Ciencia y Desarrollo. Universidad Alas Peruanas
http://revistas.uap.edu.pe/ojs/index.php/CYD/index

Recibido 20 de abril 2025 - Aceptado 10 de mayo 2025

# MODELO DE GESTIÓN DE RIESGOS EN INFRAESTRUCTURA TECNOLÓGICA: GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN FLAVIO ALFARO

# RISK MANAGEMENT MODEL FOR TECHNOLOGICAL INFRASTRUCTURE: DECENTRALIZED AUTONOMOUS MUNICIPAL GOVERNMENT OF FLAVIO ALFARO

**Julissa Jamileth Mazamba Muñoz[1], Natacha Yubiri Quijije Delgado[2], Miguel Ángel Napa Gonzalez[3]**

## RESUMEN

El estudio surge ante la evidente vulnerabilidad tecnológica del GAD Municipal de Flavio Alfaro, caracterizada por el uso de infraestructura obsoleta, ausencia de planes de contingencia, y limitadas medidas de seguridad física y lógica, lo que expone a la institución a pérdidas de información, fallos operativos y ciberataques. Por ello, el objetivo fue diseñar un modelo de gestión de riesgos basado en la metodología AMFE, orientado a identificar, evaluar y mitigar los riesgos tecnológicos, fortaleciendo la infraestructura y garantizando la continuidad de los servicios públicos. La investigación aplicó un enfoque mixto: cuantitativo mediante encuestas a 148 trabajadores y cualitativo con entrevistas al personal de TI. Entre los resultados más relevantes, se determinó que el 32 % de los encuestados reconoció que todos los factores, obsolescencia, resiliencia baja y pérdida de datos, afectan conjuntamente la infraestructura; el 49 % señaló que el seguimiento debe incluir todas las etapas del proceso de gestión de riesgos; y el 89 % consideró urgente implementar un modelo más eficiente. En conclusión, la aplicación de un modelo estructurado como AMFE es esencial para optimizar los recursos tecnológicos, reducir la exposición a amenazas y garantizar una infraestructura segura y resiliente alineada a estándares internacionales.

**Palabras clave: Gestión de riesgos, infraestructura tecnológica, municipio, ciberseguridad, metodología AMFE.**

## ABSTRACT

The study arose from the evident technological vulnerability of Flavio Alfaro's Municipal Autonomous Government (GAD), characterized by the use of obsolete infrastructure, the absence of contingency plans, and limited physical and logical security measures, which exposes the institution to data loss, operational failures, and cyberattacks. Therefore, the objective was to design a risk management model based on the FMEA methodology, aimed at identifying, evaluating, and mitigating technological risks, strengthening the infrastructure and ensuring the continuity of public services. The research applied a mixed approach: quantitative through surveys of 148 employees and qualitative through interviews with IT staff. Among the most relevant results, it was determined that 32% of respondents recognized that all factors—obsolescence, low resilience, and data loss—jointly affect the infrastructure; 49% indicated that monitoring should include all stages of the risk management process; and 89% considered it urgent to implement a more efficient model. In conclusion, the application of a structured model like FMEA is essential to optimize technological resources, reduce exposure to threats, and ensure a secure and resilient infrastructure aligned with international standards.

**Keywords: Risk management, technological infrastructure, municipality, cybersecurity, FMEA methodology.**

1. Universidad Estatal del Sur de Manabí. mazamba-julissa4100@unesum.edu.ec. https://orcid.org/0009-0004-9756-4685
2. Universidad Estatal del Sur de Manabí.quijije-natacha2760@unesum.edu.ec. https://orcid.org/0009-0002-8021-3171
3. Universidad Estatal del Sur de Manabí. napa-miguel3701@unesum.edu.ec. https://orcid.org/0009-0006-9381-9681

RESUMO

O estudo aborda os problemas relacionados às limitações na gestão orçamentária do GAD da Paróquia de Noboa, o que dificultou a execução eficiente de projetos comunitários e criou lacunas entre o planejamento e os resultados. O objetivo foi analisar como a gestão orçamentária impacta a execução dos projetos dentro da entidade. Foi aplicada uma abordagem de método misto, utilizando métodos de pesquisa indutivo-dedutiva, analítico-sintética, de campo e bibliográfica, com questionários direcionados aos dez dirigentes do GAD e uma entrevista com seu presidente. Entre os resultados mais relevantes, 60% dos entrevistados consideraram o uso dos recursos completamente eficiente, enquanto 40% perceberam níveis variados de ineficiência; Além disso, 100% classificaram o relacionamento entre a comunidade e as autoridades como transparente. Em relação à execução orçamentária, foram alcançados percentuais expressivos, como 100% em transferências correntes, 98,52% em vendas de ativos e 94,59% em receitas de financiamento. Em conclusão, constatou-se que o planejamento é participativo, mas limitado por fatores financeiros; A execução é eficiente em algumas áreas, embora sejam necessárias melhorias no monitoramento e na comunicação institucional; e uma percepção geral positiva é reconhecida, com necessidade de maior clareza na alocação de recursos.

**Palavras-chave: Orçamento, execução de projetos, freguesia, eficiência financeira, planeamento territorial.**

## INTRODUCCIÓN

A nivel mundial, la infraestructura tecnológica es fundamental para el desarrollo de las organizaciones, ya que permite la optimización de procesos, el acceso a la información y la mejora continua de los servicios. Según Martínez (2024) menciona que, a pesar de ello, el crecimiento exponencial de las amenazas cibernéticas, los desastres naturales y las fallas técnicas ha incrementado la necesidad de implementar modelos de gestión de riesgos que salvaguarden tanto los datos como los sistemas críticos.

