UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE CIENCIAS EMPRESARIALES

ESCUELA DE CONTABILIDAD

Riesgos del uso de herramientas TI en los procesos operativos, en relación con la auditoría interna de las cajas municipales

TESIS PARA OPTAR EL TÍTULO DE

CONTADOR PÚBLICO

AUTOR

Hector Nicanor Garcia Paz

ASESOR

Flor de María Beltran Portilla

https://orcid.org/0000-0002-7161-4208

Chiclayo, 2025

Riesgos del uso de herramientas TI en los procesos operativos, en relación con la auditoría interna de las cajas municipales

PRESENTADA POR

Hector Nicanor Garcia Paz

A la Facultad de Ciencias Empresariales de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de

CONTADOR PÚBLICO

APROBADA POR

Cynthia Katterine Perez Rios
PRESIDENTE

Rosita Catherine Campos Diaz
SECRETARIO

Flor de Maria Beltran Portilla
VOCAL

Dedicatoria

Esta investigación de tesis la dedico a Dios por darme la valentía para afrontar cada reto de la mejor manera y a mis padres que son mi motivación constante de que todo lo que uno se propone lo cumple por más pequeños que sean los pasos significan grandeza para uno mismo depositando su confianza y siendo mi apoyo incondicional en esta etapa universitaria velando por mi educacion y bienestar.

Agradecimientos

Esta investigación va agradecida para mi madre por darme el ejemplo y lucha constante y a mí padre por ser mi base y fuerza interior y a Dios por ser mi protector.

Riesgos del Uso de herramientas TI en los procesos operativos, en relación a la Auditoría Interna de las Cajas Municipales

INFORME DE ORIGINALIDAD

16%	15%	5%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	vlex.com.mx Fuente de Internet	3%
2	tesis.usat.edu.pe Fuente de Internet	1%
3	www.coursehero.com Fuente de Internet	1%
4	hdl.handle.net Fuente de Internet	1%
5	infosen.senado.gob.mx Fuente de Internet	1%
6	www.studocu.com Fuente de Internet	<1%
7	www.scribd.com Fuente de Internet	<1%
8	Submitted to Infile Trabajo del estudiante	<1%
9	Submitted to Universidad Católica Santo Toribio de Mogrovejo Trabajo del estudiante	<1%
10	americanae.aecid.es Fuente de Internet	<1%
11	uvadoc.uva.es Fuente de Internet	<1%

Índice

Resumen **6**

Abstract **7**

Introducción **8**

Revisión de literatura **9**

Materiales y métodos **18**

Resultados y discusión **21**

Conclusiones **36**

Recomendaciones **37**

Referencias **38**

Anexos **40**

Resumen

Actualmente, las instituciones financieras, incluidas las Cajas Municipales de Ahorro y Crédito, dependen cada vez más de la tecnología para brindar servicios eficientes y de calidad. Sin embargo, esta transformación digital también conlleva riesgos significativos, como ciberataques, fallos en la seguridad de la información, dependencia excesiva de sistemas automatizados y falta de capacitación del personal, lo que puede afectar el desarrollo normal de sus operaciones. La presente investigación tuvo como objetivo identificar los riesgos derivados del uso de (TI) en los procesos operativos de las Cajas Municipales, y analizar su relación con la labor de las auditorías internas, con el fin de comprender el nivel de adaptación tecnológica y los riesgos asociados. El estudio se llevó a cabo bajo un enfoque cualitativo, mediante entrevistas a los jefes de operaciones de una muestra seleccionada, así como la revisión documental de revistas especializadas y el reglamento de Auditoría Interna de cinco Cajas Municipales. Los resultados revelaron la presencia de múltiples riesgos tecnológicos en los procesos operativos, incluyendo malware, inyecciones SQL, ataques de tipo XSS, phishing, DDoS, configuraciones erróneas de cookies, rastreo e incompatibilidades entre sistemas. Estos hallazgos muestran una conexión directa entre los riesgos tecnológicos y la labor de la Auditoría Interna, la cual se ve limitada por la falta de estrategias sólidas de gestión de riesgos. Por ello, se destaca la necesidad de establecer medidas más robustas de protección, fortalecer los controles internos y promover la capacitación continua del personal, con miras a una gestión tecnológica más segura y eficiente.

Palabras clave: Auditoría Interna, Riesgos TI, Tecnología, Cajas Municipales de Ahorro y Crédito

Abstract

Currently, financial institutions, including Municipal Savings and Credit Unions (SCUs), increasingly rely on technology to provide efficient, high-quality services. However, this digital transformation also entails significant risks, such as cyberattacks, information security breaches, overreliance on automated systems, and lack of staff training, which can affect the normal development of their operations. This research aimed to identify the risks arising from the use of IT in the operational processes of Municipal Savings and Credit Unions (SCUs) and analyze their relationship with the work of internal audits, in order to understand the level of technological adaptation and associated risks. The study was conducted using a qualitative approach, through interviews with the heads of operations of a selected sample, as well as a documentary review of specialized journals and the Internal Audit Regulations of five Municipal Savings and Credit Unions (SCUs). The results revealed the presence of multiple technological risks in operational processes, including malware, SQL injections, XSS attacks, phishing, DDoS, cookie misconfigurations, tracking, and system incompatibilities. These findings show a direct connection between technological risks and the work of Internal Audit, which is limited by the lack of solid risk management strategies. Therefore, the need to establish more robust protection measures, strengthen internal controls, and promote ongoing staff training is highlighted, with a view to more secure and efficient technological management.

Keywords: Internal Audit, IT Risks, Technology, Municipal Savings and Credit Banks.

Introducción

En un entorno financiero cada vez más digitalizado, las Cajas Municipales de Ahorro y Crédito en Perú han integrado las tecnologías de la información (TI) como un componente esencial para mejorar la eficiencia operativa y la calidad del servicio mejorando su desarrollo tecnológico y adaptación a los nuevos cambios. De la misma forma se enfrentan al desafío de poder gestionar, identificar y mitigar los riesgos asociados al uso intensivo de TI en sus procesos operativos. Como lo describió Maurer y Arthur (2021) advierten que el sistema financiero global enfrenta una vulnerabilidad creciente, teniendo en cuenta el progreso acelerado de la conversión digital, que se ve facilitada por la innovación, la competencia y el impacto pandémico a largo plazo. Aunque muchas amenazas actuales tienen objetivos financieros, los ataques cibernéticos están aumentando, lo que tiene como objetivo causar roturas o lesiones deliberadas. Del mismo modo, con el conocimiento técnico, el atacante logra familiarizarse con las redes y operaciones financieras, facilitando ataques más graves contra el futuro o comercializar esta información con un tercero. (p.3). En efecto, la tecnología ha facilitado la automatización del proceso y mejorando la precisión y la velocidad de las transacciones, pero también está sujeta a riesgos importantes para las cajas municipales, como los ataques cibernéticos y las vulnerabilidades.

Es por ello, que la problemática central de esta investigación radica en identificar los riesgos en la utilización herramientas TI, que, aunque han optimizado la eficiencia, han introducido nuevos riesgos que pueden comprometer la integridad, confiabilidad de los procesos financieros y efectividad de la auditoría interna que podría verse afectada si los riesgos tecnológicos no se gestionan adecuadamente. Ante ello, se deprende la pregunta que guía esta investigación **¿Cuáles son los riesgos asociados al uso de herramientas TI en los procesos operativos y su relación con la auditoría interna de las Cajas Municipales?**

En este contexto, la presente investigación se justifica en comprender de manera profunda la gestión de los riesgos inherentes a la adopción de herramientas tecnológicas en el sector financiero, particularmente en lo que respecta en sus operaciones cotidianas. Asimismo, busca evaluar la relación de la auditoría interna en su rol de supervisión y control dentro de estas instituciones financieras locales, considerando los desafíos que implica la transformación digital en sus procesos operativos.

Esta investigación desarrolló como objetivo general el análisis de los riesgos asociados al uso de herramientas tecnológicas en los procesos operativos y su relación con la auditoría interna. A partir de este, se desprendieron objetivos específicos donde se identificó los tipos de sistemas y/o herramientas tecnológicas empleadas en los procesos operativos de las Cajas

Municipales de Ahorro y Crédito; analizar los reglamentos que rigen el proceso de auditoría interna en el control de riesgos relacionados con el uso de dichas tecnologías; e identificar los tipos de riesgos generados, con el propósito de formular recomendaciones que fortalezcan tanto la gestión de riesgos como la efectividad de la auditoría interna en estas instituciones.

Revisión de literatura

En el estudio plasmado por la (Secretaría General de la Organización de Estados Americanos [OEA], 2020), tuvo como objetivo proporcionar información verdadera sobre la situación de seguridad cibernética en el sector bancario en América Latina y el Caribe. El estudio fue estructurado en dos enfoques: el primero en ser para instituciones financieras, que cubrieron el total de 191 bancos en la región; Y el otro está orientado hacia los usuarios del sistema bancario, teniendo en cuenta los extractos de los clientes 722. Para obtener datos, OAS desarrolló herramientas especiales para cada grupo de destinatarios en colaboración con el banner. Como resultado del análisis, el 72 % de la mayor administración de las unidades bancarias recibió indicadores periódicos e informes de gestión de riesgos relacionados con la seguridad digital. Sin embargo, el 60 % de los encuestados dijo que el mayor liderazgo de invertir en soluciones de seguridad digital causa dificultades moderadas, a pesar de la importancia de estas inversiones, especialmente con respecto a la prevención.

Chengyou et. al (2025) en su investigación plantea que la tecnología financiera ha impulsado tanto la diversificación de las operaciones de los bancos comerciales como el crecimiento de la competencia del sector, lo que plantea desafíos para su gestión de riesgos. Este documento selecciona datos de panel de 154 bancos comerciales entre 2011 y 2023 y construye un indicador de desarrollo de la tecnología financiera basado en alianzas estratégicas con empresas externas de tecnología financiera para examinar su impacto en la toma de riesgos de los bancos. Los hallazgos son los siguientes: (1) La tecnología financiera aumenta significativamente los niveles de toma de riesgos de los bancos comerciales, y el resultado se mantiene sólido tras diversas pruebas de sensibilidad. (2) El impacto de la tecnología financiera en la toma de riesgos es heterogéneo. Tiene un efecto más sustancial en los bancos más pequeños que en los más grandes, y es más pronunciado en regiones con menores niveles de comercialización. (3) La tecnología financiera afecta los de activos y pasivos de los bancos comerciales mediante efectos de desplazamiento del mercado y proporciona apoyo tecnológico a la innovación mediante efectos de contagio tecnológico, lo que incrementa significativamente la asunción de riesgos. Por lo tanto, esta investigación ofrece una mayor comprensión de la relación intrínseca entre la tecnología financiera y asunción de riesgos de los bancos comerciales.

Bashaija, (2022). Este estudio se realizó para probar el impacto del control interno en las empresas no financieras, que se refiere al intercambio de Vietnam. Los datos se recopilaron mediante la inspección de 506 cuestionarios realizados por empresas no financieras mencionadas en el mercado de valores. Se utilizaron métodos de investigación cuantitativos para evaluar el impacto del control de rendimiento interno. Los resultados muestran que los controles internos que contienen cinco componentes tienen un impacto significativo en los resultados financieros y los componentes de control, basado en verificación de riesgos, actividades de control y comunicación donde tienen un impacto positivo directo en el rendimiento no financiero.

