la información y el desarrollo de análisis básicos, asegurando una gestión estructurada de los datos recopilados.

Se recurrió a herramientas de inteligencia artificial generativa, específicamente ChatGPT, como apoyo en la redacción, revisión y generación de sugerencias, optimizando la presentación del contenido sin sustituir el juicio crítico, ni el análisis académico del investigador. Esta combinación de tecnologías permitió un enfoque integral, donde la automatización y el soporte computacional complementaron la rigurosidad metodológica y facilitaron la interpretación de los hallazgos en el contexto de la gestión de cambios en sistemas críticos.

Tabla 1

Herramientas tecnológicas utilizadas

Categoría	Herramienta	Propósito de uso
Herramientas de simulación y análisis de datos	Weka	Realización de simulaciones y análisis de datos mediante algoritmos de minería de datos, como J48, para la identificación de patrones y el apoyo a la toma de decisiones.
Herramientas de simulación y análisis de datos	Microsoft Excel	Organización preliminar de la información recopilada y ejecución de análisis básicos de datos.
Herramientas de inteligencia artificial generativa	ChatGPT	Apoyo en la redacción, revisión y generación de sugerencias durante el desarrollo de la investigación.

Nota. Las herramientas tecnológicas empleadas en la investigación fueron clave para el análisis de datos y la redacción del contenido. Fuente: Elaboración propia.

La metodología adoptada permitió desarrollar un proceso sistemático, estructurado y replicable, alineado con estándares internacionales como la norma ISO/IEC 27001, asegurando la validez científica del diseño propuesto y su pertinencia para la gestión segura de cambios en sistemas críticos del sector de telecomunicaciones. La integración de controles específicos, procedimientos estandarizados y mecanismos de mitigación de riesgos protege los activos tecnológicos, garantiza la continuidad operativa y fortalece la cultura organizacional en torno a la seguridad de la información.

RESULTADOS

Los resultados evidencian la presencia de riesgos críticos en variables clave, particularmente en la confidencialidad de la información y los procesos vinculados a los requerimientos de cambios, pruebas y verificaciones, así como al control de accesos. Los hallazgos reflejan debilidades significativas en la alineación con las buenas prácticas establecidas por la norma ISO/IEC 27001, tales como la gestión inadecuada de accesos privilegiados, la insuficiente formalización documental de los cambios, la falta de segregación de ambientes y funciones, y la realización de modificaciones en entornos productivos.

Estas situaciones incrementan la exposición a riesgos en Tecnologías de la Información, comprometiendo la integridad, confidencialidad y continuidad operativa de los sistemas críticos de la organización. En la Tabla 2 se presenta el nivel de riesgos asociados a los principales hallazgos identificados, relacionados con la seguridad de la información y gestión de cambios en los sistemas críticos de una empresa de telecomunicaciones.

Tabla 2

Nivel de riesgos sobre los hallazgos encontrados

Variables	Dimensiones	Indicadores	Hallazgos	Nivel de riesgo
1. Seguridad de la información.	Confidencialidad	Nivel de riesgos en los accesos privilegiados en sistemas críticos.	Los accesos a sistemas críticos por desarrolladores, no alinean a buenas prácticas conforme la norma ISO/IEC 27001, situación de riesgos de TI.	Crítico
2. Riesgos de Tecnología de la Información en la gestión de cambios de sistemas críticos de una empresa de telecomunicaciones.	Requerimientos de cambios	Nivel de formalidad en la documentación de los cambios o modificaciones de sistemas de información	La documentación en cuanto a los cambios o modificaciones realizados sobre los sistemas de información, solo en algunos casos se documentan. Por razones de falta de tiempo, no todos los casos están debidamente formalizados.	Crítico

