Modelo Integral de Gestión de Incidentes para Mejorar la Continuidad Operativa en Redes Corporativas

Comprehensive Incident Management Model to Improve Operational Continuity in Corporate Networks

Autor: Ernesto Armando Salvatierra Arteaga

Universidad Autónoma Gabriel René Moreno (UAGRM), Bolivia

Cómo citar este artículo:

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

Salvatierra Arteaga, E.A. (2025). Modelo integral de gestión de incidentes para mejorar la continuidad operativa en redes corporativas. *Boletín Científico Fronteras Tecnológicas*, *1*(1), 123-146.

Institute of Electrical and Electronics Engineers (IEEE):

E.A. Salvatierra Arteaga, "Modelo integral de gestión de incidentes para mejorar la continuidad operativa en redes corporativas", *Boletín Científico Fronteras Tecnológicas*, vol. 1, no. 1, 123-146, 2025. [En línea].

RESUMEN

El estudio desarrolla un modelo integral de gestión de incidentes fundamentado en los lineamientos de la norma ISO/IEC 27035, el marco ITIL v4 y los controles CIS, con el propósito de reducir el impacto de los incidentes en la red convergente de la Empresa Internacional de Servicio Courier Express. La investigación adopta un enfoque propositivo y aplicado, sustentado en un diagnóstico del estado actual mediante encuestas, entrevistas y análisis de datos, cuyos resultados revelaron problemas de disponibilidad, tiempos de respuesta y repetición de incidentes. El modelo diseñado incorpora procedimientos estandarizados, roles definidos y flujos de atención orientados a mejorar la detección, análisis y resolución de incidentes. Su validación, realizada a través de indicadores clave de desempeño y análisis estadístico no paramétrico, evidenció mejoras significativas en la disponibilidad de la red, la reducción de incidentes repetidos y la satisfacción de los usuarios internos. Los resultados confirman que la adopción de marcos internacionales y controles de seguridad contribuye de manera efectiva a la continuidad operativa y la optimización del servicio tecnológico.

Palabras clave: gestión de incidentes**,** ISO/IEC 27035**,** ITIL v4**,** continuidad del negocio**,** redes corporativas.

ABSTRACT

The study develops a comprehensive incident management model based on the guidelines of ISO/IEC 27035, the ITIL v4 framework, and CIS Controls, with the aim of reducing the impact of incidents on the converged network of the International Courier Express Service Company. The research takes a proactive and applied approach, based on a diagnosis of the current state through surveys, interviews, and data analysis, the results of which revealed problems with availability, response times, and incident recurrence. The model designed incorporates standardized procedures, defined roles, and service flows aimed at improving incident detection, analysis, and resolution. Its validation, carried out through key performance indicators and non-parametric statistical analysis, showed significant improvements in network availability, reduction of repeated incidents, and internal user satisfaction. The results confirm that the adoption of international frameworks and security controls effectively contributes to operational continuity and the optimization of technological services.

Keywords: incident management, ISO/IEC 27035, ITIL v4, business continuity, corporate networks.

INTRODUCCIÓN

Las redes y telecomunicaciones han crecido y se han convertido en un factor importante e imprescindible para la continuidad de los negocios en las empresas a nivel mundial y local, por consecuente, se trata de implementar procedimientos para mantener en correcto funcionamiento todo el proceso de telecomunicación. Es así como las compañías se ven con la necesidad de implementar mecanismos de gestión de incidentes óptimos en sus procesos de telecomunicaciones con el fin de garantizar la continuidad del negocio (Jimenez, 2023).

Este es el caso de la Empresa Internacional de Servicio Courier Express, existente en 220 países, empresa líder en la gestión logística y carga, con visibilidad en sus sistemas sobre todos sus envíos desde la partida hasta la entrega en su país de destino. Por esta razón, la gestión de incidentes en la infraestructura es de vital importancia para la continuidad del negocio. La mitigación de riesgos está siempre presente, sin embargo, de una u otra forma los incidentes van a existir, de tal forma el análisis del impacto juega un papel imprescindible para continuar con la operativa esperada con la menor afectación.

El presente trabajo propone entregar un Modelo de Gestión de incidentes de redes para reducir el impacto en la infraestructura de red convergente de esta empresa, para controlar la calma y crisis de los usuarios al presenciar la caída de sus servicios y de esta forma reducir los reclamos en el servicio, mantener conformes a los clientes internos y externos y por, sobre todo: garantizar la continuidad del negocio.

La investigación se fundamenta en la necesidad de comprender y aplicar los controles establecidos por el Center for Internet Security (CIS) y las directrices de la Norma ISO 27035 en el contexto de la gestión de incidentes de seguridad en redes convergentes. Al explorar conceptos teóricos y estudios relacionados, se busca determinar cómo mitigar los riesgos inherentes a la

infraestructura de red de la Empresa Internacional de Servicio Courier Express finalizando con la aplicación de las buenas prácticas de ITIL V4.