Alvares et. al, (2024) establecen que la infraestructura digital está cada vez más interconectada, tanto dentro de los centros de datos como entre ellos. Esto se debe a la virtualización, la nube y las estrategias híbridas en TI, así como a los avances en la monitorización remota, telemetría, sensores y gestión inteligente de instalaciones. Estos avances hacen que los centros de datos sean más complejos y aumentan la variedad de amenazas cibernéticas. A pesar de que la industria sigue los estándares de seguridad para mejorar la resiliencia digital, los ciberataques se vuelven más sofisticados y a menudo superan las medidas defensivas, como las actualizaciones de software. Por esta razón, el Instituto de Tiempo de Actividad, propietario de la empresa española Leet Seguridad, llevó a cabo una investigación ilustrativa titulada 'Encuesta de seguridad del centro de datos', en la que consultó a más de 300 profesionales que trabajan en este entorno, ya sea como propietarios o como clientes corporativos, sobre sus principales preocupaciones relacionadas con la ciberseguridad y sus estrategias para mitigar y responder a los riesgos digitales. Destaca que el 93% de los clientes empresariales de centros de datos solicitan activamente "más" información sobre la postura de ciberseguridad y cómo se han reforzado aspectos específicos.

Zheng et. al (2025) en su documento examina el impacto de la experiencia en TI del comité de auditoría en la divulgación de riesgos de ciberseguridad corporativa, en un contexto de creciente complejidad y frecuencia de ciberataques. Observamos que la experiencia en TI de los comités de auditoría mejora significativamente la divulgación de riesgos de ciberseguridad. Este efecto es más pronunciado en empresas con informes financieros menos transparentes, con una gobernanza más débil y con menor asimetría de información. Además, el nivel de adopción de inteligencia artificial, la calidad de los controles internos y la calidad de la divulgación de información son posibles factores de influencia. El enfoque de este trabajo sobre la divulgación de riesgos de ciberseguridad se centra en la enumeración de las distintas palabras clave de riesgo de ciberseguridad presentes en los informes anuales de las empresas chinas que cotizan en

bolsa. Los resultados subrayan una variación significativa en la divulgación del riesgo de ciberseguridad entre las empresas que cotizan en bolsa en sus informes anuales. El valor promedio de AC_IT, una métrica que mide la experiencia en TI del comité de auditoría, es de 0.173, lo que denota que solo el 17.3% de los miembros del comité de auditoría en las empresas de la muestra poseen experiencia laboral y de aprendizaje relacionada con TI

Lizárraga et. al (2022) en su estudio desarrollo el impacto de la auditoría en la tecnología de la información (TI) se probó en instituciones públicas y privadas entre 2017 y 2022, utilizando bases de datos como Dialnet Plus, Daaj, Scielo, Core y Academic Google. Los resultados revelan que la revisión le permite identificar riesgos, fortalecer la seguridad de la información y mejorar los procesos tecnológicos, lo que significa una mayor eficiencia. También contribuyen al fortalecimiento de la gestión de riesgos al identificar amenazas y vulnerabilidades tempranas, lo que afecta positivamente la productividad y reduce el tiempo improductivo. Por otro lado, el uso de auditorías tecnológicas crea una ventaja competitiva al aumentar la confiabilidad y confianza de los aliados estratégicos y estratégicos en la seguridad y la confiabilidad del sistema. En resumen, el estudio concluye que una revisión es una herramienta básica para garantizar la sostenibilidad y la eficiencia de las empresas en el entorno digital moderno.

Zarate et. al (2022) acuerda que su investigación se enfoca en comprender el funcionamiento de las instituciones financieras a nivel mundial, así como las amenazas y desafíos que enfrentan diariamente. Se busca analizar el nivel de seguridad informática de estas instituciones y cómo reaccionan ante las amenazas mediante estadísticas y métodos de análisis. Se investigará cómo el enfoque de Zero Trust puede proporcionar una capa adicional de seguridad a los sistemas de las entidades financieras, destacando sus diferencias con los métodos de seguridad actuales y explorando su implementación teniendo en cuenta sus puntos fuertes y débiles. La metodología adoptada es cuali-cuantitativa, combinando métodos teóricos y empíricos para obtener datos en cada etapa de la investigación. Se realizarán estudios exploratorios, descriptivos y explicativos. La justificación del estudio y la determinación del problema se abordaron en la primera etapa, la cual fue exploratoria-descriptiva. Los resultados obtenidos hasta ahora incluyen una evaluación del estado de las entidades financieras, así como la identificación de problemas y ataques sufridos. Se pretende demostrar cómo el enfoque de Zero Trust puede mejorar la seguridad en estas instituciones.

López (2021) recomendó el estudio de los riesgos asociados al uso de la tecnología de la información que el auditor debe tener en cuenta durante la fase de planificación de la Comisión. El autor comienza con el hecho de que está asociado con un método de auditoría basado en el

riesgo al introducir el concepto de cibercríka y realizar este tipo de factores relacionados con el riesgo, lo que enfatiza su importancia en el trabajo del auditor. En el estudio, se utilizó un análisis bibliográfico como un método principal de recopilación de datos para clasificar y describir varios factores de riesgo. Entre los resultados más importantes, se ha identificado que el entorno de TI no siempre refleja un riesgo mayor que otras áreas, aunque los elementos de auditoría más críticos están relacionados con la seguridad de la información, el control interno y las consecuencias legales.

Encalada (2023) centró su estudio en un análisis estratégico de roles de las tecnologías de información y comunicación en la gestión del conocimiento relacionado con el capital intelectual, así como su función preventiva contra los ataques cibernéticos utilizando forensicismo. El enfoque metodológico fue el estudio, la película descriptiva y documental, enfatizando la seguridad cibernética, la prevención de fraude y la administración de conocimiento organizacional. Los resultados, utilizando representaciones gráficas y esquemáticas, reflejan que la articulación entre la auditoría forense, la seguridad cibernética y la gestión del conocimiento de la organización permite crear mecanismos efectivos para prevenir y detectar manualidades de computadora, corrupción y fraude. Además, esta integración garantiza la disponibilidad de evidencia de procesos legales y fortalece los activos de las computadoras, lo que facilita las decisiones estratégicas en diferentes áreas de la organización.

López et. al (2023) analiza Análisis de digitalización de procesos de auditoría interna y su impacto en la gestión de riesgos tecnológicos en las unidades financieras. El estudio utilizó un enfoque mixto que combinó el estudio de documentos regulatorios, investigaciones dirigidas a auditores y entrevistas con expertos en seguridad de la información. Los resultados mostraron que la inclusión de herramientas digitales ha contribuido significativamente a la mejora de las auditorías internas y la precisión, lo que permite una mejor identificación de operaciones y riesgos de seguridad cibernética. Sin embargo, también se identificaron restricciones, como la falta de regulaciones y los cambios organizacionales en la resistencia. El estudio enfatiza la necesidad de una estrategia integral que incluya capacitación continua, adaptación a los estándares de seguridad cibernética y la adopción de un marco como COBIT o ISO 27001 para reducir los riesgos obtenidos de la automatización. En resumen, se concluye que una auditoría interna digitalizada, proactiva es la clave para mejorar la seguridad regulatoria y el cumplimiento de las instituciones financieras.

Bases Teóricas Científicas

Riesgo

Ríos et al. (2022), en su obra Análisis de riesgo, explican que el riesgo constituye un elemento propio de las sociedades contemporáneas, ya que se relaciona con posibles amenazas que afectan diversos sectores como el financiero, político y tecnológico. Los autores subrayan la necesidad de aplicar metodologías rigurosas que permitan analizar y gestionar dichos riesgos, con la finalidad de anticipar y reducir sus efectos adversos (p. 12). Por otra parte, la Norma International Organization for Standardization 31000 (ISO, 2018) define el riesgo como el efecto de la incertidumbre sobre los objetivos enfatizando la relación entre la incertidumbre y el cumplimiento de los objetivos organizacionales.

En la misma línea, Castañeda (2016) define el riesgo como el resultante de la relación entre factores tanto internos como externos, los cuales pueden favorecer la aparición de eventos desfavorables que interfieren con el crecimiento normal de un proceso. Este concepto abarca componentes como la amenaza, la vulnerabilidad y el grado de exposición a dichos factores. (p. 4).

Castañeda (2016) establece que el ámbito del riesgo existe varias clasificaciones.

Riesgos Internos

a) Estratégicos: Son aquellos que se originan en los niveles más altos de toma de decisiones dentro de la organización. Involucran aspectos como el liderazgo directivo, la imagen institucional y la interacción con los diferentes grupos de interés.
b) Operacionales: Se relacionan con las funciones y tareas ejecutadas por el personal dentro de la entidad. Estos riesgos se consideran parte de la gestión interna e incluyen, por ejemplo, el control y manejo de las áreas contables.

Riesgos Externos

a) Comerciales: Incluyen todos los elementos que pueden afectar la cadena de suministros, desde las actividades logísticas como la adquisición externa de insumos, hasta la producción y la distribución. Estas últimas pueden implicar tanto factores internos como externos a la organización.
b) Mercadeo y ventas: Se vinculan tanto con las acciones que realiza la empresa en su entorno como con los factores externos que influyen en la implementación de estrategias comerciales, la obtención de resultados previstos, la fidelización de los clientes y la calidad en el servicio ofrecido.

c) Financieros: Se refieren a los factores que impactan negativamente en la rentabilidad esperada de la organización, ya sea de forma parcial o total. Aquí se incluyen riesgos asociados al sistema financiero, la disponibilidad de crédito y la liquidez.
d) Económicos: Son riesgos derivados del contexto macroeconómico, los cuales están influenciados por decisiones tomadas desde los niveles superiores del gobierno y por organismos internacionales que regulan el comportamiento económico global. (p.15)

Riesgo Cibernético

Según el Consejo de Investigación de Instituciones Financieras de Estados Unidos (FFIE, 2020), un ciberataque consiste en una acción destinada a causar daño, interrumpir o acceder sin autorización a sistemas informáticos, computadoras o redes de comunicación electrónica. Este tipo de ataque, realizado a través del ciberespacio, tiene como objetivo afectar o controlar de manera maliciosa una infraestructura tecnológica, comprometer la integridad de los datos o sustraer información sensible. (p.2)

Tipos de Ciberataques

De acuerdo con el glosario de términos utilizado por el National Institute of Standards and Technology (NIST, 2021), se tienen los siguientes conceptos:

Malware: la expresión simplificada es la designación del "código malicioso" y consiste en este software destinado a realizar un proceso no autorizado que afectará negativamente la confidencialidad, la integridad o la disponibilidad del sistema de información. En esta categoría, existen principalmente los siguientes tipos: Virus: una sección oculta y un software de computadora repetido que se propaga para infectar (es decir, insertarse en otro programa y convertirse en parte de él). El virus no puede correr solo; Necesita su programa de invitados para activarlo.

