AÑO 4. No. 2
ISSN:2992-7978

APLICACIÓN DEL MODELO FAIR PARA LA CUANTIFICACIÓN FINANCIERA DEL RIESGO CIBERNÉTICO EN PYMES

Vicente Alfredo Campos Rosado[1]
Cadena Martinez, Rodrigo[2]

[1] Doctorando, Universidad Americana de Europa (UNADE).Correo: vcamposr@uteq.edu.ec
[2] Profesor-Investigador, Universidad Americana de Europa (UNADE). Correo: rodrigo.cadena@unade.edu.mx

AÑO 4. No. 2
ISSN:2992-7978

RESUMEN

Las pequeñas y medianas empresas (PYMES) enfrentaron un incremento sostenido en su exposición a riesgos cibernéticos, caracterizado por limitaciones presupuestarias, ausencia de modelos formales de cuantificación y toma de decisiones basada principalmente en criterios técnicos no financieros. Esta situación generó una brecha significativa entre la identificación de amenazas y la evaluación económica de su impacto real, dificultando la priorización estratégica de inversiones en ciberseguridad. Ante esta problemática, el presente estudio tuvo como objetivo aplicar el modelo FAIR (Factor Analysis of Information Risk) para cuantificar financieramente el riesgo cibernético en PYMES y evaluar su utilidad como herramienta de apoyo a la gestión estratégica. Metodológicamente, se desarrolló un estudio cuantitativo aplicado en un conjunto de PYMES del sector servicios, donde se identificaron activos críticos, amenazas relevantes y escenarios de pérdida. Se estimaron la frecuencia de eventos de amenaza, la probabilidad de vulnerabilidad y la magnitud de la pérdida, integrando estos componentes para calcular la pérdida anual esperada (Annualized Loss Expectancy). Se incorporaron simulaciones probabilísticas para modelar distintos escenarios de riesgo. Los resultados evidenciaron que la aplicación estructurada del modelo permitió traducir riesgos técnicos en métricas financieras concretas, facilitando la priorización de controles de seguridad con base en análisis costo-beneficio. Se concluyó que el modelo FAIR constituyó una herramienta viable y técnicamente consistente para fortalecer la gestión estratégica del riesgo cibernético en PYMES, promoviendo decisiones fundamentadas en evidencia económica cuantificable.

Palabras clave: Ciberseguridad; Modelo FAIR; Cuantificación del Riesgo.

ABSTRACT

Small and medium-sized enterprises (SMEs) experienced a sustained increase in exposure to cyber risks, characterized by budget constraints, absence of formal risk quantification models, and decision-making processes primarily based on technical rather than financial criteria. This situation created a significant gap between threat identification and the economic assessment of potential impacts, limiting the ability to prioritize cybersecurity investments strategically. In response to this challenge, the present study aimed to apply the FAIR (Factor Analysis of Information Risk) model to financially quantify cyber risk in SMEs and evaluate its usefulness as a strategic risk management tool. A quantitative applied study was conducted in a group of service-sector SMEs. Critical assets, relevant threat scenarios, and potential loss events were identified. Threat event frequency, vulnerability probability, and loss magnitude were estimated and integrated to calculate the Annualized Loss Expectancy (ALE). Probabilistic simulations were incorporated to model different risk scenarios and enhance the robustness of financial estimations. The results demonstrated that the structured application of the FAIR model translated technical cyber risks into concrete financial metrics, enabling cost-benefit analysis and prioritization of security controls. The study concluded that the FAIR framework represented a viable and technically consistent approach for strengthening strategic cyber risk management in SMEs by supporting evidence-based financial decision-making.

Keywords: Cybersecurity; FAIR Model; Risk Quantification.

AÑO 4. No. 2
ISSN:2992-7978

INTRODUCCIÓN

Las pequeñas y medianas empresas (PYMES) enfrentan una exposición creciente a riesgos cibernéticos debido a su dependencia de infraestructuras digitales para la gestión de procesos administrativos, operativos y financieros. Sin embargo, muchas de estas organizaciones continúan utilizando enfoques cualitativos para evaluar dichos riesgos, lo que limita la estimación objetiva de su impacto económico y dificulta la priorización de inversiones en ciberseguridad (Bouveret, 2023; Eling & Schnell, 2024). Esta situación resulta especialmente crítica en las PYMES del sector servicios, donde las restricciones presupuestarias, la falta de personal especializado y la limitada madurez en gestión de riesgos incrementan la vulnerabilidad frente a amenazas como ransomware, phishing y fuga de información (El-Hajj & Mirza, 2024).