Se destaca el trabajo de Tibaquira (2015), que subraya la importancia de realizar la valoración del riesgo mediante una metodología estructurada, así como la evaluación de los incidentes de acuerdo con los criterios definidos para cada actividad. También señala que, aunque se trabaje en paralelo estas actividades, la definición de un plan de tratamiento del riesgo constituye un insumo para la decisión de la acción que se debe ejecutar según los resultados de la evaluación (Tibaquira, 2015). En el proceso de gestión de incidentes se da una respuesta al mismo, y se validan las lecciones aprendidas; por otro lado, se toma una decisión frente al riesgo ocasionado por el incidente, se comunica y realiza un monitoreo sobre el mismo, según los criterios definidos para la gestión de riesgos. Estos elementos se analizan a partir del estudio de la Empresa Internacional de Servicio Courier Express.

La Empresa Internacional de Servicio Courier Express enfrenta desafíos en la gestión de incidentes en su red convergente. La aplicación de un modelo basado en estándares reconocidos como ISO 27035 y los Controles CIS, permite reducir el impacto de los incidentes y garantizar la continuidad del negocio. A partir de esta comprensión, el estudio se orienta al diseño de un modelo estructurado de gestión de incidentes adaptado a la realidad tecnológica de la organización, articulado con los principios de ISO 27035, ITIL v4 y CIS.

El modelo propuesto integra procesos, roles, flujos de atención y mecanismos de documentación destinados a mejorar la detección, análisis y resolución de incidentes. Se realiza la validación mediante pruebas de funcionamiento, seguimiento sistemático de incidencias y análisis de indicadores clave de desempeño permitirá determinar su efectividad para reducir el impacto

operativo, mejorar la satisfacción de los usuarios y fortalecer la continuidad del negocio dentro de la Empresa Internacional de Servicio Courier Express.

METODOLOGÍA

Luego de realizar un estudio descriptivo sobre el impacto de la gestión de incidentes en la red y servicios, se propone un modelo de gestión de incidentes para la red convergente, basado en los lineamientos de la norma ISO 27035, ITIL v4 y controles CIS, dirigido a reducir el impacto en la gestión de incidentes de redes en la Empresa Internacional de Servicio Courier Express. Esta investigación permite brindar solución a los problemas prácticos relacionados con la gestión de incidentes de redes en la red convergente de la Empresa Internacional de Servicio Courier Express.

La población de la presente investigación estuvo constituida por el personal de la Empresa Internacional de Servicio Courier Express, conformada por 90 colaboradores. Este grupo incluyó a todos los empleados que participan directa o indirectamente en los procesos operativos y administrativos de la empresa, lo que permitió abarcar distintos niveles de responsabilidad y áreas funcionales. La selección de esta población se fundamenta en la necesidad de comprender de manera integral la gestión de incidentes y su impacto en la continuidad operativa, garantizando que los datos recopilados reflejen la realidad de los procedimientos internos y la toma de decisiones en la organización.

El proceso metodológico de la presente investigación se estructuró en cuatro fases, orientadas a garantizar el rigor científico y la replicabilidad del estudio. En una primera fase, se realizó un diagnóstico de la situación actual de la gestión de incidentes en la red corporativa de la empresa objeto de estudio, mediante la identificación, clasificación y análisis de los incidentes registrados, así como de los procedimientos existentes para su atención. Esta etapa permitió reconocer debilidades, riesgos operativos y brechas en la continuidad del servicio.

En una segunda fase, se desarrolló el marco teórico, sustentado en la revisión sistemática de literatura especializada, normas y buenas prácticas relacionadas con la gestión de incidentes y la continuidad operativa, tales como ISO/IEC 27035, ITIL v4 y controles CIS. Este análisis teórico proporcionó los fundamentos conceptuales y normativos necesarios para orientar el diseño de la propuesta de solución.

En la tercera fase se elaboró la propuesta de solución, consistente en un modelo integral de gestión de incidentes, diseñado a partir de los hallazgos del diagnóstico y alineado con los lineamientos establecidos en los marcos normativos analizados. La propuesta incorporó procesos, roles, controles y mecanismos de monitoreo orientados a mejorar la disponibilidad de la red y fortalecer la continuidad operativa.

En la cuarta fase, se llevó a cabo la validación de la propuesta, mediante la evaluación de su pertinencia, coherencia y aplicabilidad en el contexto organizacional estudiado. Esta validación permitió verificar el cumplimiento de los objetivos planteados y determinar el potencial impacto del modelo propuesto en la mejora de la gestión de incidentes y la continuidad del negocio.

Con el propósito de garantizar el tratamiento sistemático de la información y un adecuado soporte al proceso metodológico, la investigación empleó diversas herramientas tecnológicas orientadas al análisis de datos, la gestión bibliográfica, la simulación y modelado de procesos. La selección de estas herramientas respondió a criterios de accesibilidad, confiabilidad y pertinencia con los objetivos del estudio, asegurando su adecuada aplicación en cada fase de la investigación. Estas herramientas permitieron organizar, procesar y representar la información de manera clara y estructurada, contribuyendo a la rigurosidad del estudio y la correcta interpretación de los resultados.