Spyware: software instalado en un sistema de información secreto o secreto para recopilar información sobre individuos u organizaciones sin conocimiento. Anuncios: software que reproduce o elimina automáticamente material publicitario en su computadora después de instalar el software o cuando usa la aplicación. El programa malicioso está diseñado para mostrar anuncios no deseados en la computadora de la víctima sin su permiso, las ventanas pop -up o los anuncios son incontrolables y tienden a ser irregulares, generalmente aparece muchas veces en la pantalla y es aburrido para cerrarlos. (p.10)

Rootkit: un conjunto de herramientas utilizadas por el atacante después del acceso al nivel de raíz en el host para ocultar el host de actividad del atacante y permitirle mantener el acceso a nivel de raíz al host a través de medios secretos. En otras palabras, le da a su computadora a

Pirates acceso a una computadora o red o controla la red. Son difíciles de determinar porque se activan incluso antes de que comience el sistema operativo del sistema..

Trojan Horseun: programa de computadora que parece tener una característica útil pero que también tiene una función oculta y potencialmente maliciosa que evita los mecanismos de seguridad y, a veces, utiliza un dispositivo de permiso legítimo que llama al programa.

Worm: es una expresión simplificada para denotar que consiste en un programa de computadora que se puede hacer de forma independiente, puede distribuir una versión completa de otros hosts o redes y puede consumir recursos en una computadora destructiva. En otras palabras, también es un código malicioso que se copia y se extiende a otras computadoras, sistema o red.

Ransomware: este es un virus que evita que el usuario acceda a archivos o programas, y eliminarlos debe pagar "rescate" utilizando ciertos métodos de pago en línea. Una vez que se paga la cantidad, el usuario puede reanudar utilizando su sistema.

Keylogger: un programa diseñado para determinar qué teclas se presionan en el teclado de la computadora que se utiliza para obtener contraseñas o teclas de cifrado.

Botnet: esta es una red de dispositivos infectados con malware como el virus. Los atacantes pueden controlar la red de robots como un grupo sin conocimiento del propietario con el objetivo de aumentar el tamaño de sus ataques. A menudo, la red de robots se usa para superar el ataque del Servicio Distribuido del Sistema (DDoS).

Phishing: una forma de tratar de obtener datos confidenciales, como cuentas bancarias, números, utilizando una aplicación fraudulenta en E -Past o en el sitio donde se introduce el autor a través de un negocio legítimo o una persona con reputación. (p.11)

Man-in-the-middle attack (MitM): Un ataque MitM s cuando el atacante cambia la comunicación entre dos usuarios que cruzan a ambas víctimas para manipular y acceder a sus datos. Los usuarios no saben que realmente se comunican con el atacante en lugar de ellos.

Distributed denial-of-service attack (DDoS): Este tipo de ataque se basa en saturar sistemas, servidores o redes con una gran cantidad de tráfico, lo cual consume sus recursos y ancho de banda, impidiendo que respondan a solicitudes legítimas. Cuando este ataque se lleva a cabo desde varios dispositivos comprometidos simultáneamente, se le denomina ataque distribuido de denegación de servicio.

SQL injection: Este ataque ocurre cuando un cibercriminal introduce comandos maliciosos en aplicaciones que utilizan SQL (Lenguaje de Consulta Estructurado). Este tipo de ataque solo es efectivo si existe una falla de seguridad en el software, y puede permitir al atacante acceder o cambiar información en la base de datos.

Zero-day attack: Se refiere a la explotación de una vulnerabilidad desconocida en hardware o software. Estas fallas pueden ser aprovechadas por delincuentes informáticos antes de que los desarrolladores las detecten y desarrollen un parche. El riesgo aumenta si se utiliza software desactualizado que aún no ha sido corregido. (p.12)

Auditoría Interna

La definición vigente dada por The Institute of Internal Auditors de EEUU (IIA, 2004) también adoptada por el Instituto de Auditores Internos de Argentina (IAIA), como entidad afiliada nos habla que la auditoría interna se entiende como una actividad imparcial e independiente que brinda servicios de aseguramiento y asesoramiento. Su finalidad es aportar valor y optimizar el funcionamiento de la organización. Para ello, aplica un enfoque metódico y estructurado que permite analizar y fortalecer la eficiencia en los procesos relacionados con la gestión de riesgos, el control interno y el gobierno corporativo. (p.8)

Tecnología de la Información

La Real Academia Española (RAE, 2006) entiende la tecnología como el conjunto de conocimientos teóricos y prácticos que permiten aplicar la ciencia de manera útil. En esa línea, el Centro de Innovación del BBVA (2015) define a las empresas fintech como aquellas que brindan servicios financieros utilizando tecnología, respondiendo así a las necesidades emergentes del mercado. Por su parte, Polo (2016) detalla que estas empresas operan en diversas áreas del sector financiero, ya sea mediante la incorporación de procesos innovadores o el desarrollo de productos nuevos, incluyendo soluciones en ciberseguridad y mecanismos para obtener información valiosa a través de herramientas tecnológicas.

Tipos de TI utilizadas e en el Sistema Financiero

Según Mooverang, (2016) se establecen la clasificación de los tipos de tecnología en el sector financiero:

Medios de pago: Este es uno de los temas clave para el futuro inmediato en el entorno financiero, involucrando a bancos, empresas Fintech, grandes tecnológicas (GAFAs) y compañías de telecomunicaciones. La tendencia apunta hacia el uso creciente de monedas digitales en lugar del dinero físico.

Bitcoin y criptomonedas: Existen empresas enfocadas en el uso y gestión de monedas virtuales como el bitcoin, que permiten realizar transacciones en línea sin necesidad de intermediarios. Estas monedas son descentralizadas, no están controladas por ningún gobierno y pueden convertirse fácilmente en otras divisas.

Herramientas de inversión: Son plataformas, generalmente digitales, que ofrecen asesoramiento automático en inversiones. Utilizan algoritmos para recomendar estrategias, activos y condiciones de inversión personalizadas, todo de forma online.

Préstamos: Algunas Fintech se especializan en ofrecer créditos en línea de forma rápida, sencilla y segura. Aunque operan como los bancos tradicionales, sus tasas de interés suelen ser más elevadas.

Agregadores financieros: Este modelo emergente se centra en ayudar a los usuarios a gestionar sus finanzas personales. Ofrecen servicios como organización de cuentas, control de gastos, elaboración de presupuestos y recomendaciones para el ahorro.

Divisas: Se refiere a plataformas que realizan cambios de moneda extranjera con tasas más competitivas que las ofrecidas por los bancos convencionales.

Financiación: Este rubro abarca distintas iniciativas destinadas a otorgar fondos a diversos sectores. Un ejemplo es el crowdfunding, que permite a las personas aportar dinero a proyectos específicos a través de plataformas digitales, generalmente a cambio de beneficios no monetarios. (p.32)

Caja Municipal de Ahorro y Crédito

De acuerdo con lo establecido en el artículo 282 de la Ley N.º 26702, que regula el Sistema Financiero, el de Seguros y la estructura de la Superintendencia de Banca, Seguros y AFP, las entidades financieras especializadas se clasifican de la siguiente manera:

Caja Rural de Ahorro y Crédito es una institución que recibe depósitos del público y cuya función principal es otorgar financiamiento, principalmente a micro, pequeñas y medianas empresas ubicadas en zonas rurales.

Caja Municipal de Ahorro y Crédito también capta fondos del público, y su actividad se centra en brindar financiamiento, orientándose preferentemente a satisfacer las necesidades de las pequeñas y microempresas.

Caja Municipal de Crédito Popular se enfoca en conceder créditos con garantía prendaria al público en general. Adicionalmente, está autorizada a realizar operaciones tanto de captación como de colocación de recursos con los concejos provinciales y distritales, así como con las entidades municipales bajo su dependencia, a quienes también puede ofrecer servicios bancarios.

Empresa de Desarrollo de la Pequeña y Microempresa (EDPYME) se especializa en proporcionar financiamiento principalmente dirigido a emprendedores y empresarios pertenecientes al segmento de la pequeña y microempresa.

Materiales y métodos

La presente investigación adopta un enfoque cualitativo donde se identificó y analizo los riesgos derivados del uso de herramientas tecnológicas en los procesos operativos de las Cajas Municipales y su relación con las auditorías internas. Se desarrollo un estudio descriptivo y de tipo aplicado, que busca ofrecer una visión integral del problema a través de la identificación de sistemas tecnológicos, el análisis normativo del reglamento de auditoría interna y la detección de riesgos específicos que están sujetas las CMAC. Quecedo y Castaño (2002), la investigación cualitativa se caracteriza por la generación de datos con un enfoque descriptivo, como pueden ser expresiones verbales —ya sean orales o escritas— y conductas observables. Por su parte, Ortega (2024) señala que la investigación aplicada tiene como propósito principal resolver problemas concretos y optimizar la eficiencia de procesos y tecnologías en diversos ámbitos. En esa misma línea, Hernández et al. (2014) afirman que estudios descriptivos buscan detallar y precisar las cualidades, atributos o perfiles de individuos, grupos sociales, comunidades, objetos, procesos u otros fenómenos sometidos a análisis.

Se desarrollo un diseño de investigación no experimental, basado en la observación sin manipulación de variables. Se aplicaron entrevistas con preguntas cerradas dirigidas a los jefes de operaciones y una revisión documental del reglamento de Auditoría Interna. La población estuvo conformada por 12 Cajas Municipales de Chiclayo, con una muestra no probabilística de 5 entidades seleccionadas según el uso de herramientas tecnológicas y la experiencia del personal operativo.

Los procedimientos incluyeron entrevistas a los jefes de Operaciones de las 5 CMAC para identificar herramientas tecnológicas en uso, así como un análisis detallado de los requisitos normativos de auditoría. Los datos recolectados fueron organizados y clasificados con software de gestión, permitiendo una mejor comprensión de la relación entre tecnología y riesgos operativos. Se respetó la confidencialidad de las instituciones y participantes, utilizando los resultados únicamente con fines académicos, conforme a principios éticos de investigación.