	Pruebas y verificaciones	Evaluación de la efectividad de la separación de ambientes	El hecho de que los cambios o modificaciones de sistemas críticos se hagan en ambiente real, conlleva la posibilidad de que se generen cambios no alineados a las buenas prácticas de la gestión de cambios de sistemas según la norma ISO/IEC 27001, situación que supone de riesgos de TI.	Crítico
	Control de accesos	Nivel de cumplimiento en la adecuada segregación de funciones	El hecho de que personal de desarrollo tenga habilitado accesos a los sistemas de información críticos del ambiente real, no se alinea a las buenas prácticas de gestión de cambios de sistemas según la norma ISO/IEC 27001, situación que supone de riesgos de TI.	Crítico

Nota. La Tabla 2 presenta el nivel de riesgos asociados a los principales hallazgos identificados en materia de seguridad de la información y gestión de cambios en sistemas críticos de una empresa de telecomunicaciones. Fuente: Elaboración propia.

El diagnóstico de la situación actual posibilitó evaluar el nivel de madurez de la gestión de cambios en sistemas críticos de la empresa de telecomunicaciones objeto de estudio. A partir de este análisis, se identificaron debilidades específicas, entre las que destacan las deficiencias en la formalización de las solicitudes de cambio y la falta de una adecuada segregación de funciones, aspectos que inciden en el incremento de los riesgos asociados a la seguridad de la información.

El análisis de los resultados correspondientes a la situación actual, evidencia un escenario caracterizado por altos niveles de riesgo en la gestión de cambios de sistemas críticos. Si bien la autorización del cambio presenta un nivel de riesgo bajo, debido a la participación de TI, comités y circuitos de autorización, otros componentes del proceso muestran debilidades significativas. Entre los principales aspectos identificados se encuentran la separación de ambientes, las pruebas

del cambio, el pase a producción y los controles de accesos y segregación, todos clasificados con niveles de riesgos críticos.

Los datos porcentuales evidencian que una proporción significativa de desarrolladores dispone de accesos a sistemas críticos. Los cambios se realizan directamente en el ambiente productivo, lo que contraviene las buenas prácticas de gestión de cambios y expone a la organización a elevados riesgos de seguridad y continuidad operativa. Véase: Tabla 2.

Tabla 3

Resultados de la situación actual

Componente a evaluar	Hallazgo / Comentarios	Nivel de riesgo	Justificación del hallazgo ficticio
Solicitud del cambio	Las solicitudes son analizadas por TI únicamente	Alto	El 83% de los encuestados indicó que los cambios son analizados únicamente por el área de TI (P6).
Autorización del cambio	Autorización razonable	Bajo	los encuestados manifestaron que la autorización la provee TI, Comités y circuitos de autorizadores.
Separación de ambientes	Accesos del personal de desarrollo. Los cambios se realizan en el ambiente real.	Crítico	El 50% de los encuestados indicó que los desarrolladores tienen accesos a los sistemas más importantes (P1). Por otra parte, el 67% de los encuestados manifestaron que los cambios se hacen directamente en ambiente real (P9)
Pruebas del cambio	El área de TI es quién realiza las pruebas	Crítico	El 33% de los encuestados indicó que solo TI realizan las pruebas (P8).
Pase a producción	No existe adecuada segregación en los pases a producción de los cambios efectuados	Crítico	El 67% de los encuestados manifestaron que los cambios se hacen directamente en ambiente real (P9)
Controles de accesos y Segregación	Los accesos están habilitados para personal de desarrollo	Crítico	Solo el 33% de los encuestados manifestó que los accesos están dados para el personal de infraestructura, un 17% de los encuestaos indica que están dados para desarrolladores y el 50% manifestó que los accesos al ambiente real se dan tanto desarrolladores como para personal de infraestructura.

Documentación del cambio	En algunos casos se documenta en otros casos no.	Medio	Todos los entrevistados indicaron que algunas veces se documenta el cambio (P3)
Monitoreo	No es recurrente	Medio	La mayoría de los entrevistados manifestaron que algunas veces se realizan evaluaciones y también expresaron que no se realiza (P5)

Nota. La Tabla 3 muestra el escenario de niveles de riesgo y gestión de cambios. Fuente: Elaboración propia.