En este contexto, la cuantificación del riesgo cibernético se vuelve necesaria para traducir los eventos técnicos en métricas financieras comprensibles para la toma de decisiones. El modelo FAIR permite descomponer el riesgo en variables medibles, como frecuencia de eventos, vulnerabilidad y magnitud de pérdida, y expresarlo en términos monetarios, lo cual facilita la comparación de escenarios y la priorización de controles de seguridad (Jones & Rosenthal, 2022; FAIR Institute, 2022; Safe Security, 2024). Asimismo, la simulación probabilística, especialmente mediante Monte Carlo, permite representar la incertidumbre inherente a los escenarios de pérdida y obtener rangos más realistas de exposición financiera, algo particularmente útil en contextos donde no existen historiales amplios de incidentes (FAIR Institute, 2022; Khan et al., 2026).

Por ello, el presente estudio se justifica en la necesidad de ofrecer a las PYMES una base cuantitativa para gestionar su riesgo cibernético con criterios financieros y estratégicos. A diferencia de las evaluaciones cualitativas tradicionales, este enfoque permite identificar qué activos concentran la mayor exposición económica, cuánto podría costar un incidente y qué nivel de control reduce de forma más efectiva la pérdida esperada (The Open Group, 2023; NIST, 2022). De este modo, el artículo aporta evidencia útil para la gestión de la seguridad de la información en organizaciones con recursos limitados.

El objetivo general del estudio es aplicar el modelo FAIR para cuantificar financieramente el riesgo cibernético en PYMES del sector servicios mediante simulación probabilística y estimación de la pérdida anual esperada (ALE), con el propósito de fortalecer la toma de decisiones estratégicas en ciberseguridad. Los objetivos específicos son: identificar y categorizar los activos digitales críticos y sus escenarios de amenaza más frecuentes; estimar la frecuencia y magnitud de las pérdidas económicas asociadas a dichos escenarios; y calcular la pérdida anual esperada mediante el modelo FAIR para comparar distintos niveles de exposición al riesgo.

A partir de lo anterior, la pregunta de investigación es: ¿Cómo contribuye el modelo FAIR a la cuantificación financiera del riesgo cibernético en PYMES mediante la estimación probabilística de la pérdida anual esperada (ALE)? La hipótesis plantea que la aplicación del modelo FAIR permite cuantificar financieramente el riesgo cibernético en PYMES mediante estimaciones probabilísticas de la pérdida anual esperada (ALE), mejorando la precisión analítica frente a métodos cualitativos tradicionales (Jones & Rosenthal, 2022; Eling & Schnell, 2024).

ESTADO DEL ARTE

En los últimos años, la digitalización de los procesos organizacionales incrementa la exposición de las empresas a riesgos cibernéticos y, con ello, la necesidad de contar con enfoques que permitan estimar su impacto económico de manera más precisa. En este contexto, la literatura reciente coincide en que las pequeñas y medianas empresas (PYMES) presentan una vulnerabilidad particular debido a restricciones

AÑO 4. No. 2
ISSN:2992-7978

presupuestarias, menor madurez en seguridad y menor disponibilidad de capacidades técnicas especializadas (El-Hajj & Mirza, 2024; Chaudhary et al., 2023).

La investigación sobre riesgo cibernético muestra que los métodos cualitativos tradicionales resultan insuficientes cuando el objetivo es traducir incidentes técnicos en pérdidas financieras comprensibles para la alta dirección. La principal limitación de estos enfoques es que simplifican el riesgo en matrices de probabilidad e impacto, sin reflejar con suficiente precisión la incertidumbre ni la magnitud monetaria de las pérdidas potenciales (Bouveret, 2023; Eling & Schnell, 2024). Por esta razón, la cuantificación financiera del riesgo cibernético gana relevancia como una vía para mejorar la toma de decisiones y la asignación de recursos de ciberseguridad.

Dentro de este campo, el modelo FAIR se consolida como uno de los marcos más reconocidos para cuantificar el riesgo cibernético en términos financieros. FAIR descompone el riesgo en factores observables y medibles, como frecuencia de eventos de amenaza, vulnerabilidad y magnitud de pérdida, permitiendo expresar los resultados en unidades monetarias y compararlos entre escenarios de riesgo (Jones & Rosenthal, 2022; Safe Security, 2024). La literatura especializada también destaca que FAIR facilita la comunicación entre áreas técnicas y directivas, ya que convierte el lenguaje de la ciberseguridad en lenguaje de negocio (FAIR Institute, 2022; The FAIR Standard, 2024).

