PACHA
Revista de Estudios Contemporáneos del Sur Global

Evaluación del impacto de las inversiones en ciberseguridad sobre los costos operativos y la rentabilidad en Instituciones Financieras

Assessment of the Impact of Cybersecurity Investments on Operational Costs and Profitability in Financial Institutions

Jonathan Israel Toctaguano Basantes, Verónica Paulina Moreno Narváez

Resumen

En los últimos años, las amenazas cibernéticas han aumentado de forma notable, obligando a las instituciones financieras a invertir en mecanismos de protección para salvaguardar sus activos digitales. En 2022, las pérdidas globales por incidentes cibernéticos superaron los 6 billones de dólares, lo que evidencia la magnitud del problema. En este contexto, las pequeñas y medianas instituciones financieras de Latacunga, Ecuador, se enfrentan al desafío de equilibrar sus inversiones en ciberseguridad con la eficiencia operativa y la rentabilidad. Este estudio se enfoca en analizar cómo estas inversiones influyen en los costos operativos y en el rendimiento financiero de dichas entidades. A través de un enfoque cuantitativo, no experimental y deductivo, se aplicaron encuestas y se realizó una revisión documental. Los resultados revelan que la inversión en ciberseguridad incrementa los costos operativos, aunque su impacto en la rentabilidad es moderado. Se identificó que la capacitación del personal y la actualización tecnológica mejoran la eficiencia organizacional.

Palabras: seguridad; estrategia; tecnología; formación; datos.

Jonathan Israel Toctaguano Basantes
Universidad Católica de Cuenca | Cuenca | Ecuador | jonathan.toctaguano.15@est.ucacue.edu.ec
https://orcid.org/0009-0005-1797-8819
Verónica Paulina Moreno Narváez
Universidad Católica de Cuenca | Cuenca | Ecuador | veronica.moreno@ucacue.edu.ec
https://orcid.org/0000-0002-6137-2460

http://doi.org/10.46652/pacha.v6i18.427
ISSN 2697-3677
Vol. 6 No. 18 mayo-agosto 2025, e250427
Quito, Ecuador

Enviado: febreo 28, 2025
Aceptado: abril 19, 2025
Publicado: mayo 14, 2025
Publicación Continua

Abstract

In recent years, cyber threats have increased considerably, forcing financial institutions to invest in protection mechanisms to safeguard their digital assets. In 2022, global losses from cyber incidents exceeded $6 trillion, highlighting the magnitude of the problem. In this context, small and medium-sized financial institutions in Latacunga, Ecuador, face the challenge of balancing their investments in cybersecurity with operational efficiency and profitability. This study focuses on analyzing how these investments influence the operating costs and financial performance of these entities. Through a quantitative, non-experimental, and deductive approach, surveys were conducted and a document review was conducted. The results reveal that investment in cybersecurity increases operating costs, although its impact on profitability is moderate. Staff training and technological updating were identified as improving organizational efficiency.

Keywords: security; strategy; technology; training; data.

Introducción

En las instituciones financieras globales existe un enfrentamiento, un entorno cada vez más digitalizado, en el que las amenazas cibernéticas se han convertido en un desafío sistémico. El costo promedio de una filtración de datos en América Latina en 2024 fue de 2,76 millones de dólares, cifra que aumenta debido a la creciente complejidad de estos incidentes y las mayores demandas a los equipos de ciberseguridad (TeleSemana, 2024). Debido a que las organizaciones no cuentan con métodos claros para evaluar el riesgo cibernético en términos financieros, es complicado comunicar de manera efectiva las ciberamenazas y el impacto que generan dentro de la organización. Este escenario ha impulsado un cambio de paradigma en la gestión de riesgos, exigiendo que las organizaciones integren la ciberseguridad como un elemento fundamental de su estrategia corporativa.

El Ecuador refleja tendencias similares a las globales en cuanto a la digitalización y ciberseguridad. Las instituciones financieras del país han incrementado sus inversiones en tecnologías de protección como *firewalls* avanzados, sistemas de detección de intrusos y capacitaciones especializadas para su personal. No obstante, persisten incertidumbres respecto al impacto de estas inversiones en los costos operativos y la rentabilidad, la complejidad en el cumplimiento normativo. La mitigación de riesgos reputacionales y la preservación de la confianza del cliente continúan siendo prioridades para estas entidades, aunque los efectos financieros asociados no siempre son fáciles de cuantificar, los riesgos pueden surgir en cualquier actividad, incluso en las más sencillas. Por ello es fundamental implementar mecanismos de control que permitan gestionarlos como es debido (Guerrero, 2020).

Las instituciones financieras de la ciudad de Latacunga enfrentan barreras que las colocan en una posición vulnerable ante las amenazas cibernéticas. Las pequeñas y medianas entidades, en particular, a menudo carecen de los recursos suficientes para implementar medidas de ciberseguridad efectivas, lo que incrementa su exposición a ataques. Las características de cada institución, como su infraestructura tecnológica y nivel de digitalización, determinan los riesgos específicos que enfrentan. Las percepciones de los gerentes y empleados sobre la necesidad y efectividad de estas inversiones juegan un papel en la aplicación y éxito de las estrategias de ciberseguridad.

