FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

PROPUESTA DE ANÁLISIS DE RIESGOS CON COBIT 2019 E ITIL 4 PARA OPTIMIZAR LA GESTIÓN DEL SOFTWARE DE CAJEROS AUTOMÁTICOS EN BANCO FICOHSA

SUSTENTADO POR:
JAIME OSCAR MOLINA ORDÓÑEZ
JEAN CARLOS NÚÑEZ RAMÍREZ

PREVIA INVESTIDURA AL TÍTULO DE
MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

TEGUCIGALPA, FRANCISCO MORAZÁN, HONDURAS, C.A.

29 DE ENERO, 2026

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA FACULTAD DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

PROPUESTA DE ANÁLISIS DE RIESGOS CON COBIT 2019 E ITIL 4 PARA OPTIMIZAR LA GESTIÓN DEL SOFTWARE DE CAJEROS AUTOMÁTICOS EN BANCO FICOHSA

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR

JORGE RAÚL MARADIAGA CHIRINOS

MIEMBROS DE LA TERNA:

JULISSA JAMILETH CORTÉS

ELVIN OSMAN BOBADILLA

JOSUÉ DAVID MEJÍA

FACULTAD DE POSTGRADO

PROPUESTA DE ANÁLISIS DE RIESGOS CON COBIT 2019 E ITIL 4 PARA OPTIMIZAR LA GESTIÓN DEL SOFTWARE DE CAJEROS AUTOMÁTICOS EN BANCO FICOHSA

JAIME OSCAR MOLINA ORDÓÑEZ
JEAN CARLOS NÚÑEZ RAMIRES

Resumen

La presente investigación aborda el problema de optimizar la gestión del software de cajeros automáticos (ATM) de Banco Ficohsa para mitigar vulnerabilidades y deficiencias operativas. El objetivo general es desarrollar un análisis de riesgos basado en COBIT 2019 e ITIL 4 para proponer estrategias que fortalezcan la continuidad del servicio, la resiliencia operativa y el cumplimiento normativo en la institución. El Marco Metodológico adopta un enfoque Documental-Observacional con un diseño Descriptivo-Evaluativo. Las Metodologías principales fueron COBIT 2019 (para la gobernanza y gestión de riesgos) e ITIL 4 (para la gestión de servicios y la creación de valor), que sirvieron como base para la propuesta. El Alcance se limitó a los procesos de gestión de software ATM en Banco Ficohsa, Honduras. La población de estudio incluyó los procesos y el personal de TI involucrado en la gestión ATM. Las principales variables analizadas fueron el Riesgo en la Gestión del Software ATM y la Aplicación de Prácticas de COBIT/ITIL. Se utilizaron instrumentos como: listas de verificación y guías de observación, diseñadas con indicadores de ambos marcos. La propuesta final integra estas metodologías para optimizar el servicio y la seguridad.

Palabras claves: Análisis de riesgos, COBIT 2019, ITIL4, Cajeros automáticos, Gestión de software

GRADUATE SCHOOL

PROPOSAL FOR RISK ANALYSIS WITH COBIT 2019 AND ITIL 4 TO OPTIMIZE THE MANAGEMENT OF ATM SOFTWARE AT BANCO FICOHSA

JAIME OSCAR MOLINA ORDÓÑEZ
JEAN CARLOS NÚÑEZ RAMIRES

Abstract

The present investigation addresses the problem of optimizing the management of Automatic Teller Machine (ATM) software at Banco Ficohsa to mitigate vulnerabilities and operational deficiencies. The general objective is to develop a risk analysis based on COBIT 2019 and ITIL 4 to propose strategies that strengthen service continuity, operational resilience, and regulatory compliance in the institution. The Methodological Framework adopts a Documentary-Observational approach with a Descriptive-Evaluative design. The Main Methodologies were COBIT 2019 (for governance and risk management) and ITIL 4 (for service management and value creation), which served as the basis for the proposal.

The Scope was limited to the ATM software management processes at Banco Ficohsa, Honduras. The study population included the IT processes and personnel involved in ATM management. The main variables analyzed were Risk in ATM Software Management and the Application of COBIT/ITIL Practices. Instruments used included: checklists and observation guides, designed with indicators from both frameworks. The final proposal integrates these methodologies to optimize service and security.

Keywords: Risk analysis, COBIT 2019, ITIL 4, Automated Teller Machines, Software Management.

DEDICATORIA

El presente Trabajo Final de Graduación está dedicado, en primer lugar, **a Dios**, por haberme permitido culminar esta etapa académica, brindándome sabiduría, entendimiento, fortaleza y perseverancia para alcanzar este logro, el cual contribuye significativamente a mi crecimiento personal y profesional.

De manera especial, dedico este trabajo a la memoria de **mis padres**, Jaime Oscar Molina (Q.D.D.G.) y Ramona Ordoñez (Q.D.D.G.), quienes con su sacrificio, amor y apoyo incondicional me inculcaron los valores de la disciplina, la responsabilidad y la constancia, enseñándome que con esfuerzo y dedicación es posible alcanzar las metas propuestas.

A mi esposa, Evelyn Visseth Hernández de Molina, por su apoyo incondicional, comprensión y motivación constante, siendo un pilar fundamental durante el desarrollo de esta maestría y en cada uno de los retos enfrentados a lo largo de este proceso académico.

Finalmente**, a mis hermanas y demás familiares**, quienes han sido parte esencial de mi vida, brindándome siempre su respaldo, palabras de aliento y buenos deseos para mi desarrollo profesional y personal.

- Jaime Oscar Molina Ordóñez

Dedico este trabajo, en primer lugar, **a Dios**, por ser mi guía constante, por brindarme fortaleza, sabiduría y perseverancia, y por permitirme culminar una etapa más de mi formación profesional.

A mis padres, por su amor incondicional, su apoyo permanente y por creer en mí incluso en los momentos más difíciles. Gracias por los sacrificios realizados, por los valores inculcados y por ser el pilar fundamental que me ha permitido avanzar con determinación hacia mis metas. Este logro también les pertenece.

A mi hermano y a todos mis amigos, por su apoyo, comprensión y palabras de aliento durante este camino académico. Su compañía y motivación hicieron más llevadero este proceso y contribuyeron de manera significativa a la culminación de este trabajo.

- Jean Carlos Núñez Ramires

AGRADECIMIENTO

Expreso un profundo agradecimiento a Dios por haber concedido la oportunidad de culminar esta etapa académica, brindando fortaleza, guía y sabiduría para superar las adversidades y alcanzar las metas profesionales planteadas.

De manera especial, agradezco a las autoridades académicas y al cuerpo docente de la Universidad Tecnológica Centroamericana (UNITEC), quienes, desde el inicio del proceso formativo hasta su culminación, contribuyeron de manera significativa al desarrollo académico y profesional de mi persona, mediante la transmisión de conocimientos, principios y valores, y la provisión de una educación de calidad. Al Ing. Jorge Maradiaga, nuestro asesor metodológico, por ser un guía invaluable durante la realización de este proyecto. Gracias por su apoyo constante y por motivarnos a alcanzar esta nueva meta con confianza y determinación.

Asimismo, extiendo un sincero agradecimiento a Banco Ficohsa, institución donde laboro, así como a mi jefatura, por el respaldo brindado para la ejecución del presente proyecto, permitiendo su desarrollo dentro del área de trabajo y facilitando las condiciones necesarias para su realización.

Finalmente, agradezco de manera especial a mi esposa, a mis padres (Q. D. D. G.), hermanas, sobrinos, amistades y compañeros, por su acompañamiento constante a lo largo de este proceso, así como por las oraciones, consejos, palabras de aliento y apoyo incondicional que fueron fundamentales para la culminación exitosa de esta etapa académica.

- Jaime Oscar Molina Ordóñez

Agradezco principalmente a Dios, por otorgarme la fortaleza, la sabiduría y la constancia necesarias para enfrentar cada desafío presentado durante el desarrollo de este trabajo, y por iluminar mi camino en los momentos de incertidumbre.

De manera especial, expreso mi más sincero agradecimiento al Ingeniero Jorge Maradiaga, por su valiosa orientación y acompañamiento académico durante el desarrollo de esta investigación, cuyos aportes y recomendaciones fueron fundamentales para fortalecer la calidad del trabajo y lograr su culminación.

- Jean Carlos Núñez Ramires

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

La presente investigación aborda un análisis de riesgos y la formulación de estrategias de mitigación orientadas a optimizar la gestión del software de cajeros automáticos (ATM) de Banco Ficohsa, tomando como base los marcos internacionales COBIT 2019 e ITIL 4. En la actualidad, las instituciones financieras dependen de manera crítica de sistemas tecnológicos que garanticen continuidad operativa, seguridad de la información y eficiencia en la prestación de servicios. Dentro de este ecosistema, el software que administra la red de cajeros automáticos constituye un activo estratégico, pues opera como un canal de autoservicio esencial para los clientes y está directamente influenciado por la disponibilidad, confiabilidad y percepción de seguridad que proyecta el banco. El Capítulo I presenta el planteamiento del problema, los antecedentes, la definición del problema, las preguntas de investigación, los objetivos y la justificación del estudio.

El Capítulo II desarrolla el marco teórico, incorporando los conceptos, tendencias y marcos de referencia relevantes, entre ellos COBIT 2019 e ITIL 4, así como los elementos del macro y microentorno que influyen en la gestión del software ATM, la cual enfrenta desafíos crecientes derivados de la complejidad tecnológica, el aumento sostenido de amenazas cibernéticas, la evolución de los riesgos operativos y el cumplimiento de estrictas disposiciones regulatorias nacionales e internacionales. En este entorno, cualquier falla en el servicio, incidente de seguridad o deficiencia operacional puede traducirse en pérdidas financieras, sanciones por incumplimiento, interrupciones en la continuidad del negocio y deterioro en la confianza del cliente.

El Capítulo III describe el enfoque metodológico, el diseño de la investigación, la población y muestra objeto de estudio, así como los instrumentos, técnicas e indicadores utilizados para la recopilación y análisis de la información. Asimismo, se detalla el procedimiento seguido para la identificación, evaluación y priorización de los riesgos asociados a la gestión del software de cajeros automáticos, alineando las prácticas de COBIT 2019 e ITIL 4 con el contexto operativo y regulatorio de Banco Ficohsa, con el fin de garantizar la validez, confiabilidad y coherencia de los resultados obtenidos.

El Capítulo IV expone los resultados obtenidos a partir de la aplicación de los instrumentos de investigación, el análisis de riesgos identificado en la gestión del software de cajeros

automáticos, la evaluación del nivel de madurez de los procesos y los principales hallazgos del estudio, los cuales permiten evidenciar las brechas existentes frente a las buenas prácticas establecidas por COBIT 2019 e ITIL 4 y sirven como base para la formulación de propuestas de mejora.

El Capítulo V presenta las conclusiones y recomendaciones derivadas del estudio, en coherencia con los objetivos planteados, destacando las principales implicaciones del análisis de riesgos y la evaluación de madurez, así como las acciones estratégicas y operativas sugeridas para fortalecer la gestión del software de cajeros automáticos, mitigar los riesgos identificados y contribuir a la mejora continua y sostenibilidad de los servicios tecnológicos de Banco Ficohsa.

Finalmente, el Capítulo VI desarrolla la aplicabilidad de la propuesta, detallando cómo COBIT 2019 e ITIL 4 pueden implementarse de manera articulada para fortalecer la gobernanza, la operación, la continuidad y la resiliencia del software de cajeros automáticos dentro del banco. Esta estructura permite comprender de forma integral la problemática, analizarla desde un enfoque técnico y metodológico, y construir una propuesta sólida para mejorar la gestión del software ATM en Banco Ficohsa, alineada a estándares internacionales y al contexto operativo de la institución.

1.2 ANTECEDENTES DEL PROBLEMA

En el ámbito global de los servicios bancarios y financieros, la gestión de riesgos en sistemas tecnológicos críticos, como el software de cajeros automáticos (ATM), se ha convertido en una prioridad estratégica. El incremento sostenido de las amenazas cibernéticas, la creciente sofisticación de los ataques y la acelerada digitalización de los procesos financieros han aumentado la vulnerabilidad de estos sistemas, afectando directamente la continuidad operativa, la seguridad de la información y la confianza de los clientes (Ojeda, Moreno, & Torres, 2020).

De acuerdo con estudios internacionales, los marcos de referencia como COBIT 2019 e ITIL 4 constituyen herramientas clave para alinear la tecnología con los objetivos de negocio, estandarizar procesos y definir métricas que favorecen la resolución rápida de incidentes y la reducción de los tiempos de recuperación (Graglia, 2024). Según De Haes et al. (2019), la gobernanza de TI se basa en estructuras y mecanismos que permiten generar valor a partir de la tecnología; en este marco, COBIT 2019 se destaca por ofrecer un enfoque integral y adaptable para fortalecer la resiliencia tecnológica en sectores críticos como el financiero.

Figura 1: *Modelo de Adopción (Mejora Continua).*

Fuente: The continual improvement model, ITIL® Foundation: ITIL ® 4 edition, Official Book

En países como Estados Unidos, Reino Unido, Singapur y Australia, los incidentes clasificados como críticos (Prioridad 1) en cajeros automáticos deben resolverse en plazos que rara vez superan las cuatro horas, garantizando el cumplimiento de los acuerdos de nivel de servicio (SLA) y evitando pérdidas financieras significativas. La aplicación de marcos internacionales ha permitido estandarizar los procesos de gestión de incidentes, establecer tiempos de respuesta y recuperación definidos, y mantener la confianza de los usuarios en los servicios automatizados (Whtiman & Mattord, 2022).

En América Latina, la modernización tecnológica ha incrementado la dependencia de canales electrónicos y de los sistemas de software bancario, lo que ha derivado en un aumento de la frecuencia y severidad de incidentes en la banca en línea, las transferencias electrónicas y las redes de cajeros automáticos (FELABAN, 2018).

En el caso de Honduras, la Comisión Nacional de Bancos y Seguros (CNBS) reporta que existen aproximadamente 3,500 cajeros automáticos en operación, de los cuales más de 500 pertenecen a Banco Ficohsa (Banco Ficohsa, 2025), lo que lo posiciona como uno de los principales proveedores de este servicio. Sin embargo, estudios recientes advierten que los tiempos promedio de recuperación de incidentes críticos en cajeros superan las 8 horas, mientras que en estándares internacionales rara vez exceden las cuatro. Además, las pérdidas anuales asociadas a fraudes y fallas tecnológicas en el sistema financiero hondureño han superado los USD 3 millones entre 2020 y 2022 (CNBS, 2021). Estos datos evidencian la magnitud del problema y la urgencia de implementar un modelo integral de análisis de riesgos y estrategias de mitigación adaptado al

contexto local.

Para Banco Ficohsa, los incidentes asociados al software que administra la red de cajeros automáticos representan riesgos operativos, estratégicos y reputacionales de gran impacto (Banco Ficohsa. 2025. Documento interno no publicado). Una interrupción del servicio, incluso de corta duración, puede generar pérdidas financieras por transacciones no procesadas, incumplimiento de SLA, sanciones regulatorias y deterioro en la percepción de seguridad de los clientes (AXELOS, 2019).

El análisis de la situación evidencia la existencia de vacíos críticos en cuatro áreas principales:

Metodológicos: Ausencia de una metodología integral y específica para el análisis de riesgos y la mitigación de incidentes en el software de cajeros automáticos.

Operativos: Deficiencias en la trazabilidad de incidentes recurrentes que impiden establecer procesos de aprendizaje y prevención efectivos.

Métricos: Falta de indicadores clave de desempeño (KPIs) que permitan monitorear de manera consistente la calidad del servicio, los tiempos de resolución y los niveles de satisfacción del cliente.

De alineación: Escasa integración de los procesos actuales con las mejores prácticas de COBIT 2019 e ITIL 4, lo que limita la capacidad de implementar un ciclo de mejora continua.

Estos vacíos no solo reflejan debilidades en la gestión actual de Banco Ficohsa, sino que justifican la necesidad de esta investigación (Banco Ficohsa 2024 Datos operativos de la red de cajeros automáticos [Comunicación personal]). En este sentido, el estudio se orienta a resolver directamente las brechas detectadas: se propone una metodología integral basada en COBIT 2019 para la gestión de riesgos, complementada con las prácticas de ITIL 4 para la gestión de incidentes y servicios; se diseñarán estrategias de mitigación que fortalezcan la operación del software de cajeros automáticos; y se definirán KPIs y métricas específicas que permitan evaluar los tiempos de recuperación, la efectividad de las respuestas y el nivel de confianza del usuario (ISACA, 2019).

De esta forma, la investigación no solo describe los problemas existentes, sino que plantea una solución concreta y contextualizada que permitirá a Banco Ficohsa optimizar la gestión de su red de cajeros automáticos, asegurar la continuidad del servicio y alinear su operación con

estándares internacionales de gobernanza y gestión de TI.

1.3 DEFINICIÓN DEL PROBLEMA

La gestión de software ATM en instituciones financieras, como Banco Ficohsa, es un área crítica de acceso a los servicios, cumplimiento de las promulgaciones regulatorias, la seguridad cibernética y la experiencia del cliente. Sin embargo, a pesar de su importancia estratégica, el banco actualmente no tiene métodos formales e integrados para identificar, evaluar y mitigar los riesgos tecnológicos relacionados con ese software. Esta deficiencia causa vulnerabilidades que pueden convertirse en términos de servicio, pérdida de datos confidencial, reputación institucional y sanciones por violaciones regulatorias.

Aunque el Banco ha adoptado el control operativo y la práctica, no se adaptan a los marcos de gestión de TI estandarizados de TI y los marcos de gestión de TI como COBIT 2019, o que incluyen sistemáticamente las mejores prácticas de ITIL 4. Limita la capacidad de la organización para tomar decisiones basadas en sus activos tecnológicos y debilita su resistencia a eventos internos o amenazas externas.

Además, el entorno dinámico y digitalizado en el sector financiero requiere una respuesta cada vez más diestra, proactiva y coordinada a los riesgos tecnológicos. A este respecto, surge la siguiente pregunta de investigación: ¿Cómo puede Banco Ficohsa diseñar e implementar una propuesta de análisis de riesgos basada en los marcos de referencia COBIT 2019 e ITIL 4 que permita identificar, evaluar y mitigar de manera efectiva los riesgos tecnológicos asociados a la gestión del software de cajeros automáticos, contribuyendo a la optimización del servicio, el cumplimiento regulatorio y el fortalecimiento de la seguridad y continuidad operativa?

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

¿Cómo puede un análisis de riesgos basado en COBIT 2019 e ITIL 4 contribuir a la formulación de estrategias de mitigación para optimizar la gestión del software de cajeros automáticos en Banco Ficohsa, garantizando continuidad operativa, seguridad y cumplimiento regulatorio?

1.4.2 PREGUNTAS ESPECÍFICAS

1. ¿Cuáles son las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software de cajeros automáticos de Banco Ficohsa, considerando los procesos, métricas

y prácticas vigentes?

2. ¿Cómo se pueden adaptar y aplicar los principios y prácticas de COBIT 2019 e ITIL 4 para el análisis de riesgos y gestión de incidentes en el contexto específico del software de cajeros automáticos de Banco Ficohsa?

3. ¿Qué indicadores clave de desempeño (KPIs) y métricas de seguimiento permitirán evaluar la efectividad de las estrategias de mitigación propuestas y fomentar un ciclo de mejora continua?

4. ¿Cómo puede diseñarse un modelo de optimización que integre COBIT 2019 e ITIL 4 para fortalecer la gestión del software de cajeros automáticos y responder a los requisitos del entorno financiero actual?

5. ¿Qué beneficios obtendrá Banco Ficohsa a futuro al aplicar la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4 para optimizar la gestión del software de cajeros automáticos?

1.5 OBJETIVOS DEL PROYECTO

1.5.1 OBJETIVO GENERAL

Desarrollar un análisis de riesgos basado en COBIT 2019 e ITIL 4 para proponer estrategias de mitigación en la gestión de software de cajeros automáticos optimizando la continuidad del servicio, asegurando el cumplimiento normativo y fortaleciendo la resiliencia operativa en Banco Ficohsa.

1.5.2 OBJETIVOS ESPECÍFICOS

1. Identificar las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software de cajeros automáticos de Banco Ficohsa, considerando los procesos, métricas y prácticas vigentes.

2. Evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 al análisis de riesgos y gestión de incidentes en el software de cajeros automáticos de Banco Ficohsa, con el fin de proponer acciones de mejora.

3. Definir indicadores clave de desempeño (KPIs) y métricas de seguimiento que permitan evaluar la efectividad de las estrategias de mitigación propuestas y fomenten un ciclo de mejora continua en la gestión del software de cajeros automáticos.

4. Diseñar un modelo integrado de gestión basado en COBIT 2019 e ITIL 4 que fortalezca la administración del software de cajeros automáticos y responda de manera efectiva a los requisitos del entorno financiero actual.

5. Identificar los beneficios que Banco Ficohsa podría obtener a futuro al implementar la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4 para la optimización del software de cajeros automáticos.

1.6 JUSTIFICACIÓN

El presente estudio responde a una necesidad crítica del sector financiero: fortalecer la gestión de riesgos tecnológicos asociados al software que opera los cajeros automáticos (ATM), un canal de autoservicio fundamental para la operación bancaria, la continuidad del negocio y la experiencia del cliente. Estos sistemas no solo procesan transacciones esenciales, sino que también son altamente sensibles a fallos operativos, vulnerabilidades de seguridad y eventos que pueden comprometer la disponibilidad del servicio. En el caso de Banco Ficohsa, cuya estrategia institucional se sustenta en la eficiencia operativa, el cumplimiento regulatorio y la satisfacción del usuario, la ausencia de un marco metodológico estructurado y alineado a estándares internacionales representa una brecha significativa con impacto directo en la resiliencia tecnológica.

Desde el punto de vista teórico, esta investigación se fundamenta en los marcos COBIT 2019 e ITIL 4, ampliamente reconocidos por su capacidad para orientar la gobernanza, la gestión y la mejora continua de los servicios de TI. COBIT 2019, desarrollado por ISACA, proporciona un sistema holístico basado en principios, componentes y objetivos de gobernanza que permiten alinear la tecnología con los objetivos estratégicos, controlar el rendimiento de los servicios y reducir los riesgos tecnológicos de manera estructurada. Por su parte, ITIL 4 ofrece un enfoque práctico orientado al valor, centrado en la experiencia del cliente, la continuidad del servicio y la colaboración entre equipos técnicos y de negocio.

La complementariedad de ambos marcos resulta especialmente pertinente para la gestión del software ATM. Mientras COBIT 2019 establece las directrices, roles y procesos necesarios para la toma de decisiones informada y el control de riesgos, ITIL 4 proporciona las prácticas operativas necesarias para asegurar la disponibilidad, confiabilidad y calidad del servicio. Su integración dentro de una propuesta metodológica adaptada al contexto de Banco Ficohsa permite

abordar el problema desde una perspectiva estratégica y operativa al mismo tiempo.