Por su parte, en América Latina, diversas investigaciones revelan que la región presenta vulnerabilidades significativas en términos de infraestructura tecnológica debido a inversiones limitadas en seguridad, deficiente planificación de contingencias y escasa adopción de normas internacionales de gestión de riesgos (Comisión Económica para América Latina y el Caribe, 2021). Estos factores han expuesto a las instituciones públicas y privadas a pérdidas económicas y operativas considerables.

En el contexto nacional, Ecuador no es ajeno a esta realidad, aunque se han realizado avances en políticas de seguridad informática y en normas de protección de datos, muchos gobiernos locales, especialmente en zonas rurales y semiurbanas, presentan debilidades en la protección de sus infraestructuras tecnológicas (Ávila, 2024). La falta de planes de contingencia adecuados y de protocolos de seguridad estructurados aumenta el riesgo de interrupciones en los servicios esenciales.

De manera particular, en el Gobierno Autónomo Descentralizado Municipal del cantón Flavio Alfaro, se evidencian diversas problemáticas relacionadas con la vulnerabilidad de la infraestructura tecnológica, destacándose fallas en la seguridad de hardware y software, carencia de planes de gestión de riesgos y ausencia de medidas preventivas ante fenómenos naturales como incendios, inundaciones o terremotos. Estos riesgos comprometen no solo la continuidad de los servicios municipales, sino también la integridad de la información institucional.

Ante esta situación, el objetivo principal del estudio es diseñar un modelo de gestión de riesgo para la infraestructura tecnológica en el GAD Municipal de Flavio Alfaro, permitiendo identificar, evaluar y mitigar los riesgos existentes. De este modo, se busca fortalecer la resiliencia institucional, proteger los activos tecnológicos y garantizar la prestación continua de los servicios públicos a la ciudadanía.

Gestión de riesgos

La gestión de riesgos es un proceso esencial dentro de cualquier organización, pública o privada, que busca identificar, evaluar y controlar los eventos potenciales que puedan afectar el logro de sus objetivos. Según Cando y Medina (2021), la gestión de riesgos implica reconocer la existencia constante de amenazas derivadas de cambios tecnológicos, competitivos y del entorno, proponiendo estrategias que permitan minimizar su impacto negativo. De esta manera, gestionar los riesgos no solo implica reaccionar ante eventos adversos, sino anticiparlos de manera sistemática y organizada para proteger los activos y garantizar la continuidad operativa.

En consecuencia, la importancia de la gestión de riesgos en las organizaciones públicas resulta aún más crítica debido a que estas instituciones son responsables de la provisión de servicios esenciales y del manejo de información sensible de la ciudadanía. Como afirman López y Anías (2020), las entidades públicas deben establecer mecanismos sólidos de prevención y mitigación de riesgos para asegurar su eficiencia, transparencia y resiliencia frente a situaciones de crisis. Además, la adecuada gestión de riesgos contribuye a fortalecer la confianza ciudadana y a garantizar la sostenibilidad institucional a largo plazo, aspectos fundamentales en la administración pública contemporánea.

A partir de ello, resulta pertinente destacar los principios establecidos por la norma ISO 31000:2018, la cual proporciona directrices internacionales para la gestión eficaz de riesgos. De acuerdo con la Organización Internacional de Normalización (2019), entre los principios fundamentales se encuentran la integración de la gestión de riesgos en todos los procesos organizacionales, la adopción de un enfoque estructurado y sistemático, la consideración explícita del contexto externo e interno, y la toma de decisiones basada en la mejor información disponible.

Asimismo, ISO 31000 enfatiza la necesidad de personalizar el sistema de gestión de riesgos a las características específicas de cada organización y de promover la mejora continua del proceso mediante la revisión y retroalimentación constante.

Riesgos tecnológicos

En el contexto de la transformación digital, los riesgos tecnológicos son una amenaza constante para las organizaciones, especialmente aquellas del sector público. Según Llamas (2020), el riesgo tecnológico se refiere a las pérdidas o daños potenciales ocasionados por el uso, implementación o falla de la tecnología, y puede originarse tanto en factores técnicos como humanos, naturales o sociales. Estas amenazas pueden afectar la integridad, disponibilidad y confidencialidad de la información, así como el funcionamiento de los sistemas críticos institucionales.

De acuerdo con Celestino (2023), los riesgos tecnológicos presentan una diversidad de tipologías que deben ser consideradas para una adecuada gestión. El riesgo digital comprende amenazas vinculadas al uso de software y plataformas informáticas, como malware, ransomware o accesos no autorizados.

El riesgo de hardware, en cambio, se refiere a fallas físicas de dispositivos como servidores, routers o discos duros, que pueden derivar en interrupciones del servicio. Asimismo, el riesgo asociado a las redes y comunicaciones abarca la vulnerabilidad de los sistemas de conectividad, los cuales pueden ser explotados mediante ataques como el sniffing o el man-in-the-middle.

Y el riesgo provocado por desastres naturales representa una amenaza significativa para la infraestructura tecnológica, ya que fenómenos como incendios, terremotos o inundaciones pueden causar pérdidas irreparables si no se cuenta con mecanismos de respaldo y contingencia adecuados.

A continuación, se presenta una clasificación de los principales riesgos tecnológicos que afectan la infraestructura de TI:

**Tabla 1**

*Tipología de riesgos tecnológicos que afectan la infraestructura institucional*

| Tipo de riesgo | Descripción breve |
|---|---|
| Riesgo digital | Amenazas derivadas del uso de software y sistemas informáticos (malware, hackeo). |
| Riesgo de hardware | Fallas físicas de componentes tecnológicos (servidores, discos duros, UPS). |
| Riesgo de redes y comunicaciones | Vulnerabilidades en sistemas de conectividad y transmisión de datos. |
| Riesgo de desastres naturales | Daños ocasionados por eventos como terremotos, incendios, o inundaciones. |

*Nota.* Adaptado de Llamas (2020) y Celestino (2023).