En este contexto, surge el problema de investigación: ¿cómo inciden las inversiones en ciberseguridad en los costos operativos y la rentabilidad de las instituciones financieras localizadas en la ciudad de Latacunga, Ecuador? Esta interrogante busca analizar el impacto financiero de dichas inversiones, sino también comprender cómo contribuyen a la estabilidad y protección de estas organizaciones frente a amenazas cibernéticas cada vez más frecuentes. A partir de esta problemática, el objetivo de la investigación es evaluar de qué manera las inversiones en ciberseguridad afectan los costos operativos y la rentabilidad de las instituciones financieras.

Desarrollo

El valor de la protección digital e inversión en la era de los ciberataques

En la era digital la ciberseguridad se ha convertido en un aspecto fundamental para la protección de la información y la continuidad operativa de las organizaciones. La creciente dependencia de la tecnología y la interconectividad han aumentado la vulnerabilidad a ciberataques, lo que ha llevado a las empresas y gobiernos a destinar recursos significativos en la implementación de estrategias de seguridad informática. En la actualidad, el ámbito digital enfrenta múltiples retos en materia de seguridad cibernética, dado el alto nivel de dependencia de la tecnología en sus procesos operativos. La escasez de recursos suele exponer diversas amenazas y puntos vulnerables dentro de sus entornos digitales (Lucio & Campaña, 2024). La inversión en ciberseguridad responde a la necesidad de proteger datos sensibles, también es una medida preventiva para evitar pérdidas económicas, daños reputacionales y problemas legales derivados de incidentes de seguridad. Las inversiones en ciberseguridad abarcan diversas áreas, desde la adquisición de software y hardware especializados hasta la capacitación del personal y el desarrollo de normativas internas. Un componente de estas inversiones es la adopción de tecnologías avanzadas como la inteligencia artificial, el aprendizaje automático y el análisis de *big data*, que permiten detectar y responder a amenazas de manera más eficiente. El uso de herramientas de cifrado y autenticación multifactorial ha demostrado ser efectivo para mitigar riesgos asociados al acceso no autorizado a sistemas críticos. La teoría de la dependencia de la tecnología cuestiona el uso excesivo de herramientas tecnológicas, señalando las posibles vulnerabilidades que pueden aparecer, sobre todo cuando los sistemas experimentan fallos tecnológicos o son objeto de ciberataques (Brito & Franklin, 2024).

El crecimiento de los ataques cibernéticos, como el *ransomware*, el *phishing* y las brechas de datos, ha obligado a las organizaciones a destinar mayores presupuestos a la seguridad informática. Según estudios recientes, las empresas han incrementado sus inversiones en soluciones de detección y respuesta a incidentes, así como en seguros cibernéticos que les permitan mitigar el impacto financiero de un ataque exitoso. La regulación y cumplimiento normativo también juegan un papel importante en la determinación de la inversión en ciberseguridad, las normativas como el reglamento general de protección de datos y la ley de privacidad del consumidor de California exigen altos estándares de protección de la información.

Las soluciones tecnológicas, la concienciación y capacitación de los empleados son esenciales para fortalecer la ciberseguridad organizacional. La mayoría de los incidentes de seguridad se deben a errores humanos, por lo que la educación en buenas prácticas, como la gestión de contraseñas seguras y la identificación de correos electrónicos maliciosos, es una inversión para reducir vulnerabilidades.

Las inversiones en ciberseguridad benefician a las empresas, también contribuyen a la seguridad nacional y a la protección de infraestructuras críticas. Los gobiernos tienen la responsabilidad de diseñar políticas que fomenten y aseguren niveles óptimos de ciberseguridad, alineados con estándares internacionales. Esto es sobre todo para la protección de la infraestructura crítica de información a nivel nacional. Los gobiernos tienen la responsabilidad de diseñar políticas que fomenten y aseguren niveles óptimos de ciberseguridad, alineados con estándares internacionales. Esto es sobre todo para la protección de la infraestructura crítica de información a nivel nacional (Sancho, 2020).

Los gobiernos han implementado estrategias de ciberseguridad a nivel nacional para proteger sectores estratégicos como la energía, las telecomunicaciones y la banca. Estas iniciativas incluyen la creación de centros de respuesta a incidentes cibernéticos y el desarrollo de normativas que obligan a las empresas a reportar ataques y fortalecer sus medidas de protección.

A pesar de la creciente importancia de la ciberseguridad, muchas organizaciones aún enfrentan desafíos en la asignación de recursos adecuados. La falta de personal capacitado, el costo de las soluciones avanzadas y la rápida evolución de las amenazas dificultan la implementación efectiva de estrategias de seguridad. Sin embargo, los beneficios de una inversión adecuada en ciberseguridad superan en gran medida los costos, ayudan a prevenir pérdidas millonarias y protegen la reputación empresarial.