Operacionalización de Variables

Variables	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Instrumentos
Auditoría Interna	Según Blanco (2019), la auditoría interna se define como una función imparcial que proporciona tanto aseguramiento como asesoramiento, con el propósito de contribuir al fortalecimiento del valor y progreso continuo de los procesos dentro de una organización.	Evaluación periódica y sistemática de las operaciones, controles internos y sistemas de una organización	Normativa vigente	Numero de violaciones de políticas internas detectadas Numero de cumplimiento de normativas en su proceso de auditoría interna	Entrevista – Revisión Documental
			Eficacia de los controles Internos	Número de deficiencias de control identificadas. Tiempo promedio para la corrección de deficiencias	
			gestión de Riesgos	Número de riesgos identificados y evaluados Proporción de riesgos mitigados vs. riesgos identificados.	
Herramientas Tecnológicas	(KPMG (2019) consiste en convertir datos desde un soporte físico a uno digital, lo que permite que dicha información sea más accesible, flexible y fácil de gestionar.	Se entiende como un proceso de ajuste integral de transformación de procesos y del propio modelo de negocio, con el fin de responder a las nuevas demandas y a los cambios impulsados por la innovación tecnológica.	Big Data	Desarrollo de productos personalizados para sus clientes % de información de su cliente	Entrevista - Revisión Documental
			Blockchain	Permite a los bancos procesar los pagos y distintas transacciones de una forma mucho más rápida Reduce el nivel de costes	
			Internet of things,	la mejora de la experiencia del consumidor Nuevos canales de distribución y nuevos métodos	
			API´s	Facilidad de pagos online Intercambiar información entre plataformas	
			Cloud Computing	Ampliar el ámbito de actividad y prestar servicios Guardar grandes cantidades de información en un medio físico,	
Riesgos	Castañeda (2016) el riesgo surge de la interacción entre elementos internos y externos. Este riesgo se compone principalmente de amenazas, vulnerabilidades y el nivel de exposición frente a dichos factores (p. 4).	Comprende los tipos de riesgos como los operativos financieros y Tecnológicos o cibernéticos	Riesgos Operativos	Transferencias a cuentas Entrega de tarjetas o duplicados Utilización de la Información	Entrevista - Revisión Documental
			Riesgos Financieros	Mercado Financiero Crédito Liquidez	
			Riesgos Tecnológicos	Craker Malware Phishing Spam	

Problema Principal	Objetivo Principal	Variables			
		Variables		**Dimensiones**	**Indicadores**
¿¿Cuáles son los riesgos asociados al uso de herramientas TI en los procesos operativos y su relación con la auditoría interna de las Cajas Municipales?	Analizar los riesgos asociados al uso de herramientas tecnológicas en los procesos operativos, con relación a la auditoría interna de las Cajas Municipales.	Auditoría Interna		Normativa vigente	Numero de violaciones de políticas internas detectadas
					Numero de cumplimiento de normativas en su proceso de auditoría interna
				Eficacia de los controles Internos	Número de deficiencias de control identificadas.
					Tiempo promedio para la corrección de deficiencias
				Gestión de Riesgos	Número de riesgos identificados y evaluados
					Proporción de riesgos mitigados vs. riesgos identificados.
	Objetivos Específicos	**Población**			
	1. Identificar que tipos de sistemas o herramientas tecnológicas utilizadas en los procesos operativos de las Cajas Municipales.	12 cajas Municipales de Ahorro SBS	Herramientas Tecnológicas	Big Data	Desarrollo de productos personalizados para sus clientes
					Calidad de la información de su cliente
				Blockchain	Permite a los bancos procesar los pagos y distintas transacciones de una forma mucho más rápida
					Reduce el nivel de costes
		Muestra		Internet of things,	la mejora de la experiencia del consumidor
		Las 5 cajas Municipales			Nuevos canales de distribución y nuevos métodos de pago
				API´s	Facilidad de pagos online
					Intercambiar información entre plataformas
	2. Analizar el reglamento del proceso de Auditoría interna en el control de riesgo del uso de herramientas tecnológicas en los procesos operativos de las Cajas Municipales			Cloud Computing	Ampliar el ámbito de actividad y prestar servicios
					Guardar grandes cantidades de información en un medio físico,
			Riesgos	Riesgos Operativos	Transferencias a cuentas
		Técnica			Entrega de tarjetas o duplicados
Tipo		Entrevista -Análisis Documental			Utilización indebida de la Información
Aplicada				Riesgos Financieros	Mercado Financiero
Enfoque					crédito
Cualitativo	3. Identificar los tipos de riesgos generados por el uso de herramientas tecnológicas en los procesos operativos y su relación en la Auditoria Interna de las Cajas Municipales.	**Instrumento**			Liquidez
Nivel		Ficha de Análisis Documental -Ficha de Análisis de entrevista		Riesgos Tecnológicos	Cracker
Descriptivo					Malware
Diseño					Phishing
No experimental					Spam

Resultados y discusión

Identificar los tipos de sistemas o herramientas tecnológicas utilizadas en los procesos operativos de las Cajas Municipales

Las Cajas Municipales de Ahorro y Crédito son entidades financieras no bancarias orientadas a facilitar el acceso al crédito, especialmente para comerciantes, microempresarios y personas que no acceden fácilmente a la banca tradicional. Combinan sostenibilidad financiera con objetivos sociales, extendiendo sus servicios a sectores menos atendidos. Además, implementan medidas de seguridad para gestionar riesgos crediticios, operativos y de seguridad. Considerando una muestra de cinco CMAC —Cusco, Huancayo, Trujillo, Lima Metropolitana y Arequipa— se observa que, aunque cada entidad opera bajo su propia normativa interna y estrategias específicas para fortalecer su presencia en el mercado, comparten estructuras y funciones esenciales debido a la naturaleza de sus actividades financieras. Por consiguiente, se detalla una breve descripción de las principales Cajas analizadas

Caja Cusco cuenta con una sólida presencia en la región sur del país, destacándose por su impulso al desarrollo de microempresas y su compromiso con la inclusión financiera. Ha implementado estrategias tecnológicas orientadas a facilitar la bancarización en zonas rurales.

Caja Huancayo, una de las CMAC más grandes y reconocidas a nivel nacional, combina la expansión de sus servicios financieros con la innovación tecnológica, utilizando plataformas digitales para atender a clientes incluso en zonas alejadas.

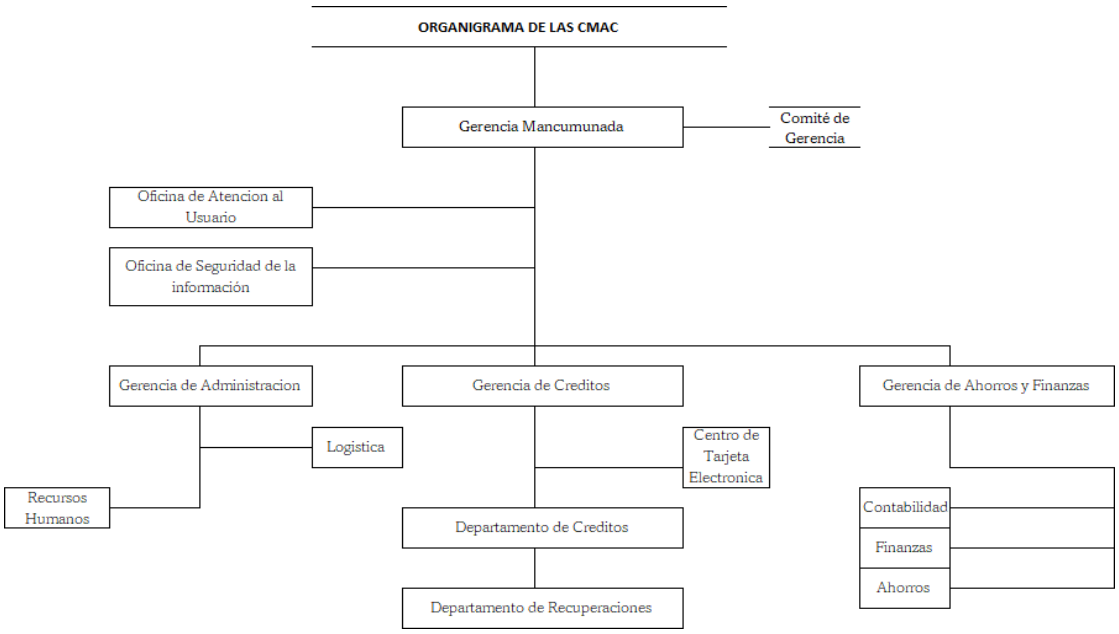
Caja Trujillo, ubicada en el norte del país, ha enfocado su gestión en atender a la pequeña y microempresa, ofreciendo créditos accesibles y productos financieros adaptados a las necesidades de sus clientes. Su apuesta por la expansión tecnológica ha fortalecido sus servicios de ahorro y crédito.

Caja Lima Metropolitana, situada en la capital, ofrece una amplia gama de servicios financieros a microempresarios urbanos. Su fuerte orientación hacia la digitalización le permite atender a un volumen elevado de clientes en un mercado altamente competitivo.

Caja Arequipa, reconocida como pionera en la adopción de tecnologías avanzadas, ha consolidado una base sólida de clientes en el sur y otras regiones del país. Su perspectiva en la gestión de riesgos y el fortalecimiento en canales electrónicos la posiciona como una de las CMAC más innovadoras.

Figura 1

Organigrama de los Procesos Operativos de la Cajas Municipales de Ahorro y Crédito



Nota: Recopilación de las 5 estructuras de Organigrama de las CMAC

La Oficina de Atención al Usuario actúa como el enlace principal entre la entidad y sus clientes, encargándose de atender consultas, solicitudes y reclamos de manera ágil y eficaz. Para ello, emplea sistemas de gestión de relaciones con el cliente (CRM), que permiten optimizar la comunicación. El desempeño de esta área resulta fundamental para fortalecer la satisfacción del cliente y promover su fidelización.

Departamento de Seguridad de la Información: Responsable de garantizar la seguridad de datos y la continuidad operativa. Utiliza herramientas, sistemas de monitoreo de seguridad (SIEM) y protocolos de cifrado. Este departamento juega un papel vital en la gestión de riesgos tecnológicos, protegiendo tanto a la institución como a sus clientes frente a amenazas cibernéticas.

Área de Logística: Encargada de la gestión de inventarios y activos físicos, asegurando que los recursos estén disponibles para soportar las operaciones diarias. Las CMAC utilizan sistemas de gestión de inventarios (ERP) para optimizar el control de sus activos, desde equipos tecnológicos hasta infraestructura. Departamento de Recursos Humano: Este departamento se enfoca en la captación y desarrollo de talento. Implementa herramientas tecnológicas para la gestión de procesos de reclutamiento y la capacitación continua, asegurando que el personal esté alineado con los objetivos estratégicos de la CMAC.

Área de Créditos: Considerado el núcleo de la actividad de las CMAC. Su misión es evaluar, otorgar y gestionar créditos, utilizando sistemas de calificación crediticia y análisis de riesgo. Esto permite a las CMAC ofrecer productos financieros adaptados a las necesidades de sus clientes, maximizando la rentabilidad. Departamento de Recuperaciones: Se encarga de la gestión de cuentas en mora, implementando estrategias para recuperar los créditos otorgados. Utiliza sistemas de gestión de cobranzas que automatizan los recordatorios de pago y facilitan la negociación con clientes para evitar pérdidas definitivas.

Área de Canales Electrónicos: Gestiona la emisión de tarjetas electrónicas y soporta plataformas digitales como aplicaciones móviles y banca por internet. Esto facilita transacciones seguras y eficientes, promoviendo la bancarización digital. Áreas de Ahorros, Contabilidad y Finanzas: Estas áreas operan de manera interrelacionada. Ahorros: Promueve la captación de depósitos. Contabilidad: Garantizar el registro correcto de todas las transacciones. Finanzas: Administra los recursos económicos, realizando proyecciones financieras y asegurando la sostenibilidad de la CMAC-Mediante la entrevista aplicada a los jefes de operaciones, con el fin de recolectar información y responder a los objetivos planteados en esta investigación, se obtuvo información relevante sobre cada área operativa que por consiguiente se explica a continuación.