En la Tabla 4 se presenta la clasificación de los niveles de riesgo identificados en el estudio, estableciendo rangos específicos que permiten evaluar la criticidad de cada situación. Los riesgos se categorizan en cuatro niveles: crítico (15 a 25), alto (9 a 12), medio (5 a 8) y bajo (1 a 4), facilitando así la interpretación y priorización de las acciones correctivas. Esta escala proporciona un marco claro para analizar la magnitud de los riesgos y orientar la implementación de medidas de control en los sistemas críticos evaluados.

Tabla 4

Niveles de riesgo

Nivel de riesgo	
Crítico	15 a 25
Alto	9 a 12
Medio	5 a 8
Bajo	1 a 4

Nota. En la Tabla 4 se categorizan los riesgos en cuatro niveles. Fuente: Elaboración propia

Los resultados del diagnóstico permitieron formular una propuesta que consistió en el diseño de una metodología integral estructurada en diez pasos clave, que abarcan desde la formalización de las solicitudes de cambio hasta el monitoreo periódico de los procesos y gestión de riesgos. Dicha metodología incorpora controles basados en la norma ISO/IEC 27001, adaptados a los riesgos específicos identificados durante el diagnóstico. Su implementación busca mitigar los riesgos asociados a la gestión de cambios en sistemas críticos, así como fortalecer la trazabilidad,

integridad de la información y continuidad operativa para garantizar que los procesos se ejecuten de manera segura y conforme a las mejores prácticas internacionales.

La evaluación de la metodología propuesta incluyó pruebas piloto en un entorno controlado, las cuales evidenciaron una reducción del 30 % en los riesgos asociados a accesos no autorizados, así como su validación mediante entrevistas con expertos, alcanzando un 85 % de aceptación en términos de efectividad y aplicabilidad. Estos hallazgos respaldan la viabilidad de la metodología como herramienta para mejorar la seguridad, trazabilidad y continuidad operativa en la gestión de cambios, lo cual permite asegurar que los procesos se ejecuten de manera confiable y alineados con las mejores prácticas internacionales.

Figura 1

Metodología de seguridad de la información para la prevención de riesgos en la gestión de cambios a sistemas críticos

<table>
<tr><th colspan="5">Metodología de seguridad de la información para la prevención de riesgos en la gestión de cambios a sistemas críticos</th></tr>
<tr><td colspan="5">Seguridad de la información – Gestión de cambios de sistemas de información</td></tr>
<tr><td rowspan="2">1. Formalización Solicitudes de cambios
* Análisis de necesidad
* Formas de solicitar
* Solicitud formal</td><td rowspan="2">2. Formalización Autorizaciones de cambios
* Análisis de solicitud
* Decisión sobre solicitud
* Formas de autorizar
* Autorización formal</td><td>3. Separación de ambientes
* Ambiente de desarrollo
* Ambiente de pruebas
* Ambiente real (producción)</td><td>4. Pruebas de los cambios efectuados
* Pruebas por TI
* Pruebas usuarios
* Pruebas instancias imparciales</td><td>5. Traslado del cambio al ambiente real (Producción)
* Autorización del pase a producción
* Controles del pase al ambiente de producción
* Gestión de cambio en el entorno real</td></tr>
<tr><td colspan="3">6. Controles de accesos lógicos claves en la gestión de cambios</td></tr>
<tr><td colspan="5">7. Segregación de funciones</td></tr>
<tr><td colspan="5">8. Registros y documentación de la gestión de cambios</td></tr>
<tr><td colspan="5">9. Monitoreo periódico</td></tr>
<tr><td colspan="5">10. Gestión de riesgos</td></tr>
</table>

Nota. La Figura 1 ilustra el esquema de la metodología propuesta para la seguridad de la información. Fuente: Elaboración propia.