Además, la simulación probabilística, particularmente Monte Carlo, se integra de forma natural al modelo FAIR porque permite representar la variabilidad e incertidumbre de los escenarios de pérdida. El FAIR Institute señala que la simulación Monte Carlo constituye una parte integral del análisis FAIR para estimar el rango de exposición a pérdidas en términos monetarios. En estudios aplicados recientes, esta combinación metodológica permite modelar múltiples escenarios, estimar distribuciones de pérdida y obtener una base más sólida para la priorización de controles y la valoración de inversiones en seguridad (Khan et al., 2026; FAIR Institute, 2022).

En síntesis, la evidencia disponible muestra que la cuantificación financiera del riesgo cibernético representa una evolución necesaria frente a los enfoques cualitativos tradicionales, especialmente en contextos donde los recursos son limitados y las decisiones deben justificarse económicamente. En ese marco, FAIR se posiciona como una herramienta adecuada para PYMES porque permite estructurar escenarios, estimar pérdidas esperadas y sustentar decisiones de mitigación con criterios financieros verificables (The FAIR Institute, 2024; NIST, 2022).

MARCO TEÓRICO

La gestión del riesgo cibernético constituye un componente central de la seguridad de la información en las organizaciones modernas. En un entorno donde los procesos empresariales dependen cada vez más de sistemas digitales, plataformas en la nube y redes interconectadas, las amenazas informáticas afectan de forma directa la continuidad operativa, la confidencialidad de la información y la estabilidad financiera de las empresas. Por ello, la literatura especializada señala que la evaluación del riesgo debe integrar no solo la identificación de amenazas y vulnerabilidades, sino también la estimación de sus impactos y de la incertidumbre asociada a su materialización (NIST, 2022; NIST SP 800-30 Rev. 1, 2012).

Desde esta perspectiva, el riesgo cibernético se entiende como la probabilidad de que una amenaza explote una vulnerabilidad y genere una pérdida para la organización. A diferencia de enfoques meramente descriptivos, los marcos contemporáneos de análisis de riesgo buscan vincular la exposición técnica con consecuencias medibles, especialmente en términos económicos. Esta transición resulta relevante en PYMES, donde las decisiones sobre ciberseguridad dependen de la capacidad de justificar inversiones con base en su posible retorno o en la reducción de pérdidas esperadas (Bouveret, 2023; Eling & Schnell, 2024).

En este campo, el modelo FAIR (Factor Analysis of Information Risk) se consolida como uno de los enfoques más difundidos para la cuantificación financiera del riesgo cibernético. FAIR traduce la descripción

AÑO 4. No. 2
ISSN:2992-7978

técnica de los eventos cibernéticos al lenguaje del negocio, ya que expresa el riesgo como la frecuencia probable y la magnitud probable de la pérdida futura. El modelo descompone el riesgo en componentes como Threat Event Frequency, Vulnerability, Loss Event Frequency y Loss Magnitude, lo que permite evaluar escenarios de exposición de forma estructurada y comparable.

Un elemento distintivo de FAIR es que no reduce el riesgo a una categoría cualitativa, sino que lo convierte en una estimación monetaria susceptible de análisis financiero. Esta característica permite valorar la exposición al riesgo en dólares o en la moneda local de la organización y facilita la comparación entre activos, amenazas y controles. Además, el modelo distingue entre pérdidas primarias y secundarias, lo que amplía la comprensión del impacto real de un incidente más allá del daño técnico inmediato.

La simulación probabilística, especialmente mediante el método Monte Carlo, forma parte del núcleo operativo de FAIR. El FAIR Institute indica que la simulación Monte Carlo es un componente integral del análisis FAIR para calcular el rango de exposición a pérdidas en términos monetarios. En estudios aplicados, esta técnica permite representar la incertidumbre mediante múltiples iteraciones y generar distribuciones de pérdida anual esperada, lo que resulta especialmente útil cuando no existen datos históricos suficientes o cuando los eventos presentan alta variabilidad.

Dentro de este marco, la métrica Annualized Loss Expectancy (ALE) ocupa un lugar central, porque permite estimar la pérdida económica anual esperada a partir de la frecuencia del evento y la magnitud de la pérdida. Su utilidad radica en que resume el riesgo en una cifra comprensible para la dirección y para los responsables de la gestión tecnológica. En consecuencia, ALE no funciona solo como un resultado numérico, sino como una base para priorizar controles, comparar escenarios y justificar decisiones de inversión en ciberseguridad (Jones & Rosenthal, 2022; Safe Security, 2024).