Tabla 1

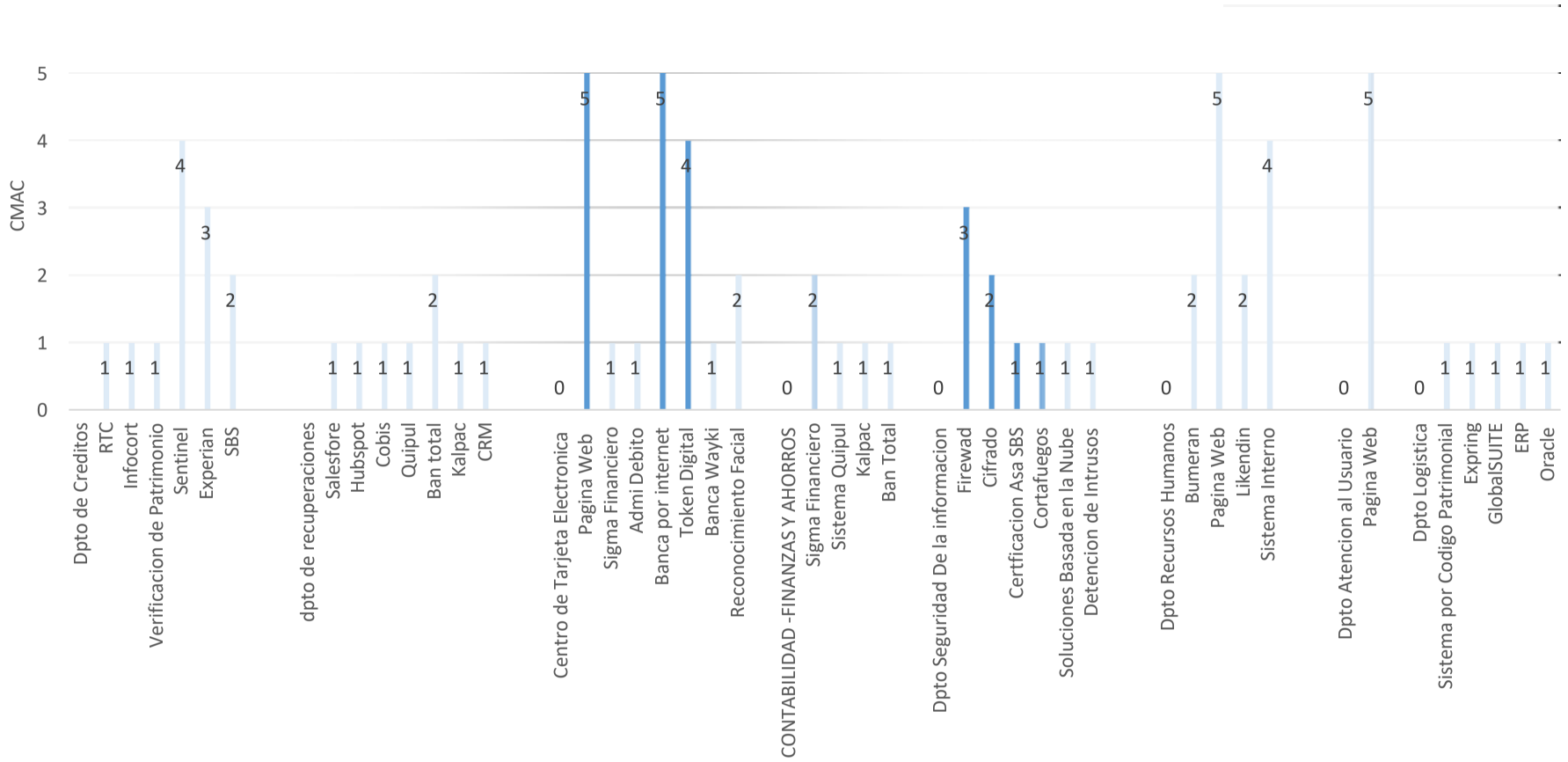
Herramientas Utilizadas en los Departamentos de Procesos Operativos de las Cajas Municipales de Ahorro y Crédito

CMAC	Atención al Usuario	Seguridad de la Información	Logística	Recursos Humanos	Créditos
Cuzco	Página Web	Corta Fuegos y Sistemas de detección de intrusos	Sistema por Código Patrimonial	Bumerán- Pagina Web-Interno	Infocorp- RTC- Verificación Patrimonial
Lima Metropolitana	Página Web	Soluciones de seguridad basadas en la nube	Expring	Bumerán- Pagina Web-Interno	Sentinel- Experian
Huancayo	Página Web	Cifrado y firewalls	Global SUITE	Página Web-Interno	Sentinel- SBS
Trujillo	Página Web	Cifrado y firewalls	ERP	LinkedIn- Pagina Web-Interno	Sentinel- Experian- SBS
Arequipa	Página Web	Herramientas de Certificación ASA	Oracle	LinkedIn- Pagina Web-Interno	Sentinel- Experian

CMAC	Recuperaciones	Centro de Tarjetas Electrónicas	Contabilidad- Ahorro y Finanzas
Cuzco	Salesforce - HubSpot	Página Web -Sigma Financiero-Admi Debito -Banca por Internet- Token Digital-Banca Wayki	Sigma Financiero
Lima Metropolitana	Cobis	Página Web -Banca Por internet	Sigma Financiero
Huancayo	Quipul- CRM	Página Web -Banca Por internet - Token Digital	Sistema Quipul
Trujillo	Ban total- Kalpac	Página Web -Banca Por internet - Token Digital- Reconocimiento Facial	Kalpac
Arequipa	Ban total	Página Web -Banca Por internet - Token Digital- Reconocimiento Facial	Ban Total

Figura 2:

Herramientas Ti Identificadas en los Procesos Operativos de las CMAC



El análisis de las herramientas tecnológicas en las Cajas Municipales de Ahorro y Crédito (CMAC) revela una estrategia enfocada en la digitalización y optimización de procesos. Cada área funcional implementa soluciones específicas para mejorar su eficiencia y gestión. El Departamento de Atención al Usuario utiliza sistemas internos y plataformas web para mejorar la experiencia del cliente. En el Departamento de Seguridad de la Información, se aplican herramientas como firewalls y cifrado para proteger datos y mitigar riesgos tecnológicos. El Área de Logística gestiona el inventario y activos mediante sistemas especializados, mientras que Recursos Humanos emplea plataformas como LinkedIn para convocar nuevos talentos. En el Área de Créditos, se utilizan sistemas como RTC e Infocorp para evaluar el historial crediticio de los clientes. El Departamento de Recuperaciones aplica plataformas como Salesforce para gestionar la recuperación de deudas. El Centro de Tarjetas Electrónicas moderniza los servicios financieros con herramientas como la banca por internet y reconocimiento facial. Finalmente, las áreas de Contabilidad, Ahorros y Finanzas trabajan con SIGMA Financiero para garantizar precisión y sostenibilidad económica. Estas herramientas mejoran la eficiencia operativa y refuerzan la competitividad de las CMAC, apoyando sus objetivos de inclusión financiera y sostenibilidad.

Resultado 2

Analizar el reglamento del proceso de Auditoría interna en el control de riesgo del uso de herramientas tecnológicas en los procesos operativos de las Cajas Municipales

Mediante La Resolución SBS N° 11699-2008 de la Superintendencia de Banca, Seguros y AFP (SBS) aprobó el Reglamento de Auditoría Interna donde establece los estándares y requisitos de auditoría interna para las empresas del rubro financiero, de seguros y las Administradoras Privadas de Fondos de Pensiones (AFP). Es por ello que En esta segunda fase de recolección de información, se ha realizado un análisis del reglamento interno de auditoría utilizado por cada Caja Municipal de Ahorro y Crédito de la muestra, para conocer su procedimiento política y gestión de riesgo que tienen en relación a sus procesos operativos Este reglamento es fundamental para asegurar que la CMAC opere de manera eficiente y en conformidad con las mejores prácticas, protegiendo los intereses de sus clientes y fortaleciendo su sostenibilidad financiera.

A continuación, se detallan los hallazgos clave en términos de procedimientos, gestión de riesgos, políticas de seguridad y desempeño financiero en relación con el uso de herramientas tecnológicas de cada CMAC.

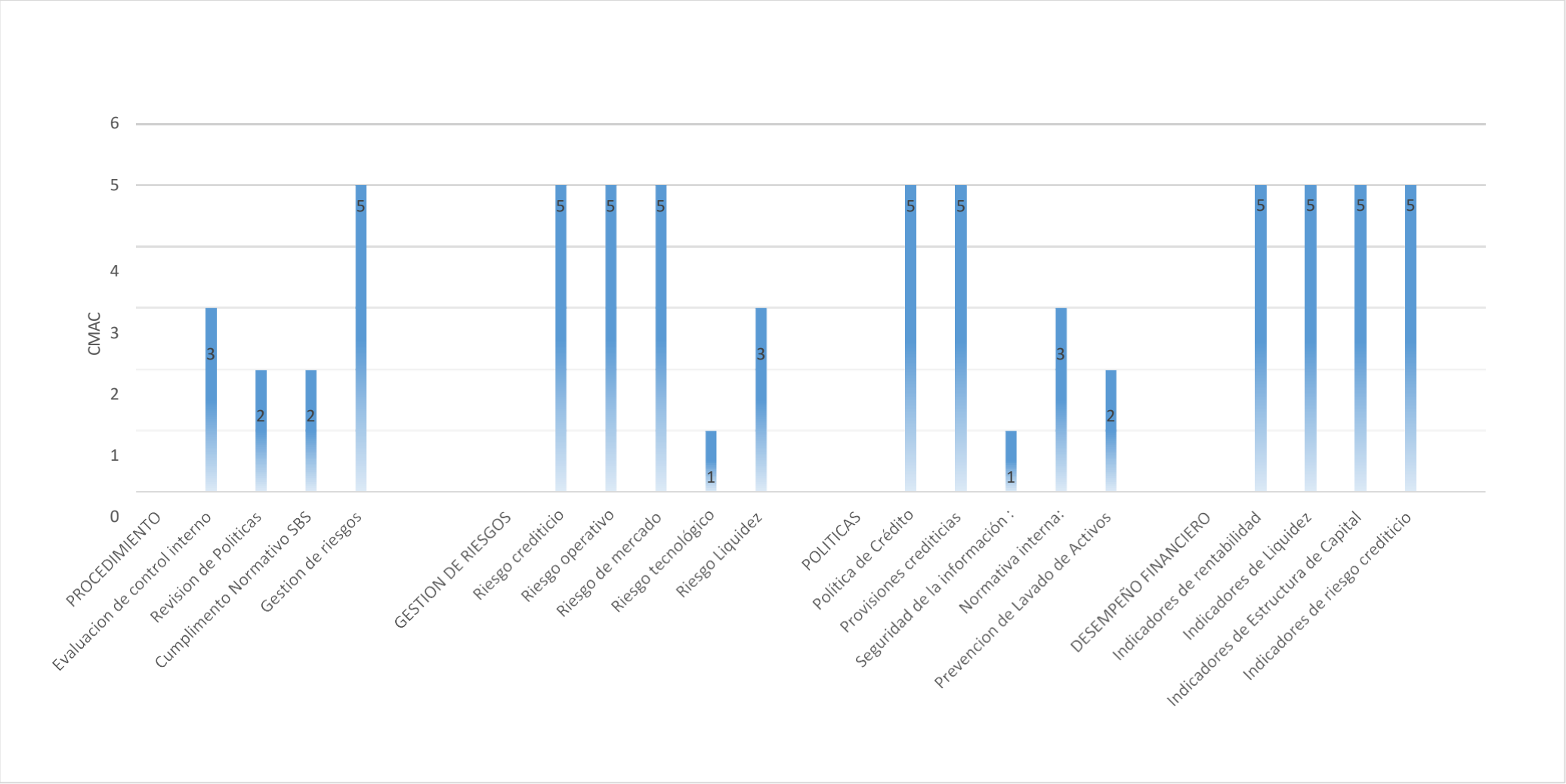
Tabla3

Cuadro de Análisis de Procedimiento del Reglamento de Auditoría Interna de las CMAC