Los impactos que generan estos riesgos en instituciones públicas pueden ser múltiples y severos. Como señala Jiménez (2022), la interrupción de servicios tecnológicos afecta directamente la capacidad operativa de las entidades, reduciendo su eficiencia, exponiendo información sensible a filtraciones, y generando desconfianza ciudadana. Además, la pérdida de datos institucionales y la paralización de procesos administrativos comprometen la continuidad del servicio público, afectando no solo la reputación del organismo, sino también el cumplimiento de sus obligaciones legales y sociales.

Infraestructura tecnológica

La infraestructura tecnológica constituye el conjunto de elementos físicos y lógicos que permiten a una organización operar eficazmente en entornos digitales. Según Carrasco et al. (2021), se trata de una arquitectura integrada por hardware, software, redes y sistemas de almacenamiento que garantizan la conectividad, el procesamiento de información y la prestación de servicios. Esta estructura es esencial para el cumplimiento de objetivos institucionales, ya que proporciona la base sobre la cual se ejecutan los procesos tecnológicos y administrativos de las entidades públicas y privadas.

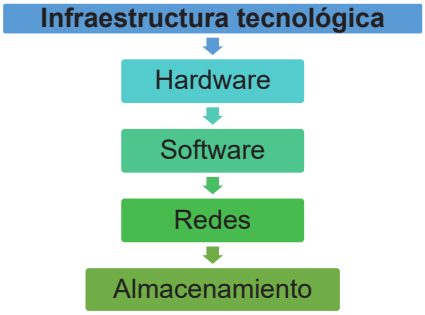
Dentro de esta infraestructura, el hardware comprende todos los componentes físicos como servidores, computadoras, routers y dispositivos de almacenamiento, los cuales actúan como soporte operativo del sistema (Vélez, 2024).

El software, por su parte, incluye sistemas operativos, plataformas de gestión, bases de datos y aplicaciones que permiten el manejo automatizado de la información. Las redes facilitan la interconexión entre los dispositivos, permitiendo el intercambio de datos tanto en ambientes internos como externos. El almacenamiento de datos representa la capacidad de guardar, recuperar y proteger la información crítica de la organización, ya sea en servidores locales o en la nube.

A continuación, se representa gráficamente la estructura de estos componentes principales:

**Figura 1**

*Componentes esenciales de la infraestructura tecnológica en una organización pública*




*Nota.* Elaboración propia con base en Carrasco et al. (2021) y Vélez (2024).

Sin embargo, la presencia de una infraestructura tecnológica no garantiza por sí sola la continuidad operativa, ya que existen vulnerabilidades que pueden comprometer su funcionalidad. De acuerdo con Campi (2024), entre las debilidades más comunes se encuentran la falta de actualizaciones del software, configuraciones incorrectas en los dispositivos, uso de contraseñas débiles, insuficiencia de respaldos automáticos, y escasa capacitación del personal en prácticas de seguridad. Estas fallas pueden ser explotadas por amenazas externas como el malware o internas por errores humanos, generando pérdidas de datos, interrupciones de servicio e incluso daños reputacionales.

Modelos de gestión de riesgos en tecnología

En el ámbito de la gestión tecnológica, diversos modelos han sido desarrollados para abordar los riesgos de manera estructurada y eficiente. Entre los modelos tradicionales, destaca el propuesto por el Project Management Institute (PMI) a través del PMBOK, el cual plantea la identificación, análisis, respuesta y monitoreo de los riesgos como fases fundamentales dentro de la gestión de proyectos (Project Management Institute, 2017).

Asimismo, la norma ISO 21500 establece directrices generales para la gestión de proyectos, incorporando la gestión de riesgos como un proceso continuo que debe ser adaptado a la naturaleza y complejidad de cada organización (Organización Internacional de Normalización, 2012).

De forma complementaria, el enfoque PRINCE2, desarrollado en el Reino Unido, introduce una metodología basada en procesos donde la gestión de riesgos se vincula directamente con la planificación y control de proyectos (Axelos, 2017).

Por otro lado, COBIT 5 se enfoca en el gobierno y la gestión de tecnologías de la información, proporcionando un marco que integra la gestión de riesgos tecnológicos como parte integral del cumplimiento de objetivos organizacionales (ISACA, 2012).

En función de las necesidades específicas de infraestructura tecnológica, han surgido modelos más especializados que consideran la criticidad de los sistemas de hardware, software, redes y almacenamiento. Según Machado (2019), modelos como ITIL y el Análisis Modal de Fallos y Efectos (AMFE) han demostrado ser eficaces para identificar vulnerabilidades en la infraestructura, priorizar riesgos y establecer mecanismos de recuperación y continuidad operativa.

Estos modelos permiten no solo una gestión reactiva, sino una planificación preventiva que fortalece la resiliencia tecnológica de las instituciones.

De esta manera, implementar un modelo de gestión de riesgos aporta beneficios tangibles y estratégicos para las organizaciones, como se presenta a continuación:

**Tabla 2**

*Ventajas de la implementación de un modelo de gestión de riesgos en infraestructura tecnológica*

| Ventaja | Descripción breve |
|---|---|
| Prevención de fallos críticos | Permite identificar vulnerabilidades antes de que causen interrupciones. |
| Mejora en la toma de decisiones | Ofrece información estructurada para decisiones estratégicas de TI. |
| Aumento de la resiliencia | Fortalece la capacidad de recuperación ante incidentes tecnológicos. |
| Optimización de recursos | Minimiza pérdidas económicas mediante la planificación preventiva. |
| Cumplimiento normativo | Asegura el cumplimiento de estándares y regulaciones de seguridad. |

*Nota.* Elaboración propia con base en PMI (2017), ISO (2012), y Machado (2019).