La aplicación de FAIR adquiere especial relevancia en las PYMES, debido a que estas organizaciones suelen contar con recursos limitados, menor formalización en sus procesos de seguridad y menor capacidad para absorber pérdidas derivadas de un incidente cibernético. En este contexto, cuantificar el riesgo en términos financieros ayuda a definir prioridades reales de protección y a identificar cuáles activos concentran mayor exposición económica. Por ello, el modelo FAIR se ajusta bien a estudios aplicados en PYMES, porque permite construir escenarios realistas de riesgo aun cuando la información disponible sea parcial o estimada (El-Hajj & Mirza, 2024; FAIR Institute, 2022).

En síntesis, el marco teórico de este estudio se apoya en la relación entre riesgo cibernético, cuantificación financiera, modelo FAIR, simulación probabilística y ALE. Esta articulación conceptual permite sostener que la gestión del riesgo en PYMES no solo requiere identificar amenazas, sino también estimar con rigor económico el posible impacto de los incidentes y las oportunidades de mitigación asociadas (The FAIR Standard, 2024; NIST, 2022).

METODOLOGÍA

El estudio se desarrolló bajo un enfoque cuantitativo, con diseño aplicado, no experimental y de alcance descriptivo-analítico. Este diseño permitió estimar el impacto financiero del riesgo cibernético sin manipular variables, en coherencia con los enfoques actuales de gestión del riesgo que priorizan la identificación de amenazas, vulnerabilidades, impactos e incertidumbre como base del análisis (FAIR Institute, 2024; FAIR Institute, 2025).

La técnica principal de investigación fue el análisis documental, complementado con modelación de escenarios de riesgo. Para sustentar los supuestos del estudio, se revisaron fuentes institucionales, literatura científica reciente y documentos técnicos sobre cuantificación del riesgo cibernético en PYMES, especialmente en contextos latinoamericanos y ecuatorianos donde la exposición a phishing, ransomware y otras amenazas sigue aumentando (Lucio-Vásquez & Campana-Ortega, 2024; Revista de Seguridad Ecuatoriana, 2023; FAIR Institute, 2025).

El área de estudio correspondió al cantón Quevedo, en la provincia de Los Ríos, Ecuador. Esta delimitación territorial resultó pertinente porque las PYMES de Quevedo operan en un entorno de creciente digitalización y presentan necesidades concretas de fortalecimiento en ciberseguridad, aspecto señalado en investigaciones recientes sobre empresas ecuatorianas y sobre la realidad de las pymes locales en materia de seguridad informática (Universidad Técnica Estatal de Quevedo, 2015; Lucio-Vásquez & Campana-Ortega, 2024; Guía FAIR, 2025).

La población de referencia estuvo constituida por PYMES del sector servicios ubicadas en Quevedo, debido a su dependencia de sistemas digitales para procesos administrativos, financieros y de atención al cliente. La muestra no fue probabilística ni de campo directo, sino una muestra conceptual de análisis construida con base en escenarios representativos de PYMES similares reportadas en la literatura y en fuentes técnicas, dado que el estudio no contó con levantamiento primario suficiente para sostener una medición empírica completa (Lucio-Vásquez & Campana-Ortega, 2024; FAIR Institute, 2025).

En cuanto al método, se empleó el modelo FAIR para descomponer el riesgo en frecuencia de eventos, vulnerabilidad y magnitud de la pérdida, y luego se aplicó simulación Monte Carlo para obtener una distribución de la pérdida anual esperada (ALE). La literatura reciente sobre FAIR resaltó que este enfoque permitió expresar el riesgo en términos financieros y facilitar comparaciones entre escenarios, mientras que la simulación probabilística mejoró la estimación de pérdidas al representar incertidumbre y variabilidad en los resultados (FAIR Institute, 2024; FAIR Institute, 2025; GuidePoint Security, 2025).

Para asegurar coherencia metodológica, los valores de entrada se definieron como rangos mínimo, probable y máximo derivados de literatura especializada y reportes sectoriales, en lugar de presentarlos como observaciones directas no verificadas. Esta decisión metodológica resultó consistente con la lógica de la cuantificación del riesgo cibernético, que trabaja con distribuciones de probabilidad y escenarios de pérdida para producir estimaciones defendibles desde el punto de vista financiero y técnico (FAIR Institute, 2024; FAIR Institute, 2025).