Las inversiones en ciberseguridad son una necesidad en el entorno digital actual. La adopción de tecnologías innovadoras, la capacitación del personal y el cumplimiento normativo son factores para garantizar una protección efectiva contra amenazas cibernéticas. A medida que los riesgos continúan evolucionando, las organizaciones deben priorizar la seguridad informática como una estrategia integral que garantice su sostenibilidad y resiliencia ante los desafíos digitales.

Desafíos y soluciones en la inversión en ciberseguridad

En la era digital, la ciberseguridad se ha convertido en un aspecto fundamental para la protección de la información y la continuidad operativa de las organizaciones. La creciente dependencia de la tecnología y la interconectividad han aumentado la vulnerabilidad a ciberataques, lo que ha llevado a las empresas y gobiernos a destinar recursos significativos en la implementación de estrategias de seguridad informática. Entre 2016 y 2020, se observa una gran diversidad en las iniciativas individuales para desarrollar una política nacional de ciberseguridad. Mientras algunos países, como Chile, Uruguay y Colombia, han logrado avances significativos, otros, como El

Salvador, República Dominicana y Haití, permanecen casi sin cambios en este ámbito (Aguilar, 2021).

La inversión en ciberseguridad aparte de responder a la necesidad de proteger datos sensibles también es una medida preventiva para evitar pérdidas económicas, daños reputacionales y problemas legales derivados de incidentes de seguridad. Las inversiones en ciberseguridad abarcan diversas áreas, desde la adquisición de software y hardware especializados hasta la capacitación del personal y el desarrollo de normativas internas. Un componente de estas inversiones es la adopción de tecnologías avanzadas como la inteligencia artificial, el aprendizaje automático y el análisis de *big data*, que permiten detectar y responder a amenazas de manera más eficiente. El uso de herramientas de cifrado y autenticación multifactorial ha demostrado ser efectivo para mitigar riesgos asociados al acceso no autorizado a sistemas críticos. Durante un evento sobre ciberseguridad realizado en 2024 en Quito, especialistas informaron que los ciberataques en Ecuador han incrementado entre un 24 % y un 30 % en el último año, lo que ha puesto a las empresas del país ante riesgos considerables (LEXIS, 2024).

El crecimiento de los ataques cibernéticos, como el *ransomware*, el *phishing* y las brechas de datos, ha obligado a las organizaciones a destinar mayores presupuestos a la seguridad informática. Según estudios recientes, las empresas han incrementado sus inversiones en soluciones de detección y respuesta a incidentes, así como en seguros cibernéticos que les permitan mitigar el impacto financiero de un ataque exitoso. La regulación y cumplimiento normativo también juegan un papel importante en la determinación de la inversión en ciberseguridad, normativas como el reglamento general de protección de datos y la ley de privacidad del consumidor de california exigen altos estándares de protección de la información (Ordoñes & Quezada, 2022).

En este marco, la infraestructura tecnológica es relevante, sino también el factor humano. La mayoría de los incidentes de seguridad se deben a errores humanos, por lo que la educación en buenas prácticas, como la gestión de contraseñas seguras y la identificación de correos electrónicos maliciosos, es una inversión para reducir vulnerabilidades. Las inversiones en ciberseguridad benefician a las empresas, también contribuyen a la seguridad nacional y a la protección de infraestructuras críticas. Los gobiernos han implementado estrategias de ciberseguridad a nivel nacional para proteger sectores estratégicos como la energía, las telecomunicaciones y la banca. Estas iniciativas incluyen la creación de centros de respuesta a incidentes cibernéticos y el desarrollo de normativas que obligan a las empresas a reportar ataques y fortalecer sus medidas de protección.

Un riesgo significativo en la investigación de mercados digitales es la alteración de datos. En 2020 la firma de análisis de datos *Cambridge analítica* estuvo involucrada en un gran escándalo luego de que se descubriera que había adquirido sin autorización los datos personales de millones de usuarios de Facebook y los usó para influir en procesos electorales y estrategias publicitarias (Conforme & Calle, 2024).

A pesar de la creciente importancia de la ciberseguridad, muchas organizaciones aún enfrentan desafíos en la asignación de recursos adecuados. La falta de personal capacitado, el costo de las

soluciones avanzadas y la rápida evolución de las amenazas dificultan la implementación efectiva de estrategias de seguridad. Sin embargo, los beneficios de una inversión adecuada en ciberseguridad superan en gran medida los costos ayudan a prevenir pérdidas millonarias y protegen la reputación empresarial.

Metodología

El estudio fue diseñado utilizando un enfoque cuantitativo, no experimental, con un alcance explicativo y una finalidad transversal. Este diseño permitió analizar cómo las estrategias de ciberseguridad afectan los aspectos financieros y operativos en el contexto específico de las instituciones financieras en la región.