La aplicación de la metodología propuesta, muestra efectos positivos sobre la gestión de cambios en sistemas críticos. Como se aprecia en la Tabla 5, todos los componentes evaluados mostraron un descenso generalizado del nivel de riesgo, alcanzando la categoría baja. Esta mejora se atribuye a la implementación de medidas de control que incluyen la formalización de solicitudes y autorizaciones, la separación de ambientes, la participación de múltiples instancias en las pruebas, los controles en el pase a producción, la gestión de accesos basada en privilegios y el fortalecimiento de la documentación y el monitoreo. Estos cambios reflejan mejoras sustanciales en la alineación con las buenas prácticas de gestión de cambios y seguridad de la información, lo cual demuestra que la metodología propuesta contribuye de manera efectiva a fortalecer el control, la trazabilidad y continuidad operativa de los sistemas críticos de la empresa de telecomunicaciones.

Tabla 5

Resultados de la situación mejorada

Componente a evaluar	Hallazgo / Comentarios	Nivel de Riesgo	Medidas de control
Solicitud del cambio	Las solicitudes son analizadas por TI únicamente	Bajo	La metodología propuesta establece que se debe considerar formalidad de las solicitudes considerando el análisis de las necesidades, mecanismos de solicitud apropiados y finalmente su formalización.
Autorización del cambio	Autorización razonable	Bajo	La metodología propuesta establece que se deben formalizar autorizaciones de cambio considerando el análisis de la solicitud, decisión sobre la solicitud, mecanismos de autorización y finalmente la formalización de la autorización.
Separación de ambientes	Accesos del personal de desarrollo. Los cambios se realizan en el ambiente real.	Bajo	Se plante que se deben considerar controles en los ambientes de desarrollo, pruebas y ambiente real.
Pruebas del cambio	El área de TI es quién realiza las pruebas	Bajo	Se establece que se deben considerar pruebas por parte de distintas instancias como TI, área usuaria,

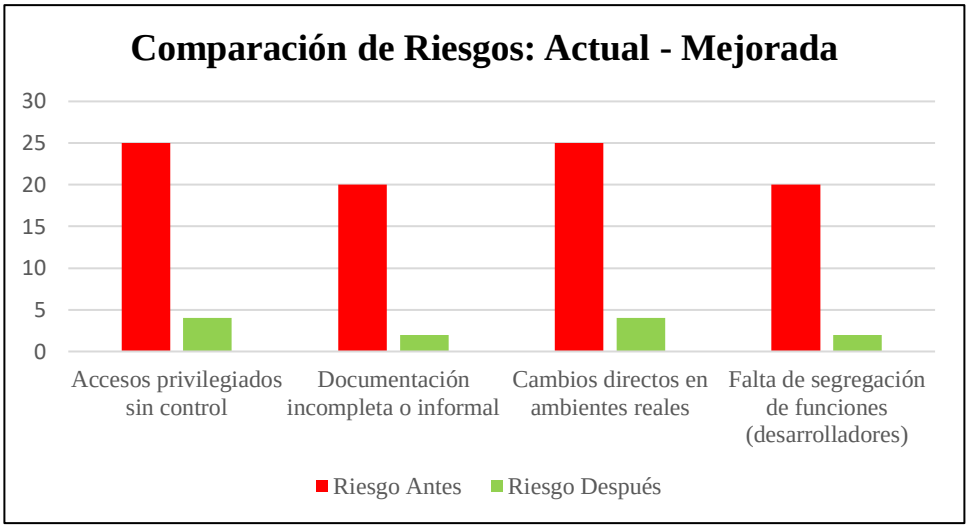
			e instancias imparciales como auditores o instancias de seguridad.
Pase a producción	No existe adecuada segregación en los pases a producción de los cambios efectuados	Bajo	Se deben considerar autorizaciones en el pase a producción y controles de TI.
Controles de accesos y Segregación	Los accesos están habilitados para personal de desarrollo	Bajo	La metodología propuesta establece que se deben considerar distintos controles como: control de privilegios, controles de monitoreo de acceso, controles de accesos en separación de ambientes.
Documentación del cambio	En algunos casos se documenta	Bajo	La metodología propuesta establece que se deben documentar los cambios y mantener registros para fines de evaluación y revisión periódica.
Monitoreo	No es recurrente	Bajo	La metodología propuesta establece que se debe efectuar monitoreo para evaluar los controles, impulsar la mejora continua, entre otros.