Variables y operacionalización

La variable principal del estudio fue el riesgo cibernético cuantificado financieramente mediante FAIR. Esta variable se analizó a partir de su expresión monetaria en términos de pérdida anual esperada (ALE), lo que permitió traducir eventos técnicos en resultados financieros útiles para la toma de decisiones, en línea con el enfoque de FAIR sobre la comunicación del riesgo en términos de negocio (FAIR Institute, 2024; FAIR Institute, 2025).

La primera dimensión correspondió a la frecuencia de eventos de amenaza, entendida como la probabilidad anual de ocurrencia de incidentes como phishing, ransomware o pérdida de disponibilidad. Esta dimensión se operacionalizó a partir de rangos mínimo, probable y máximo, con el fin de representar la variabilidad e incertidumbre de los escenarios analizados, siguiendo la lógica probabilística utilizada en FAIR para modelar exposición y pérdida (FAIR Institute, 2024; FAIR Institute, 2025).

La segunda dimensión fue la magnitud de la pérdida, definida como el impacto económico esperado por incidente sobre activos críticos de la organización. Esta dimensión se estimó en dólares estadounidenses y se estructuró mediante escenarios de pérdida diferenciados según el activo afectado, lo que permitió comparar la severidad financiera entre tipos de eventos y priorizar la atención sobre los procesos más vulnerables (Fair Institute, 2025; Safe Security, 2024).

La tercera dimensión fue la pérdida anual esperada (ALE), calculada como el producto entre la frecuencia anual estimada y la pérdida por evento. Esta métrica sintetizó el efecto combinado de frecuencia e impacto, y fue utilizada como indicador central para comparar escenarios de riesgo bajo, base y alto, en coherencia con los reportes recientes del FAIR Institute sobre la necesidad de cuantificar el riesgo en lenguaje financiero para mejorar la alineación con objetivos estratégicos (FAIR Institute, 2025; GuidePoint Security, 2025).

Criterios de inclusión y exclusión

AÑO 4. No. 2
ISSN:2992-7978

Se incluyeron como referencia analítica las PYMES del sector servicios ubicadas en Quevedo que dependían de sistemas digitales para la gestión administrativa, financiera y de atención al cliente. También se consideraron escenarios representativos donde existía exposición a amenazas comunes como phishing, ransomware y pérdida de disponibilidad, porque estos eventos aparecen de forma recurrente en la literatura reciente sobre pequeñas empresas y ciberseguridad (Lucio-Vásquez & Campana-Ortega, 2024; Cybersecurity Challenges and Strategies for Small Businesses, 2024; IBM, 2024).

Se excluyeron los contextos empresariales que no dependían de infraestructura digital para sus operaciones principales, así como los casos sin exposición clara a activos de información críticos. También se excluyeron los escenarios sin sustento documental suficiente o sin posibilidad de construir rangos razonables de frecuencia y pérdida, ya que FAIR requiere supuestos defendibles para producir estimaciones probabilísticas consistentes (FAIR Institute, 2024; FAIR Institute, 2025).

Procedimiento de simulación

El procedimiento de simulación se desarrolló en tres etapas. Primero, se identificaron los activos críticos y los escenarios de amenaza relevantes para PYMES del sector servicios en Quevedo, con especial atención a aquellos eventos que la literatura reciente destaca como de mayor recurrencia e impacto, como phishing, ransomware y compromiso de sistemas de información (Lucio-Vásquez & Campana-Ortega, 2024; IBM, 2024; Cybersecurity Challenges and Strategies for Small Businesses, 2024).

Segundo, se asignaron valores mínimo, probable y máximo a la frecuencia anual de ocurrencia y a la pérdida económica por evento, a partir de evidencia documental y reportes recientes sobre ciberseguridad y gestión del riesgo. Esta forma de parametrización fue consistente con el uso de FAIR para trabajar con incertidumbre y comunicar el riesgo en términos financieros defendibles (FAIR Institute, 2024; FAIR Institute, 2025; Safe Security, 2024).

Tercero, se aplicó simulación Monte Carlo para generar una distribución de la pérdida anual esperada (ALE) y estimar escenarios de riesgo bajo, base y alto. La simulación permitió visualizar la dispersión de posibles pérdidas y mejorar la calidad de la decisión al representar la incertidumbre de forma cuantitativa, tal como recomiendan los enfoques recientes de FAIR para comunicar riesgo y orientar decisiones ejecutivas (FAIR Institute, 2024; GuidePoint Security, 2025).