Este estudio adquiere mayor relevancia considerando que, en Honduras, no existe una metodología pública o institucional específicamente orientada al análisis de riesgos en redes de cajeros automáticos, ni un modelo que combine de forma funcional los marcos COBIT 2019 e ITIL 4 en aplicaciones críticas. Por ello, la presente investigación llena un vacío importante al proponer un enfoque que facilita identificar riesgos tecnológicos específicos, priorizarlos según su impacto y probabilidad, y definir estrategias de mitigación implementables por las áreas técnicas del banco.

Asimismo, el trabajo se justifica por las crecientes amenazas tecnológicas y regulatorias que enfrentan las instituciones financieras en la región. La transformación digital, si bien ofrece beneficios operativos, también incrementa la exposición al ciberdelito, los incidentes de indisponibilidad y las exigencias de auditoría interna y externa. En este entorno, contar con una metodología sólida permite responder oportunamente a los eventos, mantener los niveles aceptables de servicio y cumplir con los estándares regulatorios y competitivos que exige el sector.

Finalmente, la viabilidad de esta propuesta se sustenta en la disponibilidad de marcos robustos, flexibles y personalizables como COBIT 2019 e ITIL 4, así como en la capacidad técnica interna de Banco Ficohsa para validar, adaptar e implementar las recomendaciones derivadas del presente estudio.

CAPÍTULO II. MARCO TEÓRICO

2.1 MACROENTORNO

2.1.1 MERCADO E INDUSTRIA DE CAJEROS AUTOMÁTICOS Y SOFTWARE BANCARIO A NIVEL GLOBAL

El mercado global de software para cajeros automáticos (ATM) se encuentra en una fase de crecimiento sostenido, impulsado por la necesidad de ofrecer soluciones que no solo sean más seguras y eficientes, sino que también se adapten a las crecientes demandas de los clientes en un ecosistema financiero cada vez más digital. Los ATMs han trascendido su función original como simples dispensadores de efectivo para convertirse en terminales multifuncionales que facilitan pagos, transferencias y otros servicios personalizados, reflejando la transformación digital del sector (Alonge, Eyo, & Ubanadu, 2021).

En esta dinámica, el segmento de cajeros multifuncionales es líder en innovación, mientras que las soluciones de seguridad informática han escalado para convertirse en las áreas de mayor inversión, debido al persistente y creciente aumento de los fraudes y ataques cibernéticos Regionalmente, aunque América del Norte mantiene su dominio gracias a su avanzada infraestructura, regiones como Asia-Pacífico exhiben un crecimiento acelerado en la instalación de nuevas unidades, con potencias como Estados Unidos y China impulsando la adopción e innovación tecnológica. En términos de volumen, el mercado global de ATMs se valoró en USD 25.29 mil millones en 2024, con una proyección de alcanzar los USD 31.64 mil millones para 2030, lo que confirma su relevancia crítica dentro de la infraestructura financiera mundial (Alonge, Eyo, & Ubanadu, 2021).

El desafío más acuciante a nivel internacional es la ciberseguridad bancaria. Los reportes especializados evidencian un crecimiento constante de los fraudes en ATMs a través de malware especializado, ataques de jackpotting (vaciamiento de efectivo) y skimming (captura de datos), con pérdidas millonarias registradas en regiones como Europa. Estos incidentes subrayan la necesidad urgente de fortalecer las defensas de las redes de cajeros e implementar estrategias más robustas de gestión de incidentes y continuidad operativa. Al mismo tiempo, el mercado experimenta una profunda transformación tecnológica, evidenciada en mercados líderes como México y Colombia (Vergara & Diao, 2024).

Estas naciones se han posicionado a la vanguardia mediante la adopción de tecnologías disruptivas como el software multivendor, que permite gestionar cajeros de diferentes fabricantes desde una única plataforma; la biometría para una autenticación más segura; y las transacciones sin tarjeta física a través de tecnologías como NFC o códigos QR, conocidas como el "pre-stage" de transacciones. Además, la búsqueda de eficiencia operativa ha impulsado el desarrollo de la tecnología de cajeros recicladores, donde el mismo efectivo recibido en depósitos es utilizado para entregas, optimizando el manejo de efectivo y explorando la efectividad económica del canal (Vergara & Diao, 2024).

Frente a estos riesgos y tendencias de innovación, la comunidad internacional ha formalizado un marco regulatorio estricto. Se han adoptado estándares esenciales como ISO/IEC 27001 para la gestión de la seguridad de la información, PCI DSS para la protección de transacciones electrónicas, y los lineamientos de Basilea III/IV para la gestión de riesgos financieros. En Europa, directivas como NIS2 y PSD2 establecen regulaciones para la ciberseguridad y los pagos digitales. Incluso en regiones donde el uso de efectivo ha disminuido, los gobiernos han reforzado las regulaciones para garantizar el acceso al efectivo, subrayando la importancia estratégica de proteger la infraestructura de cajeros (Valora Analitik, 2024).

Este entorno de alta volatilidad y exigencia regulatoria ha consolidado el rol estratégico de los marcos de referencia de TI. COBIT 2019 se posiciona como el modelo integral de gobernanza de TI que facilita la alineación entre la estrategia tecnológica y los objetivos de negocio. Complementariamente, ITIL 4 aporta las directrices para la gestión de servicios, con un enfoque primordial en la disponibilidad, la continuidad y la experiencia del cliente. La integración de estos marcos, junto con otros como NIST Cybersecurity Framework, se vuelve esencial para que las instituciones financieras, incluyendo Banco Ficohsa, garanticen la resiliencia tecnológica y la seguridad de sus operaciones críticas ante la dinámica global (Valora Analitik, 2024).

2.1.1.1 TENDENCIAS CLAVE EN EL SOFTWARE BANCARIO

La industria bancaria está experimentando una rápida evolución para satisfacer las nuevas expectativas de los consumidores, quienes exigen servicios más rápidos, seguros y convenientes. Esta transformación está siendo impulsada por diversas tendencias tecnológicas. Por un lado, el auge de las super aplicaciones y las opciones de pago flexible, como "Comprar Ahora, Pagar Después" (BNPL), están revolucionando el mercado minorista, lo que obliga al software bancario

a ofrecer soluciones integradas y fluidas. Concomitantemente, las instituciones financieras están migrando a la nube y utilizando las APIs (Interfaces de Programación de Aplicaciones) para modernizar su infraestructura, logrando ser más ágiles y escalables, con un 68% de los bancos ya monetizando el desarrollo de dichas APIs (Gaol, Prabowo, & Purwandari, 2022).

Por otro lado, la implementación de la Inteligencia Artificial (IA) y el Aprendizaje Automático (ML) se ha vuelto esencial, ya que estas tecnologías se utilizan para predecir las necesidades del cliente, optimizar procesos de toma de decisiones y, crucialmente, reforzar los sistemas de seguridad y detección de fraude. De hecho, ante el incremento de las ciber amenazas, la ciberseguridad y el cumplimiento normativo se han consolidado como prioridades absolutas, impulsando la inversión en software para proteger los datos sensibles y reducir los riesgos (Gaol, Prabowo, & Purwandari, 2022).

El mercado del software financiero personalizado ha crecido significativamente gracias al auge de los startups Fintech, que han capitalizado las deficiencias históricas de la banca tradicional. La inclinación de los usuarios hacia las Fintech se debe, en gran medida, a que los bancos tradicionales a menudo operan con sistemas heredados obsoletos que son inherentemente lentos, ineficientes y difíciles de integrar con las innovaciones modernas. Además, el carácter conservador y la aversión al riesgo de los grandes bancos resultan en una lenta adopción de nuevas tecnologías, dejándolos rezagados en un mercado que evoluciona rápidamente. Esta situación se agrava por la experiencia de usuario (UX) deficiente de muchas aplicaciones bancarias tradicionales, un área en la que las Fintech han sobresalido, priorizando la facilidad y la intuición en sus interfaces (Gutiérrez, 2023).

La inversión estratégica en nuevas soluciones de software bancario ofrece múltiples beneficios. En primer lugar, se traduce en una notable eficiencia operativa y ahorro de costos. Por ejemplo, se estima que las monedas digitales de los bancos centrales podrían reducir los costos de transacción empresariales en casi 100 mil millones de dólares anuales. En segundo lugar, las soluciones digitales son un motor directo para el crecimiento de ingresos y la expansión de la base de clientes, evidenciado por el aumento global en la tasa de adopción de Fintech, que pasó del 16% en 2015 al 64% en 2019. Por último, el uso de IA y el análisis de datos proporciona un enfoque más inteligente para la mitigación de riesgos y la detección de fraudes, lo que no solo fortalece la seguridad, sino que también promete generar ahorros de hasta un billón de dólares para 2030,

incrementando la rentabilidad y la robustez del negocio (Gutiérrez, 2023).

2.1.1.2 TIPOS DE SOFTWARE BANCARIO PERSONALIZADO

El desarrollo de software bancario personalizado comprende una amplia gama de soluciones que responden a las necesidades operativas y estratégicas de las instituciones financieras. Uno de los componentes más relevantes son los Sistemas Bancarios Centrales (CBS), los cuales constituyen la infraestructura principal del banco al gestionar cuentas, transacciones y el registro contable que soporta todas las operaciones esenciales (IFC, 2020).

Otro tipo de software ampliamente utilizado son las plataformas de banca en línea y móvil. Estas soluciones permiten a los usuarios realizar operaciones financieras desde cualquier lugar, aprovechando arquitecturas de microservicios y enfoques orientados a mejorar la experiencia del cliente. Su importancia radica en la creciente demanda de servicios remotos, ágiles y accesibles (IFC, 2020).

Las pasarelas de pago también forman parte del ecosistema tecnológico del sector bancario. Este tipo de software actúa como intermediario entre los clientes, los comercios y las entidades financieras, garantizando que los pagos electrónicos se procesen de forma rápida y segura. Su uso se ha incrementado debido al crecimiento del comercio digital y las transacciones electrónicas (IFC, 2020).

Asimismo, el software de gestión de relaciones con clientes (CRM) se ha convertido en una herramienta clave para fortalecer los vínculos con los usuarios. Estos sistemas integran capacidades de análisis de datos e inteligencia artificial que permiten personalizar las interacciones, anticipar necesidades y optimizar los procesos comerciales del banco (Ortega, Ramírez, & Zúgiña, 2022).

Finalmente, los bancos recurren a plataformas de análisis avanzado para examinar grandes volúmenes de datos y generar información valiosa para la toma de decisiones. Estas herramientas facilitan la identificación de tendencias, la evaluación del comportamiento del mercado y la proyección de escenarios que apoyan la planificación estratégica (Ortega, Ramírez, & Zúgiña, 2022).

En conjunto, estos tipos de software muestran que la inversión en soluciones tecnológicas a medida no es simplemente una opción, sino una decisión esencial para competir en un entorno

financiero dinámico donde la agilidad, la seguridad y la experiencia del usuario determinan la sostenibilidad y el éxito institucional (Ortega, Ramírez, & Zúgiña, 2022).

2.1.2 ENTORNO ECONÓMICO Y DE SERVICIOS FINANCIEROS INTERNACIONALES

El mercado de software bancario está siendo moldeado por las demandas de los consumidores de servicios más rápidos, seguros y convenientes, una tendencia que se refleja en la evolución de los ATMs. La innovación tecnológica está dominada por el auge de las superaplicaciones y las nuevas opciones de pago, obligando al software bancario a ofrecer soluciones integradas. Las instituciones financieras están migrando masivamente a la nube y adoptando APIs para modernizar su infraestructura y mejorar su agilidad, mientras que la Inteligencia Artificial (IA) y el Aprendizaje Automático (ML) son tecnologías cruciales para la detección de fraudes, la optimización de precios y la automatización de procesos clave (Muñiz, Loor, & Cedeño, 2021).

Este dinamismo, sin embargo, se enfrenta al desafío de los sistemas heredados obsoletos de la banca tradicional, cuya aversión al riesgo y deficiente experiencia de usuario han sido capitalizadas por las Fintech. La inversión en nuevo software se justifica plenamente al ofrecer eficiencia operativa y un potencial de ahorro de costos de hasta 100 mil millones de dólares anuales a través de la digitalización, además de mejorar la mitigación de riesgos gracias a la IA, lo que podría generar ahorros por un billón de dólares para 2030 (Muñiz, Loor, & Cedeño, 2021).

A nivel regional, el mercado de servicios administrados por ATMs en América presenta un crecimiento sostenido, impulsado por la expansión de redes, la modernización tecnológica y la creciente subcontratación de operaciones por parte de bancos para reducir costos. Estados Unidos lidera la región, con grandes alianzas estratégicas para instalar cajeros fuera de las sucursales, como la de 7-Eleven y NCR Atleos Corp, reforzando la tendencia a la externalización de la gestión y el mantenimiento (Wolrd Bank , 2020).

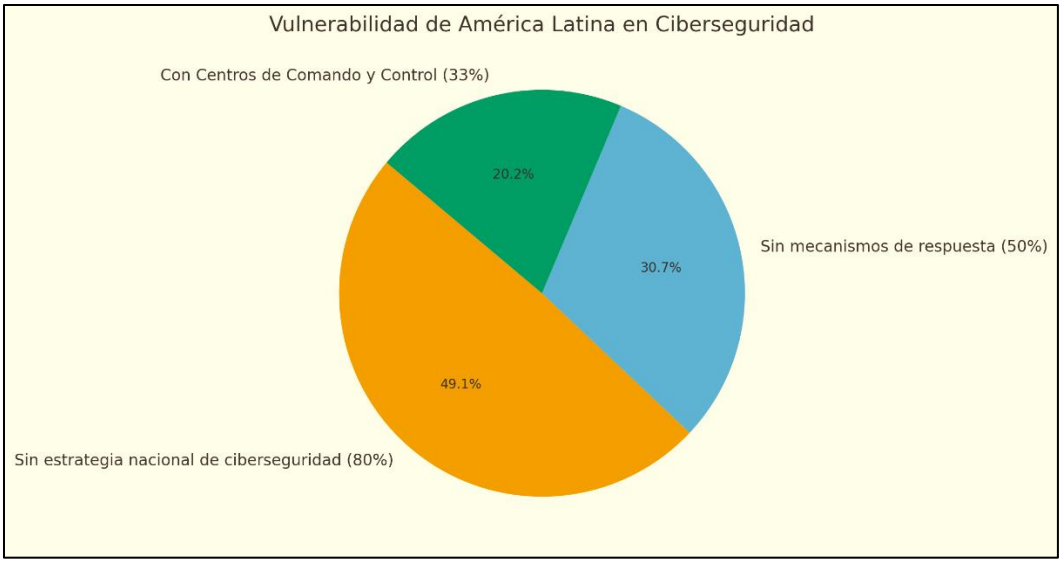
Paralelamente, en América del Sur, países como Brasil, Chile y Argentina impulsan el mercado mediante la inclusión financiera y la adopción de tecnologías emergentes como IoT y Blockchain. A pesar de la restricción que impone el auge de los pagos digitales y las billeteras móviles, el desarrollo de cajeros multifuncionales e inteligentes con servicios avanzados (retiro sin tarjeta, pagos de facturas y biometría) sigue abriendo nuevas oportunidades, consolidando la

gestión de ATMs como un componente estratégico de la banca moderna (Wolrd Bank , 2020).

No obstante, el principal factor de riesgo en el macroentorno es la ciberseguridad. La incidencia del ciberdelito en el sector financiero representa un costo económico de magnitud global, con pérdidas anuales estimadas en 400.000 millones de dólares y que ascendieron a 575.000 millones de dólares en años recientes. América Latina ha sido particularmente afectada, registrando pérdidas de 90.000 millones de dólares. El sector bancario sufre el impacto directo de esta amenaza; por ejemplo, el malware LOTA ha causado pérdidas de hasta 450 millones de dólares en un solo banco global, con un promedio de 50.000 dólares por ATM atacado exitosamente (Wolrd Bank , 2020).

Estos incidentes amplifican la vulnerabilidad, especialmente en países con limitada capacidad de respuesta, lo que obliga a las entidades a destinar recursos significativos a la prevención, monitoreo y recuperación. En respuesta a estos desafíos, la comunidad internacional ha adoptado estándares rigurosos como ISO/IEC 27001, PCI DSS y los lineamientos de Basilea III/IV. A nivel metodológico, COBIT 2019 e ITIL 4 han adquirido un rol estratégico para gestionar estos riesgos, facilitando la alineación tecnológica con los objetivos de negocio y mejorando la disponibilidad, continuidad y experiencia del cliente (Wolrd Bank , 2020).

Figura 2: *Vulnerabilidad en ciberseguridad de América Latina.*



Fuente: Representación de las principales debilidades de ciberseguridad en el sistema bancario del continente americano.

2.1.3 TRANSFORMACIÓN DIGITAL Y TENDENCIAS TECNOLÓGICAS GLOBALES EN BANCA

En los últimos años se presenta la banca digital como una fuerza disruptiva que está transformando radicalmente el panorama monetario a nivel mundial. Este fenómeno no se limita a la simple transferencia de servicios físicos al ámbito online, sino que implica una reestructuración profunda del modelo de negocio bancario y una redefinición completa de la experiencia ofrecida al cliente. La esencia de esta tendencia radica en la capacidad de la tecnología para generar valor y eficiencia, obligando a las instituciones financieras tradicionales a adaptarse para evitar la obsolescencia (Nwoke, 2024).

El núcleo impulsor de esta macrotendencia es la innovación tecnológica y la automatización de procesos. Se observa una implementación creciente de tecnologías avanzadas como la Automatización Robótica de Procesos (RPA), la cual, junto con el desarrollo de aplicaciones móviles robustas, se convierte en el cimiento para crear soluciones de software ajustadas a las necesidades específicas de cada negocio. Estos avances están orientados a optimizar las operaciones internas, reducir significativamente los costos operativos y mejorar la eficiencia general, permitiendo a las entidades financieras ofrecer servicios con mayor agilidad (Nwoke, 2024).

Un pilar fundamental de la banca digital es el enfoque centrado en el cliente. La migración de servicios busca ofrecer conveniencia, rapidez y accesibilidad sin precedentes. Los servicios clave que sustentan esta promesa incluyen las Firmas Digitales, los sistemas ERP adaptados y las Aplicaciones Móviles. Estos elementos permiten a los usuarios gestionar sus finanzas de manera integral y segura desde cualquier lugar y en cualquier momento, promoviendo una gestión financiera más fluida e integrada y redefiniendo el valor que el cliente espera recibir de su banco (Vargas, 2021).

Aunque la tendencia se caracteriza por sus beneficios en eficiencia y experiencia de usuario, la adopción de la banca digital plantea desafíos críticos, especialmente en materia de seguridad y riesgo. La mención de la Política de seguridad como un recurso corporativo subraya la importancia ineludible de la seguridad de la información y la privacidad de los datos. En este entorno digitalizado, la gestión eficaz de los riesgos cibernéticos es un componente inseparable de la estrategia de cualquier institución que busque capitalizar el potencial de la banca digital (Vargas, 2021).

Figura 3: *Banca móvil personalizada con IA generativa.*

Fuente: Rootstack, 2025, servicios que marcarán la pauta en 2026

2.1.3.1 TRANSFORMACIÓN DIGITAL EN EL SECTOR FINANCIERO

La transformación digital en el sector financiero ha impulsado la modernización acelerada del software que opera los cajeros automáticos, incorporando capacidades de automatización que permiten optimizar procesos y reducir la intervención manual. Los ATMs actuales utilizan motores transaccionales más eficientes, sistemas de autodiagnóstico, actualizaciones remotas y mecanismos de monitoreo en tiempo real que facilitan la detección de fallos, la gestión de incidentes y la continuidad del servicio. Estas mejoras aumentan la disponibilidad operativa y permiten que las instituciones financieras reduzcan costos, agilicen la gestión de su red de dispositivos y fortalezcan la experiencia del usuario (Dapp, 2022).

Al mismo tiempo, los cajeros automáticos han evolucionado hacia modelos de multicanalidad, integrándose con plataformas digitales del banco para ofrecer una experiencia coherente en todos los puntos de contacto. El software ATM ya no funciona como un sistema aislado, sino como una extensión del ecosistema digital, permitiendo consultas, transferencias, actualizaciones de seguridad y funcionalidades alineadas a la banca móvil y la banca en línea. Esta convergencia facilita que los clientes utilicen múltiples canales de forma fluida y que el banco gestione servicios unificados bajo modelos de arquitectura moderna, como API banking y microservicios (Dapp, 2022).

Además, la integración con la banca móvil se ha convertido en uno de los avances más

relevantes, impulsada por el incremento del uso de smartphones y la preferencia por servicios financieros inmediatos. Funciones como retiros sin tarjeta, autenticación biométrica, generación de códigos dinámicos y validación mediante aplicaciones móviles han transformado la operación tradicional de los cajeros automáticos. Esta integración no solo incrementa la seguridad, al reducir la dependencia de tarjetas físicas, sino que también amplía las capacidades del ATM como canal digital, habilitando transacciones más ágiles, seguras y alineadas con las expectativas de los clientes modernos (Dapp, 2022).

2.1.3.2 CIBERSEGURIDAD BANCARIA A NIVEL MUNDIAL

La ciberseguridad se ha convertido en uno de los principales focos de preocupación para el sector bancario a nivel global. El volumen de ataques no solo ha aumentado, también lo ha hecho su complejidad, impulsado por tecnologías como la inteligencia artificial y nuevas tácticas como el phishing avanzado o el vishing (Wolrd Bank , 2020).

Tabla 1: *Ciberseguridad en el Sector Financiero*

Región	Principal Riesgo e Incidencia	Datos Clave de Ataques e Inversión
Europa	La ciberseguridad es el principal riesgo percibido por el 82% de los directores de Riesgo.	El 34% de los ciudadanos ha sido víctima de amenazas cibernéticas, siendo el *phishing* la modalidad más común, afectando al 26% de los encuestados.
América Latina	Las instituciones financieras son 300 veces más propensas a sufrir ciberataques que otros sectores.	La inversión media anual en ciberseguridad es de USD 18.5 millones, lo que representa un 40% más que en otras industrias.
Estados Unidos	Aumento de ataques cibernéticos destructivos en el sector financiero.	El 71% de las instituciones financieras experimentó un aumento en los ataques destructivos. Se registraron más de 4.480 intrusiones interactivas en 2024, con el 79% de los ataques siendo "malware-free" (basados en abuso de credenciales o ingeniería social).

Fuente: resume los datos clave sobre el riesgo de ciberseguridad en las instituciones financieras de Europa, América Latina y Estados Unidos.