Por lo tanto, el uso de modelos de gestión de riesgos no solo representa una práctica recomendada, sino una necesidad estratégica para garantizar la continuidad, eficiencia y sostenibilidad de la infraestructura tecnológica en entornos públicos y privados.

Normativas y estándares de seguridad informática
La adopción de normativas y estándares de seguridad informática resulta fundamental para proteger la información y garantizar la continuidad de las operaciones en las organizaciones modernas. De acuerdo con la, la norma ISO/IEC 27001 establece los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI), cuyo objetivo principal es preservar la confidencialidad, integridad y disponibilidad de los datos mediante un enfoque basado en la gestión de riesgos. Esta norma no solo define la estructura que debe seguirse, sino que también exige una mejora continua del sistema, impulsando a las organizaciones a adaptarse constantemente a nuevas amenazas y vulnerabilidades.

Complementariamente, la norma ISO/IEC 27002 proporciona un conjunto detallado de controles de seguridad que apoyan la implementación efectiva de la ISO/IEC 27001. Como señalan Bañales y García (2021), ISO/IEC 27002 funciona como una guía práctica que describe buenas prácticas para la gestión de riesgos asociados con la información, ofreciendo lineamientos específicos para áreas críticas como el control de accesos, la seguridad física, la gestión de incidentes y la protección de activos informáticos. La combinación de ambas normativas permite a las instituciones públicas y privadas estructurar políticas de seguridad robustas que responden a un entorno tecnológico cada vez más dinámico y complejo.

Por otro lado, en el contexto de garantizar la continuidad de las operaciones, se destaca la norma ISO 22301, orientada a la gestión de la continuidad del negocio. Según Guillén (2023), esta normativa específica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión que proteja a las organizaciones contra interrupciones disruptivas. La implementación de la ISO 22301 permite identificar amenazas potenciales, analizar sus impactos y desarrollar estrategias de recuperación que aseguren la prestación ininterrumpida de servicios esenciales, aspecto crítico especialmente en entidades públicas como los gobiernos municipales.

De esta manera, la integración de normativas como ISO/IEC 27001, ISO/IEC 27002 e ISO 22301 en las políticas institucionales no solo fortalece los niveles de seguridad informática, sino que también mejora la capacidad de respuesta y adaptación ante situaciones adversas, garantizando la resiliencia organizacional en un entorno cada vez más dependiente de la tecnología.

## MATERIALES Y MÉTODOS

La investigación adoptó un enfoque mixto, combinando el método cuantitativo, orientado al análisis de las percepciones de los trabajadores del GAD Municipal de Flavio Alfaro, con un enfoque cualitativo, a través de entrevistas dirigidas al encargado del departamento de Tecnologías de la Información. Además, se trató de un estudio de tipo correlacional, debido a que se buscó identificar la relación entre la gestión de riesgos y el estado de la infraestructura tecnológica, bajo una metodología de investigación no experimental. Para la recolección de datos se emplearon técnicas empíricas como la observación, las encuestas aplicadas al personal municipal y entrevistas semiestructuradas a los responsables del área de TI, permitiendo así detectar las principales debilidades y riesgos presentes en la infraestructura tecnológica.

Con respecto a los métodos utilizados, se recurrió al método de inducción y deducción, el cual permitió analizar los problemas existentes y proponer hipótesis de mejora relacionadas con la infraestructura tecnológica. Se aplicó también el método analítico descriptivo para interpretar de manera crítica los antecedentes teóricos y los modelos de gestión de riesgo previamente implementados en otras organizaciones. El método estadístico matemático fue fundamental para procesar y analizar la información cuantitativa obtenida de las encuestas realizadas a los trabajadores, mientras que el método bibliográfico permitió sustentar conceptualmente el estudio a partir de fuentes como libros, artículos científicos y tesis. Para la propuesta de solución se utilizó la metodología AMFE (Análisis Modal de Fallos y Efectos), la cual facilitó la identificación y priorización de riesgos asociados a la infraestructura tecnológica, proponiendo medidas preventivas para mitigar posibles fallos futuros.

Respecto a la población, esta estuvo compuesta por los 240 trabajadores activos del GAD Municipal de Flavio Alfaro, según datos proporcionados por la Secretaría Municipal. Para determinar la muestra representativa se aplicó la fórmula estadística basada en la distribución normal, considerando un nivel de confianza del 95 % ($Z = 1,65$), una probabilidad de éxito del 50 % ($p = 0,5$), una probabilidad de fracaso del 50 % ($q = 0,5$) y un margen de error del 5 % ($e = 0,05$), lo que arrojó un tamaño de muestra de 148 encuestados. Este grupo seleccionado permitió obtener datos relevantes para el análisis, garantizando la fiabilidad y validez de los resultados que sustentan el diseño del modelo de gestión de riesgo para la infraestructura tecnológica.

## RESULTADOS Y DISCUSIÓN

Con el propósito de estructurar y analizar la información obtenida a través de la entrevista realizada al encargado del área de Tecnologías de la Información del GAD Municipal de

Flavio Alfaro, se elaboró la siguiente matriz de indicadores. En ella se sintetizan las principales observaciones y propuestas relacionadas con la gestión de riesgos en la infraestructura tecnológica, permitiendo identificar áreas críticas y oportunidades de mejora.