RESULTADOS

La aplicación del modelo FAIR permitió identificar que los activos digitales con mayor exposición financiera en las PYMES del sector servicios de Quevedo fueron el correo electrónico corporativo, las bases de datos operativas, los sistemas de gestión administrativa y los servidores de almacenamiento. Estos activos concentran el mayor nivel de criticidad porque soportan procesos esenciales de comunicación, facturación, registro de clientes y continuidad operativa, por lo que cualquier incidente sobre ellos genera una pérdida económica directa o indirecta de alta relevancia. La literatura reciente sobre pequeñas empresas confirma que estos activos suelen ser los primeros puntos de impacto en ataques como phishing, ransomware y compromisos de disponibilidad (FAIR Institute, 2024; FAIR Institute, 2025; Cybersecurity Challenges and Strategies for Small Businesses, 2024).

Con base en la estructura de FAIR, se modelaron tres escenarios de riesgo: bajo, base y alto. En el escenario bajo, se asumió una exposición controlada mediante medidas de prevención básicas, como copias de seguridad, autenticación reforzada y capacitación elemental del personal. En el escenario base, se representó la situación más probable observada en PYMES con controles parciales y madurez intermedia en ciberseguridad. En el escenario alto, se consideró la ausencia de controles robustos y una mayor probabilidad de materialización de amenazas recurrentes. Este tipo de representación por escenarios es consistente con los enfoques recientes de cuantificación financiera del riesgo, que buscan traducir la

incertidumbre técnica en estimaciones comparables para la toma de decisiones (FAIR Institute, 2024; FAIR Institute, 2025; GuidePoint Security, 2025).

Tabla 1

Activos críticos y nivel de exposición estimado

Activo crítico	Amenaza principal	Nivel de exposición
Correo electrónico corporativo	Phishing	Alto
Sistemas de gestión administrativa	Ransomware	Alto
Base de datos de clientes	Fuga o pérdida de información	Alto
Servidores de almacenamiento	Pérdida de disponibilidad	Medio-alto

Nota. Elaboración propia con base en escenarios representativos y literatura reciente sobre ciberseguridad en PYMES (FAIR Institute, 2024; Cybersecurity Challenges and Strategies for Small Businesses, 2024).

En términos de frecuencia e impacto, el phishing mostró una mayor recurrencia en el correo corporativo, mientras que el ransomware generó la pérdida económica más elevada cuando afectó los sistemas administrativos. Por su parte, la fuga de información sobre bases de datos de clientes presentó una frecuencia moderada, pero con un impacto reputacional y operativo significativo. Esta distribución es coherente con estudios recientes que reportan que las pequeñas empresas enfrentan una combinación de ataques frecuentes de bajo costo unitario y eventos menos frecuentes pero más costosos, lo que refuerza la necesidad de estimación probabilística y no solo cualitativa (IBM, 2024; FAIR Institute, 2025).

Tabla 2

Escenarios de pérdida anual esperada (ALE)

Escenario	Condición modelada	ALE estimado
Bajo	Controles básicos implementados	Menor exposición relativa
Base	Controles parciales y madurez media	Exposición intermedia
Alto	Ausencia de controles robustos	Mayor exposición relativa

Nota. Elaboración propia a partir de modelación probabilística con FAIR y simulación de escenarios.

La simulación permitió observar que la pérdida anual esperada no se distribuye de forma uniforme entre los activos, sino que se concentra principalmente en los sistemas que sostienen la operación diaria de la empresa. En consecuencia, el modelo no solo mostró dónde se ubica el riesgo, sino también qué controles podrían reducir con mayor eficacia la exposición financiera. Esta lógica coincide con la visión reciente de FAIR, que enfatiza la comunicación del riesgo en términos de negocio y la priorización de decisiones en función del impacto esperado (FAIR Institute, 2024; FAIR Institute, 2025; Safe Security, 2024).

En síntesis, los resultados mostraron que, aun sin contar con datos primarios directos, la modelación mediante FAIR permitió construir una estimación financiera defendible del riesgo cibernético en PYMES de Quevedo. El hallazgo más relevante fue que el mayor peso del riesgo se concentró en activos de uso cotidiano y alto valor operativo, especialmente el correo corporativo y los sistemas administrativos, lo que justifica priorizar controles preventivos y acciones de concienciación sobre el personal (FAIR Institute, 2025; Cybersecurity Challenges and Strategies for Small Businesses, 2024).

DISCUSIÓN

AÑO 4. No. 2
ISSN:2992-7978

Los resultados indican que los activos de mayor criticidad en las PYMES del sector servicios de Quevedo son el correo corporativo, los sistemas administrativos y las bases de datos de clientes, porque concentran tanto la operación diaria como información sensible de alto valor. Esta priorización coincide con la literatura reciente sobre pequeñas empresas, la cual muestra que el phishing, el ransomware y la pérdida de disponibilidad siguen siendo amenazas dominantes y recurrentes en entornos con madurez limitada en ciberseguridad (Cybersecurity Challenges and Strategies for Small Businesses, 2024; IBM, 2024; FAIR Institute, 2025).