Estrategias clave para fortalecer la ciberseguridad bancaria:

Las estrategias clave para fortalecer la ciberseguridad bancaria se centran en un enfoque integral que combina tecnología avanzada, vigilancia constante, desarrollo de talento humano y

colaboración externa. En primer lugar, es crucial adoptar la autenticación multifactorial y la biometría. Esto implica el uso de varias formas de verificación para proteger el acceso a los servicios digitales, incluyendo sistemas biométricos y modelos como KYC (Know Your Customer), que ayudan a prevenir fraudes por suplantación de identidad. Esta práctica incrementa significativamente la seguridad sin comprometer en exceso la experiencia del usuario (Wolrd Bank , 2020).

Una segunda estrategia vital es la monitorización continua y el análisis en tiempo real. A través de algoritmos de aprendizaje automático, las instituciones deben supervisar constantemente las transacciones para detectar patrones sospechosos. Esto permite identificar amenazas de forma inmediata, reduciendo la ventana de oportunidad de los atacantes y reforzando la confianza en los canales digitales al actuar antes de que el fraude se materialice (Yarosh, 2023).

La tercera área de enfoque es la formación interna y la cultura de seguridad. La capacitación continua del personal es esencial para que reconozcan técnicas de manipulación comunes como el phishing o la ingeniería social. El objetivo es crear una conciencia de que la ciberseguridad es una responsabilidad compartida por toda la organización, garantizando que existan procedimientos claros para una respuesta rápida y coordinada ante cualquier amenaza (Yarosh, 2023).

En cuanto a la colaboración con organismos y alianzas estratégicas; es imperativo que los bancos trabajen juntamente con proveedores de tecnología, Fintechs, organismos reguladores y redes sectoriales. Esta cooperación permite compartir información y mejores prácticas, facilitando la anticipación a amenazas emergentes, la alineación de estrategias con regulaciones futuras como PSD3 y el fomento de un entorno de protección integral frente a riesgos compartidos (Yarosh, 2023).

2.1.4 ENTORNO REGULATORIO Y MARCOS DE REFERENCIA DE TI A NIVEL INTERNACIONAL

2.1.4.1 NORMATIVAS Y ESTÁNDARES INTERNACIONALES RELEVANTES

ISO/IEC 27001 (gestión de seguridad de la información).

La norma ISO/IEC 27001 es el estándar internacional para la gestión de la seguridad de la información. Su objetivo es proporcionar un marco de trabajo para que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) (NQA, 2024).

Este estándar ayuda a proteger la información crítica de una empresa mediante un enfoque sistemático basado en la gestión de riesgos, asegurando la confidencialidad, integridad y disponibilidad de los datos (NQA, 2024).

Los tres pilares de la seguridad de la información.

La ISO 27001 se basa en los siguientes principios para salvaguardar los activos de información:

- Confidencialidad: Asegura que la información solo sea accesible para las personas autorizadas.
- Integridad: Protege la exactitud y exhaustividad de la información y sus métodos de procesamiento.
- Disponibilidad: Garantiza que la información esté disponible y accesible para los usuarios autorizados cuando sea necesario.

PCI DSS (seguridad en transacciones electrónicas).

El Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS, por sus siglas en inglés) es un conjunto de requisitos diseñados para proteger la información de los titulares de tarjetas durante su almacenamiento, procesamiento y transmisión (Josepht & Fred, 2025).

Objetivos del Estándar PCI DSS para la Protección de Datos

El objetivo principal de PCI DSS es prevenir el fraude y el robo de datos de tarjetas, estableciendo un marco de buenas prácticas que todas las empresas que manejan transacciones con tarjetas deben seguir (Josepht & Fred, 2025).

El estándar PCI DSS (Payment Card Industry Data Security Standard) se estructura en torno a seis metas principales que, al ser implementadas, aseguran la protección de la información de los titulares de tarjetas, y es de obligatorio cumplimiento para toda organización que procese, almacene o transmita datos de tarjetas de crédito o débito (Josepht & Fred, 2025).

Las primeras dos metas se centran en la protección de la infraestructura y los datos. Esto exige construir y mantener una red y sistemas seguros mediante la instalación de firewalls y la prohibición del uso de contraseñas o parámetros de seguridad predeterminados del proveedor. Además, se debe proteger los datos del titular de la tarjeta cifrando la información de la cuenta

cuando está almacenada y durante su transmisión a través de redes públicas abiertas (Josepht & Fred, 2025).

La tercera meta se enfoca en la gestión proactiva de riesgos, que implica mantener un programa de gestión de vulnerabilidades. Esto incluye la protección constante de los sistemas contra malware, la actualización regular de los programas antivirus y el desarrollo y mantenimiento de aplicaciones y sistemas seguros para prevenir explotaciones (Josepht & Fred, 2025).

Las siguientes dos metas abordan el control estricto de accesos y la supervisión. Se deben implementar medidas sólidas de control de acceso para restringir la disponibilidad de los datos sensibles solo al personal que estrictamente lo requiera para su trabajo, asegurando que cada persona posea un identificador único, y limitando también el acceso físico a los datos y sistemas críticos. Complementariamente, es esencial supervisar y probar las redes con regularidad, rastreando y auditando todo el acceso a los recursos de la red y a los datos de los titulares de tarjetas, además de probar regularmente los sistemas y procesos de seguridad para verificar su efectividad (Josepht & Fred, 2025).

La sexta meta requiere mantener una política de seguridad de la información integral para todo el personal. El nivel de cumplimiento requerido varía para cada organización según el volumen anual de transacciones que procese (Josepht & Fred, 2025).

Tabla 2: *Marcos Regulatorios Internacionales: Basilea III/IV*

Marco Regulatorio	Foco Principal	Objetivos y Cambios Clave
Basilea III	Mejorar la calidad y cantidad de capital y liquidez de los bancos.	Publicado tras la crisis de 2008. Buscó aumentar la capacidad de los bancos para absorber pérdidas, reforzar la supervisión y la gestión de riesgos en todo el sector, y reducir el efecto procíclico del sistema financiero.
Basilea IV (Finalización de Basilea III)	Reducir la variabilidad y mejorar la comparabilidad en la medición de las posiciones de riesgo (Activos Ponderados por Riesgo - APR).	Riesgo de Crédito: Restringe el uso de modelos internos avanzados. Riesgo de Mercado: Reemplaza el Valor en Riesgo (VaR) por el Déficit Esperado (ES). Riesgo Operacional: Reemplaza modelos internos por un enfoque estandarizado único basado en la rentabilidad de la institución. Límite de Salida (*Output Floor*): Establece que los APR calculados con modelos internos no pueden ser inferiores al 72.5% del valor calculado con el enfoque estándar.

Fuente: Basilea III/IV (Gestión de Riesgos Financieros): Basilea IV no es un acuerdo nuevo, sino

la finalización de Basilea III, cuyo objetivo es reforzar la estabilidad bancaria al reducir la variabilidad en el cálculo del riesgo y establecer un umbral mínimo (Output Floor) para los requisitos de capital.

Directivas europeas sobre ciberseguridad (NIS2) y pagos digitales (PSD2)

El marco regulatorio de la Unión Europea aborda la ciberseguridad y los pagos digitales a través de dos directivas fundamentales. Por un lado, la Directiva NIS2 se ha establecido como la legislación clave para asegurar un nivel común y elevado de ciberseguridad en todos los Estados miembros, expandiendo significativamente su alcance para proteger sectores críticos e importantes, como la banca, las infraestructuras del mercado financiero, la energía y los servicios digitales. Esta directiva obliga a las entidades afectadas a implementar rigurosas medidas de gestión de riesgos técnicos y organizacionales, incluyendo la seguridad de la cadena de suministro y el uso de cifrado, y exige la notificación de incidentes significativos a las autoridades competentes en un plazo de 24 horas. El incumplimiento de esta normativa conlleva la posibilidad de imponer sanciones elevadas, que pueden ascender hasta 10 millones de euros o el 2 % de la facturación anual global (Comisión Europea, 2025).

De manera complementaria, la Directiva PSD2 se enfoca en la regulación de los servicios de pago y el dinero electrónico, con el objetivo de promover la competencia, la innovación y, fundamentalmente, aumentar la seguridad en las transacciones en línea para reducir el fraude. Su característica central es la implementación de la Autenticación Reforzada de Cliente (SCA), la cual exige una autenticación multifactorial con al menos dos elementos independientes para verificar la identidad del usuario en los pagos electrónicos. Adicionalmente, la PSD2 impulsó la Banca Abierta (Open Banking), permitiendo a través de APIs seguras la creación de nuevos servicios como los de iniciación de pagos e información de cuentas (PIS y AIS), lo que otorga a los consumidores un mayor control sobre sus datos financieros y prohíbe a los comerciantes imponer recargos adicionales por el uso de tarjetas de crédito o débito (Comisión Europea, 2025).

2.1.4.2 MARCOS DE REFERENCIA DE TI A NIVEL GLOBAL

COBIT 2019: gobierno y gestión de ti en organizaciones financieras.

COBIT (Control Objectives for Information and related Technology) es un marco de referencia desarrollado por ISACA (Information Systems Audit and Control Association) que promueve la gobernanza transparente, eficiente y segura de los sistemas de TI, siendo fundamental

para profesionales y auditores de TI. La versión COBIT 2019 ofrece una guía exhaustiva para alinear los objetivos de TI con los del negocio, optimizando los recursos y gestionando los riesgos (Ilori, Naiho, & Nwosu, 2024).

En el sector financiero, COBIT 2019 es particularmente relevante para establecer un marco de gobierno de TI orientado a la ciberseguridad que fomente la confianza y la credibilidad de los clientes, y que ayude a cumplir con estrictos requisitos normativos y de cumplimiento (Ilori, Naiho, & Nwosu, 2024).

COBIT 2019 se basa en seis principios clave para un sistema de gobierno efectivo:

1. Satisfacer las Necesidades de las Partes Interesadas: El sistema de gobierno debe considerar las necesidades y prioridades de la alta dirección, clientes, reguladores, etc.
2. Cubrir la Empresa de Extremo a Extremo: No se limita solo al departamento de TI, sino que abarca toda la información y tecnología, sin importar dónde residan.
3. Aplicar un Marco Integrado Único: Debe ser un marco coherente y unificado para la gobernanza de TI, evitando duplicidades.
4. Habilitar un Enfoque Holístico: El gobierno requiere un enfoque sistémico que considere los diversos componentes (procesos, estructuras organizacionales, información, cultura, etc.) como interdependientes.
5. Separar la Dirección de la Gestión: Distingue claramente entre las actividades de Gobierno (Evaluar, Dirigir, Monitorizar - EDM) y las actividades de Gestión (Planificar, Construir, Ejecutar, Monitorizar - PCEM/APO, BAI, DSS, MEA).
6. Diseñar un Sistema de Gobierno Adaptado: Permite a la organización personalizar su sistema de gobierno usando "Factores de Diseño" (como estrategia empresarial, perfil de riesgos, requisitos regulatorios, etc.). (Villamizar, 2023)

COBIT 2019 estructura sus 40 Objetivos de Gobierno y Gestión en cinco dominios principales:

Tabla 3: *Dominios de COBIT 2019*

Dominio	Acrónimo	Propósito Principal
Gobernar (Evaluar, Dirigir y Monitorizar)	EDM	La junta directiva o cuerpo de gobierno Evalúa las opciones estratégicas, Dirige la alta gerencia

		sobre las opciones elegidas y Monitoriza el rendimiento.
Alinear, Planificar y Organizar	APO	Se centra en la estrategia, la arquitectura, la innovación y la Gestión de Riesgos de TI (APO12) y la Seguridad de la Información (APO13).
Construir, Adquirir e Implementar	BAI	Trata la definición y gestión de programas, la Gestión del Cambio Organizacional (BAI02) y la Administración de Cambios en sistemas (BAI06).
Entregar, Dar Servicio y Soporte	DSS	Se enfoca en las operaciones diarias, la Gestión de la Seguridad de los Servicios (DSS05), las operaciones y la Gestión de Incidentes (DSS02).
Monitorizar, Evaluar y Valorar	MEA	Se ocupa de la Evaluación del Cumplimiento (MEA01) y el rendimiento, asegurando que los controles internos son efectivos.

Fuente: Universidad de San Luis Potosí. 2023.

COBIT es particularmente fuerte en Gobernanza de Riesgos y Cumplimiento. Los procesos clave como EDM03 (Asegurar la optimización del riesgo), APO12 (Gestionar el riesgo) y APO13 (Gestionar la seguridad), junto con la cascada de metas, permiten a las organizaciones, especialmente en el sector financiero o regulado, traducir los requisitos regulatorios en prácticas de TI medibles y controlables, protegiendo la información y los activos (Ilori, Naiho, & Nwosu, 2024).

ITIL 4: Gestión de servicios de TI enfocados en disponibilidad, continuidad y experiencia del cliente.

ITIL 4 (Information Technology Infrastructure Library) es un marco de gestión de servicios de TI (ITSM) que adopta un enfoque más integral y adaptable, orientado a la creación de valor (Gil, Gamboa, & De los Santos, 2025).

Se enfoca en:

- Experiencia del cliente: Hace hincapié en el principio rector de "Centrarse en el valor," buscando comprender y satisfacer las necesidades del cliente.
- Disponibilidad y Continuidad: Incorpora prácticas de gestión de servicios como la Gestión de la Disponibilidad y la Gestión de la Continuidad del Servicio para asegurar que los servicios de TI puedan respaldar el negocio incluso en situaciones adversas.

- Sistema de Valor del Servicio (SVS): Reemplaza el enfoque de ciclo de vida de versiones anteriores, centrando la gestión en cómo las entradas (oportunidades o demanda) se transforman en valor (salidas) a través de la cadena de valor del servicio y prácticas de gestión.

ITIL 4 reorganiza los "procesos" de versiones anteriores en 34 Prácticas de Gestión (de las cuales 17 son de Gestión de Servicios), haciendo énfasis en el valor y la flexibilidad (Gil, Gamboa, & De los Santos, 2025).

- Gestión de Incidentes: Objetivo: restaurar la operación del servicio a la normalidad tan pronto como sea posible y minimizar el impacto negativo en las operaciones de negocio.
- Gestión de Problemas: Objetivo: reducir la probabilidad y el impacto de incidentes, identificando las causas raíz (*Root Causes*) y gestionando los errores conocidos.
- Gestión del Nivel de Servicio (SLM): Objetivo: establecer y gestionar acuerdos de servicio con el cliente, asegurando que el servicio es capaz de cumplir con los niveles de servicio acordados (Utilidad y Garantía).

Comparación con otros marcos (NIST, ISO 38500) para darle mayor validez académica.

Tabla 4: *Objetivos de Control*

Marco/Estándar	**Publicado por**	**Propósito Principal**	**Alcance/Enfoque**	**Naturaleza**
COBIT 2019	ISACA	Gobernanza y Gestión (G&M) de la I&T empresarial. Asegura que la I&T apoya los objetivos de negocio y la creación de valor.	Abarca todo el ciclo de vida de la I&T: desde la estrategia hasta la operación y el monitoreo. Proporciona 40 objetivos de G&M.	Marco de Referencia Integral. Proporciona un modelo conceptual completo y componentes de gobernanza.
ITIL 4	AXELOS / PeopleCert	Gestión de Servicios de TI (ITSM). Crea, entrega y mejora continuamente servicios habilitados por tecnología, enfocándose en la co-creación de valor.	Se centra en el Sistema de Valor del Servicio (SVS) y 34 prácticas detalladas para la gestión de servicios.	Modelo de Mejores Prácticas. Es un conjunto de guías para la ejecución de la ITSM.
ISO/IEC	ISO/IEC	Gobernanza Corporativa	Se enfoca en el nivel	Estándar de

38500		de TI. Proporciona principios para que el órgano de gobierno (Junta Directiva) evalúe, dirija y monitoree el uso de la TI.	directivo/estratégico de la organización (el "qué" se debe gobernar, no el "cómo").	Principios. Establece los cimientos y el vocabulario para la gobernanza de la TI.
NIST CSF 2.0	NIST	Gestión de Riesgos de Ciberseguridad. Ayuda a las organizaciones a comprender, gestionar, reducir y comunicar su riesgo de ciberseguridad.	Se centra estrictamente en la Ciberseguridad, estructurado en 6 funciones (Gobernar, Identificar, Proteger, Detectar, Responder, Recuperar).	Marco de Referencia de Riesgos. Es una taxonomía de resultados de ciberseguridad, no prescriptivo.

Fuente: COBIT 2019.

Europa: En el plano internacional, la Asociación Europea de Transacciones Seguras (EAST, 2023) reportó que los fraudes en cajeros automáticos mediante malware especializado, jackpotting, skimming y técnicas de intrusión lógica generaron pérdidas superiores a los 100 millones de euros en Europa durante el primer semestre de 2023. Estos eventos confirman que las interrupciones en la red de cajeros automáticos no solo causan pérdidas millonarias diarias, sino que también afectan de manera directa la confianza de los usuarios en los servicios financieros (Kaspersky News, 2024).

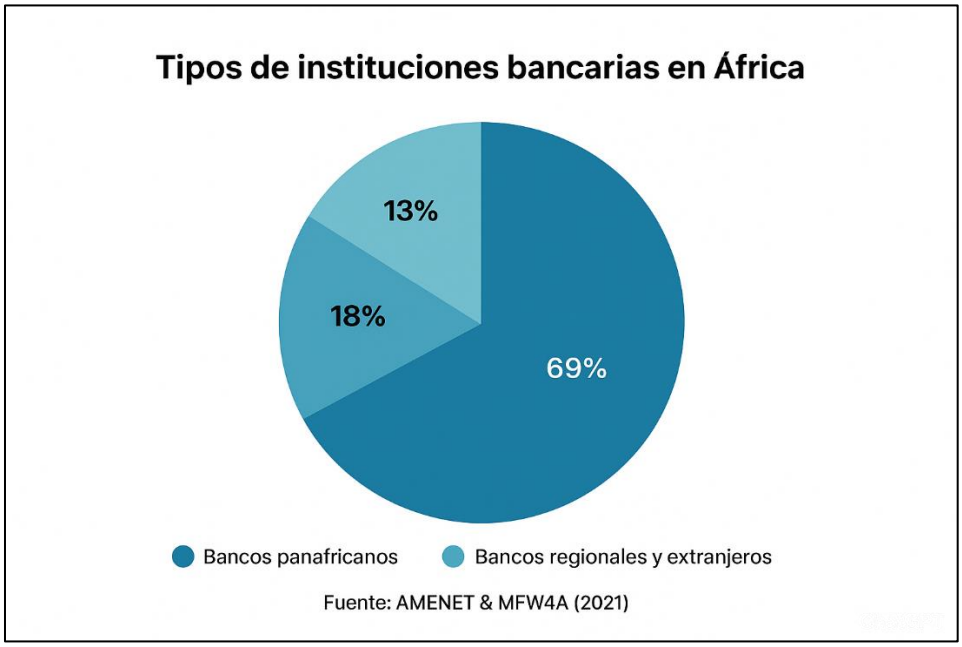
África: El sector bancario en África ha experimentado una profunda y notable evolución, pasando de un sistema dominado por cooperativas y cajas de ahorro en la década de 1970 a un proceso de expansión y modernización en las décadas siguientes, impulsado por la liberalización financiera, la privatización de bancos estatales y una regulación más efectiva. Tras la crisis financiera global de 2008, se produjo una transformación significativa, donde los bancos europeos y americanos fueron reemplazados progresivamente por un grupo de bancos panafricanos, principalmente liderados por Sudáfrica, Nigeria y Marruecos. Este crecimiento se vio reflejado en la consolidación del mercado financiero africano, con la expansión de las bolsas de valores (Hernández, 2021).

La innovación tecnológica ha desempeñado un papel crucial en la inclusión financiera de la región, destacando la penetración de la banca telefónica o móvil, un ámbito en el que África se ha posicionado como líder mundial. El aumento en la penetración de internet y dispositivos móviles ha acelerado la adopción de soluciones digitales y el comercio electrónico. Las tecnologías de pago móvil han sido fundamentales, permitiendo a amplios sectores de la población, incluso

aquellos sin acceso a la banca tradicional, realizar pagos y transacciones en línea de manera sencilla y segura (Hernández, 2021).

En este ecosistema digital en expansión, los cajeros automáticos (ATMs) han cumplido un papel esencial como infraestructura complementaria y como un puente entre los servicios bancarios tradicionales y las soluciones digitales innovadoras. Inicialmente clave para el acceso a efectivo en zonas remotas, los ATMs han evolucionado para facilitar la utilización de plataformas de pago móvil y transacciones electrónicas, promoviendo así una mayor inclusión financiera y favoreciendo el desarrollo continuo del comercio electrónico en la región (Hernández, 2021).

Figura 4: *Tipos de instituciones bancarias en África.*



Fuente: estimaciones sobre la vulnerabilidad en ciberseguridad en América Latina, considerando la falta de estrategias nacionales, mecanismos de respuesta y centros de control. La región enfrenta además una respuesta jurídica lenta, lo que incrementa la exposición frente a las amenazas cibernéticas.

Asia: La región de Asia-Pacífico está experimentando un rápido crecimiento en los servicios de banca digital debido a la expansión de su economía digital, la creciente adopción de teléfonos inteligentes y un marco regulatorio favorable en países como India, China y Singapur.

El crecimiento del sector está impulsado por las crecientes expectativas de los

consumidores por soluciones de pago instantáneas, las iniciativas gubernamentales para fomentar la inclusión financiera a través de la banca digital y las inversiones en computación en la nube para crear infraestructuras bancarias escalables. Existen numerosas oportunidades de desarrollo, como la implementación de chatbots con inteligencia artificial para la atención al cliente, el uso de tecnología blockchain para asegurar las transacciones transfronterizas y la formación de alianzas con empresas fintech locales para adaptar soluciones a las necesidades específicas de los diversos mercados regionales (Mordor Intelligence, 2024).

Asia-Pacifico: Sigue siendo la región de más rápido crecimiento con más de 1,4 millones de ATM´S, de los cuales casi el 68% se gestionan externamente. China e India lideran la región con importantes inversiones en infraestructura de ATM, particularmente en áreas rurales y suburbanas. La adopción de servicios de cajeros automáticos biométricos e impulsados por la IA ha aumentado en un 34% en esta región (Mordor Intelligence, 2024).

2.1.5 ENTORNO TECNOLÓGICO Y CIBERSEGURIDAD EN EL SISTEMA FINANCIERO GLOBAL Y REGIONAL

2.1.5.1 ENTORNO TECNOLÓGICO

Las medidas de protección incluyen lectores EMV certificados, mecanismos anti-skimming, inhibidores de señal, autenticación biométrica y cifrado de extremo a extremo en las transacciones. No obstante, la efectividad de estas medidas depende de la implementación de una gestión integral de riesgos respaldada por marcos como COBIT e ITIL, que faciliten tanto la prevención como la respuesta efectiva ante incidentes (Al-Bassam & Al-Alawi, 2022).