El enfoque cuantitativo se basa en la recolección y el análisis de datos numéricos para establecer patrones, determinar relaciones entre variables y generalizar resultados a una población mayor. Según Torres (2015), el enfoque cuantitativo se caracteriza por su intento de explicar fenómenos sociales mediante la recolección y el análisis de datos numéricos, utilizando instrumentos como encuestas y cuestionarios. Este tipo de enfoque se enfoca en la objetividad y la medición precisa de los fenómenos bajo estudio.

El diseño no experimental se refiere a la observación y análisis de fenómenos sin manipular las variables independientes. En este tipo de investigación, el investigador no controla ni manipula las variables, observa las relaciones tal como se presentan en su contexto natural. Según Aucancela (2021), en el diseño no experimental, el investigador no tiene intervención directa sobre las variables, y las situaciones son observadas tal como ocurren.

El alcance explicativo se centra en identificar las causas o explicaciones de un fenómeno. Este tipo de investigación busca explicar las relaciones entre variables, en lugar de solo describir o identificar su existencia. Según Ramos (2020), una investigación explicativa tiene como propósito el establecer las causas y efectos de los fenómenos, ayudando a entender cómo y por qué ocurren. Este enfoque busca proporcionar una comprensión más profunda y detallada de los hechos observados.

Una investigación de finalidad transversal se refiere a la recolección de datos en un solo momento o periodo de tiempo, sin que haya intervención a lo largo de un tiempo prolongado. En este tipo de estudios, los datos se recopilan de forma puntual para obtener una visión instantánea de la situación. Según Maguiña & Soto (2021), la investigación transversal implica la recolección de datos en un único punto temporal, permitiendo una visión instantánea de los fenómenos.

El método adoptado fue deductivo, lo que implicó partir de teorías generales relacionadas con la ciberseguridad y su gestión de riesgos, para llegar a conclusiones específicas basadas en los datos recolectados. A través de este método se buscó entender las interacciones entre las inversiones en ciberseguridad, los costos operativos asociados y la rentabilidad obtenida, considerando las particularidades del entorno financiero local.

La unidad de análisis de la investigación fueron las instituciones financieras ubicadas en Latacunga, Ecuador. Para seleccionar las instituciones participantes, se empleó un muestreo por conveniencia, dado que el acceso a las instituciones se facilitó a través de contactos disponibles en la región. De un universo de 20 instituciones financieras, se seleccionaron 10 para la investigación con base en un muestreo intencional, priorizando aquellas que contaban con información accesible, disposición para participar y un historial de implementación de medidas de ciberseguridad. Esta selección permitió un análisis más detallado y profundo de los datos, enfocándose en la calidad y relevancia de la información obtenida, en lugar de ampliar el alcance de forma superficial.

La recolección de datos se llevó a cabo mediante encuestas estructuradas, estas encuestas se enfocaron en varios aspectos como el presupuesto asignado a ciberseguridad, la frecuencia de actualización tecnológica, la capacitación del personal, y su percepción sobre el impacto de estas inversiones en los costos y la rentabilidad.

Además de las encuestas, se realizó un análisis de documentos financieros, informes de auditoría y estadísticas vinculadas a la ciberseguridad, lo que facilitó un examen más detallado de los indicadores. Esta combinación de encuestas y revisiones documentales garantizó una comprensión más amplia y detallada sobre cómo las inversiones en ciberseguridad influyen en los resultados financieros y operativos de las instituciones financieras.

Los resultados obtenidos permitieron analizar las relaciones entre los costos operativos y la rentabilidad, así como identificar las áreas donde las inversiones en ciberseguridad son más efectivas en la mitigación de riesgos y la mejora de la sostenibilidad financiera. Este enfoque metodológico aportó evidencia empírica sobre la relación entre la ciberseguridad y el desempeño financiero, también ofreció una base sólida para la formulación de políticas y estrategias en ciberseguridad adaptadas a las particularidades locales de las instituciones financieras en Latacunga.

Resultados y discusión

Los hallazgos obtenidos a partir de la encuesta a diversas instituciones revelan aspectos sobre la relación entre la inversión en ciberseguridad y su impacto en los costos y la rentabilidad. Estos resultados destacan las tendencias y patrones emergentes de las respuestas recopiladas, lo que proporciona una visión más clara sobe cómo las inversiones en ciberseguridad afectan a las operaciones y los costos.