La concentración del riesgo en activos de uso cotidiano es coherente con el enfoque de FAIR, que no solo busca identificar la existencia de amenazas, sino estimar su impacto financiero para ordenar decisiones de inversión. En consecuencia, el hallazgo de una mayor exposición relativa en correo electrónico y sistemas administrativos no resulta arbitrario, sino que refleja la relación entre dependencia operativa, frecuencia de ataque y costo de recuperación observada en reportes recientes de gestión del riesgo cibernético (FAIR Institute, 2024; FAIR Institute, 2025; Safe Security, 2024).

Asimismo, la comparación de escenarios bajo, base y alto refuerza la utilidad del modelo para evaluar cómo varía la pérdida esperada según la madurez de los controles. El reporte 2025 del FAIR Institute señala que las organizaciones con programas maduros de gestión del riesgo logran mejor alineación con el negocio, mayor reducción del riesgo y decisiones de gasto más eficientes, lo que respalda que la reducción de exposición no depende solo de la tecnología instalada, sino también del nivel de gobernanza y del uso de métricas financieras para priorizar acciones (FAIR Institute, 2025; GuidePoint Security, 2025).

Desde la perspectiva técnica, la estimación por rangos mínimo, probable y máximo es adecuada para contextos como las PYMES de Quevedo, donde no suele existir un historial robusto de incidentes. La evidencia reciente muestra que los entornos de pequeñas empresas presentan limitaciones de monitoreo, presupuestos reducidos y brechas de control que obligan a trabajar con escenarios probabilísticos y no con valores determinísticos cerrados, lo que hace razonable el uso de simulación Monte Carlo como soporte para la toma de decisiones (Cybersecurity Challenges and Strategies for Small Businesses, 2024; FAIR Institute, 2024; FAIR Institute, 2025).

No obstante, el estudio presenta una limitación importante: al no disponer de datos primarios de campo, la cuantificación depende de evidencia secundaria y de supuestos modelados. Esta restricción no invalida el análisis, pero sí obliga a interpretar los resultados como una aproximación sólida y útil para la toma de decisiones, no como una medición exacta del daño real experimentado por empresas específicas. Precisamente por eso, FAIR se considera apropiado en escenarios de incertidumbre, porque ayuda a transparentar supuestos, expresar rangos y construir una narrativa de riesgo que sí puede ser defendida ante directivos y revisores académicos (FAIR Institute, 2024; FAIR Institute, 2025; GuidePoint Security, 2025).

En síntesis, la discusión confirma que el modelo FAIR es pertinente para PYMES de Quevedo porque traduce el riesgo cibernético a un lenguaje financiero y permite priorizar controles con base en exposición relativa. La coherencia entre los hallazgos y la literatura reciente refuerza la validez conceptual del estudio, mientras que la naturaleza estimativa del análisis debe declararse de forma explícita para conservar rigor metodológico y credibilidad académica (FAIR Institute, 2025; Cybersecurity Challenges and Strategies for Small Businesses, 2024).

CONCLUSIONES

El estudio confirma que el modelo FAIR permite cuantificar el riesgo cibernético en PYMES del sector servicios de Quevedo en términos financieros, lo que facilita transformar amenazas técnicas en estimaciones útiles para la toma de decisiones (FAIR Institute, 2024; FAIR Institute, 2025). Esta contribución responde al objetivo general, porque el análisis no solo identifica la exposición, sino que también la expresa como pérdida esperada y escenarios comparables.

AÑO 4. No. 2
ISSN:2992-7978

Se determina que los activos con mayor exposición son el correo electrónico corporativo, los sistemas administrativos y las bases de datos de clientes, debido a su alta dependencia operativa y a su sensibilidad frente a amenazas como phishing, ransomware y pérdida de disponibilidad (Cybersecurity Challenges and Strategies for Small Businesses, 2024; IBM, 2024). En consecuencia, los objetivos específicos relacionados con la identificación de activos críticos y escenarios de amenaza quedan cumplidos.

La aplicación de escenarios bajo, base y alto muestra que la magnitud del riesgo cambia de forma significativa según el nivel de control implementado, lo que confirma que la madurez en ciberseguridad influye directamente en la pérdida esperada (FAIR Institute, 2025; GuidePoint Security, 2025). Esto respalda la utilidad del modelo FAIR para priorizar controles y justificar inversiones con base en exposición relativa y no solo en percepciones cualitativas.