Las tecnologías de comunicaciones e Internet se van convirtiendo de manera gradual en una herramienta de uso frecuente para los grupos delictivos vinculados al narcotráfico, el tráfico de armas y de personas, entre otros. Estos grupos no sólo se sirven de ellas para obtener recursos sino también para controlar las ganancias derivadas de su actividad (Al-Bassam & Al-Alawi, 2022).

La situación del ciberdelito en América Latina se magnifica a la luz de la vulnerabilidad institucional para hacer frente a este flagelo. Por ese motivo el BID efectuó un llamamiento a los países de la región “para comenzar a dar los primeros pasos para proteger esta infraestructura clave del Siglo XXI” en un informe publicado en marzo 2016. Si bien la mayoría de los países de la región ha avanzado en iniciativas para fortalecer sus sistemas jurídicos y organismos de

Ciberseguridad, la velocidad con que surgen las nuevas tecnologías, así como las nuevas formas de emplearlas para fines delictivos requiere una vigilancia constante y una capacidad de adaptación tanto del sector gubernamental como privado (Al-Bassam & Al-Alawi, 2022).

Los cajeros automáticos han evolucionado hacia terminales multifuncionales capaces de realizar pagos, transferencias, consultas y otros servicios más allá de la simple dispensación de efectivo. Esta expansión funcional, se ha acompañado de un aumento significativo en las amenazas tecnológicas, entre las que destacan:

Ataques lógicos (logical attacks), como el jackpotting, que permiten manipular el software para dispensar efectivo.

Uso de malware especializado para obtener control total del sistema.

Ataques a nivel de red, explotando vulnerabilidades en routers, switches y canales de comunicación.

La vulnerabilidad de américa latina en cifras

El 80% de los países de América Latina carece de una estrategia nacional de Ciberseguridad para proteger las Infraestructuras Críticas.

El 50% carece de mecanismos institucionales de respuesta apropiados

Solamente un tercio posee un Centro de Comando y Control para hacer frente a estas amenazas

Casi todos presentan una respuesta jurídica lenta frente al ciberdelito. Si bien Colombia y la República Dominicana poseen un sistema jurídico sólido, persisten debilidades en los procedimientos.

Tabla 5: *Entorno Tecnológico y Ciberseguridad en América Latina*

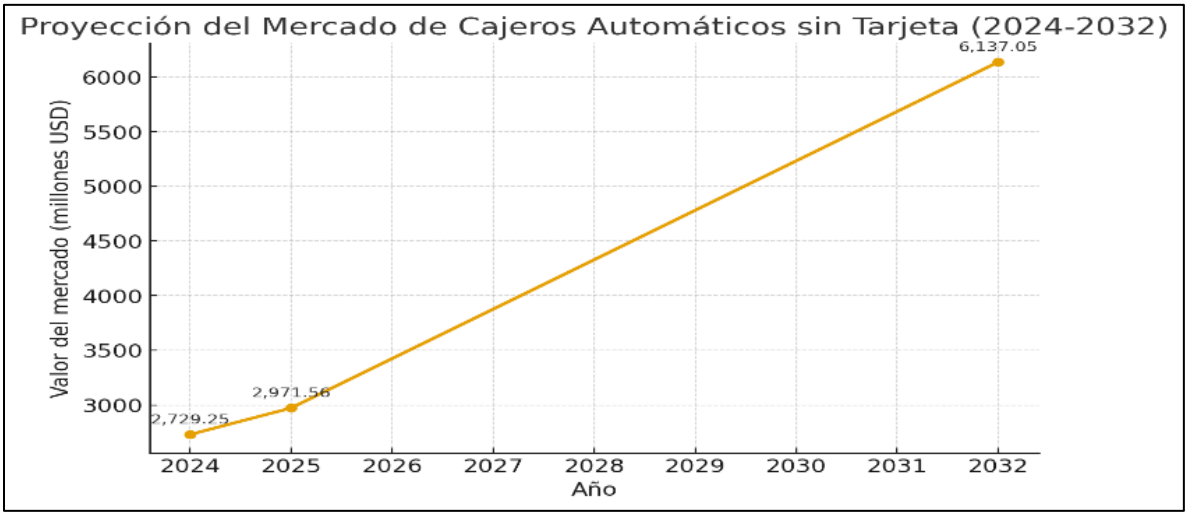
Aspecto	Medidas/Avances	Riesgos/Amenazas	Situación en América Latina
Protección en Cajeros Automáticos	Lectores EMV certificados, mecanismos anti-skimming, inhibidores de señal, autenticación biométrica, cifrado extremo a extremo	Ataques lógicos (jackpotting), malware especializado, ataques a nivel de red	Implementación parcial, dependiente de la gestión de riesgos (COBIT, ITIL)

Evolución de Cajeros Automáticos	Terminales multifuncionales: pagos, transferencias, consultas, servicios adicionales	Mayor exposición a ciberataques y fraudes tecnológicos	Avance moderado, acompañado de mayores amenazas
Uso de Tecnologías por Crimen Organizado	Aprovechamiento de Internet y comunicaciones para obtener recursos y controlar ganancias	Narcotráfico, tráfico de armas, trata de personas	Vulnerabilidad institucional para enfrentar el ciberdelito
Ciberseguridad Institucional	Marcos de gestión (COBIT, ITIL), centros de comando y control, respuesta jurídica	Velocidad de aparición de nuevas amenazas tecnológicas	80% sin estrategia nacional de ciberseguridad; 50% sin mecanismos de respuesta; Solo 1/3 con Centros de Comando y Control; Respuesta jurídica lenta
Panorama Regional	Avances en algunos países (ej. Colombia y República Dominicana con marcos jurídicos más sólidos)	Debilidades en procedimientos y falta de adaptación tecnológica	Persisten deficiencias en seguridad tanto en sector público como privado

Fuente: La información presentada en la tabla ha sido elaborada a partir de diversas fuentes como McAfee (2014) y el informe del BID (2016), con el fin de resumir el panorama del entorno tecnológico y de ciberseguridad en América Latina. Los datos reflejan tanto los avances en medidas de protección como las principales vulnerabilidades regionales frente al ciberdelito.

2.1.5.2 MERCADO DE CAJEROS AUTOMÁTICOS SIN TARJETA (CONTACTLESS): TAMAÑO, PARTICIPACIÓN, TENDENCIAS DEL SECTOR Y PREVISIONES (2025-2032)

Figura 5: *Proyección del mercado de cajeros automáticos sin tarjeta (2024-2032).*



Fuente: Crecimiento esperado en millones de USD.

El mercado de cajeros automáticos sin tarjeta (Cardless ATM) está experimentando un

crecimiento significativo, con proyecciones de alcanzar los USD 6.137 millones en 2032, partiendo de USD 2.729 millones en 2024, lo que implica una Tasa de Crecimiento Anual Compuesta (CAGR) del 10.7% (CBI, 2025). Esta evolución se basa en la capacidad de estas máquinas para facilitar transacciones sin la necesidad de una tarjeta física, utilizando tecnologías integradas en aplicaciones móviles como códigos QR, NFC y, crucialmente, la autenticación biométrica (Innowise, 2025).

El principal motor de este crecimiento es la demanda de transacciones más seguras y sin contacto, tendencia que se aceleró tras la pandemia de COVID-19. La adopción masiva de la banca móvil y las billeteras digitales como Apple Pay o Google Pay ha impulsado la integración de estas funcionalidades, ya que no solo aumentan la comodidad del usuario, sino que también reducen sustancialmente los riesgos de fraude y robo de identidad (Innowise, 2025).

A pesar del optimismo del mercado, el principal desafío reside en la infraestructura tradicional, la cual requiere fuertes inversiones en la actualización de hardware y software para ser compatible con estas nuevas tecnologías. En la segmentación tecnológica, aunque las soluciones basadas en códigos QR lideran actualmente el mercado por su simplicidad y bajo costo de implementación, la tecnología NFC se proyecta como el segmento con mayor tasa de crecimiento. Regionalmente, Asia Pacífico encabeza la expansión gracias a la digitalización e inclusión financiera en países como China e India, mientras que América del Norte mantiene una fuerte presencia y Europa se fortalece gracias a la regulación impulsada por la directiva PSD2. El mercado, que se perfila hacia una banca digital más segura y eficiente, ve a actores clave como Citigroup, JPMorgan y Grupo Santander invirtiendo fuertemente en innovación para consolidar la tendencia (Innowise, 2025).

2.1.6 ENTORNO SOCIOCULTURAL Y USO DEL EFECTIVO / ATMS A NIVEL MUNDIAL

El uso de cajeros automáticos (ATMs) se encuentra profundamente arraigado en la experiencia bancaria cotidiana, y a pesar del auge de la banca digital, el efectivo continúa siendo el medio de pago preferido en gran parte del mundo por razones prácticas, culturales y emocionales. Por ejemplo, en el Reino Unido, los ATMs dispensaron £129 mil millones en 2016, lo que equivale a más de £2.000 por habitante, demostrando su vigencia incluso en economías altamente digitalizadas (Bujalance & Trillo, 2025).

Los cajeros automáticos aún son considerados por los clientes como un mecanismo importante para acceder a los servicios bancarios y al dinero. Sin embargo, cuando tres cuartas partes de las personas están preocupadas por retirar dinero de los cajeros automáticos, está claro que los bancos, minoristas y otros proveedores de ATMs están fallando en implementar medidas que construyan confianza en los clientes. Esto es algo que necesita cambiar si el cajero automático va a seguir prosperando en los próximos 50 años, como lo ha hecho durante el último medio siglo (Bujalance & Trillo, 2025).

No obstante, la percepción de seguridad constituye un desafío crítico. Diversos estudios revelan que cerca del 31% de los usuarios manifiestan sentirse inseguros al utilizar cajeros automáticos debido a amenazas físicas y electrónicas, lo que afecta directamente la confianza de los clientes en el sistema financiero. En este sentido, los bancos y proveedores de ATMs tienen un interés estratégico en asegurar que los clientes se sientan seguros y confiados al usarlos, ya que la rentabilidad de estas plataformas depende de su uso frecuente (Bujalance & Trillo, 2025).

Investigaciones recientes han demostrado que algunas medidas sencillas pueden contribuir significativamente a mejorar la percepción de seguridad. Por ejemplo, más de la mitad de los usuarios encuestados (54 %) respondieron con valores de 5, 6 o 7 en una escala de 1 a 7, al ser consultados si un simple letrero de videovigilancia les haría sentir más seguros al usar un cajero automático. Asimismo, la presencia de un guardia de seguridad fue considerada en varios países como la medida más efectiva, aunque en mercados como el Reino Unido la videovigilancia ocupó el primer lugar, seguida en China por la implementación de un botón de alarma personal (Batiz, Bautista, & González, 2021).

Los resultados también evidencian que los usuarios priorizan los beneficios de seguridad frente a posibles preocupaciones de privacidad: menos de una cuarta parte de los encuestados consideró que la videovigilancia afectaba negativamente su privacidad, mientras que la mayoría la valoró como un mecanismo disuasivo de la delincuencia (Batiz, Bautista, & González, 2021).

Finalmente, la creciente demanda de servicios 24/7, ubicaciones estratégicas y rapidez en las operaciones obliga a las instituciones bancarias a expandir y optimizar sus redes de cajeros automáticos. En este contexto, garantizar una experiencia segura, confiable y accesible constituye no solo un factor esencial para la satisfacción del cliente, sino también un elemento diferenciador en la competitividad y reputación de las instituciones financieras (Batiz, Bautista, & González,

2021).

2.1.7 FACTORES AMBIENTALES Y RIESGOS FÍSICOS QUE AFECTAN LA INFRAESTRUCTURA ATM

Aunque el factor ambiental no incide directamente en el software de los cajeros automáticos, sí puede afectar su operatividad física. Factores como inundaciones, tormentas o cortes prolongados de energía pueden interrumpir el servicio y provocar pérdidas económicas (Rodríguez, Espinosa, Mendoza, & Quirós, 2023).

Desde precios más altos hasta cajas negras, a medida que los delincuentes llegan a un cajero automático. Todos sabemos cuán ingeniosos pueden ser los delincuentes, y un estudio reciente de Europa sólo confirma esta creatividad implacable. En general, los delincuentes intentarán impulsar sus ataques a los cajeros automáticos a través de sistemas operativos y plataformas de proveedores para usar errores y agujeros de seguridad para engañar al sistema y acceder al efectivo (Rodríguez, Espinosa, Mendoza, & Quirós, 2023). Los métodos que prefieren criminales son:

Precio mayor: uno de los ataques más comunes, se realiza de dos maneras. O el delincuente utiliza un software malicioso que envía comandos al dispensador o usa su dispositivo de hardware directamente conectado al dispensador para eliminar el cajero automático y vaciarlo de efectivo (Sundas, Contreras, Mujahid, Beneyto, & Vehi, 2024).

Malware: el ataque de malware consta de dos fases. Primero, el criminal infecta con malware el cajero automático. Después de eso, el software malicioso espera en el cajero automático hasta que el criminal visita el cajero automático y activa el comando de dispensación utilizando un PIN especial o un comando de pantalla táctil (Sundas, Contreras, Mujahid, Beneyto, & Vehi, 2024).

Ataques de Caja Negra: los ataques de caja negra incluyen una interrupción de los cajeros automáticos. El dispositivo externo "black box", como una computadora portátil o tableta, se conecta y se conecta y se vuelve emparejar de manera fraudulenta con el dispensador y envía comandos para la salida de dinero directamente al dispensador de efectivo (Sundas, Contreras, Mujahid, Beneyto, & Vehi, 2024).

Hombre en el medio: estos ataques se centran en la comunicación entre la PC del ATM y el sistema host del comprador. El software malicioso falsifica la respuesta del host para dispensar dinero sin debitar la cuenta del criminal. Por lo general, el malware se activa durante las

transacciones con números de tarjeta preconfigurados (Rodríguez, Espinosa, Mendoza, & Quirós, 2023).

Skimming: El calzado de software, el desarrollo de malware "Skimming", incluye la interrupción y/o manipulación entre la tarjeta EMV y la interfaz de un lector de tarjetas en el cajero automático, lo que al mismo tiempo le da al delincuente la capacidad de retirar dinero en otro cajero automático (Rodríguez, Espinosa, Mendoza, & Quirós, 2023).

Fraude de reversión de transacciones: esto incluye un ataque que genera múltiples códigos de error y reembolso del pago innecesario. Estos ataques pueden ser difíciles de aislar y detectar antes de que ocurran pérdidas financieras, especialmente si se necesitan cambios en las aplicaciones de host ATM (Rodríguez, Espinosa, Mendoza, & Quirós, 2023).

2.2 MICROENTORNO

2.2.1 MERCADO E INDUSTRIA DE CAJEROS AUTOMÁTICOS Y SOFTWARE BANCARIO EN HONDURAS

2.2.1.1 ANÁLISIS DEL MICROENTORNO FINANCIERO EN HONDURAS: ATMS, REGULACIÓN Y RIESGOS

El microentorno financiero de Honduras, en el cual operan los cajeros automáticos (ATMs), constituye una compleja red de interacciones entre los bancos, los entes reguladores, los proveedores de tecnología y los usuarios finales. Este entorno está fuertemente influenciado por factores económicos, tecnológicos y normativos, así como por la evolución de la digitalización y las expectativas de un cliente cada vez más exigente en términos de rapidez, seguridad y disponibilidad de los servicios financieros (Banco Central de Honduras, 2024).

La banca desempeña un papel esencial en la economía hondureña, no solo como intermediaria de recursos financieros, sino también como promotora de inclusión y acceso al crédito. Los ATMs representan un componente crítico dentro de la infraestructura financiera, permitiendo a los clientes realizar transacciones rápidas, seguras y accesibles, incluso fuera del horario bancario tradicional. La digitalización de los servicios financieros ha avanzado en Honduras, con la adopción de aplicaciones móviles, banca en línea y canales electrónicos, posicionando a los cajeros automáticos como un puente clave para la inclusión financiera y la cobertura de zonas con acceso limitado a sucursales físicas (Banco Central de Honduras, 2024).

El sistema financiero hondureño enfrenta riesgos y desafíos específicos que impactan

directamente en la operatividad y seguridad de los ATMs. Entre estos se incluyen:

- Brechas de ciberseguridad: vulnerabilidades en la infraestructura tecnológica bancaria que podrían ser explotadas por malware, accesos no autorizados o ataques de phishing.
- Fraudes y ataques a cajeros automáticos: intentos de fraude, clonación de tarjetas y sabotajes a dispositivos, afectando la confianza del cliente.
- Retos de disponibilidad: interrupciones eléctricas, fallos de software o errores humanos que afectan la continuidad del servicio.

Regulación y Normativa Nacional

La Comisión Nacional de Bancos y Seguros (CNBS) regula y supervisa el sistema financiero hondureño, estableciendo normas que buscan proteger al consumidor y garantizar la estabilidad de los servicios electrónicos. Entre las más relevantes se encuentran:

- Legislación de protección al consumidor financiero.
- Normativas de seguridad informática y protección de datos personales, alineadas con estándares internacionales.

El marco regulatorio hondureño ha evolucionado para fortalecer la estabilidad financiera, especialmente después del Decreto 160-2016, que introdujo un enfoque de supervisión basado en riesgo sistémico tras la liquidación del Banco Continental. Este se complementa con la Ley de Instituciones del Sistema Financiero (Decreto 170-95). Aunque las MIPYME representan un sector clave de la economía, aún enfrentan barreras para acceder a crédito, y varias instituciones han comenzado a adoptar marcos como COBIT e ITIL, mientras el Banco Central impulsa iniciativas de ciberseguridad (CNBS, 2024).

En este contexto, Banco Ficohsa se consolida como líder financiero con una amplia red de cajeros automáticos. Sin embargo, al compararse con estándares internacionales, se identifican áreas de mejora en continuidad, eficiencia y seguridad del software ATM. La revisión normativa permite integrar estas exigencias en el diseño del sistema de gestión propuesto, asegurando cumplimiento regulatorio y reduciendo riesgos para la institución (CNBS, 2024).

2.2.1.2 EL SISTEMA FINANCIERO Y LA RELEVANCIA DE LOS CAJEROS AUTOMÁTICOS

El sistema bancario hondureño se caracteriza por su notable crecimiento en los últimos años, acompañado de una progresiva solidez y diversificación de servicios. A septiembre de 2024, los activos totales de la banca alcanzaron los 42.6 mil millones de dólares, reflejando un crecimiento interanual del 15.7%, mientras que la cartera de préstamos mostró un incremento del 15.9%, llegando a 26.4 mil millones de dólares. Estas cifras colocan al sistema financiero hondureño como uno de los más dinámicos de la región centroamericana, con una expansión sostenida que impulsa la necesidad de plataformas tecnológicas más eficientes y seguras (Adane, Wale, & Meried, 2021).

En este escenario, los cajeros automáticos representan un pilar estratégico para la inclusión financiera, ya que facilitan el acceso a servicios bancarios en un país donde la bancarización aún enfrenta retos estructurales. Para 2020, los ATM ya constituían el 20% de todos los puntos de servicio del sistema financiero nacional, consolidándose como un canal esencial, sobre todo en áreas rurales o semiurbanas donde la presencia de sucursales bancarias es limitada. Su función se ha ampliado más allá del retiro de efectivo, incluyendo operaciones como el pago de servicios públicos, transferencias entre cuentas, depósitos, consultas de saldos y en algunos casos la integración con billeteras electrónicas. La relevancia de los ATM no solo radica en la comodidad para el cliente, sino también en la reducción de costos operativos para los bancos, ya que permiten atender a un mayor número de usuarios sin necesidad de infraestructura física adicional (Adane, Wale, & Meried, 2021).

2.2.2 ENTORNO ECONÓMICO Y DE SERVICIOS FINANCIEROS EN HONDURAS

La gestión de los cajeros automáticos, como un componente crítico del microentorno financiero, se articula bajo una estrategia de automatización inteligente (Grupo Financiero Ficohsa, 2024). Esta estrategia impulsa la contratación de perfiles especializados para diseñar e implementar soluciones que optimicen procesos y generen experiencias innovadoras, lo cual tiene aplicación directa en la red de ATMs como puntos de servicio clave (CNBS, 2020).

Según Kal (2025), los principales impulsores de innovación en cajeros automáticos se centran en:

- Métodos de dispensación y depósito de efectivo: incluyen sistemas avanzados para billetes y monedas, recicladores de efectivo y dispensación de artículos especiales como oro o joyas.

- Pantallas e interactividad: incorporación de pantallas táctiles, video y funcionalidades similares a dispositivos móviles para mejorar la experiencia del cliente.
- Tecnologías de autenticación: transición de banda magnética a EMV, reconocimiento biométrico (como venas de los dedos) y tecnologías como Magneprint.
- Protección de bóvedas: cerraduras reforzadas, retardos programados y uso de tinta de seguridad.
- Seguridad del cliente: fortalecimiento de tecnologías como EPP y RKL, y el uso de aplicaciones móviles para reducir la dependencia de lectores de tarjetas.
- Supervisión remota: mantenimiento predictivo y monitoreo en tiempo real para prevenir fallos y ahorrar costos.
- Gestión multivendor: integración de diferentes tipos de hardware bajo una plataforma uniforme, lo que incrementa la eficiencia operativa y facilita la innovación.

El compromiso del banco con la mejora continua lo ha llevado a adoptar tecnologías de vanguardia como Robotic Process Automation (RPA) e Inteligencia Artificial (IA), las cuales permiten fortalecer la sostenibilidad operativa mediante el monitoreo constante y la investigación de nuevas tendencias (CNBS, 2020).

Asimismo, la gestión del software de ATMs requiere un análisis robusto de los riesgos tecnológicos. Investigaciones académicas sugieren la aplicación de marcos de control como COBIT 2019 e ITIL 4, que optimizan la seguridad, la eficiencia y la continuidad del servicio (CNBS, 2020).

Este análisis es clave para el proyecto, ya que permite determinar las áreas de mejora tecnológica y operativa en la administración del software ATM de Banco Ficohsa. La adopción de metodologías como COBIT 2019 e ITIL 4 contribuirá directamente a estandarizar procesos, reducir vulnerabilidades y fortalecer la resiliencia tecnológica del banco (CNBS, 2020).

2.2.3 TRANSFORMACIÓN DIGITAL Y ADOPCIÓN TECNOLÓGICA EN EL SISTEMA FINANCIERO HONDUREÑO Y EN BANCO FICOHSA

Un sistema de gestión de cumplimiento (CMS) es un sistema integrado que se utiliza para cumplir con los requisitos normativos, las políticas internas y los estándares de la industria. Un CMS eficaz ayuda a las organizaciones a evitar áreas de incumplimiento y a lograr un

cumplimiento normativo continuo.

Para implementar un sistema de gestión de cumplimiento (CMS) eficaz, las organizaciones deben considerar adoptar un enfoque estratégico que comience por comprender las necesidades de su negocio y continúe con el despliegue y el soporte continuo (IBM, 2025).