Tabla 1. Impacto en costos

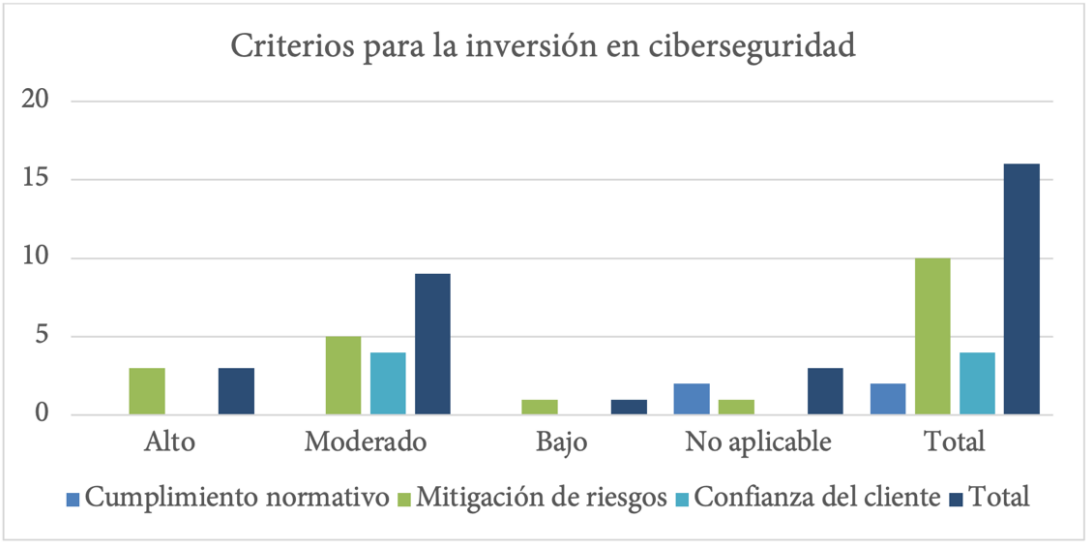
Porcentaje presupuesto ciberseguridad	Los ha incrementado de forma notable	Los ha incrementado con moderación	Los ha reducido	No ha tenido impacto	Total
Menos del 1%	3	1	0	3	7
Entre el 1% y el 5%	2	5	1	0	8
Entre el 6% y el 10%	0	1	0	0	1
Más del 10%	0	1	0	0	1

Porcentaje presupuesto ciberseguridad	Los ha incrementado de forma notable	Los ha incrementado con moderación	Los ha reducido	No ha tenido impacto	Total
Total	5	8	1	3	17

Fuente: elaboración propia
Nota. La tabla muestra la relación entre inversión en ciberseguridad y su impacto en costos y rentabilidad.

La mayoría de las instituciones 47.1% destinan entre el 1% y el 5% de su presupuesto a ciberseguridad, de las cuales el 62.5% reporta un incremento moderado en los costos operativos. Por su parte el 41.2% de las instituciones que asignan menos del 1% señala que los costos se incrementaron en términos amplios o no tuvieron impacto 42.9% cada uno. Las instituciones que destinan entre el 6% y el 10% o más del 10% representan el 5.9% cada una y perciben un impacto moderado en los costos. Esto evidencia que un mayor presupuesto en ciberseguridad en su mayoría está asociado con aumentos moderados en los costos operativos.

Figura 1. Criterio para inversión



Fuente: elaboración propia
Nota. La tabla muestra que la mitigación de riesgos es el principal criterio para la inversión en ciberseguridad, asociado con un ROI alto o moderado.

El retorno sobre la inversión ROI en ciberseguridad parece estar sobre todo vinculado al criterio de mitigación de riesgos. Del total de casos, el 62.5% 10 de 16 seleccionó la mitigación de riesgos como el criterio, y entre ellos, el 30% reporta un ROI alto, mientras que el 50% señala un ROI moderado. La confianza del cliente fue elegida por el 25% de los participantes 4 de 16, y está asociada solo a un ROI moderado. Por otro lado, el cumplimiento normativo, seleccionado por el 12.5% 2 de 16, está relacionado con casos en los que el ROI no es aplicable. Esto sugiere que la mitigación de riesgos es el principal impulsor de la inversión en ciberseguridad, en particular cuando se busca un retorno moderado o alto.

Tabla 2. Sostenibilidad Financiera

Impacto en rentabilidad	Mucho	De forma controlada	Poco	Nada	Total
Positivo y significativo	1	3	0	1	5
Positivo y moderado	0	7	0	0	7
Sin impacto	0	1	1	1	3
Negativo	0	1	1	0	2
Total	1	12	2	2	17

Fuente: elaboración propia
Nota. La tabla muestra la relación entre impacto en rentabilidad global y sostenibilidad financiera.

La relación entre el impacto en la rentabilidad global y la sostenibilidad financiera muestra que un impacto positivo, ya sea significativo o moderado, está estrechamente relacionado con una contribución moderada a la sostenibilidad. Del total de instituciones, el 70.6% reporta un impacto positivo 29.4% significativo y 41.2% moderado), y dentro de este grupo, el 71.4% indica que la ciberseguridad contribuye moderadamente a la sostenibilidad financiera. Por otro lado, las instituciones que no perciben impacto 17.6% se distribuyen equitativamente entre contribuciones moderadas, bajas o inexistentes. En cuanto al impacto negativo 11.8%, la mitad reporta una contribución moderada y la otra mitad, baja. Esto sugiere que un impacto positivo en la rentabilidad global favorece una percepción de sostenibilidad financiera moderada, mientras que la falta de impacto o efectos negativos tienden a diluir esta relación.