Tabla 1

Herramientas tecnológicas utilizadas en la investigación

Categoría	Herramienta / Tecnología	Uso en la investigación
Análisis de datos	Microsoft Office	Procesamiento, organización y análisis básico de datos, así como elaboración de tablas y gráficos para la presentación de resultados.
Gestión bibliográfica	Microsoft Office	Organización y sistematización de referencias bibliográficas y apoyo en la redacción del marco teórico.
Simulación y modelado	Microsoft Visio	Diseño y modelado de diagramas de procesos, flujos de gestión de incidentes y representación gráfica del modelo propuesto.
Simulación y modelado	Lucidchart	Elaboración de diagramas y esquemas conceptuales para la visualización de la arquitectura del modelo de gestión de incidentes.

Nota. La tabla incluye las herramientas tecnológicas utilizadas en la investigación. Fuente: Elaboración propia.

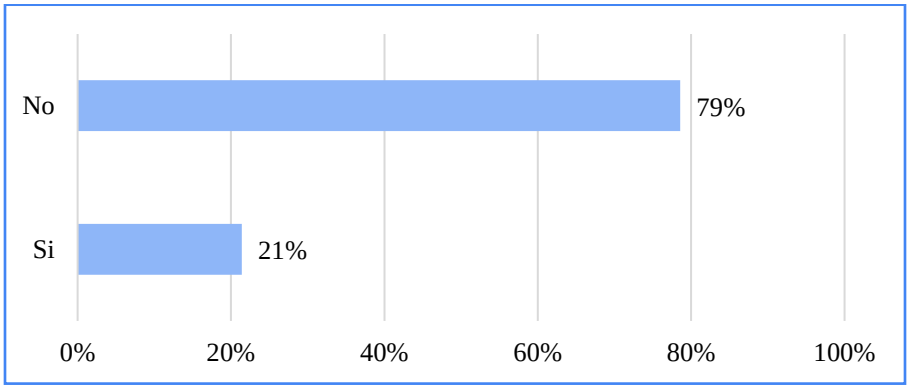
La metodología adoptada permitió analizar de manera sistemática la gestión de incidentes en la red convergente de la Empresa Internacional de Servicio Courier Express mediante la articulación del diagnóstico de la situación actual, un sustento teórico-normativo relevante y el diseño de una propuesta alineada con estándares internacionales. La secuencia de fases desarrolladas, junto con la participación integral de la población de estudio y el uso de herramientas tecnológicas pertinentes, garantizó la rigurosidad, validez y replicabilidad del proceso investigativo. Todo ello proporcionó una base metodológica consistente con la evaluación del modelo propuesto para su contribución a la mejora de la continuidad operativa y la disponibilidad de los servicios de red.

RESULTADOS

Al inicio del proceso investigativo, el análisis de la frecuencia de incidentes recurrentes en la red evidenció que el 79 % de los encuestados manifestó no haber tenido que reportar el mismo problema de red de forma reiterada durante el mes previo a la aplicación de la encuesta. Como se puede apreciar en la Figura 1, el 21 % indicó haber enfrentado incidentes repetidos, lo que pone de manifiesto la existencia de recurrencias que requieren atención.

Figura 1

Porcentaje de frecuencia de problemas repetidos de red



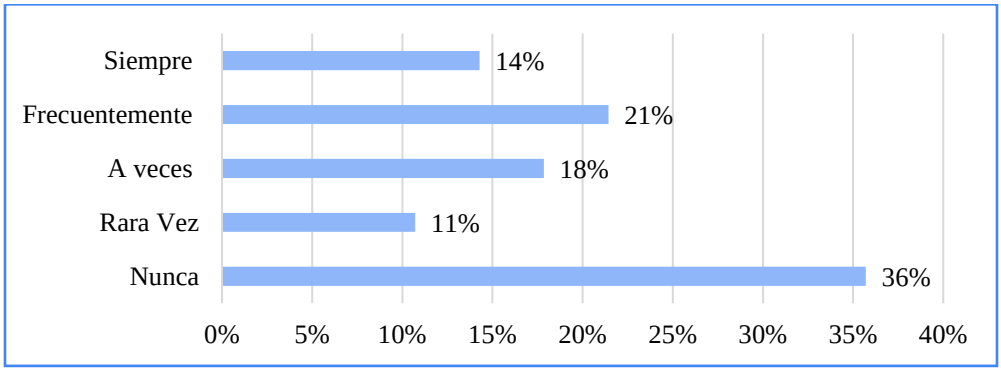
Nota. La figura muestra en porciento la frecuencia de problemas repetidos en la red. Fuente: Elaboración propia.

Los resultados obtenidos muestran que el 35,7 % de los encuestados señaló no haber experimentado interrupciones durante la ejecución de tareas críticas, lo que sugiere un nivel aceptable de estabilidad en determinados procesos de la red; sin embargo, el 17,9 % indicó que las interrupciones se presentan de manera ocasional, mientras el 21,4 % manifestó que estas ocurren con frecuencia. Asimismo, un 14,3 % afirmó que las interrupciones se producen de forma constante, evidenciando la presencia de fallas recurrentes que pueden afectar la continuidad

operativa y el desempeño de las actividades críticas de la organización, tal como se ilustra en la Figura 2.

Figura 2

Porcentaje de frecuencia de interrupciones en tareas críticas



Nota. La figura muestra la frecuencia de las interrupciones en tareas críticas mediante una escala de Likert. Fuente: Elaboración propia.