**Tabla 3**

*Matriz de indicadores y respuestas basada en la entrevista*

| Indicador | Respuesta |
|---|---|
| Modelo actual de gestión de riesgos en infraestructura tecnológica utilizado por el GAD Municipal de Flavio Alfaro | Actualmente, el GAD Municipal utiliza un modelo tradicional de gestión de riesgos, en el cual la infraestructura está ubicada en un área específica que cumple con condiciones adecuadas para el funcionamiento de los sistemas de información. La red de conectividad es compartida entre los diferentes departamentos y dispositivos institucionales. |
| Identificación de riesgos presentes en la infraestructura tecnológica del GAD Municipal | Se identifican riesgos debido a que la infraestructura tradicional presenta deficiencias que amenazan la seguridad de los datos y equipos. Se destaca la necesidad urgente de fortalecer los recursos tecnológicos para salvaguardar tanto la información como los dispositivos, especialmente en el servidor principal. |
| Aspectos que requieren mejora en la infraestructura tecnológica del GAD Municipal | Se requiere una mejora integral de toda la infraestructura tecnológica. Actualmente, la dependencia de un sistema tradicional limita la seguridad y eficiencia operativa. Sin embargo, la falta de recursos económicos constituye un obstáculo para la renovación tecnológica inmediata. |
| Modelo de gestión de riesgos sugerido para optimizar la infraestructura tecnológica del GAD Municipal | Se recomienda implementar el modelo Punt Sistemes, orientado a blindar la información institucional y adoptar mecanismos de seguridad avanzados que permitan reducir significativamente los riesgos asociados a la infraestructura tecnológica. |
| Importancia de aplicar el modelo Punt Sistemes en la infraestructura tecnológica del GAD Municipal | Aplicar el modelo Punt Sistemes es fundamental debido al incremento de riesgos de ciberataques. Fortalecer la seguridad física y lógica de la infraestructura tecnológica es prioritario para proteger los activos digitales y garantizar la continuidad operativa del GAD Municipal. |

*Nota.* Entrevista dirigida a la persona encargada del departamento de tecnología de la información del GAD municipal de Flavio Alfaro.

Los resultados obtenidos a partir de la entrevista indican que el GAD Municipal de Flavio Alfaro actualmente emplea un modelo tradicional para la gestión de riesgos en infraestructura tecnológica. Esta situación evidencia una carencia de políticas sistemáticas para la protección de los activos digitales, lo cual, conforme señala Ávila (2024), es una deficiencia común en las instituciones públicas ecuatorianas, donde aún persisten prácticas de gestión poco estructuradas. Esta ausencia de un modelo formal incrementa la vulnerabilidad frente a amenazas tanto físicas como cibernéticas.

La identificación de riesgos en toda la infraestructura tecnológica, especialmente en el servidor principal, confirma lo planteado por Jiménez (2022), quien advierte que las infraestructuras tecnológicas tradicionales, carentes de mecanismos actualizados de protección, se encuentran altamente expuestas a brechas de seguridad.

Asimismo, Cando y Medina (2021) destacan que el crecimiento de las amenazas digitales exige el fortalecimiento tanto de los componentes físicos como lógicos de la infraestructura, situación que en el GAD Municipal de Flavio Alfaro aún no ha sido adecuadamente atendida.

Respecto a la necesidad de mejorar integralmente la infraestructura tecnológica, el entrevistado plantea como solución la implementación del modelo Punt Sistemes. Este enfoque de fortalecimiento coincide con las buenas prácticas sugeridas por Bañales y García (2021), quienes sostienen que un sistema robusto de seguridad debe integrar controles físicos, lógicos y de gestión de la información bajo estándares internacionales como ISO/IEC 27002.

Además, la propuesta de blindar la infraestructura frente a ciberataques responde a los lineamientos de continuidad del negocio promovidos por Guillén (2023), quien resalta la importancia de aplicar modelos de gestión de continuidad como ISO 22301 para proteger las operaciones esenciales de entidades públicas ante eventos disruptivos.

Por otro lado, el énfasis del entrevistado en adoptar medidas de protección ante riesgos tecnológicos en línea es consistente con los hallazgos de Celestino (2023), quien afirma que las amenazas cibernéticas actuales representan uno de los principales riesgos operativos para las organizaciones públicas y privadas.

En este sentido, López y Anías (2020) recomiendan que la gestión de infraestructuras tecnológicas contemple no solo la actualización de equipos, sino también la implementación de modelos de gestión de riesgos que permitan anticiparse y mitigar los efectos de posibles incidentes.

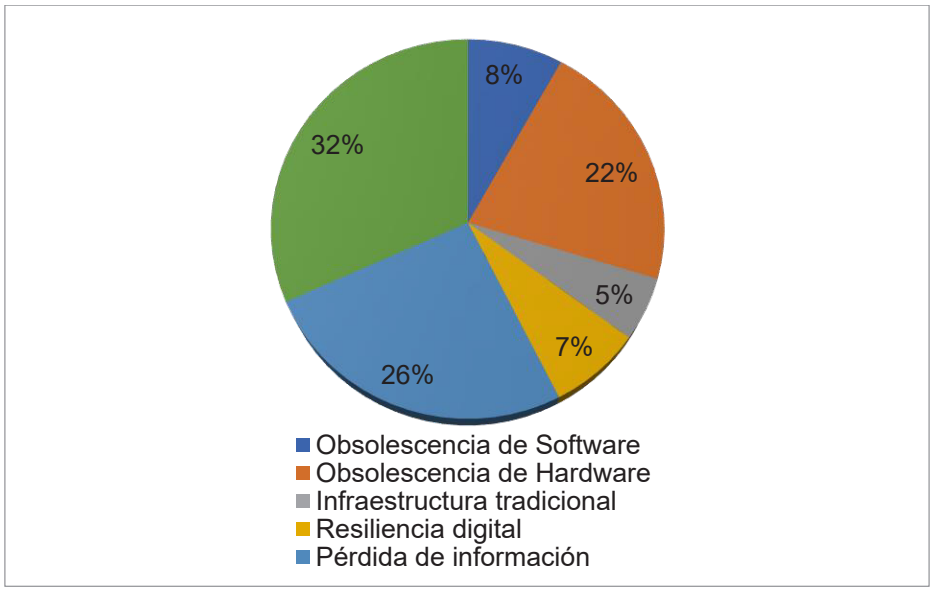
El análisis ratifica que, como señala Martínez (2024), una infraestructura tecnológica desactualizada limita la capacidad de respuesta institucional y compromete la eficiencia administrativa.