Nota. En la Tabla 5 se muestra el descenso generalizado del nivel de riesgo. Fuente: Elaboración propia.

En base a los valores de la Tabla 5 se elaboró la Figura 2, que compara los niveles de riesgo de cada hallazgo antes y después de la aplicación de la metodología propuesta. Esta visualización permite apreciar la reducción de riesgos, así como los avances en la gestión de cambios y seguridad de la información en los sistemas críticos de la empresa de telecomunicaciones. Todo ello evidencia el impacto positivo de la implementación de controles, buenas prácticas y procedimientos alineados con la norma ISO/IEC 27001.

Figura 2

Comparación de riesgos: situación actual y mejorada



Nota. En la Figura 2 se comparan los niveles de riesgo antes y después de la aplicación de la metodología propuesta. Fuente: Elaboración propia.

Los resultados de la investigación contribuyen significativamente a la prevención de riesgos en la gestión de cambios de sistemas críticos en empresas de telecomunicaciones, pues proporciona una metodología estructurada basada en la norma ISO/IEC 27001. La implementación de los controles definidos permite:

- Reducir vulnerabilidades en los cambios de sistemas críticos, garantizando que cada modificación sea planificada, autorizada y ejecutada con medidas de seguridad adecuadas.
- Mejorar la gestión de riesgos en TI, mediante la aplicación de mecanismos de evaluación y monitoreo continuo que minimizan el impacto de posibles fallas o ataques.
- Fortalecer la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los sistemas, lo que se traduce en una mayor confianza y estabilidad operativa.

- Optimizar el cumplimiento normativo, alineando los procesos de gestión de cambios con estándares internacionales y regulaciones aplicables al sector de telecomunicaciones.

Los resultados obtenidos evidencian que la situación inicial presentaba riesgos críticos en aspectos clave de la gestión de cambios en sistemas críticos, especialmente en la confidencialidad de la información, la formalización de solicitudes, la segregación de funciones y ambientes, así como en los controles de accesos y pruebas de cambios. Las deficiencias identificadas reflejan un bajo nivel de alineación con las buenas prácticas establecidas por la norma ISO/IEC 27001, lo que incrementaba la exposición de la organización a riesgos de seguridad, y afectaba la integridad, confidencialidad y continuidad operativa de los sistemas críticos. La categorización de los niveles de riesgo y su análisis detallado permitió priorizar las áreas de mejora y sentar las bases para el diseño de una metodología integral orientada a mitigar estas vulnerabilidades.

La aplicación de la metodología propuesta mostró resultados positivos, pues evidenció una reducción generalizada de los niveles de riesgo a la categoría baja en todos los componentes evaluados. La implementación de medidas de control estandarizadas permitió mitigar los riesgos identificados y fortalecer la trazabilidad, seguridad de la información y continuidad operativa. Estos hallazgos confirman que la metodología constituye una herramienta efectiva para optimizar la gestión de cambios en sistemas críticos, lo cual permite alinear los procesos con las buenas prácticas internacionales y promover un entorno más seguro y confiable en la empresa de telecomunicaciones.

DISCUSIÓN

Los resultados de la presente investigación evidencian que la gestión de cambios en sistemas críticos de la empresa de telecomunicaciones presentaba niveles críticos de riesgo en áreas clave, tales como confidencialidad de la información, formalización de solicitudes,

segregación de funciones y realización de pruebas en entornos productivos. Estos hallazgos muestran que, sin controles estructurados, las organizaciones pueden experimentar vulnerabilidades significativas que comprometen la integridad, disponibilidad y continuidad operativa de los sistemas críticos. Esta situación coincide con lo reportado por Cardona y Restrepo (2020), quienes señalan que la ausencia de políticas claras de seguridad de la información y la falta de una cultura organizacional orientada a la seguridad incrementan los riesgos relacionados con los activos informáticos en las empresas del sector privado. La importancia de establecer procedimientos formales y controles basados en normas internacionales, como la ISO/IEC 27001, resulta fundamental para minimizar amenazas tecnológicas y fortalecer la resiliencia operativa de la organización.