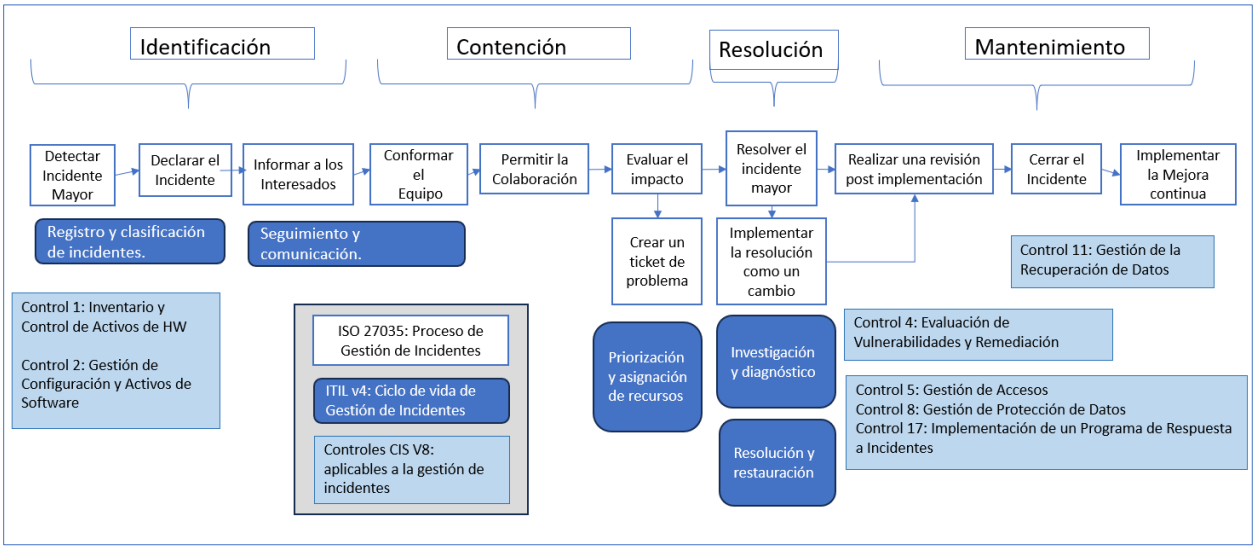
En la Figura 3 se ilustra el modelo de gestión de incidentes propuesto para la Empresa Internacional de Servicio Courier Express, diseñado con el objetivo de reducir el impacto de los incidentes en la infraestructura de red y fortalecer la continuidad operativa. El modelo se sustenta en marcos de referencia reconocidos internacionalmente, como la norma ISO/IEC 27035, ITIL v4 y los controles CIS aplicables a la gestión de incidentes en redes, los cuales aportan lineamientos estructurados para la detección, respuesta y recuperación ante incidentes.

En coherencia con las características y dinámicas internas de la organización, el modelo propuesto fue adaptado a la realidad operativa y organizacional de la empresa, tomando en cuenta sus procesos internos, la disponibilidad de recursos tecnológicos y humanos, así como sus necesidades específicas en materia de gestión de incidentes. Esta adecuación permitió que el modelo responda de manera efectiva a las condiciones reales del entorno estudiado, pues favorece

su aplicabilidad práctica en la mejora de la continuidad operativa y estabilidad de la infraestructura de red.

Figura 3

Modelo de Gestión de Incidentes de Redes en la Empresa Internacional de Servicio Courier Express



Nota. Se muestra la estructura del Modelo de Gestión de Incidentes de redes en la Empresa Internacional de Servicio Courier Express. Fuente: Elaboración propia.

Los resultados obtenidos evidencian el impacto positivo de la implementación del modelo integral de gestión de incidentes en la continuidad operativa de la red corporativa de la Empresa Internacional de Servicio Courier Express. El análisis se sustenta en los datos recolectados durante el diagnóstico inicial y la evaluación posterior a la aplicación del modelo, tomando en cuenta indicadores clave de desempeño relacionados con la recurrencia de incidentes, la disponibilidad de la red y los tiempos de respuesta ante eventos críticos.

En relación con la recurrencia de incidentes, el diagnóstico inicial mostró que, si bien el 79 % de los encuestados indicó no haber tenido que reportar el mismo problema de red en repetidas ocasiones, un 21 % afirmó haber enfrentado incidentes recurrentes. Este porcentaje, aunque minoritario, resulta significativo en una organización con operaciones altamente dependientes de la infraestructura tecnológica, ya que la repetición de fallas sugiere deficiencias en los procesos de análisis y la aplicación de acciones correctivas sostenibles.

Sobre la continuidad del servicio durante la ejecución de tareas críticas, los resultados del diagnóstico reflejaron un escenario heterogéneo. Mientras que el 35,7 % de los usuarios no experimentó interrupciones, un porcentaje significativo reportó afectaciones recurrentes: el 21,4 % indicó que las interrupciones eran frecuentes y el 14,3 % afirmó que se producían de manera constante. Estos hallazgos ponen de manifiesto vulnerabilidades en la gestión de incidentes, especialmente en la capacidad de respuesta oportuna y la prevención de impactos sobre los procesos críticos del negocio.