REGLAMENTO DE AUDITORIA INTERNA	Procedimiento	Gestión de Riesgos	Políticas	Desempeño Financiero
CAJA MUNICIPAL DE AHORRO Y CREDITO CUZCO	Revisiones periódicas de informes financieros examen de estrategias, informan hallazgos y recomiendan a la alta dirección	Riesgo crediticio Riesgo operacional Riesgo de Mercado	Política de Crédito Provisiones para pérdidas de préstamos Capacitación Seguridad de la información:	Indicadores de rentabilidad Indicadores de Liquidez Indicadores de Estructura de Capital Indicadores de riesgo crediticio
CAJA MUNICIPAL DE AHORRO Y CREDITO LIMA METROPOLITANA	Evaluar la situación financiera, La implementación del control interno, revisiones de riesgos operativos, mercado y tecnológico, Asegurar que cumple con las regulaciones de SBS	Riesgo crediticio Riesgo operativo Riesgo de mercado Riesgo tecnológico	Provisiones crediticias Prevención de lavado de activos Seguridad de la información	ROA (Rentabilidad sobre activos) ROE (Rentabilidad sobre el patrimonio) Cartera de créditos en mora Ratio de eficiencia
CAJA MUNICIPAL DE AHORRO Y CREDITO AREQUIPA	Revisión de sistemas de control interno, gestión de riesgos, Ejerce apoyo de auditoría externa en evaluaciones anuales	Riesgo crediticio Riesgo Operacional Riesgo de Liquidez Riesgo de mercado	Política de gestión de riesgos Normativa interna: Prevención de lavado de activos	Cartera de créditos Rentabilidad (ROE - ROA) Ratio de Liquidez Ratio de Provisiones
CAJA MUNICIPAL DE AHORRO Y CREDITO HUANCAYO	Se auditan los procedimientos de la entidad para identificar ineficiencias, fraudes, errores y áreas de mejora. La auditoría también revisa que las políticas internas se apliquen adecuadamente en las diferentes áreas	Riesgo crediticio Riesgo Operacional Riesgo de Liquidez Riesgo de mercado	Política de Crédito Prevención de lavado de activos: Actualización de Normativa	Gestión de riesgos financieros Riesgo de crédito
CAJA MUNICIPAL DE AHORRO Y CREDITO TRUJILLO	Evaluación de Control Interno, Cumplimiento de las disposiciones de la SBS, gestión de Riesgos Tecnológicos	Riesgo crediticio Riesgo Operacional Riesgo de Liquidez Riesgo de mercado	Gestión de riesgos financieros Riesgo de crédito	Rentabilidad Cartera de crédito Ratio de Liquidez

Figura 3:

Reglamento del Proceso de Auditoría Interna de las CMAC



En la Caja Municipal de Ahorro y Crédito Cuzco establece en su reglamento de Auditoría Interna la realización de revisiones periódicas de sus informes financieros. Este proceso permite priorizar la gestión de riesgos, destacando el riesgo crediticio en sus operaciones diarias y, en el ámbito externo, el riesgo de mercado. En sus políticas, la Caja incluye políticas de crédito para mitigar estos riesgos y también destaca la seguridad de la información como una prioridad. Se enfatiza la capacitación continua para prevenir ciberataques y protegerse contra posibles amenazas informáticas, lo que demuestra una estrategia proactiva ante los riesgos tecnológicos. Sin embargo, aunque la seguridad de la información es tratada como una política importante en su plan de auditoría, se observa una falta de enfoque específico en el riesgo tecnológico como parte de sus deficiencias operativas. En la misma línea, la Caja Municipal de Ahorro y Crédito Lima Metropolitana establece en su reglamento de auditoría interna un enfoque integral que prioriza la evaluación financiera, la implementación de un control interno riguroso y revisiones periódicas de riesgos operativos, de mercado y tecnológicos, priorizando el cumplimiento de las regulaciones de la SBS. La gestión de riesgos se centra en el riesgo crediticio, operativo, de mercado y tecnológico, con políticas específicas que incluyen provisiones crediticias, prevención de lavado de activos y seguridad de la información. En cuanto al desempeño financiero, utiliza indicadores clave como el ROA (rentabilidad sobre activos), ROE (rentabilidad sobre el patrimonio), cartera de créditos en mora y ratio. Este conjunto de prácticas refuerza la solidez operativa a excepto de la seguridad informática de la entidad. La Caja Municipal de Arequipa, a través de su reglamento de Auditoría Interna, establece procedimientos para la identificación de ineficiencias, fraudes, errores y áreas de mejora, abordando estas cuestiones dentro de sus procesos vinculados a la actividad económica. Asimismo, su gestión de riesgos se enfoca principalmente en los riesgos operativos, de liquidez y crediticios, sustentándose en políticas de crédito, prevención de lavado de activos y actualizaciones normativas. Sin embargo, se evidencia una ausencia de gestión específica del riesgo tecnológico. A pesar de que el proceso de auditoría operativa contribuye al desempeño financiero y a la mitigación del riesgo crediticio, el riesgo tecnológico no recibe la misma prioridad. Por otra parte, la Caja Municipal de Ahorro y Crédito Trujillo, según su procedimiento, implementa una evaluación continua de su control interno y ha integrado la gestión de riesgos tecnológicos como parte fundamental de sus procesos. Este enfoque refuerza la prioridad en dicha área, alineándose con la creciente digitalización, Además, su gestión de riesgos abarca los riesgos crediticios, operacional, de liquidez y de mercado, fundamentándose en políticas sólidas de gestión de riesgos financieros y de crédito. Finalmente, la Auditoría Interna de la CMAC Huancayo tiene como objetivo principal asegurar el cumplimiento

normativo, la eficacia de los controles internos y la razonabilidad de los estados financieros. La gestión de riesgos abarca riesgos crediticios, operacionales, de liquidez y de mercado, apoyándose en herramientas como GlobalSUITE para el control operacional y en planes de contingencia para riesgos de liquidez. Sin embargo, se evidencia una ausencia de gestión específica del riesgo tecnológico. A pesar de que el proceso de auditoría operativa contribuye al desempeño financiero y a la mitigación del riesgo crediticio, el riesgo tecnológico no recibe la misma prioridad. Esto deja una brecha significativa en la estrategia de gestión de riesgos, especialmente en un contexto donde la digitalización y la seguridad de la información son cruciales para la continuidad y la eficiencia.

El análisis de los reglamentos de Auditoría Interna de las CMAC revela una realidad compleja respecto a la gestión de riesgos tecnológicos y al control interno. Si bien todas las oficinas realizan revisiones periódicas, existen enfoques marcadamente distintos. Por ejemplo, la CMAC Huancayo profundiza en la evaluación de riesgos, mientras que la CMAC Arequipa se enfoca principalmente en el cumplimiento de políticas. Esta diferencia en prioridades dificulta la conformación de una visión unificada sobre los riesgos de TI en todo el sistema. Además, la dependencia de auditorías externas en algunas oficinas, como Cuzco y la misma Huancayo, podría generar demoras en la identificación y respuesta ante nuevas amenazas tecnológicas en procesos clave. Aunque todas las CMAC reconocen los riesgos operativos y tecnológicos, la diversidad en la forma de gestionarlos sugiere que algunas entidades no les otorgan la misma relevancia, lo cual podría aumentar su nivel de vulnerabilidad. En cuanto a las normativas de seguridad de la información, únicamente Arequipa y Huancayo mencionan explícitamente contar con lineamientos formales, lo que evidencia una falta de uniformidad que podría exponer a otras oficinas a mayores riesgos. Finalmente, la gestión de riesgos TI y su implementación varía entre entidades, lo que refleja un control desigual sobre las herramientas tecnológicas empleadas, generando posibles puntos débiles en el cumplimiento normativo.

Resultado 3

Identificar los tipos de riesgos generados por el uso de herramientas tecnológicas en los procesos operativos de las Cajas Municipales y su relación en la Auditoria Interna.

La identificación de los riesgos tecnológicos en los procesos operativos de las CMAC es fundamental para la seguridad y continuidad de sus servicios, y su relación con la Auditoría Interna es clave. La dependencia tecnológica de las CMAC (plataformas web, cifrado, cortafuegos, banca en línea) las expone a diversos riesgos que la Auditoría Interna debe evaluar para asegurar controles efectivos y una gestión de riesgos fijos con los objetivos de las CMAC.