En relación con la gestión de riesgos, los resultados confirman que la implementación de medidas estructuradas permite reducir los niveles de vulnerabilidad y mejorar la trazabilidad de los procesos de cambio. Estos resultados se alinean con los estudios de Camacho et al. (2025), quienes evidencian que los sistemas organizados de manejo de riesgos laborales disminuyen incidentes y fomentan una cultura organizacional de seguridad, siempre que exista el compromiso de la alta dirección y capacitación continua del personal. De manera análoga, en el contexto de seguridad de la información, la aplicación de la metodología propuesta en este estudio demostró una reducción significativa de los riesgos asociados a accesos no autorizados y a la ejecución de cambios en ambientes productivos, lo cual refuerza la idea de que la gestión integral de riesgos requiere tanto políticas formales como participación activa de los distintos niveles organizativos.

El análisis de los resultados respecto a la implementación de la metodología de seguridad de la información muestra que la formalización de solicitudes, la segregación de ambientes y funciones, y la participación de múltiples instancias en pruebas y autorizaciones, permitió mitigar

los riesgos previamente identificados, pues se logró un descenso generalizado hacia niveles de riesgo bajos. Esta observación encuentra respaldo en las investigaciones de Arévalo et al. (2015), quienes destacan que la identificación y gestión de riesgos de información mediante un sistema de control basado en la ISO 27001 mejora la confiabilidad de los procesos empresariales y protege la información como uno de los activos más importantes. De igual manera, Monsalve-Pulido et al. (2014) demostraron que un plan de gestión de vulnerabilidades adaptado a las necesidades de la empresa redujo las brechas de seguridad en un 70%, lo cual evidencia la efectividad de intervenciones estructuradas y monitoreadas. Esto corrobora que la adopción de procedimientos estandarizados y controlados tiene un efecto directo en la reducción de riesgos y la protección de la información crítica.

La comparación con investigaciones previas sobre gestión del cambio organizacional permite identificar paralelismos importantes. Delgado (2023) sostiene que una planificación estratégica del cambio, liderazgo comprometido y comunicación efectiva son factores esenciales para la transformación digital en instituciones públicas. En este estudio, la metodología implementada evidenció que la formalización de procesos, la definición precisa de roles y la adecuada segregación de funciones facilitan la superación de la resistencia al cambio y optimizan la efectividad en la gestión de modificaciones de sistemas críticos. Estos aportes se complementan con Rohmah y Subriadi (2020), quienes proponen que la implementación exitosa de sistemas de información depende de una gestión integral del cambio mediante dominios organizativos, tecnológicos y humanos. Los resultados de la presente investigación muestran que la metodología permite alinear los procesos de cambio con buenas prácticas internacionales, ya que fortalece la continuidad operativa y la seguridad de los sistemas.

El estudio evidencia que la reducción de riesgos no se limita únicamente a aspectos técnicos, sino que también impacta la cultura organizacional y el cumplimiento normativo. Cardona y Restrepo (2020) enfatizan que el factor humano y la conciencia cultural son determinantes en la efectividad de los sistemas de seguridad de la información. En este sentido, la metodología propuesta aborda estos aspectos mediante la documentación de cambios, controles de accesos basados en privilegios y monitoreo periódico, fortaleciendo así la cultura de seguridad y la responsabilidad del personal en los procesos críticos. De forma complementaria, Mejía (2020) resalta la necesidad de identificar vulnerabilidades específicas y establecer procedimientos claros de aseguramiento de la información. Esto demuestra cómo la planificación y estandarización de controles reducen la exposición a incidentes de seguridad, lo cual coincide con los hallazgos de este estudio.