Tabla 3. Tabla de eficiencia operativa impacto

Frecuencia de actualización	Mejora significativa	Mejora moderada	Sin impacto	Total
Anualmente	1	6	1	8
Cada 2-3 años	1	3	0	4
Cada 4-5 añoso	0	1	0	1
No se actualizan	1	1	2	4
Total	3	11	3	17

Fuente: elaboración propia
Nota. La tabla muestra la relación entre actualización de tecnologías y eficiencia operativa.

La frecuencia de actualización de tecnologías parece estar estrechamente relacionada con el impacto en la eficiencia operativa. El 47.1% de las instituciones actualiza sus tecnologías anualmente, y de estas, el 75% reporta una mejora moderada en la eficiencia. Por otro lado, el 23.5% actualiza cada 2-3 años, donde también predomina la percepción de mejora moderada (75%). Aquellas instituciones que no actualizan tecnologías (23.5%) muestran una menor percepción de mejora, con el 50% indicando que no hay impacto en la eficiencia. Las actualizaciones más esporádicas, cada 4-5 años, representan solo el 5.9% de los casos y están asociadas principalmente a una mejora moderada. Esto sugiere que una mayor frecuencia de actualización está vinculada a mejoras más evidentes en la eficiencia operativa.

Tabla 4. Ataques priorizados mitigar

Proporción personal capacitado	Ransomware	Phishing	Denegación de servicio (DDoS)	(	Total
Ninguno	1	0	1	4	6
Menos del 25%	3	5	1	1	10
Entre el 25% y el 50%	1	0	0	0	1
Total	5	5	2	5	17

Fuente: elaboración propia
Nota. La tabla muestra la relación entre capacitación del personal y mitigación de ciberataques.

La relación entre la capacitación del personal y la mitigación de ciberataques muestra que las instituciones con menor proporción de personal capacitado tienden a priorizar una gama más diversa de ataques. El 58.8% de las instituciones tienen menos del 25% de su personal capacitado, y en este grupo, el 50% prioriza mitigar ransomware y phishing, mientras que el resto se enfoca en ataques de denegación de servicio 10% u otros tipos 10%. Por otro lado, las instituciones sin personal capacitado 35.3% se enfocan mayoritariamente en "otros" ataques 66.7% o denegación de servicio 16.7%. En contraste, solo una institución 5.9% capacita entre el 25% y el 50% de su personal, enfocándose exclusivamente en ransomware. Esto sugiere que la capacitación limitada conduce a priorizar ataques específicos, mientras que una ausencia total de capacitación dispersa los esfuerzos hacia otros riesgos.

Tabla 5. Retorno sobre inversión

Impacto en costos	Alto	Moderado	Bajo	No aplicable	Total
Los ha incrementado significativamente	2	2	0	1	5
Los ha incrementado moderadamente	0	6	1	0	7
Los ha reducido	1	0	0	0	1
No ha tenido impacto	0	1	0	2	3
Total	3	9	1	3	16

Fuente: elaboración propia
Nota. La tabla muestra la relación entre impacto en costos y retorno sobre activos/patrimonio.

La relación entre el impacto en los costos y el retorno sobre activos/patrimonio ROA/ROE evidencia que los incrementos moderados en los costos están más asociados con un retorno moderado. Del total de instituciones, el 43.8% reportó un incremento moderado en costos, y de estas, el 85.7% indica un retorno moderado. Por otro lado, un incremento significativo en costos 31.3% se distribuye de forma equitativa entre retornos altos 40% y moderados 40%, mientras que un 20% considera que no aplica. Las instituciones que lograron reducir los costos 6.3% reportan exclusivamente un retorno alto. Finalmente, aquellas que no percibieron impacto en costos 18.8% se dividen principalmente entre retornos moderados 33.3% y no aplicable 66.7%. Esto sugiere que el

aumento moderado en costos suele estar correlacionado con un retorno moderado, mientras que la reducción de costos podría favorecer un retorno alto.

La ciberseguridad ha surgido como un aspecto fundamental en la gobernabilidad moderna, permite a las sociedades aprovechar de manera segura los beneficios del ciberespacio. Según Hirare (2020) destaca que el crecimiento del uso de las Tecnologías de la Información y la Comunicación ha permitido que las relaciones sociales se realicen de manera más rápida y económica, esto ha traído consigo un aumento en las amenazas cibernéticas que comprometen la seguridad de los datos e infraestructuras. Esta creciente dependencia de los servicios en línea y la expansión del internet de las cosas también han generado nuevos retos en el ámbito de la ciberseguridad, los cuales afectan tanto a la seguridad nacional como a las relaciones internacionales. La autora sobra la ciberseguridad es esencial para garantizar que las instituciones, empresas y ciudadanos puedan operar con confianza en el ciberespacio, destacando su rol como una condición previa para la confianza y el desarrollo.