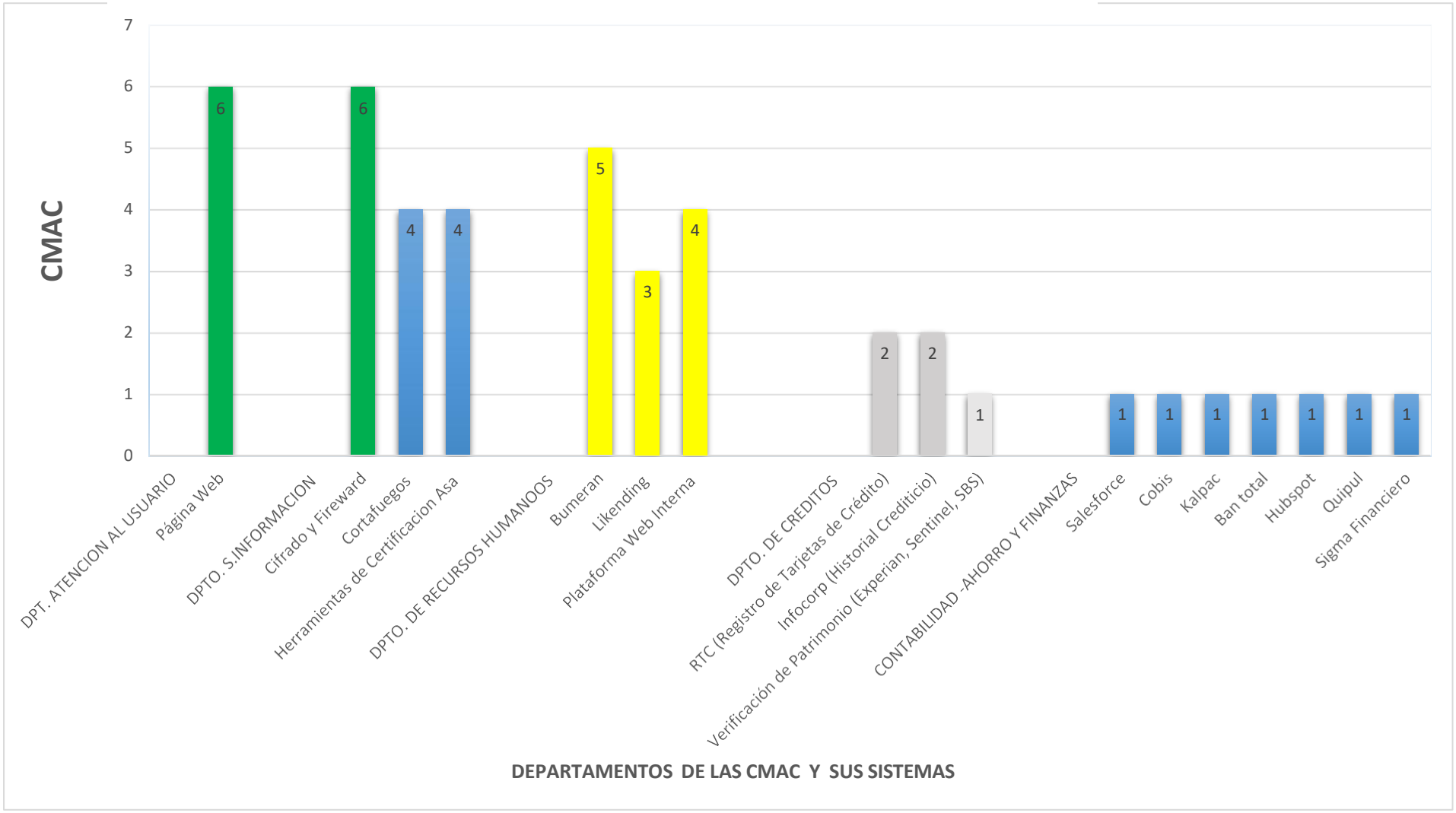
Tabla 4:

Riesgos Tecnológicos Identificados por Dpto. de Operaciones de las CMAC

Departamento	Herramientas o Sistema Ti	Riesgo Tecnológico
Oficina de Atención al Usuario	Página Web	Ataques de malware y viru Inyección SQL y ataques de scripting (XSS): Phishing: Ataques de denegación de servicio (DDoS) Mala configuración de cookies y rastreo Incompatibilidad con otros sistemas internos
Oficina de Seguridad de la Información	Cifrado y Fireward	Algoritmos obsoletos Robo o Compromiso de Claves Errores de Implementación Exposición de Claves Cifrado Débil Expiración de Certificados
	Cortafuegos	Ataques de Denegación de Servicio (DDoS) Configuración incorrecta Monitoreo Inadecuado Interrupción del Servicio
	Herramientas de Certificacion Asa	Ataques de Intermediario (MITM) Manejo Inseguro de Certificados Revocación No Efectiva Dependencia de Infraestructura de Certificación
Recursos Humanos	Bumeran	Ataques de Phishing: Vulnerabilidades de Acceso Exposición de Información Sensible Exposición de Datos de Candidatos
	Likending	Manejo Inadecuado de Datos: Suplantación de Identidad de Perfiles Corporativos Phishing a través de Mensajes Limitación de Control sobre la Información
	Plataforma Web Interna	Vulnerabilidades de Inyección SQL y XSS (Cross-Site Scripting Falta de Cifrado en Comunicaciones Acceso No Autorizado a Información Interna Interrupción de Servicio de la Página Web Interna
Créditos	RTC (Registro de Tarjetas de Crédito)	Riesgo de Phishing y Suplantación de Identidad Exposición de Datos Financieros Sensibles
	Infocorp (Historial Crediticio)	Riesgo de Robo de Identidad por Fuga de Datos Vulnerabilidad a Ataques de Ciberseguridad (SQL injection, XSS
	Verificación de Patrimonio (Experian, Sentinel, SBS)	Manipulación de Información Patrimonial
Contabilidad, Finanzas, Ahorros y Recuperaciones	Salesforce	Exposición de datos confidenciales.
	Cobis	Fallos en la integración con otros sistemas.
	Kalpac	Errores de interoperabilidad.
	Ban total	Fallos en la autenticación.
	Hubspot	Contraseñas débiles.
	Quipul	Inestabilidad con altas cargas.
	Sigma Financiero	Ataques cibernéticos.
	Admi Debito	Transacciones duplicadas.
	Banca por internet	Suplantación de identidad (phishing).
	Token Digital	Robo de tokens.
	Banca Wayki	Fraude en transferencias.

Figura 4:

Riesgos Tecnológicos Identificados por Dpto. de Operaciones de las CMAC



En el análisis de riesgos TI por proceso operativo de las Cajas Municipales, se identificó que la Oficina de Atención al Usuario enfrenta amenazas como ataques de malware, inyecciones SQL, scripting entre sitios (XSS), phishing, ataques de denegación de servicio (DDoS), configuraciones erróneas de cookies y rastreo, así como problemas de incompatibilidad con otros sistemas. En la Oficina de Seguridad de la Información, se detectaron riesgos como el uso de algoritmos obsoletos, compromiso y exposición de claves, errores de implementación en medidas de seguridad, cifrado débil, expiración de certificados, fallas en la revocación de certificados, ataques DDoS, configuraciones incorrectas, monitoreo insuficiente y alta dependencia de infraestructuras de certificación. En el Departamento de Recursos Humanos, los riesgos están orientados a phishing, vulnerabilidades de acceso, exposición de datos sensibles de postulantes, suplantación de identidad y deficiencias en el control de la información confidencial. Respecto a la Plataforma Web Interna, se hallaron vulnerabilidades por inyección SQL y XSS, ausencia de cifrado en las comunicaciones, accesos no autorizados a información interna y riesgos de interrupción de servicios críticos. En el área de Créditos, se identificaron riesgos de phishing, suplantación de identidad, exposición de información financiera sensible, robo de identidad mediante fuga de datos, ataques de ciberseguridad (como inyección SQL y XSS) y manipulación de información patrimonial. Finalmente, en las áreas de Contabilidad, Finanzas, Ahorros y Recuperaciones que operan de manera interrelacionada se identificaron fallas en transacciones, malfuncionamientos en la gestión de carteras de crédito, problemas de sincronización de datos, exposición de información sensible, errores en cálculos financieros, deficiencias en la administración de débitos automáticos, vulnerabilidades en la autenticación digital y riesgos de interrupciones en la banca en línea. Esta situación evidencia que cada área crítica de los procesos operativos de las Cajas Municipales está expuesta a amenazas tecnológicas que pueden afectar la continuidad del negocio, provocar pérdidas financieras millonarias y derivar en prolongados procesos judiciales por incumplimientos contractuales o filtración de datos personales.

Relación en la Auditoría Interna:

La presencia de estos riesgos tecnológicos tiene una relación de forma directa en el trabajo de auditoría interna, ya que obliga a modificar y ampliar el enfoque tradicional de revisión. La auditoría no solo debe verificar los procesos financieros y operativos, sino también evaluar la solidez de los controles tecnológicos, identificar vulnerabilidades informáticas y comprobar el cumplimiento de normativas de seguridad y protección de datos. En la **Oficina de Atención al**

Usuario, por ejemplo, la auditoría deberá analizar los controles contra ataques de phishing y denegación de servicio. En **la** Oficina de Seguridad de la Información, tendrá que auditar la vigencia y efectividad de los certificados digitales y los esquemas de cifrado. **En** Recursos Humanos, deberá asegurar que existan políticas claras de protección de datos personales. En Créditos, Contabilidad, Finanzas, Ahorros **y** Recuperaciones, la auditoría deberá enfocarse en la integridad de los datos financieros, la confiabilidad de las plataformas digitales, y la correcta ejecución de las transacciones. De no gestionarse adecuadamente estos riesgos, la auditoría interna puede emitir informes adversos, lo que impactaría negativamente en la imagen institucional, afectando tanto la confianza de los usuarios como la estabilidad financiera de la

El análisis realizado revela que los departamentos de Seguridad de la Información, Recursos Humanos y Contabilidad son los que concentran mayor cantidad de riesgos tecnológicos, con 12 identificados en cada uno. Entre los problemas más frecuentes se encuentran ataques de intermediarios (MITM), suplantación de identidad (phishing) y vulnerabilidades en plataformas financieras. En Atención al Usuario se detectaron seis riesgos, principalmente relacionados con software malicioso, fraudes electrónicos y problemas de compatibilidad tecnológica. Por su parte, el área de Créditos enfrenta ocho riesgos, incluyendo manipulación de datos y amenazas a los sistemas de evaluación crediticia. Esta situación evidencia la urgencia de fortalecer las medidas de protección, asegurar la integridad de la información y mejorar las competencias digitales en todo el personal. En este contexto, la auditoría interna de las Cajas Municipales cumple un papel clave al supervisar y controlar estos riesgos, verificando que los mecanismos de seguridad funcionen correctamente y que la información crítica esté debidamente resguardada. Asimismo, los riesgos detectados exigen una revisión constante de los controles, lo cual influye directamente en la frecuencia y enfoque de las auditorías realizadas.

Discusión

En concordancia con los resultados obtenidos en la identificación de los sistemas y herramientas tecnológicas utilizadas en los procesos operativos de las Cajas Municipales de Ahorro y Crédito (CMAC) reflejan un avance significativo hacia la transformación digital se identificaron herramientas TI las cuales destacan sistemas como Sigma Financiero, Ban Total y Quipul , Salesfore , CRM , Sentinel, Experian cada uno de estos de acuerdo a sus procesos operativos y su utilización en cada área relevante cuyo objetivo principal es aportar valor, mejorar la eficiencia operativa y garantizar la sostenibilidad empresarial en el sector financiero. Una implementación no planificada en gestión de Riesgos Tecnológicos de Auditoría Interna

podría generar una dependencia excesiva de la tecnología, exponiendo a las CMAC a riesgos operativos tecnológicos y de seguridad. Por ello, es crucial combinar la innovación tecnológica con una adecuada gestión de riesgos, garantizando que los beneficios derivados de la digitalización superen sus posibles amenazas. Si bien estas tecnologías potencian la productividad y la competitividad, no obstante, incrementan la exposición a amenazas cibernéticas. Ante ello se resalta la estrecha relación entre la transformación tecnológica y la gestión de riesgos TI como parte de sus procesos operativos, enfatizando la necesidad de que las CMAC se mantengan actualizadas para responder a la seguridad de la información de sus clientes, es fundamental que la adopción de estas herramientas sea estratégica y equilibrada. Estos hallazgos coinciden con lo planteado por Álvarez et al. (2024), quienes destacan que la creciente infraestructura digital, impulsada por la virtualización, la computación en la nube y estrategias híbridas, que está acompañada de avances en monitoreo remoto, telemetría, sensores y gestión inteligente de instalaciones. Dentro de la misma línea, Chengyou et. al (2025) en su investigación plantea que la tecnología financiera ha impulsado tanto la diversificación de las operaciones de los bancos comerciales como el crecimiento de la competencia en el mercado, donde se plantea desafíos para su gestión de riesgos en sus procesos operativos.