De allí la necesidad urgente de que el GAD Municipal de Flavio Alfaro transite de un modelo tradicional a uno basado en estándares internacionales de gestión de riesgos tecnológicos, como lo sugieren la ISO 31000 (Organización Internacional de Normalización, 2019) y COBIT 5 (ISACA, 2012), fortaleciendo así la seguridad, resiliencia y sostenibilidad de su infraestructura tecnológica.

**Encuesta al personal del GAD Municipal de Flavio Alfaro**

**Figura 2**

*Riesgos que afectan la infraestructura tecnológica*

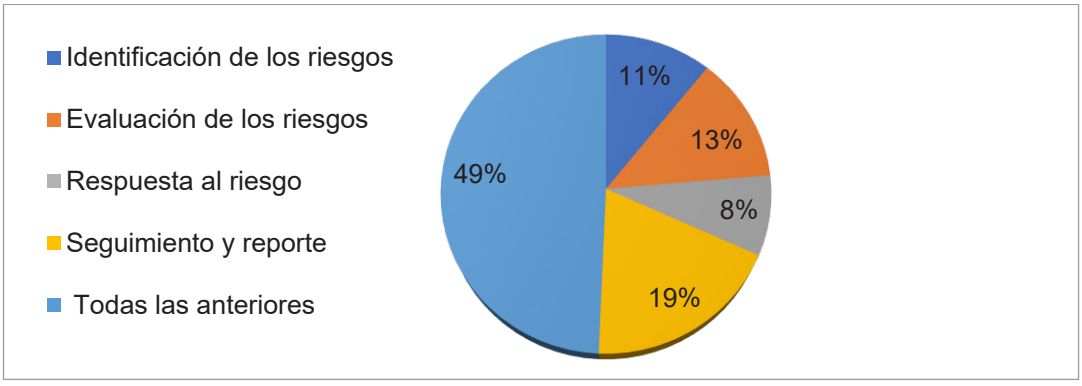



*Nota.* Elaboración propia.

El análisis de la tabla revela que el 32 % de los encuestados identificó que todos los factores listados —obsolescencia de software y hardware, infraestructura tradicional, baja resiliencia digital y pérdida de información— afectan de manera conjunta la integridad tecnológica del GAD, lo cual coincide con lo planteado por Jiménez (2022), quien advierte que las amenazas se interrelacionan y se intensifican en entornos institucionales no actualizados. Además, la pérdida de información (26 %) y la obsolescencia del hardware (22 %) fueron señaladas como los riesgos más críticos, lo que refuerza las conclusiones de Campi (2024), quien sostiene que la infraestructura obsoleta reduce la capacidad operativa y de recuperación ante incidentes.

**Figura 3**

*Seguimiento para la gestión de riesgo*

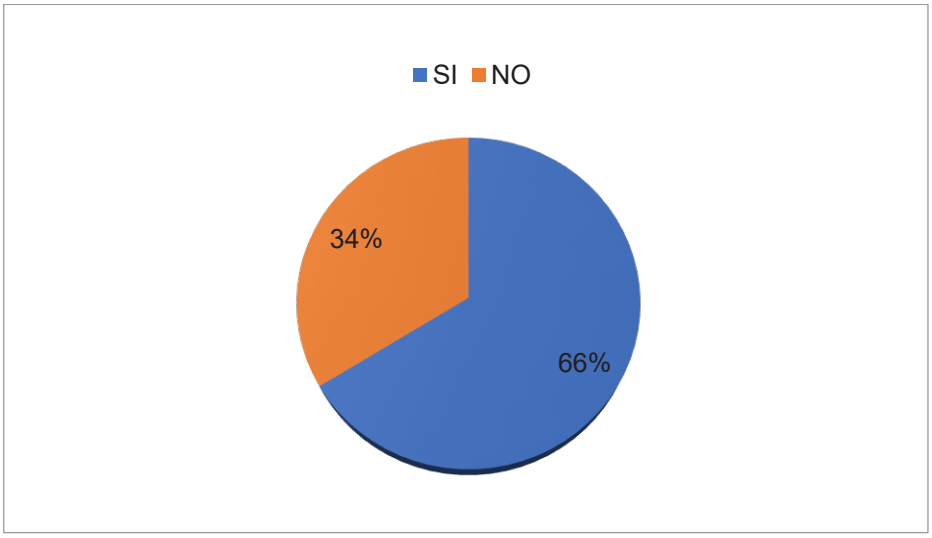



*Nota.* Elaboración propia.

El análisis de la tabla muestra que el 49 % de los encuestados considera que todas las etapas del proceso —identificación, evaluación, respuesta, seguimiento y reporte— deben aplicarse conjuntamente para una gestión de riesgos efectiva, lo cual concuerda con la norma ISO 31000 (Organización Internacional de Normalización, 2019), que establece un enfoque integral y cíclico para el tratamiento de riesgos. Esta perspectiva también coincide con lo expuesto por López y Anías (2020), quienes destacan que una gestión fragmentada reduce la efectividad de las medidas de mitigación en infraestructuras tecnológicas públicas. Asimismo, el 19 % de los participantes resalta la importancia del seguimiento y reporte, etapa clave señalada por Guillén (2023) como un pilar para garantizar la mejora continua y la resiliencia institucional frente a eventos disruptivos.