Los pasos comunes para considerar incluyen:

- Evaluación de necesidades: identificar objetivos de cumplimiento y gestión de riesgos, incluyendo marcos específicos como ISO o SOX.
- Personalización del sistema: adaptar la estructura organizacional, asignar roles y asegurar integración con procesos existentes.
- Involucramiento de partes interesadas: garantizar la aceptación de la alta dirección y la junta directiva desde las fases iniciales.
- Capacitación del personal: entrenar a los empleados en el uso del CMS y en la importancia del cumplimiento continuo.
- Responsabilidad definida: establecer líneas claras de rendición de cuentas.
- Mejora continua: mantener el sistema actualizado con las necesidades cambiantes de la organización.
- En el caso de Banco Ficohsa, la gestión del cumplimiento está bajo la supervisión de la Vicepresidencia de Cumplimiento, que opera con independencia y acceso directo a la Junta Directiva. Sus compromisos clave son (Banco Ficohsa, 2025):
- Cumplimiento Normativo: asegurar la adherencia a todas las obligaciones legales y regulatorias.
- Mejora Continua: fortalecer de manera constante los procesos de cumplimiento.
- Independencia y autonomía: garantizar imparcialidad en la supervisión.
- Prevención de represalias: fomentar una cultura de reporte seguro de inquietudes o irregularidades.

El incumplimiento de este sistema podría generar consecuencias graves, incluyendo sanciones legales, pérdida de confianza y riesgos reputacionales que afectarían la estabilidad integral del banco (Banco Ficohsa, 2025).

Este componente se vincula con los objetivos específicos del proyecto al garantizar que toda innovación en el software ATM se desarrolle bajo una estructura de cumplimiento normativo. A

futuro, esto facilitará auditorías transparentes, la trazabilidad de los procesos y una cultura organizacional basada en la responsabilidad tecnológica.

2.2.3.1 EVOLUCIÓN TECNOLÓGICA Y BENCHMARKING

La transformación tecnológica en mercados líderes ofrece un referente clave para Honduras, que enfrenta el reto de mantenerse competitivo en seguridad y experiencia de usuario. En países avanzados, se han adoptado innovaciones como el software multivendor que permite gestionar cajeros de distintos fabricantes desde una sola plataforma, la biometría para autenticación y las transacciones sin tarjeta física mediante NFC (Near Field Communication).

Para el sistema bancario hondureño, estos avances implican un doble desafío:

- Competitividad: los clientes demandan rapidez, seguridad y servicios modernos.
- Inversión tecnológica: es necesario destinar recursos a plataformas escalables y flexibles que permitan actualizaciones constantes, integración de nuevas funcionalidades y adaptación a cambios regulatorios.

El benchmarking se convierte en una herramienta estratégica para guiar estas inversiones. Consiste en comparar productos, procesos y servicios con los de competidores o líderes de la industria, con el objetivo de identificar brechas y adoptar mejores prácticas (Herrero, 2024). Este análisis no solo señala áreas de mejora, sino que también impulsa la innovación. Ejemplos regionales muestran que quienes modernizan primero sus sistemas reducen significativamente la exposición a ataques, ya que la mayoría de las vulnerabilidades explotadas provienen de plataformas obsoletas o con soporte limitado. Esto podría implicar adaptar tecnologías o procesos innovadores en su propio servicio al cliente para mejorar la satisfacción del usuario, ya que una de las características que más valoran los clientes es el hecho de poder contar con la asistencia de un buen servicio postventa cuando más lo necesita (UDIT, 2023).

En este sentido, el benchmarking constante con países más avanzados permite a Honduras:

- Mejorar la seguridad de sus cajeros automáticos.
- Incrementar la eficiencia operativa.
- Optimizar la experiencia del cliente.

- Fortalecer la resiliencia del sistema financiero frente a amenazas emergentes.

La experiencia regional demuestra que quienes se anticipan en la modernización tecnológica no solo fortalecen su posición en el mercado, sino que también reducen su exposición a ataques, dado que muchas vulnerabilidades explotadas por los ciberdelincuentes se encuentran en sistemas obsoletos o con soporte limitado. Por ello, el benchmarking constante con países más avanzados se convierte en una herramienta estratégica para guiar la inversión, la innovación y la protección del ecosistema de ATM en Honduras.

2.2.3.2 PROCESOS DE OPERACIÓN, MANTENIMIENTO Y SOPORTE EN BANCO FICOHSA

Los procesos operativos de Banco Ficohsa se centran en la prestación de productos y servicios financieros innovadores con altos estándares de calidad, apalancados en la tecnología y en un recurso humano calificado. Estos procesos están regidos por un compromiso con la sustentabilidad del negocio y un robusto marco de Gestión de Cumplimiento (Grupo Financiero Ficohsa, 2011; Banco Ficohsa, 2025).

El mantenimiento de los sistemas y la infraestructura que soporta la operación, incluyendo los ATMs y la banca en línea, se gestiona implícitamente a través de las disposiciones contractuales que otorgan al banco la facultad de suspender temporalmente el servicio. Esto se realiza sin responsabilidad para el banco en caso de fallas técnicas, mantenimiento preventivo o correctivo, o por razones de seguridad (Banco Ficohsa, 2024).

La gestión operativa se fundamenta en un compromiso con la sustentabilidad del negocio y un constante esfuerzo por mejorar los procesos internos para mantener un desempeño corporativo sólido. Este enfoque en la calidad y la mejora continua es esencial para el mantenimiento y la evolución tecnológica de los servicios.

El soporte al cliente se centraliza a través del Servicio de Atención al Cliente (Call Center), un pilar histórico del soporte de la institución.

- Proceso de Reclamos: Legalmente, el proceso exige que el cliente formalice la queja por escrito. El banco, por su parte, se obliga a notificar al cliente cualquier cambio en las condiciones contractuales, tarifas o servicios a través de correo electrónico o su portal web.
- Mantenimiento Operativo: El banco se reserva la facultad de suspender los servicios

temporalmente sin responsabilidad, en caso de fallas técnicas, mantenimiento preventivo o correctivo, o por razones de seguridad. Esta potestad contractual asegura la posibilidad de realizar el mantenimiento evolutivo necesario para la mejora continua del servicio.

El mantenimiento de los servicios se apoya en un compromiso con la sustentabilidad del negocio, que implica la mejora continua de los procesos internos y la gestión empresarial (Grupo Financiero Ficohsa, 2011). En términos de continuidad operativa, el contrato de servicios faculta al banco a suspender servicios temporalmente por razones de mantenimiento, fallas técnicas o seguridad, sin incurrir en responsabilidad hacia el cliente.

2.2.4 ENTORNO REGULATORIO Y MARCOS DE REFERENCIA DE TI EN HONDURAS

El mercado bancario hondureño presenta una estructura altamente concentrada. Cinco bancos FICOHSA, Banco Atlántida, BAC Credomatic, Banco de Occidente y Banpaís, concentran alrededor del 80% de los activos totales del sector, configurando un escenario de competencia oligopólica (Rankings Latam, 2025). Esta concentración genera un doble efecto: por un lado, una fuerte estabilidad financiera debido al peso y solidez de estas entidades; y por otro, una presión competitiva intensa que obliga a los bancos a invertir continuamente en innovación tecnológica y seguridad, pues las decisiones estratégicas de uno de estos actores pueden desencadenar una reacción en cadena en el resto.

En este contexto, la gestión de los cajeros automáticos se convierte en un factor diferenciador. Bancos que invierten en software multivendor, seguridad avanzada o nuevas funcionalidades (como depósitos automatizados o autenticación biométrica) no solo ganan ventaja competitiva, sino que también elevan las expectativas del mercado, obligando a los demás a modernizar sus sistemas para no perder clientes.

La Comisión Nacional de Bancos y Seguros (CNBS) desempeña un rol fundamental en el fortalecimiento del marco regulatorio. Una de las normativas clave es la Circular CNBS No.025/2022, que exige a las instituciones financieras Implementar marcos de gobierno de TI.

2.2.4.1 VACÍOS A NIVEL DE PROTECCIÓN DE DATOS

Un aspecto crítico en el entorno hondureño es la ausencia de una ley específica de protección de datos personales, lo que genera un vacío regulatorio frente a las prácticas modernas de privacidad bancaria. Actualmente, las instituciones financieras deben diseñar y aplicar sus

propias políticas internas, basadas en el principio constitucional del Hábeas Data, que otorga a los ciudadanos el derecho a conocer, actualizar y rectificar la información recopilada sobre ellos.

Desde 2018, se encuentra en discusión en el Congreso Nacional un proyecto de ley de protección de datos personales, que busca introducir los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) en la normativa nacional (Central Law, 2022). No obstante, la falta de aprobación hasta la fecha coloca a Honduras en una posición de vulnerabilidad, ya que los bancos deben suplir este vacío con iniciativas propias de autorregulación, lo que genera heterogeneidad en las prácticas de seguridad y privacidad.

2.2.4.2 Adopción de buenas prácticas de ti

Aunque no se cuenta con información pública detallada sobre la aplicación de marcos internacionales de gestión de TI como COBIT o ITIL en Honduras, se reconoce que la Comisión Nacional de Bancos y Seguros (CNBS) ha alineado gran parte de su normativa con principios de estos estándares (ISACA, 2019; Trujillo et al., 2022). La adopción formal de dichos marcos permitiría:

- Mejorar la gestión de activos críticos de TI.
- Alinear la estrategia tecnológica con los objetivos de negocio.
- Implementar controles preventivos y correctivos frente a amenazas.
- Establecer indicadores de desempeño y auditorías más rigurosas en ciberseguridad.

En este contexto, ITIL constituye uno de los marcos más confiables y utilizados a nivel mundial. Sus mejores prácticas abarcan desde la gestión de incidentes, cambios y problemas hasta la optimización de catálogos de servicios. Con la evolución hacia ITIL 4, se fortalecen principios orientados a la excelencia operativa y a la experiencia del cliente. El módulo ITIL 4 DSV (Drive Stakeholder Value) establece siete pasos que guían el recorrido del cliente: explorar necesidades, involucrar usuarios, ofertar servicios, acordar resultados, facilitar incorporación, co-crear valor y evaluar desempeño. Este enfoque permite brindar atención 24/7, mejorar la interacción y fomentar relaciones de confianza.

Gobernanza y Cumplimiento Normativo en Banco Ficohsa

En el caso de Banco Ficohsa, la gestión del gobierno de TI se articula a través de tres ejes

principales:

1. Gobernanza y Cumplimiento Normativo

La Política de Sistema de Gestión de Cumplimiento refleja el compromiso institucional de cumplir con obligaciones regulatorias (Banco Ficohsa, 2025).

La Vicepresidencia de Cumplimiento cuenta con autonomía y acceso directo al Órgano de Gobierno, garantizando la supervisión ética y regulatoria, en concordancia con principios de COBIT.

2. Gestión de Riesgo Operativo y Resiliencia

El banco aplica criterios de gobernanza empresarial orientados a la resiliencia tecnológica (The Food Tech, 2023).

Las actividades de Gestión del Riesgo Tecnológico y de Continuidad del Negocio se ejecutan conforme a políticas internas y mejores prácticas internacionales (Grupo Financiero Ficohsa, 2024), compatibles con marcos como ITIL y COBIT.

3. Mejora Continua de Procesos

Existe un compromiso explícito con la mejora continua del Sistema de Cumplimiento y de los procesos internos (Banco Ficohsa, 2011; 2025).

Investigaciones académicas recomiendan la adopción explícita de COBIT 2019 e ITIL 4 para optimizar la gestión de riesgos en cajeros automáticos (Molina Ordóñez & Núñez Ramires, 2025).

En Honduras, la madurez en la gestión de riesgos tecnológicos aún se encuentra en desarrollo progresivo. A pesar de avances regulatorios (DPL News, 2023), persisten ataques y fraudes debido a:

- Limitada inversión en infraestructura tecnológica avanzada.
- Insuficiente capacitación continua en seguridad digital.
- Escasa concienciación de los usuarios financieros (Bonilla Cruz et al., 2025).

2.2.5 ENTORNO TECNOLÓGICO Y CIBERSEGURIDAD BANCARIA EN HONDURAS Y LA REGIÓN CENTROAMERICANA

La región centroamericana comparte características estructurales como marcos regulatorios en proceso de fortalecimiento, niveles variables de digitalización bancaria y brechas de ciberseguridad. Estas condiciones hacen que un incidente en un país pueda tener repercusiones inmediatas o indirectas en otros, lo que demanda estrategias de protección coordinadas y resilientes.

Tendencias como los pagos electrónicos, la ciberseguridad, la inteligencia artificial y muchas más demostraron la necesidad latente de contar con una buena infraestructura IT en las entidades financieras. Debido a la pandemia, la banca digital ha abierto la puerta a un nuevo estilo de pagos y consumo. Se estima que, de diez servicios bancarios, siete son posibles gracias a la banca digital en Honduras de acuerdo con la Comisión Nacional de Bancos y Seguros (Diario Quien Opina, 2021).

El ciberespacio carece de fronteras físicas, permitiendo que amenazas se propaguen rápidamente. Un ejemplo ilustrativo es el malware FiXS, detectado en México, diseñado específicamente para vaciar cajeros automáticos. Este tipo de software demuestra un alto grado de especialización, adaptándose a los protocolos, hardware y sistemas operativos utilizados en la región (Auriga, 2023). Para Honduras, este caso constituye una advertencia clara, ya que comparte similitudes tecnológicas con otros países latinoamericanos, aumentando la probabilidad de que amenazas transfronterizas impacten su sistema financiero.

Ante este panorama, la defensa no puede limitarse a la reacción post-incidente. Se requiere un enfoque proactivo que incorpore:

- Listas blancas (application whitelisting): restringir la ejecución de software no autorizado.
- Encriptación de datos: tanto en tránsito como en reposo.
- Monitoreo en tiempo real: detectar patrones sospechosos en las transacciones.
- Autenticación multifactorial: especialmente para el personal técnico que accede a la infraestructura de los ATMs.
- Capacitación continua en ciberseguridad: dirigida a personal operativo y de TI para reducir vulnerabilidades humanas.

La identificación de estas amenazas regionales permite al proyecto anticipar posibles

riesgos tecnológicos y adaptar estrategias de ciberseguridad adecuadas a la realidad de Honduras. Así, se fortalece la sostenibilidad del sistema ATM y se promueve la confianza de los usuarios en los servicios del banco.

2.2.5.1 MODELOS DE SEGURIDAD EMERGENTES

El incremento de ciberamenazas ha impulsado la evolución de modelos de seguridad más sofisticados, diseñados para anticipar, detectar y responder de manera integral a los riesgos tecnológicos que enfrentan los sistemas financieros. Estos modelos van más allá de las medidas tradicionales y se orientan hacia la resiliencia continua, asumiendo que las amenazas son inevitables y que la protección debe ser dinámica y adaptativa.

Entre los modelos más destacados se encuentran:

- Zero Trust (Confianza Cero): parte del principio de "nunca confiar, siempre verificar". Cada acceso, transacción o interacción dentro de la red debe validarse, reduciendo la probabilidad de intrusiones internas y externas. Sus pilares incluyen la segmentación de red, la autenticación multifactorial y el monitoreo constante en tiempo real.
- Defensa en Profundidad: estrategia basada en capas múltiples de protección que combinan hardware reforzado, cifrado de datos, control de aplicaciones, listas blancas, videovigilancia y programas de capacitación para empleados y usuarios. Este enfoque asegura que, aunque una capa falle, otras sigan activas para contener la amenaza.
- Seguridad Adaptativa: utiliza herramientas basadas en inteligencia artificial y machine learning para identificar patrones anómalos, aprender del comportamiento de los usuarios y responder automáticamente a incidentes, reduciendo los tiempos de detección y reacción.
- Seguridad por Diseño: modelo que integra la ciberseguridad desde la concepción de cualquier servicio o infraestructura tecnológica, garantizando que los cajeros automáticos, aplicaciones móviles y sistemas de banca digital se construyan bajo principios de seguridad preventiva.

La adopción de estos modelos representa una oportunidad para que los bancos hondureños fortalezcan la confianza del cliente, reduzcan su vulnerabilidad frente a ataques y se alineen con las mejores prácticas internacionales. En un entorno financiero cada vez más digitalizado, la integración de estas estrategias no es opcional, sino un requisito para garantizar la continuidad operativa y la sostenibilidad del sistema bancario.

Situación de ciberseguridad bancaria en Honduras

La inversión de los bancos comerciales del país en materia de ciberseguridad es constante, incrementándose en 11.8 puntos porcentuales el año pasado respecto al 2021 respecto a informática e información. Así lo subraya el Informe de Estabilidad Financiera (IEF) a diciembre de 2022 que elabora el Banco Central de Honduras (BCH) en el apartado de ciberseguridad bancaria e implicaciones para estabilidad financiera y al que tuvo acceso EL HERALDO.

En el territorio hondureño operan 15 instituciones bancarias comerciales de las que cinco cuentan con token o pin automático consistente en un elemento de seguridad para proteger las operaciones bancarias y evitar que otras personas hagan transacciones fraudulentas. Mientras que nueve bancos disponen de una sección de seguridad en el sitio web y cinco tienen una campaña contra el fraude.

Entre las principales acciones tomadas por el sistema bancario nacional en materia de ciberseguridad destaca “acelerar la implementación de nuevas estrategias digitales en productos y servicios financieros, haciendo uso de las innovaciones en seguridad tecnológica” (El Heraldo, 2023).

Marlon Molina, director del Laboratorio de Ciberseguridad, Madrid Capital Fintech, manifestó que las cifras recientes muestran que los ciberataques y estafas no sólo son más frecuentes, sino también más sofisticados, impulsados por el uso de inteligencia artificial, ransomware, deepfakes y campañas de phishing cada vez mejor diseñadas.

Durante el año 2023, se reportaron aproximadamente 1.8 millones de incidentes cibernéticos dirigidos a sistemas de empresas e instituciones estatales de Honduras.

En el primer semestre de 2025, la Dirección Policial de Investigaciones (DPI) solo en San Pedro Sula, recibió entre 5 y 7 denuncias diarias sobre fraudes digitales, que incluyen robos de cuentas de WhatsApp, suplantación de identidad, y robo de datos bancarios (La Prensa, 2025).

2.2.6 GESTIÓN INTEGRAL DE RIESGOS, DEFENSA TECNOLÓGICA Y EVOLUCIÓN INSTITUCIONAL DE BANCO FICOHSA

2.2.6.1 RIESGOS, AMENAZAS Y ADOPCIÓN DE BUENAS PRÁCTICAS

Los riesgos que enfrenta el ecosistema de cajeros automáticos en Honduras reflejan la complejidad del microentorno financiero, donde confluyen amenazas tecnológicas, factores socioeconómicos y vacíos en la cultura de seguridad digital. El reto principal radica en que las

instituciones financieras deben diseñar estrategias que no solo respondan a ataques específicos, sino que anticipen tendencias delictivas, incorporen estándares internacionales y refuercen la confianza del usuario en el sistema.

Entre los métodos más frecuentes de fraude destacan:

- Phishing: ataques que buscan engañar al usuario para obtener credenciales de acceso, las cuales luego se utilizan para realizar transacciones fraudulentas.
- Skimming: instalación de dispositivos en los cajeros para copiar la información de las tarjetas, acompañada de cámaras ocultas para capturar los PIN de los clientes.
- Malware en ATM: softwares diseñados para manipular la lógica de los cajeros, permitiendo a los atacantes extraer dinero directamente o registrar datos sensibles.
- Ingeniería social y fraudes híbridos: combinación de engaños presenciales y digitales que aprovechan la baja cultura de ciberseguridad en ciertos sectores de la población.

Estos ejemplos evidencian la necesidad de una estrategia integral que abarque tanto el componente digital como el físico de la seguridad. En lo digital, los cajeros deben contar con software robusto, capaz de detectar y bloquear intentos de ejecución de código malicioso, así como aplicar actualizaciones constantes. En lo físico, las medidas deben reforzar los puertos, ranuras y puntos de acceso de los dispositivos, además de incorporar sistemas de video vigilancia y protocolos de transporte seguro de efectivo.

Arquitectura Tecnológica, Plataformas y Gestión de Riesgos

La arquitectura tecnológica y la gestión de plataformas en Banco Ficohsa están fuertemente influenciadas por la necesidad de asegurar la Continuidad del Negocio y mitigar el Riesgo Tecnológico (Grupo Financiero Ficohsa, 2024). La CNBS (2022) obliga a las instituciones a integrar la gestión del software de los ATM dentro de un esquema más amplio de control de riesgos y ciberseguridad, lo que ha impulsado el fortalecimiento de las áreas de tecnología y seguridad, aunque con niveles de cumplimiento variables.

Riesgo Tecnológico: El banco realiza periódicamente actividades de control relacionadas con la gestión de riesgo tecnológico, mostrando resultados satisfactorios y acordes a los planes anuales. Esto es crucial para mitigar fallos de hardware, errores de software y vulnerabilidades de

ciberseguridad (Molina Ordóñez & Núñez Ramírez, 2025).

Metodologías de Desarrollo y Operación: La implementación de nuevos sistemas utiliza metodologías ágiles como Scrum, Lean Six Sigma y Design Thinking, promoviendo una arquitectura flexible y adaptable, capaz de integrar tecnologías como IA y RPA en las plataformas existentes.

Riesgos Tecnológicos y Operativos

Banco Ficohsa aborda los riesgos inherentes a su infraestructura de TI y a la operación diaria a través de procesos formales de control:

- Riesgos Técnicos y de Obsolescencia: La gestión del riesgo tecnológico se enfoca en asegurar la continuidad mediante Análisis de Impacto del Negocio (BIA) y Planes de Recuperación ante Desastres (DRP), garantizando la recuperación rápida de la infraestructura ante incidentes críticos.
- Riesgos Operativos y de Disponibilidad: Incluyen monitoreo constante de incidentes y errores humanos. La institución invierte en capacitación continua en gestión de riesgos para reducir fallos en procesos y sistemas.

El cumplimiento regulatorio y la adopción de estándares globales son esenciales para la estabilidad y reputación del banco.

- Cumplimiento Regulatorio: El banco se adhiere a la normativa local y a las disposiciones de entes supervisores, lo cual es vigilado por la Vicepresidencia de Cumplimiento (Banco Ficohsa, 2025).
- Brechas frente a COBIT/ITIL: Aunque se aplican controles internos y mejoras continuas, la falta de adopción explícita de marcos como COBIT 2019 e ITIL 4 puede generar inconsistencias en la ejecución de procesos, limitando la eficiencia y la seguridad. Investigaciones recientes sugieren su incorporación formal para optimizar la gestión del software de ATMs (Molina Ordóñez & Núñez Ramírez, 2025).

La operación bancaria se formaliza mediante un Contrato Único, que define el uso de múltiples canales de acceso al cliente:

- Canales Físicos: Sucursales y cajeros automáticos.

- Canales Digitales: Ficohsa en Línea y Call Center.