Respeto al análisis del reglamento del proceso de auditoría interna en el control de riesgos asociados al uso de herramientas tecnológicas en los procesos operativos de las Cajas Municipales, resalta la importancia de comprender que la adaptación tecnológica, aunque necesaria, conlleva a riesgos cibernéticos que pueden comprometer la confidencialidad e la información. En el análisis de los reglamentos de Auditoría Interna ejecutado hacia cada CMAC se muestra inconsistencia en el tratamiento del riesgo tecnológico de la muestra. Si bien se observó una dedicación significativa a establecer controles de gestión en procesos operativos tradicionales como liquidez y mercado, actualización de normas y políticas, evaluación de créditos y prevención de lavado de activo no todas las instituciones priorizan el riesgo inherente al uso de herramientas de TI como un componente fundamental dentro de sus procesos de auditoría interna para general una gestión de riesgos y seguridad de la información. Las auditorías internas desempeñan un papel clave al establecer en su procedimiento, gestión de riesgo y políticas efectivas para la detención de ataques cibernéticos en cada proceso operativo. Esto incluye la identificación, evaluación y mitigación de riesgos cibernéticos, fortaleciendo así la resiliencia organizacional. Estos resultados coinciden con el análisis de López, A. (2021), quien destaca que los auditores deben considerar los riesgos asociados a la tecnología de la información (TI) al planificar sus encargos, subrayando aspectos como la seguridad de la

información, el control interno y los aspectos legales. Según López, aunque el ambiente TI no es intrínsecamente más riesgoso que otros, ciertos factores presentan mayor relevancia para los auditores, especialmente en el contexto del riesgo cibernético.

Finalmente, esta investigación culmina con la identificación detallada de los riesgos específicos generados por la integración de herramientas tecnológicas en los procesos operativos de las Cajas Municipales y su relación en la Auditoría Interna. Entre los riesgos más significativos asociados a los sistemas y procesos operativos, destacan la vulnerabilidad a ataques cibernéticos como phishing, ransomware, malware, denegación de servicios (DDoS) y suplantación de identidad, así como riesgos tecnológicos relacionados con la obsolescencia de sistemas, fallos en la gestión de actualizaciones, y problemas de interoperabilidad. Estas vulnerabilidades representan una amenaza, afectando la confianza del cliente, la seguridad de la información, la continuidad del negocio y la competitividad en un mercado altamente digitalizado. Estos hallazgos refuerzan la necesidad de que las Cajas Municipales implementen una gestión integral de riesgos tecnológicos, basada en un marco robusto de auditoría interna que no solo evalúe los riesgos internos, sino que también desarrolle estrategias efectivas para mitigarlos garantizando la integridad de la información y toma de decisiones. En este contexto, los hallazgos coinciden con lo señalado de Zarate et. al (2022) acuerda que su investigación se enfoca en comprender el funcionamiento de las instituciones financieras a nivel mundial, así como las amenazas y desafíos que enfrentan diariamente en sus procesos operativos por la adaptación tecnológica. Por otra parte, Cortez et. al (2022), quienes destacan que la era tecnológica ha transformado la auditoría al presentar tanto desafíos como oportunidades. Señalan que el acceso limitado o la mala gestión de la tecnología puede generar pérdidas significativas por compromisos de confidencialidad, costos adicionales, problemas legales y pérdida de competitividad.

Conclusiones

Se concluye con la investigación, que la actual coyuntura de la digitalización donde las Cajas Municipales de Ahorro y Crédito (CMAC) están inmersas en un proceso de transformación que implica la adopción estratégica de herramientas y sistemas de Tecnología de la Información (TI). Esta adaptación busca optimizar la eficiencia operativa en cada una de sus áreas de trabajo, estas soluciones tecnológicas tienen una importancia particular en el procesamiento de datos y se erige como un motor para el progreso institucional, siempre y cuando su implementación y utilización se realicen con la máxima seguridad y responsabilidad.

A su vez se concluye que el reglamento de Auditoría Interna de las Cajas Municipales de Ahorro y Crédito (CMAC) constituye una base fundamental para la implementación de una gestión de riesgos planificada y estratégica, alineada con la operatividad de sus procesos internos. No obstante, se observa la necesidad urgente de priorizar aspectos clave relacionados con la gestión de riesgos tecnológicos, a fin de prevenir posibles vulnerabilidades a la ciberseguridad institucional además la falta de capacitación del personal es otro factor vulnerable en temas vinculados a la seguridad digital y el uso adecuado de herramientas tecnológica

Se concluye que la investigación permitió identificar riesgos tecnológicos críticos que, de no ser abordados mediante una gestión adecuada por parte de la Auditoría Interna, podrían comprometer seriamente la sostenibilidad de una empresa en marcha. Estás amenazas no solo afectan la integridad de los datos, sino que pueden desencadenar pérdidas económicas significativas e incluso llevar a la quiebra de la entidad, particularmente en el sector financiero, que ha sido uno de los más afectados por riesgos tecnológicos. En este contexto, la Auditoría Interna cumple un rol estratégico y fundamental como mecanismo de detección y mitigación, contribuyendo de manera decisiva a la reducción de estos riesgos cibernéticos

Recomendaciones

Se sugiere a las Gerencias de Ti de las CMAC, fortalecer de manera homogénea la gestión de riesgos tecnológicos mediante la incorporación de controles específicos y actualizados en sus reglamentos de Auditoría Interna. Asimismo, resulta indispensable que todas las oficinas adopten políticas formales en materia de seguridad de la información, gestión de riesgos tecnológicos y continuidad operativa, para contribuir a reducir la exposición frente a amenazas cibernéticas, pérdidas de datos sensibles y posibles fraudes, asegurando así la estabilidad y confianza en los procesos institucionales.

.

Referencias

Alvares, J., Gómez, L., & Ruiz, M. (2024). La infraestructura digital y la ciberseguridad en los centros de datos interconectados. *Revista Sistema de Información y Comunicación (SIC)*. Instituto de Tiempo de Actividad / Leet Seguridad. 14(9),50-56 https://revistasic.es/sic162/revistasic162.pdf

Bashaija, R. (2022). *Impact of internal control on non-financial firms listed on the Vietnamese Stock Exchange*. Journal of Financial Control & Strategy, 14(3), 89–102. https://www.researchgate.net/publication/369888968_Impact_of_internal_control_on_the_performance_of_non-financial_listed_firms_in_an_emerging_country

Castañeda, J. (2016). Gestión, administración de riesgos y modelos de control interno. Bogotá, Colombia: Fundación Universitaria del Área Andina. https://digitk.areandina.edu.co/bitstream/handle/areandina/2116/RP_eje1.pdf

Chengyou, L., Xiaoxia, H., & Shasha, L. (2025). *Investigación sobre el impacto de la tecnología financiera en la toma de riesgos de los bancos comerciales.* Journal of Financial Risk Analysis, 76(2), 45–67. https://doi.org/10.1016/j.ribaf.2025.102804

Encalada, V. (2023). *El Papel de las TIC en la Auditoría Forense y la Ciberseguridad Organizacional. Journal of Information Security and Cybercrime*, 10(1), 89-105. https://revistasumadenegocios.konradlorenz.edu.co/vol14-num-31-2023-auditoria-forense-riesgo-de-auditoria-fraude-y-materialidad

Fernández de Lis, S., & Urbiola Ortún, P. (2018). Transformación digital y competencia en el sector financiero (Documento de trabajo N.º 19/01). BBVA Research. Publicado en la Revista de Información Comercial Española (ICE). https://www.bbvaresearch.com/publicaciones/transformacion-digital-y-competencia en-el-sector-financiero/

International Organization for Standardization. (2018). *ISO 31000:2018 - Risk management – Guidelines*. ISO. https://csrc.nist.gov/glossary/term/Cyber-Risk

KPMG en Colombia. (2019). *Auditoría interna reimaginada: Evolucionando para nuestros clientes.* KPMG Advisory, Tax & Legal S.A.S. https://home.kpmg/co/es/home/insights/2019/09/auditoria-interna-re-imaginada.html

Lizárraga, C., Morales, J., & Peña, R. (2022). *Auditoría de tecnologías de la información y su impacto en la eficiencia institucional: Revisión sistemática*. Revista de Gestión y Tecnología, 8(2), 112–130. https://dialnet.unirioja.es/descarga/articulo/9560435.pdf

López, A. (2021). Análisis de riesgos en auditoría de TI: *Un enfoque basado en la ciberseguridad. Revista de Auditoría y Control Interno, 14(3), 215-232. https://www.researchgate.net/publication/380182651_Auditoria_de_riesgos_de_ciber seguridad_Revision_de_Literatura_propuesta_y_aplicacion*

López, M., Vargas, L., & Huamán, J. (2023). *Digitalización de auditoría interna y su impacto en la gestión de riesgos tecnológicos en instituciones financieras*. Revista de Auditoría y Tecnología, 9(4), 134–156. https://dialnet.unirioja.es/descarga/articulo/9560430.pdf

Maurer, T., & Arthur, N. (2021). La ciber amenaza mundial. *Revista Fondo Monetario Internacional (8)*, 2-4. https://www.imf.org/external/pubs/ft/fandd/spa/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf

Ortega, L. (2024). *Investigación aplicada y desarrollo tecnológico*. Instituto Nacional de Tecnología.https://www.intec.gob.do/publicaciones/investigacion-aplicada-2024

Quecedo, M. T., & Castaño, C. (2002). Introducción a la investigación cualitativa. *Revista Electrónica de Documentación en Ciencias Sociales*, (6), 1–20. https://www.redalyc.org/pdf/812/81200602.pdf

Riesgo cibernético y ciberseguridad (Documento de Trabajo No. 181). Secretaría de Hacienda y Crédito Público – Comisión Nacional de Seguros y Fianzas, México. https://www.gob.mx/cms/uploads/attachment/file/490432/181.Riesgo_Cibern_tico_y_ Ciberseguridad_2019.pdf

Secretaría General de la Organización de los Estados Americanos (OEA). (2020). *Ciberseguridad en el sector bancario de América Latina y el Caribe: Informe regional 2020*. Organización de los Estados Americanos. https://www.oas.org/es/sms/cicte/Ciberseguridad-en-el-sector-bancario-ALC-2020.pdf

Zheng, G., Xia, Z., El, F., & Xiao, Z., (2025). *IT expertise in audit committees and cybersecurity risk disclosure: Evidence from China*. Journal of Corporate Governance and Risk, 17(1), 55–78. https://doi.org/10.1016/j.jcgr.2025.01.006

Zárate, F., Muñoz, A., & Delgado, S. (2022). *Zero Trust en la seguridad de instituciones financieras globales: Desafíos y oportunidades*. Revista Internacional de Seguridad Informática, 10(3), 45–67. http://www.redalyc.org/articulo.oa?id=586061883004