A nivel global, las amenazas cibernéticas han crecido de forma amplia, lo que exige respuestas más robustas por parte de los gobiernos y empresas. Según Aguilar (2021), argumenta que América Latina se encuentra sobre todo rezagada en el desarrollo de políticas nacionales de ciberseguridad, y que este déficit ha puesto en riesgo la seguridad nacional y la política exterior de los países de la región. El autor indica que, aunque algunos países han comenzado a implementar políticas y estrategias nacionales de ciberseguridad, el progreso ha sido lento y desigual. Esto es en particular preocupante cuando se compara la situación de América Latina con regiones como Europa o Asia, donde las naciones han priorizado la seguridad cibernética como un aspecto esencial de su política exterior y su defensa nacional.

La situación en América Latina refleja una falta de integración entre las políticas públicas de ciberseguridad y la infraestructura crítica del ciberespacio. De acuerdo con Pacheco (2022), esta falta de preparación y cooperación pone en riesgo la seguridad de las infraestructuras críticas, también afecta la confianza de los ciudadanos y las empresas en la capacidad de los gobiernos para proteger sus datos y servicios esenciales, lo que agrava la vulnerabilidad económica y social de la región.

En paralelo, uno de los puntos más relevantes en la investigación de ambos autores es la creciente importancia de las inversiones en ciberseguridad para las instituciones financieras y otros sectores estratégicos. Mientras que en países desarrollados estas inversiones se ven reflejadas en la mejora de la competitividad y el desempeño financiero de las empresas, en América Latina aún se percibe una reticencia a invertir en este ámbito, lo que puede comprometer la estabilidad financiera de las empresas sino también la confianza pública en los servicios gubernamentales y empresariales. Mi investigación sobre la relación entre las inversiones en ciberseguridad y el desempeño financiero refuerza esta postura, revela que las instituciones que invierten en ciberseguridad experimentan una reducción significativa de los riesgos financieros y una mejora en su rentabilidad.

En el contexto actual, donde la transformación digital avanza a un ritmo acelerado, es esencial que las políticas públicas promuevan una integración integral entre la infraestructura tecnológica y la educación en ciberseguridad. La digitalización de servicios, el aumento de la conectividad y el crecimiento de las economías basadas en la tecnología requieren que los gobiernos fortalezcan la infraestructura digital, también preparen a la población para enfrentar los desafíos del ciberespacio de manera segura. De acuerdo con Márquez (2022), el desarrollo de habilidades en ciberseguridad mejora la seguridad en línea, también fomenta un entorno más equitativo al ofrecer a las personas y empresas las herramientas necesarias para participar por completo en la economía digital. Así, la capacitación en ciberseguridad es una pieza para avanzar hacia una inclusión digital efectiva y garantizar que los beneficios de la tecnología lleguen a todos los sectores de la sociedad.

Según Campaña (2024), destaca la importancia de una cooperación internacional más estrecha, de manera especial con países que ya cuentan con marcos robustos de ciberseguridad, para mejorar la resiliencia regional. El autor sugiere que, al integrar la ciberseguridad en la estrategia nacional de seguridad, los gobiernos latinoamericanos podrían fortalecer sus capacidades para prevenir, detectar y responder a amenazas cibernéticas, reduciendo así la vulnerabilidad frente a actores cibernéticos maliciosos.

La ciberseguridad se ha convertido en un pilar fundamental para la gobernabilidad moderna, al permitir a las sociedades aprovechar de manera segura los beneficios del ciberespacio. Según Hirare (2020), el crecimiento de las Tecnologías de la Información y la Comunicación ha acelerado las relaciones sociales, pero también ha incrementado las amenazas cibernéticas que comprometen la seguridad de los datos e infraestructuras.

Aguilar (2021), destaca que América Latina se encuentra rezagada en el desarrollo de políticas nacionales de ciberseguridad, lo que ha puesto en riesgo la seguridad nacional y la política exterior de la región. Pacheco (2022), señala que esta falta de integración entre las políticas públicas y la infraestructura crítica agrava la vulnerabilidad económica y social. Los autores coinciden en que las inversiones en ciberseguridad son esenciales para mejorar el desempeño financiero y la competitividad de las instituciones, aunque en América Latina aún persiste una reticencia en este aspecto.

En ese sentido la digitalización y la creciente conectividad exigen que las políticas públicas promuevan una mayor integración de la infraestructura tecnológica con la educación en ciberseguridad. Márquez (2022), resalta que el desarrollo de habilidades en ciberseguridad es para fomentar un entorno más equitativo y garantizar la inclusión digital. Según Campaña (2024), subraya la necesidad de una cooperación internacional más estrecha, sobre todo con países que ya tienen marcos robustos de ciberseguridad, para mejorar la resiliencia regional y fortalecer las capacidades de los gobiernos latinoamericanos en la prevención y respuesta ante amenazas cibernéticas.