El riesgo operativo asociado a estas transacciones es mitigado mediante actividades de control rigurosas, incluyendo la revisión periódica del riesgo legal y tecnológico, con resultados satisfactorios (Grupo Financiero Ficohsa, 2024).

2.2.6.2 ESTRATEGIA DE DEFENSA EN PROFUNDIDAD

La defensa en profundidad es una estrategia de ciberseguridad basada en múltiples capas de protección que buscan asegurar los activos de una organización frente a amenazas externas e internas. Su principio central es que, si una línea de defensa falla, otras capas actúan como respaldo. Este enfoque no solo protege hardware y software, sino que también contempla el factor humano, responsable de muchas brechas de seguridad.

Ante el crecimiento de ciberamenazas cada vez más sofisticadas, la defensa en profundidad integra medidas tradicionales como antivirus, firewall, VPN y puertas de enlace seguras, junto con herramientas avanzadas basadas en aprendizaje automático (ML) para detectar anomalías en el comportamiento de usuarios y dispositivos. De este modo, permite tanto prevenir ataques como contenerlos y minimizar sus impactos cuando ya están en curso (Fortinet, 2024).

La clave para fortalecer la seguridad de los ATMs hondureños radica en la adopción de un modelo de defensa en profundidad, el cual combina diversas capas de protección que actúan de manera simultánea:

- Hardware reforzado: cajeros resistentes a ataques físicos y manipulaciones externas.
- Control de aplicaciones: listas blancas que restringen la ejecución de software no autorizado.
- Encriptación de datos: protección tanto en tránsito como en reposo.
- Segmentación de la red: aislamiento de los cajeros para evitar que una intrusión comprometa toda la infraestructura bancaria.
- Monitoreo en tiempo real: análisis continuo de transacciones para identificar patrones inusuales o sospechosos.
- Capacitación y concienciación: programas dirigidos a empleados y usuarios para reducir vulnerabilidades humanas.

Al estratificar e incluso duplicar los procesos de seguridad, se minimiza la probabilidad de una violación. La mayoría de las organizaciones reconocen que una sola capa de seguridad o un producto de un solo punto (p. ej., un firewall) no llega lo suficientemente lejos como para proteger a la empresa de la creciente sofisticación de los ciberdelincuentes actuales.

2.2.6.3 HISTORIA DE BANCO FICOHSA EN CIFRAS Y EXPANSIÓN

El Grupo Financiero Ficohsa comenzó en 1991 con la creación de Financiera Comercial Hondureña S.A. y se expandió rápidamente, obteniendo la autorización de la Comisión Nacional de Bancos y Seguros (CNBS) para operar como banco en 1994 y como grupo financiero en 2005.

A partir de 2011, Ficohsa inició su expansión regional e internacional, estableciendo operaciones en Panamá, Guatemala y Estados Unidos. Estratégicamente, el grupo adquirió las operaciones de tarjetas de Citibank en Honduras en 2014, y en 2015, consolidó su posición regional al adquirir la operación completa de Citibank en Nicaragua. Además, en 2016 adquirió Seguros Alianza en Guatemala.

Fechas Clave en la Historia de Ficohsa:

- 1991: Creación de Financiera Comercial Hondureña S.A.
- 1992: Ficohsa Casa de Cambio inicia operaciones, la primera autorizada por el Banco Central de Honduras.
- 1994: Se funda Banco Ficohsa S.A.
- 2005: La CNBS autoriza la constitución del "Grupo Financiero Ficohsa".
- 2011: El banco se expande a Panamá.
- 2012: Inicia operaciones en Guatemala.
- 2014: Adquiere las operaciones de tarjetas de Citibank en Honduras.
- 2015: Adquiere Citibank Nicaragua.
- 2016: Adquiere Seguros Alianza en Guatemala.

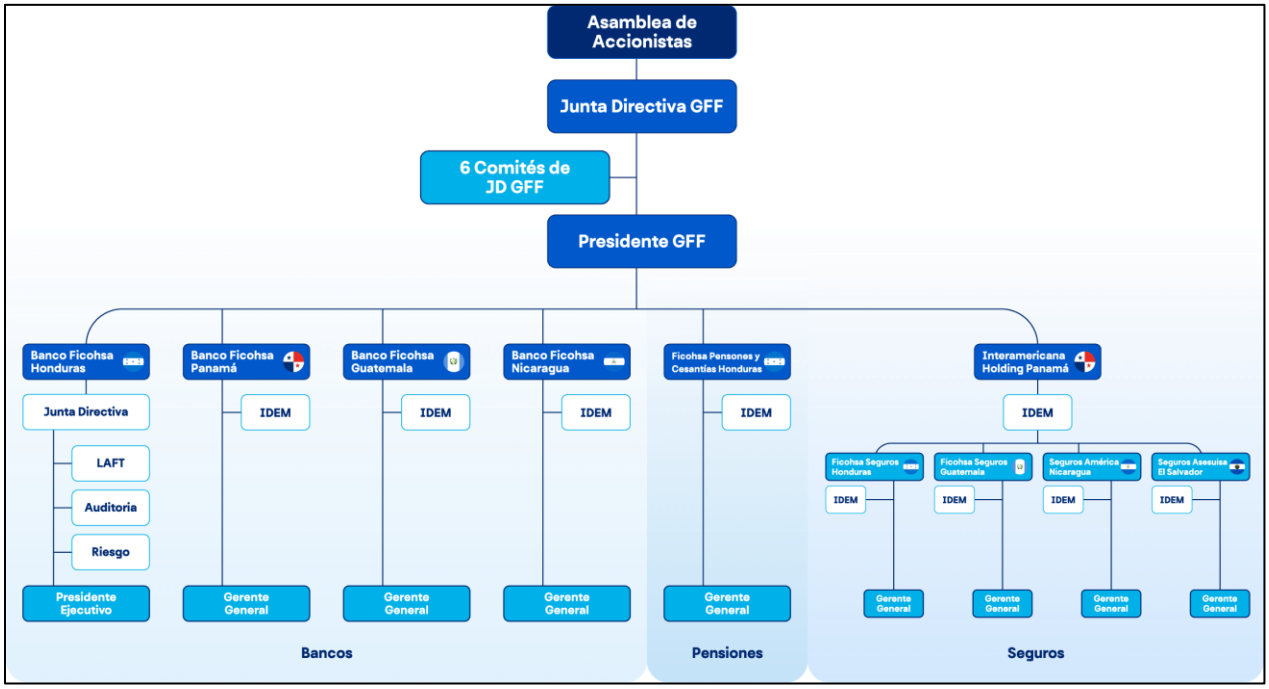
Misión y Visión

- Misión: Proporcionar productos y servicios financieros innovadores con altos estándares

de calidad y la mejor tecnología para generar seguridad y satisfacción en sus clientes.

- Visión: Ser un grupo sólido y confiable, comprometido con el desarrollo de los países donde opera, ofreciendo soluciones financieras efectivas, ágiles e innovadoras.

Figura 6: *Gobierno Corporativo Ficohsa.*



Fuente: Organigrama del gobierno corporativo de Banco Ficohsa

Figura 7: *Comités de Grupo Ficohsa y sus funciones.*

Comité	Descripción	Miembros	Cargo
Comité de Cumplimiento LA-FT	Tiene como función asistir a la Junta Directiva en relación a la gestión del sistema de cumplimiento orientado a prevenir e identificar delitos relacionados al lavado de activos, financiación al terrorismo y anticorrupción. Junto con la Unidad Corporativa de Cumplimiento, vela por la aplicación y efectividad de los diferentes programas de prevención existentes en el Grupo.	Colin Dore Veater Walter Nico Klaas Gerardus Pijl Bruce Malcolm Burdett	Presidente Miembro Miembro
Comité Financiero	Asesora a la Junta Directiva para mantener una política financiera coordinada en relación a la estructura de inversión y financiación del Grupo de acuerdo con su plan estratégico.	Camilo Alejandro Atala Faraj Luis Alberto Atala Faraj Javier Eduardo Atala Faraj Richard Aitkenhead Castillo José Alejandro Piedrahita Tello José Arturo Alvarado Cortés Colin Dore Veater Walter	Presidente Miembro Miembro Miembro Miembro Miembro Secretario Corporativo
Comité Gobierno Corporativo	Apoya a la Junta Directiva en la evaluación periódica del cumplimiento de las prácticas de Gobierno Corporativo incluidas en los Estatutos, Reglamentos y Código de Gobierno. A su vez, evalúa la experiencia de los propios miembros de la Junta Directiva, Comités y Empresas Miembro. De igual manera, es responsable de revisar y aprobar el Informe Anual de Gobierno Corporativo.	Juan José Daboub José Alejandro Piedrahita Juan Carlos Atala Faraj	Presidente Miembro Miembro

Fuente: La estructura de Comités de Junta Directiva del Grupo Ficohsa se organiza de forma escalonada en los siguientes dos (2) niveles o componentes.

2.3 TEORÍAS DE SUSTENTO

2.3.1 TEORÍA DE LA CUARTA REVOLUCIÓN INDUSTRIAL

La Cuarta Revolución Industrial representa un cambio profundo en la manera en que se organizan los sistemas productivos, sociales y económicos. El concepto de revolución implica transformaciones rápidas y radicales, impulsadas por tecnologías capaces de modificar las relaciones entre individuos, organizaciones y procesos. A diferencia de las revoluciones industriales anteriores, esta etapa se caracteriza por la integración simultánea de herramientas digitales, físicas y biológicas, generando una evolución acelerada en todos los ámbitos de la vida moderna (Rivera, Rivera, & Estévez, 2022).

El término Industria 4.0 surgió formalmente en Alemania durante la Feria de Hannover en 2011, cuando se propuso la idea de la fábrica inteligente como un nuevo modelo de producción. Este enfoque plantea la interconexión entre sistemas físicos y virtuales, permitiendo procesos flexibles, automatizados y altamente adaptables. Esta visión transforma la cadena de valor global, ya que facilita la personalización de productos, incrementa la eficiencia operativa y redefine la forma en que las empresas compiten e innovan (Rivera, Rivera, & Estévez, 2022).

Sin embargo, la Cuarta Revolución Industrial no se limita al ámbito manufacturero. Su influencia se extiende a sectores tan diversos como la salud, las telecomunicaciones, las finanzas,

la educación y la seguridad. La convergencia de disciplinas como la nanotecnología, la biotecnología, la energía renovable y la computación cuántica demuestra que esta revolución tiene un alcance mucho más amplio que cualquier proceso tecnológico previo, pues combina avances que interactúan entre sí para generar soluciones más complejas e inteligentes (Cabrera, Rodríguez, González, & Medina, 2020).

Un aspecto fundamental de esta revolución es la incorporación masiva de tecnologías emergentes que transforman los procesos productivos y de servicio. Herramientas como el Internet de las Cosas, el análisis de grandes volúmenes de datos, la inteligencia artificial, la computación en la nube, la robótica avanzada, la realidad aumentada, el blockchain, la impresión tridimensional y las redes de quinta generación permiten crear sistemas más eficientes, predictivos y automatizados. Gracias a estas tecnologías, las organizaciones pueden analizar datos en tiempo real, anticipar fallos y diseñar soluciones personalizadas con mayor rapidez (Cabrera, Rodríguez, González, & Medina, 2020).

De acuerdo con Schwab, la velocidad y el alcance de las innovaciones de esta revolución superan las de cualquier periodo industrial anterior. Su expansión es más rápida y sus efectos más profundos debido a la conectividad global y al acceso masivo a tecnologías avanzadas. Comprender los principios de la Cuarta Revolución Industrial resulta esencial para que empresas, gobiernos e instituciones puedan adaptarse a un entorno donde la automatización, la digitalización y la innovación continua son elementos centrales para la competitividad y el desarrollo sostenible (Rivera, Rivera, & Estévez, 2022).

2.3.2 TEORÍA GENERAL DE SISTEMAS

La Teoría General de Sistemas, formulada por Ludwig von Bertalanffy en 1968, plantea que todo sistema está conformado por elementos interdependientes cuyas interacciones determinan su comportamiento global. Desde esta perspectiva, una organización no puede ser entendida como un conjunto de partes aisladas, sino como un sistema abierto que intercambia información, recursos y energía con su entorno. Este enfoque resalta que el desempeño del sistema no depende únicamente de sus componentes, sino de la calidad de las relaciones que existen entre ellos (Ballesteros, Vera, & Román, 2024).

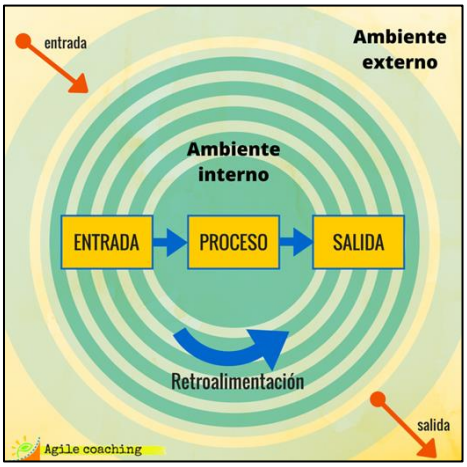
En el ámbito de las tecnologías de la información, esta teoría adquiere especial relevancia al evidenciar que los servicios de TI no pueden analizarse de manera fragmentada. Infraestructura,

aplicaciones, procesos, personal y usuarios conforman un entramado interconectado que opera en constante interacción con factores externos como proveedores, reguladores, clientes y amenazas cibernéticas. De esta manera, la gestión de TI se concibe como un sistema dinámico que requiere coordinación permanente, retroalimentación continua y capacidad de adaptación frente a los cambios del entorno (Ballesteros, Vera, & Román, 2024).

Bajo este marco conceptual, el software de los cajeros automáticos puede interpretarse como un subsistema que recibe entradas provenientes de exigencias regulatorias, necesidades de los usuarios y riesgos tecnológicos emergentes. Estas entradas son procesadas mediante prácticas de gobernanza y gestión soportadas en marcos como COBIT 2019 e ITIL 4, que permiten organizar, controlar y optimizar los procesos internos. El resultado de este procesamiento son servicios financieros más seguros, confiables y coherentes con los objetivos estratégicos de la institución (Arnold & Osorio, 2022).

En síntesis, la teoría general de sistemas fortalece la visión integral de la investigación al demostrar que la gestión de riesgos, el software de los ATMs, los marcos de referencia y los objetivos del negocio forman un conjunto interdependiente. Este enfoque justifica la necesidad de abordar el sistema ATM de manera holística, evitando soluciones aisladas y promoviendo estrategias integradas que aseguren resiliencia operativa, cumplimiento normativo y valor para el usuario final (Arnold & Osorio, 2022).

Figura 8: *Representación de la Teoría General de Sistemas desde una visión sistémica de agilidad.*



Fuente: LeaderDeProyecto.com (s. f.), *Teoría General de Sistemas y Agilismo*.

2.3.3 TEORÍA DE ALINEACIÓN ESTRATÉGICA Y SU RELACIÓN CON COBIT 2019 E ITIL 4

La teoría de alineación estratégica sostiene que una organización solo alcanza su máximo desempeño cuando sus objetivos de negocio, sus capacidades tecnológicas y sus procesos operativos avanzan en una misma dirección. De acuerdo con The Strategy Institute, este proceso implica integrar metas, estrategias y roles de forma coherente para que cada unidad contribuya al logro de una visión compartida. En este sentido, la alineación estratégica no solo mejora la coordinación interna, sino que optimiza la asignación de recursos y evita duplicaciones o esfuerzos inconexos que podrían afectar la competitividad (Adame, Popoola, Akinoso, & Okeke, 2024).

Desde esta perspectiva, la alineación se convierte en un mecanismo que fortalece la toma de decisiones, pues orienta a las organizaciones hacia las prioridades críticas del negocio. Su aplicación permite comprender con mayor claridad cómo la tecnología puede actuar como un habilitador de valor, especialmente en contextos donde la disponibilidad, la seguridad y la eficiencia operativa son determinantes, como ocurre con el software de cajeros automáticos. En el caso de Banco Ficohsa, este enfoque garantiza que las iniciativas de TI no operen como procesos aislados, sino como un soporte estratégico para la reducción de riesgos tecnológicos y la mejora de la experiencia del cliente (Adame, Popoola, Akinoso, & Okeke, 2024).

El marco COBIT 2019 se integra de manera natural en esta teoría al ofrecer un sistema de gobierno y gestión de la información y la tecnología orientado a crear valor, optimizar recursos y controlar riesgos. Su estructura flexible permite a las instituciones alinear la tecnología con los objetivos estratégicos mediante componentes como la cascada de metas, los factores de diseño y los dominios de gobierno y gestión. En entornos financieros altamente regulados, COBIT 2019 se convierte en una herramienta indispensable para asegurar que los servicios de TI, incluido el software de los ATMs, se desarrollen y operen bajo principios de control, eficiencia y cumplimiento normativo (Peña-Casanova & Anias-Calderón, 2020).

ITIL 4 complementa esta visión mediante un enfoque centrado en la creación de valor y en la gestión de servicios basada en colaboración continua, mejora permanente y orientación al cliente. Al integrarse con metodologías ágiles y con prácticas modernas de automatización y retroalimentación, ITIL 4 refuerza la capacidad de las organizaciones para responder con rapidez a las necesidades cambiantes del entorno. En conjunto, COBIT 2019 e ITIL 4 constituyen un marco articulado que permite alinear la tecnología con la estrategia empresarial, consolidando la

operación del software ATM como un componente clave para la resiliencia y la sostenibilidad del negocio (Peña-Casanova & Anias-Calderón, 2020).

2.4 METODOLOGÍAS

2.4.1 COBIT 2019

La Aplicación de COBIT 2019 para la Gobernanza de la Empresa: caso Soporte técnico en cadena farmacéutica.

Alfaro Mairena y Pineda Velásquez (2025) desarrollaron un trabajo de investigación sobre la optimización de operaciones de soporte técnico en una cadena de farmacias de Honduras, aplicando metodologías como COBIT 2019 e ITIL 4, resaltando la implementación de COBIT 2019 destacándose como una herramienta fundamental para establecer una gobernanza de tecnología de la información (TI) que estuviera alineada con los objetivos de negocio de la empresa. Este marco de referencia no fue visto simplemente como un conjunto de buenas prácticas, sino como una estructura estratégica para asegurar que los activos de información y tecnología generaran valor y contribuyeran directamente a la toma de decisiones.

El proceso de aplicación dentro de la empresa se basó en una metodología rigurosa que comenzó con un diagnóstico exhaustivo. En esta fase, el equipo de investigación se centró en la evaluación del estado actual de los procesos de TI. El objetivo era identificar de manera precisa los problemas existentes, las deficiencias operativas y los riesgos latentes que afectaban la gestión tecnológica. Esta evaluación permitió establecer una línea base de la situación y sirvió como punto de partida para todas las acciones subsecuentes.

Posteriormente, se procedió a la fase de diseño del modelo de gobernanza. En esta etapa, la investigación se enfocó en seleccionar los objetivos de COBIT 2019 que se alineaban directamente con las metas de la organización. Por ejemplo, en un estudio relacionado con la seguridad, se priorizó la aplicación de dominios como APO10 (Gestionar la seguridad) y DSS05 (Gestionar los servicios de seguridad). El propósito fue garantizar que cada control y cada proceso propuesto no solo mitigara un riesgo, sino que también fortaleciera la capacidad de la empresa para lograr sus objetivos estratégicos. La aplicación de COBIT 2019 permitió a la empresa enfocar sus esfuerzos de TI de manera más eficiente, dirigiéndolos hacia las áreas que tenían el mayor impacto en el negocio.

Resultados y Beneficios Obtenidos por la Empresa con COBIT 2019

La implementación de la metodología basada en COBIT 2019 generó resultados tangibles y beneficios significativos para la empresa. Una vez que se diseñó el modelo de gobernanza, se formuló una propuesta de implementación detallada. En esta fase, se elaboraron estrategias de mitigación de riesgos y planes de acción específicos, describiendo cómo se podrían aplicar los controles y procesos de COBIT para mejorar la seguridad y la eficiencia operativa. Aunque la implementación no se llevó a cabo en el marco de la investigación, la propuesta sirvió como una guía práctica y realista para la organización.

La fase de evaluación fue crucial para validar la viabilidad de la propuesta. Se definieron métricas de rendimiento y se establecieron indicadores clave (KPIs) para medir la efectividad de las soluciones planteadas. Esto permitió a la empresa proyectar cómo se traducirían las mejoras en la reducción de riesgos, la optimización de los procesos y, en última instancia, en un retorno sobre la inversión en tecnología. La evaluación demostró que la metodología de COBIT 2019 proporcionaba un marco para el éxito medible.

Finalmente, el proceso se concluyó con una fase de mejora continua. Este componente aseguró que el modelo de gobernanza no fuera estático, sino que se mantuviera relevante y adaptable a los cambios en el entorno tecnológico y a la aparición de nuevas amenazas. Al adoptar esta mentalidad, la empresa se preparó para sostener las mejoras a largo plazo y para asegurar que la gestión de la tecnología continuara generando valor de manera constante. La aplicación de la metodología COBIT 2019 en la empresa resultó en un análisis exhaustivo y en la formulación de una propuesta de gobernanza que no solo mejoró los procesos de TI, sino que también fortaleció la confiabilidad de la información y la toma de decisiones.

La Aplicación de COBIT 2019 en la Municipalidad de Carrillo

El caso de estudio de la Municipalidad de Carrillo, en Costa Rica, se basó en la aplicación de un método fundamentado en COBIT 2019 para la evaluación de sus procesos tecnológicos. El propósito de esta investigación fue diagnosticar el estado actual de la gobernanza de las Tecnologías de Información y Comunicación (TIC) en la entidad, con el objetivo de diseñar un sistema de gobierno que respondiera a las necesidades de la organización y generara valor público a través de sus servicios. Este estudio se llevó a cabo en respuesta a los cambios en el marco normativo de gobernanza de TI para entidades del Gobierno Central y municipalidades en Costa Rica.

La metodología que se utilizó en la investigación se centró en la aplicación de dos instrumentos principales de COBIT 2019: la Cascada de Metas y los Factores de Diseño. El uso de estos instrumentos permitió un análisis detallado y una evaluación del modelo de gestión de TI de la municipalidad, particularmente en el contexto de un proyecto de migración de sistemas operativos e informáticos.

La aplicación de la Cascada de Metas se inició con el relacionamiento de los objetivos del Plan Estratégico Municipal (PEM) con las metas empresariales genéricas de COBIT 2019. Este proceso permitió al investigador vincular las prioridades de la municipalidad con el marco de gobernanza de TI. Posteriormente, se identificaron las metas de alineamiento de la tecnología que apoyaban a las metas empresariales, lo cual sirvió para determinar los objetivos de gobierno y gestión que debían ser evaluados. Este enfoque metódico aseguró que el proceso de evaluación no se realizara de forma aleatoria, sino que se concentrara en los dominios de COBIT que eran más relevantes para los objetivos estratégicos de la municipalidad.