**Figura 4**

*Gastos elevados en la aplicación en la infraestructura tecnológica*

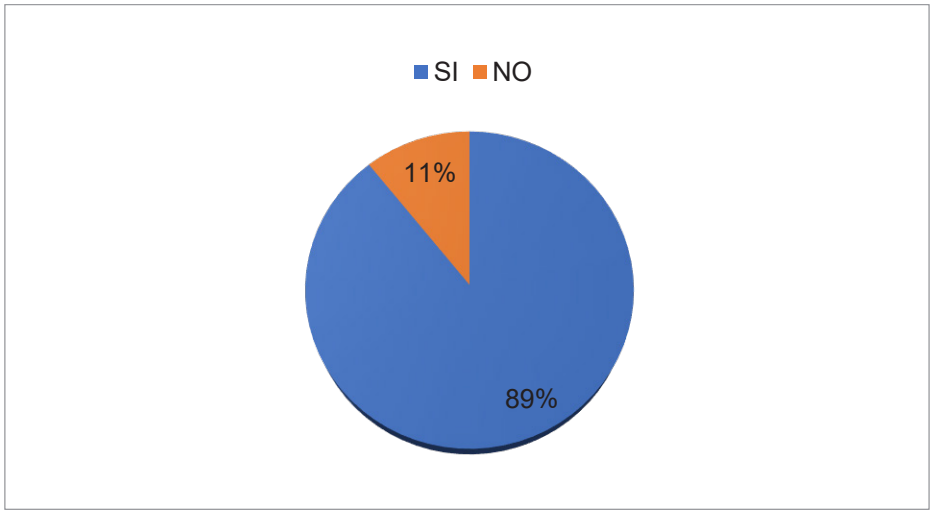



*Nota.* Elaboración propia.

El análisis de la tabla evidencia que el 66 % de los encuestados considera que la actualización de la infraestructura tecnológica implicaría gastos elevados, percepción que refleja una preocupación común en instituciones públicas con limitaciones presupuestarias. Esta apreciación coincide con lo señalado por Martínez (2024), quien afirma que la modernización tecnológica conlleva inversiones significativas en hardware, software y formación del personal. No obstante, estudios como el de Machado (2019) advierten que, si bien la inversión inicial puede ser alta, implementar modelos de gestión eficientes como ITIL permite optimizar recursos a largo plazo, reducir riesgos operativos y mejorar la sostenibilidad tecnológica.

**Figura 5**

*Necesidad de implementar un modelo para la infraestructura tecnológica*




*Nota.* Elaboración propia.

El análisis de la tabla muestra que el 89 % de los encuestados considera necesaria la implementación de un modelo más eficiente para la infraestructura tecnológica del GAD Municipal de Flavio Alfaro, lo que refleja una clara demanda institucional por modernizar los sistemas actuales. Esta opinión es coherente con lo señalado por Ávila (2024), quien destaca que la falta de modelos estructurados de gestión de riesgos en instituciones públicas ecuatorianas incrementa la vulnerabilidad operativa. Además, Celestino (2023) sostiene que la adopción de marcos eficientes mejora la continuidad del servicio y protege los activos digitales, especialmente en entornos con infraestructura obsoleta, como es el caso del GAD analizado.

**Diseño de un modelo de gestión de riesgos para la infraestructura tecnológica del GAD Municipal de Flavio Alfaro Basado en la Metodología AMFE**

La propuesta tiene como objetivo fortalecer la infraestructura tecnológica del Gobierno Autónomo Descentralizado Municipal de Flavio Alfaro, mediante el diseño de un modelo de gestión de riesgos que permita identificar, evaluar y mitigar las vulnerabilidades que afectan la seguridad, operatividad y continuidad de sus servicios digitales.

A partir del análisis situacional realizado mediante observación directa, entrevistas y encuestas, se evidenció que la infraestructura actual presenta serias deficiencias en cuanto a mantenimiento, seguridad física, actualización tecnológica, resiliencia ante desastres y protección de la información, lo cual incrementa la exposición del GAD a fallos operativos, ciberataques y pérdidas de datos.

En este contexto, se plantea la implementación de un modelo basado en la metodología AMFE (Análisis Modal de Fallos y Efectos), que permite anticipar posibles fallos en los sistemas informáticos y establecer acciones de mitigación oportunas.

El modelo propuesto se articula en tres fases principales: diagnóstico de la infraestructura tecnológica, diseño del modelo de gestión y aplicación de un plan de continuidad operativa según el ciclo PHVA (Planear, Hacer, Verificar, Actuar), conforme a los lineamientos de la norma ISO 22301. Este enfoque integral incluye tanto medidas preventivas como correctivas, el fortalecimiento de las redes mediante

cortafuegos (firewalls), la realización de respaldos automáticos alojados en la nube y la adopción de protocolos de seguridad actualizados. Además, se recomienda mejorar la calidad del cableado estructurado, proteger físicamente los servidores y capacitar permanentemente al personal responsable.

La viabilidad de la propuesta se analiza desde los aspectos operativos, técnicos y económicos. Aunque se reconoce que la renovación tecnológica representa una inversión significativa, se justifica plenamente debido al impacto positivo en la eficiencia institucional y la reducción de riesgos operativos.