Conclusiones

Las instituciones financieras enfrentan una creciente amenaza de ciberataques, lo que hace que la inversión en ciberseguridad sea más que nunca. A medida que las operaciones digitales se vuelven más comunes, la protección de los datos y sistemas de información se convierte en una prioridad. Aunque estas inversiones pueden aumentar los costos operativos, resultan esenciales para mitigar riesgos y evitar pérdidas económicas considerables, lo que demuestra su importancia desde una perspectiva de seguridad, sino también desde una visión económica.

Los datos indican que las instituciones que implementan políticas de ciberseguridad adecuadas logran mejorar su rentabilidad. A través de la protección de sus activos digitales y la reducción de la probabilidad de incidentes costosos, estas entidades se resguardan contra posibles pérdidas, también optimizan sus operaciones y pueden generar mayores ingresos. De esta manera la ciberseguridad se revela como un factor que contribuye sin rodeos al desempeño financiero positivo.

Sin embargo, las pequeñas y medianas instituciones financieras enfrentan un desafío mayor, no siempre cuentan con los recursos necesarios para implementar medidas de ciberseguridad robustas. Esta brecha en la protección las deja más expuestas a riesgos cibernéticos, lo que podría afectar su estabilidad financiera y su reputación en el mercado. Este desequilibrio resalta la necesidad urgente de apoyo y recursos para fortalecer la ciberseguridad en este segmento.

La inversión en ciberseguridad debe considerarse una estrategia a largo plazo, como un gasto adicional. La protección de los activos digitales y la confianza del cliente son esenciales para garantizar la sostenibilidad y el éxito continuo de las instituciones financieras y las inversiones en ciberseguridad protegen, también fortalecen el desempeño financiero, contribuyendo a la estabilidad y crecimiento de las organizaciones en el tiempo.

Referencias

Aguilar, A. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios internacionales Santiago*, *53*(198), 169-197.

Aucancela, B. (2021). Gestión turística como herramienta de desarrollo sostenible de la microcuenca del río chimborazo, cantón riobamba. *revista De Ciencias Sociales y Humanidades*, (13), 102-116.

Brito, S., & Franklin, R. (2024). *Inteligencia artificial y sus implicancias en la transformación de los modelos de negocios convencionales de las Pymes en Lima, 2024* [Tesis de postgrado, Universidad César Vallejo].

Campaña, M. (2024). Desafíos y estrategias de ciberseguridad para pequeñas empresas. *Gestio et Productio. Revista Electrónica de Ciencias Gerenciales*, *6*(11), 18-36.

Conforme, Y., & Calle, A. (2024). Importancia de la ciberseguridad en la investigación de mercados digital. *Ciencia y Desarrollo, 27*(2).

Guerrero, M. (2020). Procedimiento de gestión de riesgos como apoyo a la toma de decisiones. *Ingenierìa Industrial*, *41*(1),

Hernández, R., Fernández, C., & Baptista, P. (1991). *Metodología de la investigación.* McGraw-Hill.

Hirare, S. (2020). Ciberseguridad. Presentación del dossier. *URVIO: Revista Latinoamericana de Estudios de Seguridad,* (20), 8-15.

LEXIS. (2024, 28 de agosto). Ecuador enfrenta aumento de ciberataques mientras la inversión en ciberseguridad crece. https://n9.cl/6rtmj

Lucio, E., & Campaña, E. (2024). Desafíos y estrategias de ciberseguridad para pequeñas empresas. *Gestio et Productio. Revista Electrónica de Ciencias Gerenciales*, *6*(11), 18-36.

Maguiña, J., & Soto, A. 2021. Estudios transversales. *Revista de la Facultad de Medicina Humana*, *21*(1), 179-185. https://doi.org/10.25176/rfmh.v21i1.3069

Márquez, J. (2022). Ciberseguridad e Internet de las Cosas. Perspectivas para esta década. *Computación y Sistemas, 26*(3), 1201-1214.

Ordoñes, P., & Quezada, C. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & comunes, revista de políticas y problemas públicos*, *2*(15), 77-97.

Pacheco, D. (2022). Seguridad en redes de comunicaciones: Perspectivas y desafíos. *Ingeniare. Revista chilena de ingeniería*, *30*(2), 215-217.

Ramos, C. (2020). Los alcances de una investigación. *Cienciamerica*, 2.

Sancho, H. (2020). Ciberseguridad. Presentación del dossier. *URVIO Revista Latinoamericana de Estudios de Seguridad*, (20), 8-15.

TeleSemana. (2024, 21 de diciembre). El costo por incidente de ciberseguridad supera los US$ 2 millones y urge medirlo como riesgo, dice informe. TeleSemana: https://n9.cl/xyt0r

Torres, F. (2015). Acerca de los enfoques cuantitativo y cualitativo en la investigación educativa cubana actual. *Atenas, 2*(34).

Declaración

Conflicto de interés
No tenemos ningún conflicto de interés que declarar.
Financiamiento
Sin ayuda financiera de partes externas a este artículo.
Nota
El artículo es original y no ha sido publicado previamente.