Resultados y Hallazgos de la Evaluación con COBIT 2019

Tras la aplicación de la "Cascada de Metas", la investigación logró agrupar los objetivos de gobierno y gestión de COBIT 2019 que apoyaban de manera directa el cumplimiento de las metas del PEM de la Municipalidad de Carrillo. Este resultado fue considerado un insumo valioso, ya que permitió al investigador discernir sobre qué objetivos debía prestar mayor atención para abordar las brechas de cumplimiento.

Además del análisis de la "Cascada de Metas", la investigación incorporó la evaluación de los factores de Diseño de COBIT 2019. La aplicación de este instrumento sirvió para refinar el sistema de gobierno de la TI, adaptando las condiciones, expectativas y necesidades de la organización a las mejores prácticas de COBIT (Pérez & Martínez, 2021).

Figura 9: *Infografía - cascada de metas definido por Cobit 2019, propuesto para identificar los objetivos de gobierno y gestión a evaluar.*

Fuente: Cuadro de mando integral genérico establecido por COBIT 2019, para la aplicación del instrumento" Cascada de Metas", considerando los siguientes recursos: objetivos y metas definidos en el Plan Estratégico Municipal (PEM) vigente.

El estudio no solo produjo un diagnóstico de la situación actual, sino que también generó una serie de herramientas de gran valor para la empresa:

Instrumentos de evaluación: Se crearon instrumentos específicos para evaluar los objetivos de gobierno y gestión seleccionados, basándose en los siete componentes para el diseño de un sistema de gobierno de COBIT 2019.

Identificación de brechas: Se diseñaron herramientas para identificar los niveles de capacidad y las brechas de cumplimiento en los procesos asociados a las prácticas de gobernanza y gestión de TI.

Planificación estratégica: Se elaboró un instrumento gerencial que permitió planificar, priorizar y monitorear la implementación de actividades destinadas a subsanar las brechas en un horizonte de tres años.

A continuación, se muestran 3 figuras que relacionan la integración de COBIT 2019 en un ámbito empresarial:

Figura 10: *Relacionamiento Metas del PEM contra Metas Empresariales COBIT 2019.*

Tabla 1: Relacionamiento Metas del PEM contra Metas Empresariales COBIT 2019

Dimensión COBIT 2019	Metas Empresariales - COBIT 2019	Dimensión Institucional	Objetivos y Metas Plan Estratégico
Financiero	EG01-Portafolio de productos y servicios competitivos	-	-
Financiero	EG02-Gestionar los riesgos del negocio	Desarrollo Institucional	A
Financiero	EG03-Cumplimiento de leyes y regulaciones externas	Desarrollo Institucional	A
Financiero	EG04-Calidad de la información financiera	Desarrollo Institucional	A
Cliente	EG05-Cultura de servicio orientada al cliente	Desarrollo Institucional	B
Cliente	EG06-Continuidad y disponibilidad de los servicios del negocio	Desarrollo Institucional	B
Cliente	EG07-Calidad de la gestión de la información	Desarrollo Institucional	C
-	-	Desarrollo Institucional	C
-	-	Desarrollo Institucional	C
---	---	---	---

Fuente: Los signos"- - -" ubicados en la parte inferior, expresan que de acuerdo al alcance del estudio existirán más registros. Fuente: elaboración propia con base a (Cortés, 2021, p. 38)

Figura 11: *Relacionamiento entre las metas empresariales contra metas de alineamiento COBIT 2019.*

Metas Empresariales COBIT 2019		Metas de Alineamiento - COBIT 2019
Financiero	EG01-Portafolio de productos y servicios competitivos	-
Financiero	EG02-Gestionar los riesgos del negocio	AG02-Gestión de riesgo relacionado con I&T AG07-Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad
Financiero	EG03 Cumplimiento de leyes y regulaciones externas	AG01-Cumplimiento y soporte de I&T para el cumplimiento empresarial con las leyes y regulaciones externas AG11-Cumplimiento de I&T con las políticas internas
Financiero	EG04-Calidad de la información financiera	AG04-Calidad de la información financiera relacionada con la tecnología AG10-Calidad de la información sobre gestión de I&T
Cliente	EG05-Cultura de servicio orientada al cliente	AG08-Habilitar y dar soporte a procesos de negocio mediante la integración de aplicaciones y tecnología
Cliente	EG06-Continuidad y disponibilidad y de los servicios del negocio	AG07-Seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad
Cliente	EG07-Calidad de la gestión de la información	AG04-Calidad de la información financiera relacionada con la tecnología AG10-Calidad de la información sobre gestión de I&T
---	---	---

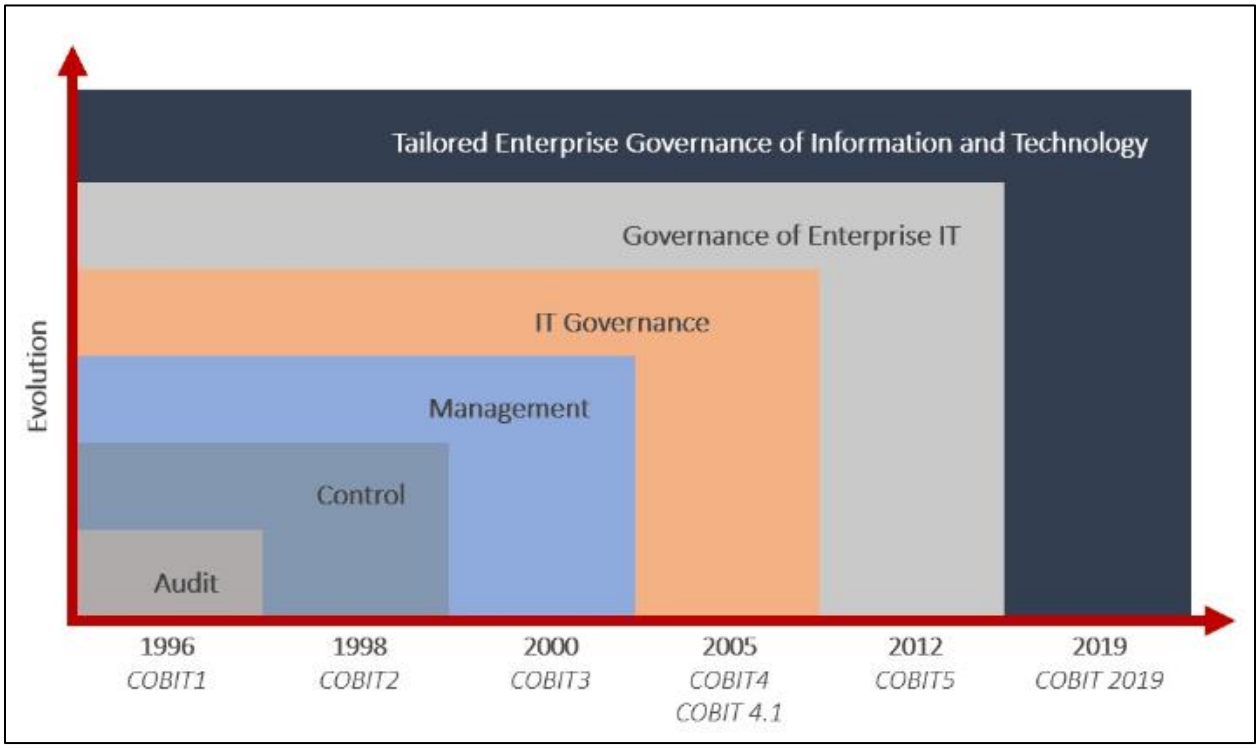
Fuente: Los signos"- - -" ubicados en la parte inferior, expresan que de acuerdo al alcance del estudio existirán más registros. Fuente: elaboración propia con base a (Cortés, 2021, p. 33).

Figura 12: *Resultado, refinamiento del proceso de cascada de metas por medio del instrumento de factores de diseño.*

Diseño del sistema de gobiernos COBIT 2019	Conclusión del alcance: Prioridad de los objetivos de gobierno/gestión	Nivel de capacidad objetivo sugerido	Nivel de capacidad objetivo decidido
EDM02-Asegurar la entrega de beneficios	35	2	2
EDM03-Asegurar la optimización del riesgo	50	3	2
EDM05-Asegurar el compromiso de las partes interesadas	40	2	2
APO01-Gestionar el marco de gestión de I&T	15	1	2
APO02-Gestionar la estrategia	0	1	2
APO05-Gestionar el portafolio	5	1	2
APO07-Gestionar los recursos humanos	30	2	2
APO08-Gestionar las relaciones	70	3	2
APO09-Gestionar los acuerdos de servicio	20	1	2
APO10-Gestionar los proveedores	-5	1	2
APO11-Gestionar la calidad	25	2	2
APO12-Gestionar los riesgos	85	4	2
APO13-Gestionar la seguridad	65	3	2
APO14-Gestionar los datos	20	1	2
BAI01-Gestionar los programas	10	1	2
BAI04-Gestionar la disponibilidad y la capacidad	5	1	2
BAI10-Gestionar la configuración	-5	1	2
BAI11-Gestionar los proyectos	-35	1	2
DSS02-Gestionar las peticiones y los incidentes de servicio	35	2	2
DSS03-Gestionar los problemas	60	3	2
DSS04-Gestionar la continuidad	65	3	2
DSS05-Gestionar los servicios de seguridad	100	4	2
DSS06-Gestionar los controles de procesos de negocio	25	2	2
MEA03-Gestionar el cumplimiento de los requisitos externos	45	2	2
MEA04-Gestionar el aseguramiento	35	2	2

Fuente: elaboración propia con base a (cortés, 2021, p. 82)

Figura 13: *Evolución de la metodología COBIT.*



Fuente: Evolución del marco COBIT, Escoute LLC

De acuerdo con el manual de usuarios de COBIT 2019, establece que esta herramienta permite hacer una evaluación de la gestión de TI en diferentes empresas donde se cuente con un departamento de este tipo, se utiliza el modelo de auditoría de gestión y control COBIT 2019 como referencia. Dicha herramienta es aplicada en Banco Ficohsa en el departamento de Cajeros automáticos.

2.4.2 ITIL 4

Según Ambit. (2024) la metodología ITIL 4 (Information Technology Infrastructure Library) establece un marco de referencia detallado para la gestión de servicios de tecnología de la información, con un enfoque en la creación de valor y la mejora continua. Un pilar fundamental dentro de este marco es la gestión de incidentes, un proceso clave para restaurar el servicio de TI a su nivel de operación normal tan pronto como sea posible, minimizando el impacto negativo en el negocio.

De acuerdo con las prácticas descritas en la literatura especializada (Ambit, 2024), el proceso de gestión de incidentes se llevó a cabo a través de una serie de pasos secuenciales y lógicos.

Fases de la Gestión de Incidentes

El proceso se iniciaba con la detección y el registro de la incidencia. Para lograr esto, se utilizaron sistemas de monitorización para identificar proactivamente los fallos en el servicio. Simultáneamente, se facilitaron herramientas multicanal (como portales web, correo electrónico y chatbots) para que los usuarios pudieran reportar los problemas. Cada incidente era registrado de forma individual, capturando datos cruciales como la hora, la fecha y una descripción del problema. A medida que avanzaba la resolución, el registro se actualizaba con información sobre las actividades realizadas y el personal asignado.

Posteriormente, se procedía con la categorización y la priorización del incidente. La categorización implicaba asignar una categoría y subcategoría al problema, lo que permitía clasificar los incidentes y revelar patrones que pudieran requerir una gestión de problemas más profunda. La priorización se determinaba en función del impacto en los usuarios y la urgencia de la situación. Los incidentes críticos, que causaban una interrupción significativa, se priorizaban sobre los de bajo impacto, lo que garantizaba el cumplimiento de los Acuerdos de Nivel de Servicio

(SLA).

Finalmente, se abordaba la resolución y el cierre del incidente. Este proceso incluía un diagnóstico inicial realizado por el personal de soporte de primer nivel. Si el problema no podía ser resuelto en esta etapa, se realizaba un escalado funcional a un grupo especializado. Para los incidentes más graves, se notificaba a los responsables a través de un escalado jerárquico. Una vez que se había encontrado y aplicado una solución, se realizaban las pruebas necesarias para asegurar que el servicio había sido restaurado. El proceso concluía con el cierre formal del incidente, momento en el que se podían recopilar comentarios de los usuarios a través de encuestas, lo que ayudaba a identificar posibles mejoras en el proceso de gestión.

La Gestión de Cambios en la Organización

La gestión de cambios se reconoció como una práctica fundamental dentro de los marcos de referencia de servicios de TI, diseñada para administrar e implementar cambios en los servicios, procesos e infraestructura de una empresa. El objetivo principal fue minimizar los riesgos de interrupciones, mejorar la eficiencia y garantizar la continuidad de los servicios frente a los cambiantes requisitos del negocio (Nexoid, 2024). Este enfoque estructurado se aplicó para planificar, ejecutar y revisar los cambios, promoviendo una colaboración efectiva entre las partes interesadas, incluyendo a los profesionales de TI, líderes empresariales y usuarios finales (Nexoid, 2024).

La metodología de gestión de cambios implicó una aproximación estructurada para planificar, ejecutar y revisar las modificaciones. El propósito fue garantizar que los cambios fueran bien comprendidos, documentados y gestionados de forma eficaz (Nexoid, 2024). Este proceso ayudó a las organizaciones a identificar y abordar los riesgos potenciales, minimizar las interrupciones del servicio y maximizar los beneficios de las iniciativas de cambio.

En la aplicación de esta metodología, los cambios se clasificaron en tres categorías principales para su gestión:

- Cambios estándar: Se trataron como cambios preautorizados y de bajo riesgo que seguían un procedimiento bien establecido.

- Cambios de emergencia: Se implementaron para resolver incidentes mayores o problemas críticos que requerían una acción urgente.
- Cambios normales: Se refirieron a cambios que no encajaban en las categorías anteriores, y su nivel de riesgo determinaba si se consideraban menores, significativos o importantes.

Para gestionar estos cambios de manera efectiva, las organizaciones a menudo utilizaron una Junta Asesora de Cambios (CAB), conformada por representantes de diversos departamentos, que se encargaba de revisar, aprobar y priorizar las solicitudes de cambio (Nexoid, 2024). Este proceso colaborativo aseguró que los cambios estuvieran alineados con los objetivos de la empresa, que se evaluaran los riesgos adecuadamente y que se implementaran de manera eficiente (Nexoid, 2024).

Subprocesos y roles clave en la gestión de cambios

La implementación de la gestión de cambios en las organizaciones se realizó a través de varios subprocesos bien definidos, cada uno con responsabilidades específicas para garantizar una ejecución controlada y exitosa.

Subprocesos de la Gestión de Cambios:

Soporte: Se estableció como la base del proceso, definiendo políticas y procedimientos, y configurando las herramientas adecuadas para la gestión de cambios.

Evaluación de la Propuesta: Se llevó a cabo una evaluación inicial de los cambios propuestos, analizando los beneficios, riesgos y el impacto en la organización antes de su clasificación y priorización.

Registro y Revisión de la Solicitud de Cambio (RFC): Se documentó formalmente el cambio propuesto en el sistema de gestión, validando la integridad y precisión de la información proporcionada.

Evaluación e Implementación de Cambios de Emergencia: Se utilizó un subproceso diseñado para manejar situaciones urgentes. Una Junta Asesora de Cambios de Emergencia (ECAB) evaluó la solicitud para su aprobación y agilización inmediata.

Evaluación del Cambio por el Administrador y el CAB: El administrador de cambios

realizó una evaluación exhaustiva y, en el caso de cambios significativos, consultó con el CAB, quienes revisaron la RFC y la evaluación para ofrecer sus recomendaciones (Nexoid, 2024).

Programación y Autorización: Una vez aprobado, se planificó la implementación del cambio y se emitió la autorización de creación, lo que permitió el desarrollo o adquisición de los recursos necesarios.

Revisión Posterior y Cierre: Se evaluó la efectividad del cambio, se identificaron problemas que surgieron durante la implementación y se documentaron las lecciones aprendidas. Finalmente, el cambio se cerró formalmente.

Roles y Responsabilidades:

Gestor de Cambios: Se consideró el responsable de supervisar el ciclo de vida completo de todos los cambios, con el objetivo de facilitar modificaciones beneficiosas con una mínima interrupción (Nexoid, 2024).

Junta Asesora de Cambios (CAB): Se definió como un grupo de partes interesadas y expertos encargados de evaluar y ofrecer recomendaciones sobre las propuestas de cambio, asegurando que se alinearan con los objetivos estratégicos.

Junta Asesora de Cambios de Emergencia (ECAB): Se encargó de tomar decisiones rápidas sobre los cambios de emergencia de alto impacto.

En resumen, ITIL 4 representa un cambio de paradigma al pasar de una gestión de procesos interna a un modelo holístico centrado en la creación conjunta de valor con el cliente. Su sistema flexible, impulsado por los principios guía y la cadena de valor, permite a las organizaciones de TI operar con mayor agilidad y alineación estratégica, lo que es esencial para la gestión de activos críticos como el software de cajeros automáticos en el sector bancario.

En ITIL 4, el concepto de "procesos" se reemplaza por el de prácticas. Las prácticas son conjuntos de recursos organizativos diseñados para llevar a cabo un trabajo o lograr un objetivo. Se dividen en tres categorías: prácticas de gestión general (como la gestión de proyectos), prácticas de gestión de servicios (como la gestión de incidentes) y prácticas de gestión técnica. Estas prácticas, que contienen los procesos, siguen siendo cruciales para la gestión interna de los proveedores de servicios, pero ahora actúan como un soporte para la cadena de valor.

La Mejora Continua es un componente central que asegura que los productos, servicios y

prácticas se mejoren constantemente a lo largo de todas las actividades de la cadena de valor. La mejora continua es un principio fundamental que permite a las organizaciones adaptarse a las demandas cambiantes y optimizar su rendimiento de manera sostenida.

2.5 INSTRUMENTOS UTILIZADOS

2.5.1 COBIT Performance Management (CPM)

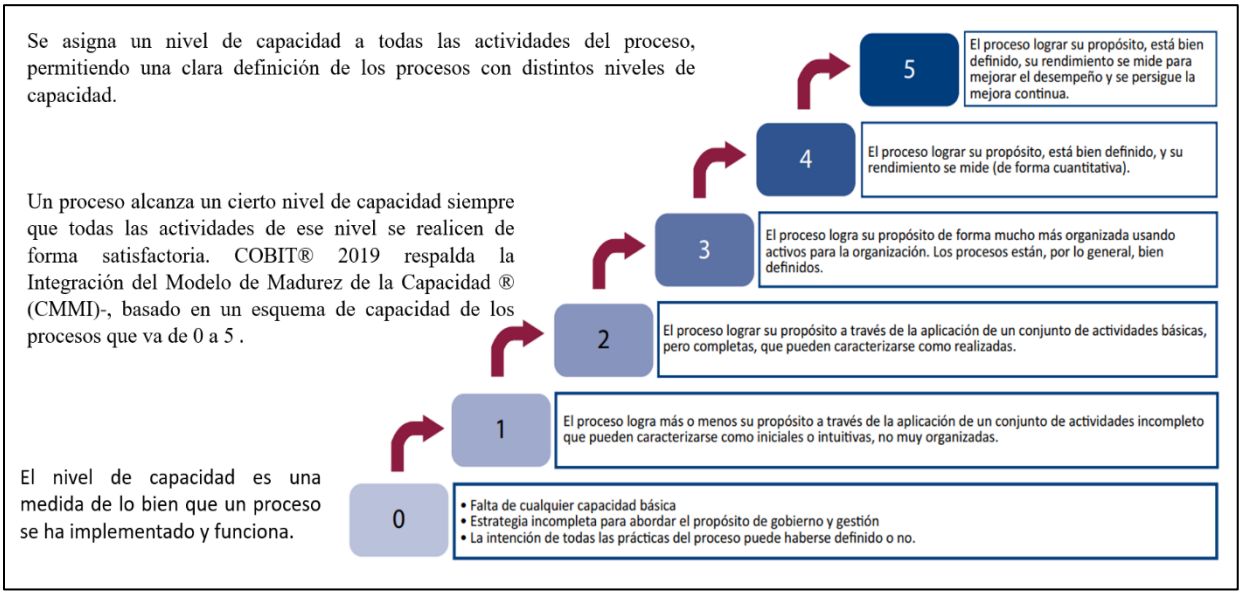
El COBIT Performance Management (CPM) es un modelo introducido en COBIT 2019 que permite evaluar, medir y mejorar el desempeño de los procesos de gobernanza y gestión de TI en una organización. Su finalidad es asegurar que los procesos se implementen de forma eficaz y eficiente, contribuyendo directamente a la creación de valor y al logro de los objetivos estratégicos del negocio.

El CPM se basa en un sistema de niveles de capacidad que permite a las organizaciones identificar el estado actual de sus procesos, establecer una línea base y definir rutas de mejora. Cada nivel describe el grado en que un proceso es capaz de alcanzar consistentemente sus propósitos, desde un nivel inicial (incompleto) hasta un nivel optimizado en el que las prácticas se encuentran plenamente institucionalizadas.

De acuerdo con ISACA (2019), el modelo de desempeño de COBIT proporciona a las organizaciones una forma estructurada de evaluar y comparar el grado de madurez de sus procesos, así como de alinear la mejora continua con las metas corporativas. Esto lo convierte en un marco de referencia práctico no solo para la gobernanza de TI, sino también para la gestión de riesgos y el aseguramiento del cumplimiento normativo.