A continuación, se presenta una síntesis de los componentes clave del modelo:

**Tabla 4**

*Componentes del modelo de gestión de riesgos propuesto*

| Componente | Descripción |
|---|---|
| **Metodología aplicada** | AMFE (Análisis Modal de Fallos y Efectos) |
| **Norma internacional guía** | ISO 22301: Gestión de continuidad del negocio |
| **Fases del modelo** | Diagnóstico, diseño del modelo, aplicación del plan de continuidad |
| **Medidas preventivas** | Firewalls, respaldos automáticos en la nube, protección física del servidor |
| **Medidas correctivas** | Plan de contingencia ante fallos, políticas de respaldo y recuperación |
| **Infraestructura prioritaria** | Servidor principal, red LAN/WAN, cableado estructurado |
| **Herramientas de control** | Matriz de riesgos, ficha AMFE, monitoreo mensual del área de TI |
| **Recurso humano involucrado** | Personal técnico de TI, áreas administrativas, coordinación institucional |
| **Costo estimado inicial** | $380 USD (viáticos, transporte e investigación) |

*Nota.* Elaboración propia con base en el documento de propuesta (Mazamba, 2024).

Esta propuesta busca no solo reducir la exposición a riesgos tecnológicos, sino también consolidar una infraestructura robusta, segura y alineada con estándares internacionales, contribuyendo al fortalecimiento institucional del GAD Municipal de Flavio Alfaro en el marco de la transformación digital del sector público.

## CONCLUSIONES

La evaluación del estado actual de la infraestructura tecnológica del GAD Municipal de Flavio Alfaro evidenció múltiples vulnerabilidades, tanto a nivel físico como lógico, producto del uso de equipos obsoletos, falta de mantenimiento preventivo y ausencia de políticas integrales de seguridad informática, lo que pone en riesgo la continuidad operativa y la protección de la información institucional.

La aplicación del modelo de gestión de riesgos basado en la metodología AMFE permitió identificar, clasificar y priorizar los principales riesgos tecnológicos presentes en el GAD, facilitando la formulación de acciones preventivas y correctivas orientadas a mitigar fallos, reforzar la resiliencia digital y establecer mecanismos de respaldo que aseguren la disponibilidad y confiabilidad de los servicios informáticos.

La implementación de un modelo estructurado de gestión de riesgos tecnológicos es no solo viable, sino esencial para mejorar la eficiencia institucional, garantizar la integridad de los activos tecnológicos y responder adecuadamente a amenazas externas e internas, siempre que se acompañe de inversión económica, capacitación continua y compromiso técnico-administrativo por parte del personal del GAD.

## REFERENCIAS BIBLIOGRÁFICAS

Ávila, C. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. Obtenido de Revista de Investigación en Ciencias Económicas y Sociales, 4(2), 140-156: https://doi.org/10.55813/gaea/jessr/v4/n2/96

Axelos. (2017). Gestión de proyectos exitosos con PRINCE2. Obtenido de (6.ª ed.). The Stationery Office.

Bañales, L., & García, M. (2021). Guía práctica para la implementación de ISO/IEC 27002 en organizaciones públicas. Obtenido de Editorial Técnica de Seguridad Informática.

Campi, V. J. (2024). Diseño de la infraestructura tecnológica para la Empresa ISP Jatnet.Net. Obtenido de [Tesis, Universidad Técnica de Babahoyo]: http://dspace.utb.edu.ec/handle/49000/17050

Cando, M. R., & Medina, R. P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. Obtenido de 3 c TIC: cuadernos de desarrollo aplicados a las TIC, 10(1), 17-41.

Carrasco, M. E., Díaz, J., & Encalada, I. Á. (2021). Infraestructura tecnológica implementada y uso de softwares educativos en el desempeño pedagógico docente del nivel secundario de la IE Politécnico Nacional del Callao, 2017. Obtenido de IGOBERNANZA, 4(15), 100–121: https://doi.org/10.47865/igob.vol4.2021.129

Celestino, D. (2023). Riesgos tecnológicos y continuidad operativa en entornos digitales críticos. Obtenido de Editorial Técnica Andina.

Comisión Económica para América Latina y el Caribe. (2021). Informe sobre la transformación digital en América Latina y el Caribe. Obtenido de Naciones Unidas.

Guillén, R. (2023). Gestión de continuidad del negocio basada en la norma ISO 22301: Estrategias y mejores prácticas. Obtenido de Editorial Innovación Empresarial.

ISACA. (2012). COBIT 5: Un marco empresarial para el gobierno y la gestión de TI empresarial.
Jiménez, A. (2022). Ciberseguridad y gestión de vulnerabilidades en instituciones públicas. Obtenido de Revista de Tecnología y Sociedad, 14(2), 85–102.

Llamas, F. (2020). Seguridad informática: Riesgos, vulnerabilidades y amenazas tecnológicas. Obtenido de Editorial Alfaomega.

López, M., & Anías, G. (2020). Modelo para la gestión de infraestructuras tecnológicas de la información. Obtenido de [Tesis, Universidad Central del Ecuador].

Machado, M. (2019). Desarrollo de un modelo de gestión de infraestructura tecnológica basado en ITIL utilizando herramientas informáticas. Obtenido de [Tesis, Universidad de Guayaquil].

Martínez, A. (2024). La importancia de la infraestructura tecnológica en las empresas. Obtenido de Icorp: https://icorp.com.mx/blog/importancia-de-la-infraestructura-tecnologica/

Organización Internacional de Normalización. (2012). ISO 21500:2012 – Guía para la gestión de proyectos. Obtenido de https://www.iso.org/standard/50003.html

Organización Internacional de Normalización. (2019). ISO 31000:2018 - Gestión de riesgos — Directrices. ISO. Obtenido de https://www.iso.org/standard/65694.html

Project Management Institute. (2017). A guide to the Project Management Body of Knowledge . Obtenido de (6th ed.). Project Management Institute.

Vélez, C. I. (2024). Auditoría de seguridad informática a la infraestructura tecnológica de la Unidad Educativa “Rumiñahui” de la parroquia Wilfrido Loor. Obtenido de [Tesis, Universidad Laica Eloy Alfaro de Manabí, Manta, Ecuador]: https://repositorio.uleam.edu.ec/handle/123456789/7375