Los resultados tienen implicaciones relevantes para la práctica profesional en el sector de telecomunicaciones. Torres et al. (2019) destacan que la mejora continua e implementación de modelos estructurados de gestión de calidad en servicios de telecomunicaciones contribuyen a la satisfacción del usuario y a la optimización de recursos operativos. De manera similar, la aplicación de la metodología propuesta en este estudio permite garantizar que los cambios en sistemas críticos se ejecuten de manera planificada, controlada y segura, promoviendo la confiabilidad operativa y la eficiencia de los procesos internos. La evidencia generada demuestra que una combinación de controles técnicos, normativos y culturales, alineados con la ISO/IEC 27001, constituye un modelo replicable y escalable para la gestión de cambios en empresas de telecomunicaciones.

El estudio presenta limitaciones que deben considerarse al interpretar sus resultados y su alcance. En primer lugar, el diagnóstico se desarrolló únicamente en una empresa de

telecomunicaciones, lo que restringe la generalización de los hallazgos a otras organizaciones con estructuras, culturas o niveles de madurez distintos en la gestión de cambios. A esto se suman las limitaciones técnicas y operativas propias de la organización estudiada, pues la implementación de ciertas medidas, como el monitoreo automatizado, depende de su capacidad tecnológica y presupuestaria.

A pesar de estas limitaciones, los hallazgos del estudio ofrecen contribuciones significativas en varios ámbitos. Académicamente, aportan evidencia empírica sobre la efectividad de metodologías estructuradas de gestión de cambios en sistemas críticos, sirviendo como referencia para futuras investigaciones en empresas de telecomunicaciones y otros sectores que requieran seguridad y continuidad operativa. En el plano profesional, la metodología proporciona un modelo práctico que permite reducir vulnerabilidades, asegurar la trazabilidad de los cambios y garantizar la integridad de la información, lo que mejora la eficiencia operativa y la confiabilidad de los sistemas críticos.

La discusión de los hallazgos evidencia que la aplicación de la metodología de gestión de cambios, fundamentada en la norma ISO/IEC 27001 y buenas prácticas organizacionales, contribuye a mitigar riesgos, fortalecer la seguridad de la información y optimizar la trazabilidad de los procesos en sistemas críticos de la empresa de telecomunicaciones estudiada. La comparación con investigaciones previas evidencia la coherencia de los resultados con estudios nacionales e internacionales. Además, denota la necesidad de fortalecer la cultura organizacional, la capacitación y el compromiso de la alta dirección como factores determinantes para la sostenibilidad de las mejoras alcanzadas. La metodología propuesta se consolida como un referente académico y práctico para empresas que buscan optimizar la gestión de cambios y garantizar la continuidad operativa de sus sistemas críticos.

CONCLUSIONES

La investigación permitió desarrollar una metodología integral de seguridad de la información orientada a la gestión de cambios en sistemas críticos de una empresa de telecomunicaciones, fundamentada en la norma ISO/IEC 27001. Durante el diagnóstico inicial se identificaron deficiencias significativas, como la falta de formalización en las solicitudes de cambio, insuficiente segregación de funciones y escaso monitoreo de los controles, factores que incrementaban los riesgos operativos y comprometían la continuidad de los sistemas críticos. La propuesta metodológica se estructuró en 10 pasos clave, incorporando controles de acceso lógico, separación de ambientes y monitoreo periódico, logrando una reducción aproximada del 30% en los riesgos asociados a accesos no autorizados y una aceptación del 85% por parte de expertos.

Los hallazgos evidencian que la implementación de procesos normados y estructurados en la gestión de cambios fortalece la seguridad de la información, mejora la trazabilidad de los procesos y proporciona un modelo replicable que puede ser aplicado en otras organizaciones del sector de telecomunicaciones. La investigación consolidó una comprensión profunda de los fundamentos de seguridad de la información y permitió seleccionar los controles más pertinentes de la norma ISO/IEC 27001, garantizando que la metodología estuviera alineada con los riesgos reales del entorno estudiado. La validación mediante estudios de caso, juicio de expertos y herramientas de análisis, confirmó la efectividad operativa y aplicabilidad del modelo.