Para la implementación del modelo se tuvieron en cuenta los siguientes aspectos:

1. **Preparación y Capacitación**

- Creación y documentación de políticas y procedimientos de gestión de incidentes de acuerdo con ISO/IEC 27035 e ITIL v4.
- Formación del IRT mediante el establecimiento de un equipo de respuesta a incidentes con roles y responsabilidades claramente definidos.
- Desarrollo de programas de capacitación para asegurar que todo el personal esté familiarizado con los procedimientos y herramientas de gestión de incidentes.

2. Implementación de Herramientas de Monitoreo y Gestión

- Identificación de problemas subyacentes y ejecución de acciones correctivas para prevenir futuras ocurrencias.
- Implementación de mejoras continuas basadas en las revisiones post-incidente.

En este sentido, la literatura científica suele centrarse en la gestión de incidentes como eventos aislados (AGETIC, 2025); sin embargo, es importante reconocer que muchos incidentes pueden repetirse y que cada ocurrencia brinda la oportunidad de optimizar los tiempos de respuesta y los procesos de gestión. La implementación de estrategias sistemáticas y aplicación de buenas prácticas permiten reducir progresivamente el impacto de los incidentes, mejorando la continuidad operativa y fortaleciendo la resiliencia de la infraestructura de red.

La mejora continua es un principio fundamental en la gestión de servicios de TI y la seguridad de la información. La integración de la ISO/IEC 27035, ITIL v4 y los controles CIS (*Center for Internet Security*) v8 proporciona un enfoque completo para gestionar incidentes de redes de manera efectiva y sostenida. Aquí se presenta un modelo de mejora continua que combina las mejores prácticas de estos marcos.

En primer lugar, se presentan los principales marcos de referencia que sustentan la mejora continua en la gestión de incidentes de redes y seguridad de la información. En ella se sintetizan los enfoques y aportes de la norma ISO/IEC 27035, el marco de buenas prácticas ITIL v4 y los Controles CIS v8, destacando cómo cada uno contribuye, desde su ámbito específico, a la estructuración de procesos orientados a la prevención, detección, respuesta y aprendizaje organizacional frente a incidentes tecnológicos.

Tabla 2

Marcos de referencia para la mejora continua en la gestión de incidentes

Marco / Norma	Enfoque principal	Aportes a la gestión de incidentes
ISO/IEC 27035	Gestión de incidentes de seguridad de la información	Define un ciclo completo que abarca la preparación, detección, análisis, respuesta, recuperación y lecciones aprendidas, orientado a la protección de la información.
ITIL v4	Gestión de servicios de TI	Proporciona un enfoque estructurado para la gestión de incidentes, problemas, cambios y la mejora continua del servicio (CSI), integrando procesos operativos y estratégicos.
Controles CIS v8	Seguridad cibernética basada en buenas prácticas	Conjunto de 18 controles esenciales que fortalecen la seguridad de redes y sistemas de TI mediante acciones técnicas, organizativas y de monitoreo continuo.

Nota. La información presentada sintetiza los principales enfoques y aportes de la norma ISO/IEC 27035, el marco de buenas prácticas ITIL v4 y los Controles CIS v8 en relación con la gestión de incidentes y la mejora continua de los servicios de tecnologías de la información. Fuente: Elaboración propia.

A continuación, se describe la aplicación de los Controles CIS v8 en el contexto de la gestión y control de incidentes, organizándolos según las áreas funcionales en las que impactan dentro de la infraestructura de redes. Esta sistematización permite evidenciar la relación directa entre los controles de seguridad y los procesos operativos de gestión de incidentes, facilitando su alineación con acuerdos de nivel de servicio (SLA) y con los principios de mejora continua establecidos en los marcos de referencia analizados.

Tabla 3

Aplicación de los Controles CIS v8 en la gestión y control de incidentes

Área de aplicación	Control CIS v8	Objetivo del control
Gestión y control automatizado	Control 4: Evaluación de Vulnerabilidades y Remediación	Identificar vulnerabilidades de forma continua y aplicar acciones correctivas oportunas.
Gestión y control automatizado / Análisis de logs	Control 6: Mantenimiento, Monitoreo y Análisis de Registros de Auditoría	Garantizar la recolección, análisis y alertas ante eventos críticos de seguridad.

Resolución de problemas con SLA definido	Control 18: Implementación de un Programa de Respuesta a Incidentes	Establecer tiempos de respuesta y resolución para incidentes de seguridad, alineados a SLA.
Inventario de activos de redes	Control 1: Inventario y Control de Activos de Empresa	Mantener visibilidad y control de los activos de hardware y software de la organización.
Conexiones seguras e identidad	Control 5: Gestión de Accesos	Asegurar el acceso a los sistemas mediante mecanismos de autenticación y control de identidades.
Defensa contra ataques de red	Control 8: Gestión de Protección de Datos	Proteger la red frente a ataques mediante mecanismos de detección y prevención.
Control de puertos, protocolos y servicios	Control 9: Control de Puertos de Red, Protocolos y Servicios	Reducir la superficie de ataque controlando servicios y puertos innecesarios.

Nota. La tabla organiza la aplicación de los Controles CIS v8, según áreas funcionales clave de la gestión y control de incidentes en redes, destacando su contribución a la seguridad, la continuidad operativa y el cumplimiento de acuerdos de nivel de servicio (SLA). Fuente: Elaboración propia.