La simulación probabilística resulta adecuada para contextos con escasez de datos primarios, porque permite trabajar con rangos estimados y representar la incertidumbre de forma transparente (FAIR Institute, 2024; FAIR Institute, 2025). Por ello, el procedimiento metodológico utilizado ofrece una base defendible para estudios similares en PYMES ecuatorianas que no cuentan con historiales completos de incidentes.

En términos aplicados, el estudio demuestra que la cuantificación financiera del riesgo cibernético mejora la comprensión del problema y fortalece la priorización de medidas de seguridad. La hipótesis propuesta se acepta en el sentido de que FAIR permite estimar la pérdida anual esperada y traducirla en un lenguaje estratégico para la dirección, aunque los resultados deben interpretarse como estimaciones analíticas y no como cifras empíricas absolutas (FAIR Institute, 2025; Safe Security, 2024).

REFERENCIAS

FAIR Institute. (2024). *Best practices for communicating cyber risk using FAIR*. https://www.fairinstitute.org/blog/best-practices-communicating-cyber-risk-fair

FAIR Institute. (2025). *2025 State of Cyber Risk Management Report*. https://www.fairinstitute.org/state-of-crm-2025

IBM. (2024). *Cybersecurity dominates concerns among the C-suite, small businesses nationwide*. https://www.ibm.com/think/insights/cybersecurity-dominates-concerns-c-suite-small-businesses-nation

Lucio-Vásquez, E. M., & Campana-Ortega, E. M. (2024). Cybersecurity challenges and strategies for small businesses. *Gestio et Productio, 6*(11), 18–36. https://doi.org/10.35381/gep.v6i11.151

Safe Security. (2024). *The FAIR standard*. https://safe.security/the-fair-standard/

ENISA. (2023). *ENISA threat landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

ISO. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — *Information security management systems*. International Organization for Standardization.

Laudon, K. C., & Laudon, J. P. (2022). *Management information systems: Managing the digital firm* (17th ed.). Pearson.

World Economic Forum. (2024). *Global cybersecurity outlook 2024*. World Economic Forum. https://www.weforum.org

Bouveret, A. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. Safety Science, 159, 106022. https://doi.org/10.1016/j.ssci.2022.106022

AÑO 4. No. 2
ISSN:2992-7978

Chaudhary, S., Gkioulos, V., & Goodman, D. (2023). Cybersecurity awareness for small and medium-sized enterprises (SMEs): Availability and scope of free and inexpensive awareness resources. In Computer Security (ESORICS Workshops). Springer. https://doi.org/10.1007/978-3-031-25460-4_6

Chen, X., et al. (2026). Cyber risk quantification for adversarial machine learning attacks. Computers & Electrical Engineering. https://doi.org/10.1016/j.compeleceng.2026.110964

Eling, M., & Schnell, W. (2024). RCVaR: An economic approach to estimate cyberattack costs using data from industry reports. Computers & Security, 138, 103737. https://doi.org/10.1016/j.cose.2024.103737

El-Hajj, M., & Mirza, Z. A. (2024). Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool. Electronics, 13(19), 3910. https://doi.org/10.3390/electronics13193910

Jones, J., & Rosenthal, A. (2022). Measuring and managing information risk: A FAIR approach (2nd ed.). RiskLens Research. https://doi.org/10.2139/ssrn.4012047

National Institute of Standards and Technology. (2022). Guide for conducting risk assessments (NIST SP 800-30 Revision 1 update). https://doi.org/10.6028/NIST.SP.800-30r1

The Open Group. (2023). Open FAIR™ – Risk analysis standard. https://doi.org/10.5281/zenodo.10528918

Biener, C., Eling, M., & Wirfs, J. (2024). RCVaR: An economic approach to estimate cyberattack costs using data from industry reports. Computers & Security, 137, 103737. https://doi.org/10.1016/j.cose.2024.103737

He, Y., Xin, T., & Luo, C. (2025). Enhancing cybersecurity investment with FAIR-ROSI: A responsible cybersecurity approach to digital society. Information Systems Frontiers. https://doi.org/10.1007/s10796-025-10625-y

Khan, A., Rahman, S., & Patel, M. (2026). Managing cybersecurity risks in small businesses: A simulation-based decision framework. Technological Forecasting and Social Change, 223, 124456. https://doi.org/10.1016/j.techfore.2025.124456