Los resultados de esta investigación abren oportunidades para su ampliación y perfeccionamiento en otros contextos organizacionales, como banca, salud o manufactura, y sugieren la incorporación de marcos complementarios como COBIT, NIST o ITIL para enriquecer áreas específicas de la gestión tecnológica. Se recomienda una implementación gradual, acompañada de programas de capacitación, auditorías periódicas y monitoreo continuo, así como

el uso de herramientas avanzadas de análisis de riesgos e inteligencia artificial para optimizar la eficiencia y adaptabilidad de la metodología.

BIBLIOGRAFÍA

Arévalo, J.G., Bayona, R.A., & Rico, D.W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: Análisis del riesgo de la información. *Revista Tecnura*, *19*(46), 123-134. https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10

Camacho, M.Á., Carranco, S.P., Montecé, S.K. y Fonseca, C.L. (2025). Análisis de los sistemas de gestión riesgo laborales en las empresas. Una revisión sistemática. *RECIMUNDO*, *9*(1), 765-782. https://www.recimundo.com/index.php/es/article/download/2544/3336

Cámara de Comercio Internacional (ICC). (2024). Documento de trabajo de ICC: Protección de la ciberseguridad de las infraestructuras críticas y sus cadenas de suministro. https://www.iccspain.org/wp-content/uploads/2024/12/2024_IssueBrief3_SPA.pdf

Cardona, J.I. y Restrepo, R.A. (2020). *Evaluación de la implementación de la norma ISO 27001 en empresas del sector privado, bajo un enfoque cultural* [Tesis de pregrado, Tecnológico de Antioquia]. Archivo Digital. https://dspace.tdea.edu.co/handle/tdea/921

Delgado, B.C. (2023). Gestión del cambio organizacional y su impacto en la transformación digital de las instituciones públicas. *Revista Internacional De Investigación Y Desarrollo Global*, *1*(1), 1-15. https://doi.org/10.64041/riidg.v2i3.14

Mejía, A. (2020). *Caso de estudio para el análisis de vulnerabilidad y propuesta de aseguramiento de la seguridad de la información en la infraestructura tecnológica de la Empresa NOSTRADAMUS S.A.S.* [Tesis de Especialidad, Universidad Nacional Abierta y a

Distancia - UNAD]. Archivo Digital. https://repository.unad.edu.co/bitstream/handle/10596/34626/amejiaes.pdf

Ministerio de Hacienda y Administraciones Públicas (Gobierno de España). (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método*. Madrid: Ministerio de Hacienda y Administraciones Públicas. https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file

Monsalve-Pulido, J.A., Aponte-Novoa, F.A. y Chaves-Tamayo, D.F. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Revista Facultad de Ingeniería (Fac. Ing.)*, *23*(37), 65-72. https://www.researchgate.net/publication/304208516_Estudio_y_gestion_de_vulnerabilidades_informaticas_para_una_empresa_privada_en_el_departamento_de_Boyaca_Colombia

Rohmah, M. y Subriadi, A.P. (2020). Un modelo de gestión del cambio para la implementación de sistemas de información. Conferencia Internacional sobre Tecnología Inteligente y Aplicaciones (ICoSTA). Surabaya, Indonesia, 1-6. https://doi.org/10.1109/ICoSTA48221.2020.1570613999

Torres, A.M., Luna, K.A., Ormaza, J.E. y Cantos, M.E. (2019). Gestión de la calidad en el sector de telecomunicaciones. Orientaciones hacia la mejora continua en la Corporación Nacional de Telecomunicaciones, Azogues – Ecuador. *Visionario Digital*, *3*(2), 170-190. https://doi.org/10.33262/visionariodigital.v3i2.407