Por último, se exponen las principales prácticas y herramientas tecnológicas asociadas a la implementación de los Controles CIS v8, enfocándose en su aplicación práctica dentro de entornos de redes corporativas. La información presentada permite comprender cómo la automatización, el monitoreo y el análisis continuo de eventos fortalecen la capacidad de respuesta ante incidentes, contribuyendo a una gestión más eficiente, proactiva y alineada con los estándares internacionales de seguridad de la información.

Tabla 4

Herramientas y prácticas tecnológicas asociadas a los Controles CIS v8

Control CIS v8	**Prácticas implementadas**	**Herramientas referenciales**
Control 4	Escaneos automatizados de vulnerabilidades y aplicación automática de parches	Nessus, OpenVAS
Control 6	Recolección, análisis automatizado de logs y alertas de eventos críticos	Splunk, ELK Stack, Graylog, QRadar
Control 18	Definición de SLA y automatización de respuestas a incidentes comunes	Demisto, Phantom (SOAR)

Control 1	Inventario automatizado de hardware y software	Lansweeper, Spiceworks, SCCM, JAMF
Control 5	Implementación de MFA y gestión de identidades y accesos	Duo, Okta, Microsoft Authenticator, Azure AD, Ping Identity
Control 8	Protección perimetral y detección de intrusiones	Palo Alto Networks, Fortinet, Snort, Suricata
Control 9	Automatización del cierre de puertos y monitoreo de servicios	Ansible, Chef, Nagios, Zabbix

Nota. Se presentan prácticas y herramientas tecnológicas referenciales asociadas a la implementación de los Controles CIS v8, orientadas a la automatización, el monitoreo y la respuesta ante incidentes en entornos de redes corporativas. Fuente: Elaboración propia.

La integración de los Controles CIS v8 en la gestión y control automatizado de redes proporciona un enfoque robusto y estructurado para mejorar la seguridad y eficiencia de las operaciones de TI. Al aplicar estos controles, las organizaciones pueden mejorar significativamente su capacidad para gestionar incidentes de seguridad, asegurar la continuidad de sus servicios de TI y proteger sus activos críticos.

El *Center for Internet Security* (CIS) proporciona los CIS *Controls Self Assessment Tool* (CSAT), una herramienta que permite a las organizaciones evaluar su implementación de los Controles CIS v8. La gestión de incidentes de redes es crucial para mantener la seguridad y la operatividad de los sistemas de TI. Los Controles CIS v8 ofrecen un conjunto de mejores prácticas para proteger estos sistemas.

Tras la implementación del modelo de gestión de incidentes, fundamentado en la norma ISO/IEC 27035, el marco ITIL v4 y los Controles CIS, se observó una mejora significativa en los indicadores evaluados. En términos de tiempo de respuesta, los resultados de la validación estadística mostraron un incremento notable en la satisfacción de los usuarios internos, lo que indica una mayor eficiencia en los procesos de detección, registro, clasificación y atención de

incidentes. La definición clara de roles, responsabilidades y flujos de trabajo contribuyó a reducir los retrasos asociados a la atención improvisada de eventos.

La disponibilidad de la red también evidenció mejoras estadísticamente significativas posterior a la aplicación del modelo. La estandarización de procedimientos y la integración de buenas prácticas internacionales permitieron fortalecer los mecanismos de monitoreo, análisis y recuperación del servicio, reduciendo las interrupciones que afectaban directamente a las operaciones logísticas de la empresa. Este resultado resulta especialmente relevante en un entorno corporativo donde la continuidad operativa constituye un factor crítico para el cumplimiento de los niveles de servicio.

Se constató una reducción significativa en la cantidad de incidentes repetidos, lo que sugiere que el modelo no solo mejora la respuesta reactiva ante eventos, sino que también contribuye a una gestión más proactiva y preventiva. La incorporación de actividades orientadas al análisis de causas raíz y a la retroalimentación continua permitió disminuir la recurrencia de fallas previamente identificadas, optimizando el desempeño global de la infraestructura de red.

Los resultados confirman que la adopción de un modelo integral de gestión de incidentes, alineado con estándares internacionales y controles de seguridad reconocidos, tiene un impacto directo y positivo en la continuidad operativa de la organización. La mejora en los tiempos de respuesta, la mayor disponibilidad de la red y la reducción de incidentes recurrentes evidencian la pertinencia y efectividad del modelo propuesto, consolidándolo como una alternativa viable para fortalecer la resiliencia tecnológica en redes corporativas complejas.

La implementación del modelo permitió reducir significativamente los tiempos de respuesta, mejorar la disponibilidad de la red y disminuir los problemas recurrentes. Estos resultados demuestran que el modelo propuesto es efectivo para mitigar el impacto de los

incidentes y asegurar la continuidad operativa de la Empresa Internacional de Servicio Courier Express.

DISCUSIÓN

Los resultados obtenidos en este estudio confirman la relevancia estratégica de la gestión de incidentes como factor determinante para garantizar la continuidad operativa en infraestructuras corporativas, en correspondencia con lo planteado por la literatura especializada sobre resiliencia tecnológica (Hubbard & Seiersen, 2023). La evidencia empírica recopilada en la Empresa Internacional de Servicio Courier Express reflejó la existencia de interrupciones recurrentes, tiempos de respuesta prolongados y una débil capacidad de identificación temprana de incidentes, elementos que coinciden con los problemas típicos señalados por la norma ISO/IEC 27035. Otros autores, como Aguilar y Abraham (2009), destacan que la ausencia de procesos estandarizados incrementa la vulnerabilidad operacional y amplifica el impacto de los incidentes en organizaciones altamente dependientes de sus sistemas de información, lo que resalta la necesidad de implementar modelos de gestión de incidentes integrales que optimicen la detección, respuesta y prevención de fallas.

En la investigación se corrobora la vigencia de los principios teóricos del enfoque preventivo y estructurado en la gestión de incidentes. La integración conceptual derivada de ISO/IEC 27035, ITIL v4 y los controles CIS permitió construir un modelo de gestión orientado a funciones críticas como la detección, el análisis, la priorización, el registro y la respuesta. Este alineamiento teórico–práctico se ajusta a lo planteado por Loayza-Uyehara (2016) y el propio ITIL v4, quienes enfatizan que la apropiada definición de roles, flujos de trabajo y métricas de desempeño incrementa la capacidad de control sobre el ciclo de vida del incidente y reduce la probabilidad de recurrencias. La mejora en la disponibilidad de la red registrada después la

implementación del modelo confirma que una gestión sistemática de incidentes, respaldada por estándares reconocidos internacionalmente, reduce la ocurrencia de fallos y fortalece la madurez operativa, tal como lo respalda la comunidad del CIS.

El estudio aporta evidencia empírica que dialoga con investigaciones previas donde se destaca la importancia de la convergencia entre monitoreo continuo, documentación estructurada y aprendizaje organizacional. Autores como Coronado-García (2024) señalan que las organizaciones que adoptan marcos integrales logran reducir significativamente los tiempos de recuperación y fortalecer los mecanismos de retroalimentación para prevenir incidentes futuros. En coherencia, el modelo propuesto integró mecanismos de registro y documentación que permitieron analizar patrones, mejorar la trazabilidad y consolidar procedimientos preventivos. Esto se tradujo en una reducción de incidentes repetidos, resultado que coincide con los beneficios esperados por los lineamientos de la seguridad basada en controles CIS.

Los hallazgos obtenidos demuestran que la aplicación de marcos internacionales no implica una adopción mecánica, sino un proceso de adaptación contextual. La literatura reciente en gestión de incidencias sugiere que los modelos deben ajustarse a las capacidades, cultura organizacional y recursos de cada entorno (Coronado-García, 2024; Menier, 2017; Loayza-Uyehara, 2016). En este trabajo, el diagnóstico situacional permitió identificar brechas específicas—como la falta de procedimientos formales, ausencia de un sistema de priorización y limitada coordinación entre áreas técnicas—que orientaron el diseño de un modelo ajustado a la realidad tecnológica y organizacional de la Empresa Internacional de Servicio Courier Express. Este enfoque contextualizado se corresponde con lo expuesto por Coronado-García (2024), Menier (2017) y Loayza-Uyehara (2016), quienes advierten que la efectividad de los centros de respuesta depende de su alineación con las necesidades reales del negocio.

La comparación de los resultados obtenidos con investigaciones previas evidencia que la implementación de ISO 27035 e ITIL v4 contribuye de manera significativa a la satisfacción de los usuarios internos, pues optimiza los tiempos de respuesta y fortalece la comunicación entre los distintos niveles operativos, lo que mejora la eficiencia y continuidad de los procesos críticos de la organización (Tibaquira, 2015). La mejora reportada en la percepción de los usuarios internos respalda esta tendencia y confirma que los flujos de trabajo claros contribuyen a una experiencia más confiable y eficiente en la operación diaria.

Esta investigación aporta evidencia relevante de que la integración de estándares internacionales y buenas prácticas en la gestión de incidentes fortalece la continuidad del negocio, incrementa la resiliencia operativa y reduce el impacto de eventos disruptivos. Los resultados reafirman que la estandarización en la detección, análisis y tratamiento de incidentes constituye un elemento crítico para organizaciones que operan sobre redes corporativas de alta demanda. El estudio confirma que la combinación entre diagnóstico situacional, adaptación contextual y validación mediante indicadores de desempeño constituye una estrategia efectiva para la mejora continua en entornos tecnológicos complejos.

La investigación presenta ciertas limitaciones que conviene considerar al interpretar los resultados. Entre ellas se encuentra la dependencia de factores externos a la organización, como la administración de los servicios CORE de la infraestructura de la red, incluyendo tecnologías SD-WAN y enlaces MPLS, los cuales son gestionados y soportados por los proveedores ISP. La gestión de incidentes relacionada con estos servicios es asumida por los respectivos *Network Operation Centers* (NOC) de los proveedores, por lo que la organización únicamente puede asumir el cumplimiento de los SLA contratados. Estas condiciones representan restricciones que podrían

influir en la efectividad percibida del modelo y constituyen posibles fuentes de error en la evaluación de la continuidad operativa.

A pesar de estas limitaciones, la implementación de un modelo de gestión de incidentes constituye un aporte significativo para la organización. Adaptarse a un modelo estandarizado representa un desafío, especialmente cuando se aplica a áreas críticas de la infraestructura tecnológica, como las telecomunicaciones; sin embargo, los beneficios de contar con una gestión de incidentes efectiva —reducción del impacto de los incidentes y garantía de continuidad del negocio— hacen que la adopción del modelo sea viable y cuente con el respaldo de la organización, demostrando su aplicabilidad práctica y valor estratégico en la gestión de redes corporativas.

CONCLUSIONES

El análisis realizado evidenció que la gestión de incidentes en la red convergente de la Empresa Internacional de Servicio Courier Express es fundamental para garantizar la continuidad operativa y la calidad del servicio. La revisión teórica de la norma ISO/IEC 27035, el marco ITIL v4 y los controles CIS proporcionó una base conceptual pertinente que permitió identificar brechas en la infraestructura tecnológica y orientar el diseño de un modelo de gestión adaptado a las necesidades reales de la organización.

El diagnóstico realizado mediante encuestas, entrevistas y análisis situacional confirmó la existencia de interrupciones recurrentes, tiempos de respuesta prolongados y limitaciones en los mecanismos actuales de identificación y resolución de incidentes. Estos hallazgos evidenciaron la necesidad de implementar un proceso estructurado y estandarizado que minimice el impacto de los incidentes sobre la operación diaria y mejore la eficiencia de la gestión.

El modelo propuesto, basado en los principios de ISO 27035, ITIL v4 y controles CIS, incorpora procedimientos claros, roles definidos y flujos de trabajo diseñados para optimizar la detección, análisis, documentación y tratamiento de incidentes. Su validación, a través de indicadores de desempeño y análisis estadísticos, mostró mejoras en la disponibilidad de la red, reducción de incidentes repetidos y mayor satisfacción de los usuarios internos, confirmando la eficacia y pertinencia del modelo. Los resultados demuestran que la adopción de estándares internacionales fortalece la resiliencia tecnológica, reduce el impacto de los incidentes y asegura la continuidad del negocio en organizaciones dependientes de su infraestructura de telecomunicaciones.

BIBLIOGRAFÍA

Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC). (2025). Informe de gestión de incidentes y vulnerabilidades informáticas. Bolivia: CSIRT. https://agetic.gob.bo/sites/default/files/2025-08/IGIV-trim_2_25-firmado_1_0.pdf

Aguilar, J. y Abraham, B. (2009). Sistema multiagente para el manejo de incidentes de seguridad. *Ciencia e Ingeniería*, *30* (3), 183-192. https://www.redalyc.org/articulo.oa?id=507550786002

CIS Critical Security Controls version 8. (s/f). CIS. https://www.cisecurity.org/controls/v8

Coronado García, B. (2024). *Gestión de incidentes de seguridad de la información*. Editorial Tutor Formación. https://editorial.tutorformacion.es

Dakic, V., Mikulic, K. & Petrunic, R. (2024). Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP), Proceedings of the 35th DAAAM. International Symposium, pp.0048-0054, B. Katalinic (Ed.), Published by DAAAM International, Vienna, Austria. https://doi.org/10.2507/35th.daaam.proceedings.007

Gupta, B.B., Martinez Perez, G., Agrawal, D. P., & Gupta, D. (2020). *Handbook of Computer Networks and Cyber Security Principles and Paradigms*. Springer Nature Switzerland AG. https://download.e-bookshelf.de/download/0012/6225/18/L-G-0012622518-0038891501.pdf

Hubbard, D.W. y Seiersen, R. (2023). Cómo medir cualquier riesgo de ciberseguridad. John Wiley & Sons. ISBN 1119892309, 9781119892304, 368 págs.

ISO. (2023). ISO/IEC 27035-1:2023. Information Technology. Information Security Incident Management: Part 1. Principles and process.

Jiménez, J. (2023). *Diseño de un Plan para la Continuidad del Negocio, para responder a incidentes que afecten la prestación de Servicios de TIC a nivel de la entidad Fuentes Geotérmicas del Instituto Costarricense de Electricidad*. [Tesis de Maestría]. Universidad Nacional, Heredia, Costa Rica.

Loayza-Uyehara, A.A. (2016). Modelo de gestión de incidentes para una entidad estatal. *Interfases*, (009), 221-254. https://doi.org/10.26439/interfases2016.n009.1247

Menier, M. (Coord.). (2017). *Manual de gestión de la información sobre incidentes de seguridad*. RedR UK, Insecurity Insight, European Interagency Security Forum. https://insecurityinsight.org/wp-content/uploads/2020/02/1-GIIS-Manual-Jan2018_ES.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). (2016). Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Sánchez, F.S., & Valles, M.Á. (2021). Influencia de ITIL V3 en la gestión de incidencias de una municipalidad peruana. *Revista cubana de ciencias informáticas*, *15*(3), 1–19.

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000300001&lng=es&tlng=en.

Tibaquira, Y.A. (2015). Metodología de gestión de incidentes de seguridad de la información y gestión de riesgos para la plataforma SIEM de una entidad financiera basada en la Norma ISO/IEC 27035 e ISO/IEC 27005. https://repository.unad.edu.co/bitstream/handle/10596/3634/80217786.pdf?sequence=1&isAllowed=y