En el contexto de la presente investigación, el CPM de COBIT 2019 se empleará como instrumento temático de análisis, ya que permitirá evaluar el nivel de desempeño de los procesos relacionados con la gestión del software de cajeros automáticos en Banco Ficohsa. De esta manera, se podrá identificar el grado de madurez actual, los riesgos asociados a posibles deficiencias en los procesos y las oportunidades de mejora que contribuyan a la continuidad y optimización del servicio. Ver Anexo 2

Figura 14: *COBIT Performance Management (CPM).*

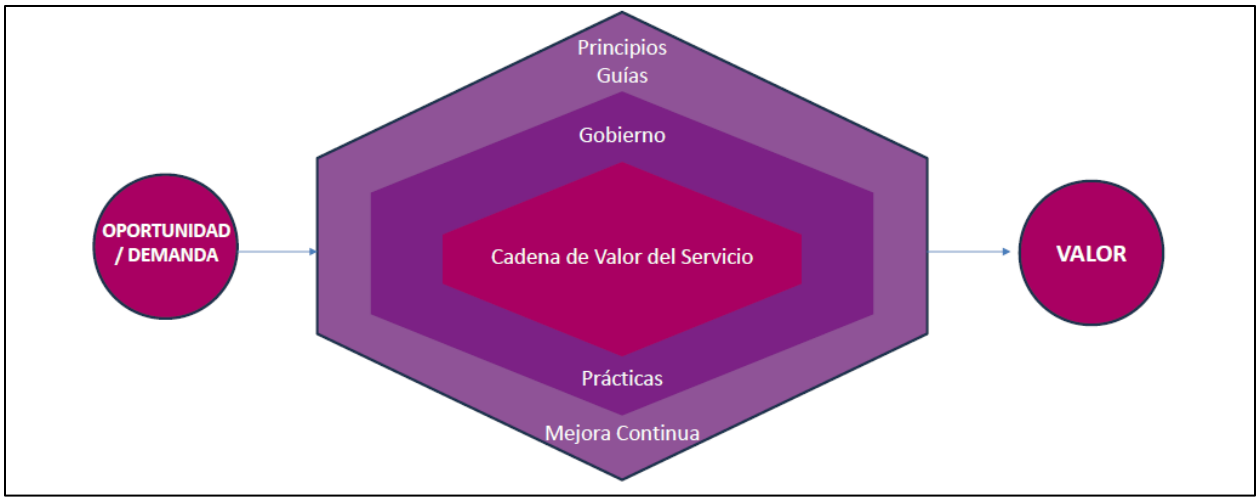


Fuente: ISACA (2019). *COBIT 2019 Framework: Governance and Management Objectives.*

2.5.2 SERVICE VALUE CHAIN (SVC) ITIL 4

El modelo central de ITIL 4 es el Sistema de Valor del Servicio (SVS), un marco operativo que transforma las oportunidades y las demandas en valor para el cliente. El SVS describe las entradas y salidas del sistema y, a partir de este marco, se deriva la Cadena de Valor del Servicio (SVC), la cual constituye un modelo operativo que describe las actividades clave necesarias para responder a la demanda y facilitar la creación de valor mediante la generación y gestión de productos y servicios.

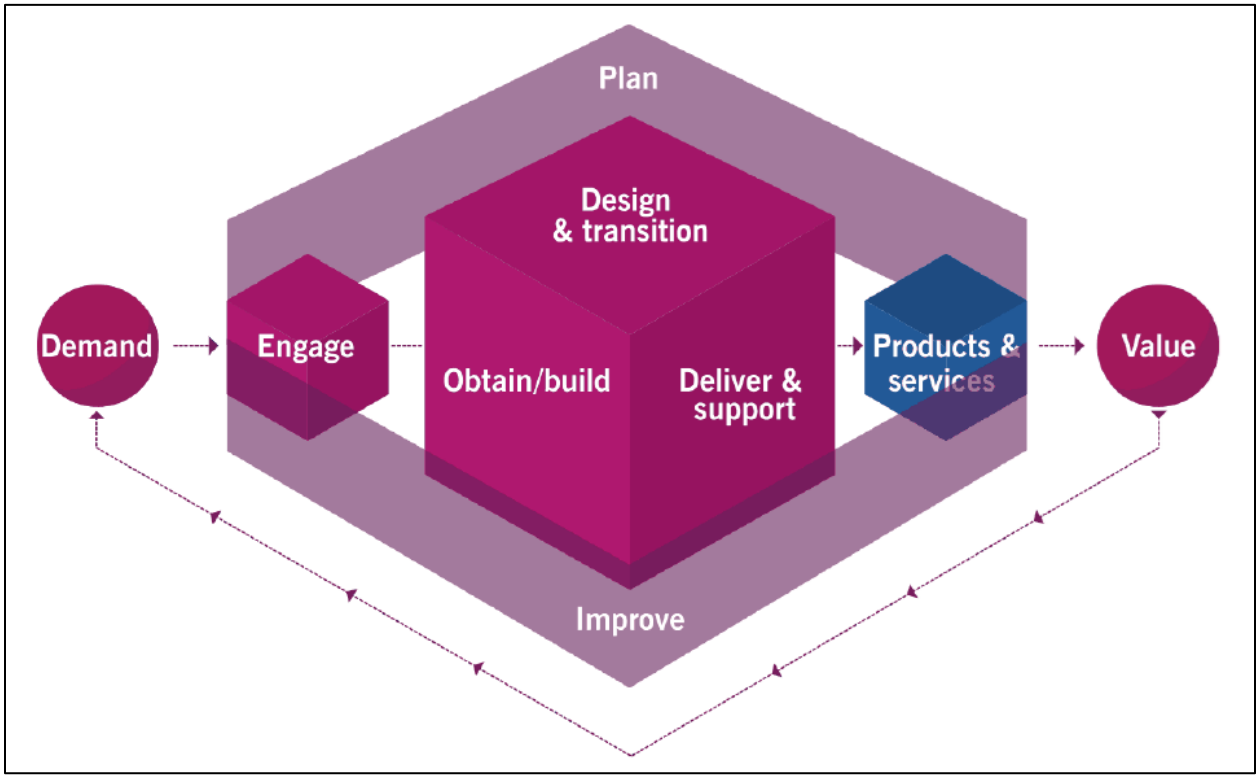
Figura 15: *Sistema de Valor del Servicio (SVS).*



Fuente: Axelos (2019). *ITIL Foundation: ITIL 4 Edition*.

De esta forma Tassier, (2020), menciona que la Cadena de Valor del Servicio (CVS) es uno de los elementos más novedosos de ITIL 4, que sustituye al ciclo de vida del servicio de ITIL v3. La CVS es un modelo operativo que define un conjunto de seis actividades interconectadas (Planificar, Mejorar, Implicar, Diseño y Transición, Obtener/Construir, y Entregar y Apoyar) que una organización combina de manera flexible y sin un orden preestablecido para crear flujos de valor. A diferencia de los procesos rígidos, los flujos de valor del servicio son secuencias específicas de estas actividades diseñadas para escenarios particulares, como la resolución de una incidencia o la entrega de un nuevo servicio. Este enfoque asegura que el trabajo esté directamente orientado a la producción de valor.

Figura 16: *Cadena de Valor del Servicio (SVC).*



Fuente: Axelos (2019). *ITIL Foundation: ITIL 4 Edition*.

En el marco de esta investigación, se empleará la Cadena de Valor del Servicio (CVS) de ITIL 4 como instrumento temático de análisis. La CVS, al ser un modelo operativo que integra seis actividades interconectadas (Planificar, Mejorar, Implicar, Diseño y Transición, Obtener/Construir, y Entregar y Apoyar), permitirá mapear y examinar las actividades críticas asociadas a la gestión del software de cajeros automáticos en Banco Ficohsa. Ver Anexo 3

2.5.3 INSTRUMENTO DE VERIFICACIÓN ITIL 4

En el marco de la investigación, además de los instrumentos ya descritos, se empleará una lista de verificación basada en prácticas de ITIL 4. Este instrumento tiene como finalidad evaluar de manera sistemática el grado de implementación y alineación de las prácticas de gestión de servicios de TI en relación con la gestión del software de cajeros automáticos. Ver Anexo 4

ITIL 4 se centra en el enfoque de valor y resiliencia a través de la Cadena de Valor del Servicio (Service Value Chain) y las 34 prácticas de gestión que integran la gestión de servicios, la gestión técnica y la gestión general. Estas prácticas proporcionan lineamientos aplicables a la

gestión de incidentes, problemas, cambios, configuraciones, disponibilidad y continuidad, entre otras áreas clave para asegurar la confiabilidad del software en un entorno bancario.

La lista de verificación se construirá a partir de las prácticas de ITIL 4 seleccionadas como más relevantes para el contexto del estudio, considerando tanto la gestión operativa como la gobernanza de servicios. Cada ítem de la lista permitirá validar la existencia, nivel de madurez o ausencia de las prácticas en la organización, generando evidencia objetiva y comparable que servirá de apoyo para el análisis posterior junto con los demás instrumentos.

Figura 17: *Prácticas ITIL 4.*

Fuente: Axelos (2019). *ITIL Foundation: ITIL 4 Edition*.

2.6 CONCEPTUALIZACIÓN

Análisis de riesgos: Es un proceso que se utiliza para identificar, evaluar y comprender los riesgos potenciales que podrían afectar a una organización, sus activos y sus procesos (ISACA, 2019).

COBIT 2019: Un marco de referencia para el gobierno y la gestión de la información y la tecnología de la empresa, que ayuda a alinear los objetivos de negocio con los de TI (ISACA, 2019).

ITIL 4: Un marco de referencia para la gestión de servicios de TI que proporciona un enfoque holístico para la creación, entrega y mejora continua de productos y servicios tecnológicos (AXELOS, 2019).

Gestión de software: El proceso de planificar, adquirir, implementar, mantener y eliminar software dentro de una organización para asegurar su uso eficiente y seguro (The Open Group., 2011).

Cajeros automáticos (ATM): Terminales bancarias electrónicas que permiten a los clientes realizar operaciones financieras como retiros, depósitos y transferencias sin la necesidad de un cajero humano (Federal Reserve Bank of Atlanta, 2020).

Amenazas cibernéticas: Eventos o acciones que tienen el potencial de causar daño a un sistema de información, una red o a los datos de una organización, con intenciones maliciosas (NIST, 2018).

SLA (Acuerdos de Nivel de Servicio): Un contrato entre un proveedor de servicios y un cliente que define el nivel de servicio que se espera, especificando métricas de calidad y responsabilidades (AXELOS, 2019).

KPIs (Indicadores Clave de Desempeño): Métricas cuantificables que miden el rendimiento de un proceso o actividad en relación con los objetivos establecidos por una organización (Kaplan & Norton, 1996).

Gobernanza de TI: El sistema por el cual se dirigen, controlan y supervisan las tecnologías de la información de una organización para apoyar el logro de los objetivos del negocio (ISACA, 2019).

Marco de referencia: Una estructura o un conjunto de estándares, pautas o mejores prácticas que proporcionan una guía para la implementación de un proceso o sistema (ISO/IEC, 2018).

Gestión de incidentes: El proceso para restaurar el servicio a la normalidad lo más rápido posible después de una interrupción, minimizando el impacto negativo en las operaciones del negocio (AXELOS, 2019).

Mejora continua: Una metodología para optimizar continuamente los productos, servicios y procesos de una organización, lo que resulta en un rendimiento mejorado y una mayor eficiencia (Deming, 2000).

Vulnerabilidades: Debilidades en el diseño, la implementación o la operación de un sistema de información que podrían ser explotadas por una amenaza (NIST, 2018).

Riesgos operativos: La probabilidad de pérdidas resultantes de la inadecuación o de fallas de procesos, personal y sistemas internos, o de eventos externos (Basel Committee on Banking Supervision, 2022).

Digitalización: El uso de tecnologías digitales para cambiar un modelo de negocio y crear nuevas oportunidades de ingresos y valor (Gartner, 2020).

Malware: Software malicioso diseñado para dañar, robar o interrumpir los datos y sistemas informáticos sin el consentimiento del usuario (NIST, 2018).

Modelo de Confianza Cero (Zero Trust): Un modelo de seguridad que asume que no hay una red interna confiable, y que todas las solicitudes de acceso deben ser verificadas de forma rigurosa, sin importar la ubicación (National Institute of Standards and Technology , 2020).

Biometría: La tecnología de autenticación que mide y analiza las características físicas o de comportamiento de una persona para verificar su identidad (Federal Bureau of Investigation, 2020).

NFC (Near Field Communication): Tecnología de comunicación inalámbrica de corto alcance que permite que dos dispositivos electrónicos intercambien datos cuando se acercan (NFC Forum, 2020).

Software multivendor: Software que permite a las organizaciones gestionar y monitorear dispositivos de diferentes fabricantes desde una sola plataforma unificada (Kalms, 2018).

Gestión de Software: Es el conjunto de prácticas, procesos y herramientas orientadas a planificar, dirigir, coordinar y controlar el desarrollo, operación y mantenimiento de sistemas de software a lo largo de su ciclo de vida, con el objetivo de entregar productos de alta calidad dentro de plazos y presupuestos, alineados con las necesidades del negocio. Aborda áreas como gestión de proyectos, requisitos, configuración, calidad, riesgos, métricas, colaboración entre partes interesadas y gestión de recursos (Sommerville, 2016).

2.7 MARCO LEGAL

2.7.1 MARCO LEGAL Y REGULATORIO DE COBIT 2019: UN MECANISMO GLOBAL PARA EL CUMPLIMIENTO

El marco COBIT (Control Objectives for Information and Related Technology), desarrollado por la ISACA, no es una ley en sí mismo, sino una guía de gobernanza y gestión de

TI diseñada para ayudar a las organizaciones a cumplir con el creciente número de requisitos legales y regulatorios a nivel mundial (Stephenson, 2024). En un entorno de constante cambio digital y amenazas cibernéticas, COBIT 2019 se ha consolidado como una herramienta fundamental para alinear los objetivos de negocio con la estrategia de TI, garantizando el cumplimiento normativo y la gestión de riesgos (Guzzi, s.f.). Su propósito es proporcionar un enfoque integral que reduzca la probabilidad de infracciones costosas y asegure la continuidad del negocio.

2.7.2 PRINCIPIOS Y FACILITADORES PARA EL CUMPLIMIENTO

El sistema de gobernanza de COBIT 2019 se sustenta en seis principios clave que guían su implementación:

Satisfacer las necesidades de las partes interesadas: Asegura que los objetivos de TI se alineen con los requerimientos de la alta dirección, gerencia, personal de TI, reguladores y proveedores (Guzzi, 2024.).

Enfoque holístico: Considera todos los componentes de la organización (personas, procesos, estructuras, cultura, información, servicios e infraestructura) para una gobernanza integrada.

Sistema de gobernanza dinámico: El marco es flexible y adaptable, permitiendo ajustes continuos para responder a los cambios tecnológicos y del negocio.

Separación de gobernanza y gestión: Establece roles y responsabilidades claras, donde la gobernanza se enfoca en la evaluación, dirección y monitoreo, y la gestión se centra en la planificación, construcción y ejecución (Stephenson, 2024).

Adaptación a las necesidades de la empresa: Utiliza factores de diseño para personalizar el sistema de gobernanza según la estrategia, el perfil de riesgo, el panorama de amenazas y los requisitos regulatorios de la organización (Stephenson, 2024).

Un sistema de gobernanza integral: Permite la integración con otros marcos de referencia como ITIL, ISO 27001 y NIST, creando un ecosistema de gobernanza coherente y unificado.

Estos principios se implementan a través de siete facilitadores que son esenciales para el éxito de los procesos de TI: principios y políticas, procesos, estructuras organizativas, cultura y ética, información, servicios e infraestructura, y las personas con sus habilidades y competencias.

Estos elementos interconectados aseguran que la gobernanza de TI sea completa y efectiva.

2.7.3 COBIT 2019 Y SU ROL EN EL CUMPLIMIENTO NORMATIVO

El marco COBIT 2019 actúa como un facilitador del cumplimiento normativo a través de su estructura y componentes. Históricamente, ha sido una herramienta clave para el cumplimiento de normativas como la Ley Sarbanes-Oxley (SOX) en EE. UU., y su evolución ha fortalecido esta capacidad. La versión 2019 introduce el Modelo Central, que consta de 40 objetivos de gobernanza y gestión agrupados en cinco dominios: Evaluar, Dirigir y Monitorear (EDM); Alinear, Planificar y Organizar (APO); Construir, Adquirir e Implementar (BAI); Entregar, Servir y Dar Soporte (DSS); y Monitorear, Evaluar y Valorar (MEA) (Stephenson, 2024).

A diferencia de otros marcos como ITIL, que se enfoca en la gestión de servicios, o NIST, que se centra en la ciberseguridad, COBIT ofrece un enfoque holístico y de alto nivel. Proporciona el "idioma común" para la gobernanza, lo que facilita la comunicación entre la dirección, los equipos de TI y los reguladores (Guzzi, s.f.). El marco permite mapear las funciones de seguridad del NIST con sus objetivos de gobernanza, asegurando que los controles de ciberseguridad estén alineados con los objetivos de negocio y la tolerancia al riesgo.

Finalmente, COBIT 2019 ayuda a las organizaciones a optimizar sus recursos, mitigar riesgos y garantizar el cumplimiento mediante la automatización de procesos. La integración con soluciones de gestión de seguridad de la información (SGSI) y software de gestión de cumplimiento permite la monitorización en tiempo real del estado de cumplimiento y optimiza los procedimientos de auditoría y documentación. En esencia, COBIT proporciona una base sólida para que las empresas naveguen por el complejo panorama de la gestión de TI y logren sus objetivos de cumplimiento normativo de manera eficaz.

2.7.4 MARCO LEGAL ITIL 4

Marco Legal de la Normativa ITIL 4: Un Enfoque de Apoyo al Cumplimiento y la Gobernanza

A diferencia de marcos como COBIT 2019, que se enfocan en la gobernanza empresarial de la tecnología, ITIL 4 es un conjunto de mejores prácticas para la gestión de servicios de TI (ITSM) (Stephen, 2025). Por lo tanto, ITIL 4 no constituye un marco legal en sí mismo, sino que funciona como una herramienta metodológica esencial para ayudar a las organizaciones a cumplir y mantener los requisitos legales y regulatorios. Su enfoque flexible y orientado al valor permite a las empresas integrar la seguridad, la gestión de riesgos y el cumplimiento normativo directamente

en la prestación de sus servicios digitales. Este rol de apoyo es crucial para garantizar que las operaciones de TI sean resilientes y se ajusten a los estándares legales de la industria (Farnham, 2025).

2.7.5 ITIL 4 COMO FACILITADOR DEL CUMPLIMIENTO NORMATIVO

El marco de ITIL 4 aborda la gestión de servicios de manera holística, incluyendo dimensiones clave que son intrínsecamente relevantes para el cumplimiento legal. Las prácticas de gestión de ITIL 4 están diseñadas para guiar a las organizaciones a través de la complejidad de la gestión de TI en el entorno digital, abordando directamente aspectos que, si no se gestionan adecuadamente, podrían acarrear riesgos legales y financieros. Las siguientes prácticas, demuestran la contribución de ITIL al marco legal de una organización:

Gestión de la Seguridad de la Información: Esta práctica es fundamental, ya que busca proteger la confidencialidad, integridad y disponibilidad de los datos. Al implementar sus directrices, las organizaciones se aseguran de que sus procesos cumplan con regulaciones de protección de datos (Irwin, 2022), lo cual es vital para evitar infracciones y daños a la reputación.

Gestión de Activos de TI: La gestión del ciclo de vida de los activos de TI, desde su adquisición hasta su disposición, es esencial para el cumplimiento. Esta práctica aborda explícitamente los requisitos regulatorios y contractuales relacionados con los activos, garantizando que su uso y retiro se adhieran a las normativas vigentes (Stephen, 2025).

Desarrollo y Gestión de Software: En el proceso de diseño y construcción de aplicaciones, ITIL 4 enfatiza la necesidad de considerar la fiabilidad, el mantenimiento, el cumplimiento normativo y la capacidad de auditoría (Irwin, 2022). Esto asegura que el software cumpla con los estándares de la industria y las leyes aplicables, lo que es crítico en sectores regulados como el bancario.

Gestión de Riesgos: ITIL 4 promueve una comprensión integral y un enfoque proactivo en la gestión de riesgos (Irwin, 2022). Al abordar los riesgos de manera temprana, las organizaciones pueden mitigar las posibles consecuencias de problemas de TI, incluidas las interrupciones del servicio y las violaciones de seguridad que podrían tener repercusiones legales.

Gobierno y Mejoramiento Continuo: ITIL 4, al igual que COBIT 2019, distingue entre gobernanza (evaluación, dirección y monitoreo) y gestión (planificación, implementación y

soporte). Esta separación refuerza la supervisión estratégica y la rendición de cuentas, elementos clave en el cumplimiento corporativo. La mejora continua es un principio fundamental que garantiza que las prácticas se adapten constantemente a las nuevas demandas del negocio y a las regulaciones en evolución (Stephen, 2025).

Aunque ITIL 4 no prescribe leyes, sus directrices de gestión de servicios brindan un marco operativo que sustenta y facilita la adhesión de una organización a los estándares regulatorios globales. Actúa como el motor que impulsa la excelencia operativa y la seguridad, ayudando a las empresas a crear una base sólida para el cumplimiento normativo y la gestión de riesgos.

2.7.6 ENTORNO LEGAL Y LEGISLATIVO HONDURAS

En Honduras, la operación de cajeros automáticos está regulada por:

El Código de Comercio y las normativas fiscales vigentes.

La Ley Contra el Lavado de Dinero u Otros Activos, que obliga a informar operaciones sospechosas.

Disposiciones de la Comisión Nacional de Bancos y Seguros (CNBS) y del Banco Central de Honduras, que establecen estándares de seguridad, disponibilidad y continuidad de negocio para los servicios financieros automatizados.

CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ENFOQUE

Este estudio pretende explorar la metodología COBIT 2019 e ITIL 4, ante un problema de riesgo en la gestión de software de cajeros automáticos de una de las compañías financieras de renombre en el sistema bancario hondureño. Para establecer el enfoque de la investigación se realiza el análisis preliminar de los objetivos propuestos:

Tabla 6: *Matriz de análisis del enfoque de los objetivos específicos.*

Objetivo específico	Enfoque
Identificar y analizar las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software de cajeros automáticos de Banco Ficohsa, considerando los procesos, métricas y prácticas vigentes.	Cualitativo
Evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 al análisis de riesgos y gestión de incidentes en el software de cajeros automáticos de Banco Ficohsa, con el fin de proponer acciones de mejora.	Cualitativo
Definir indicadores clave de desempeño (KPIs) y métricas de seguimiento que permitan evaluar la efectividad de las estrategias de mitigación propuestas y fomenten un ciclo de mejora continua en la gestión del software de cajeros automáticos.	Cuantitativo
Diseñar un modelo integrado de gestión basado en COBIT 2019 e ITIL 4 que fortalezca la administración del software de cajeros automáticos y responda de manera efectiva a los requisitos del entorno financiero actual.	Cualitativo
Identificar y analizar los beneficios que Banco Ficohsa podría obtener a futuro al implementar la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4 para la optimización del software de cajeros automáticos.	Cualitativo

Fuente: Elaboración propia

En este sentido, esta propuesta adquiere un enfoque mixto, debido a la diversidad de información que puede recolectarse, una parte de esta se medirá cuantitativamente y la otra de manera cualitativa, usar este enfoque permitirá tener un panorama más amplio ya que la información recolectada será diversa.

De acuerdo con Hernández Sampieri y Mendoza Torres (2018), se describe el enfoque cuantitativo de investigación como un proceso secuencial y riguroso que se utiliza para medir y analizar fenómenos de manera objetiva. Parte de una idea que se va delimitando hasta establecer objetivos e hipótesis que se someterán a prueba. La recolección de datos se realiza a través de mediciones numéricas, utilizando procedimientos estandarizados y métodos estadísticos para su análisis.

La meta principal de este enfoque es confirmar y predecir los fenómenos investigados,

buscando relaciones causales y regularidades para la formulación y demostración de teorías, y los resultados se interpretan a la luz de las predicciones iniciales y los estudios previos. El proceso se caracteriza por ser lo más objetivo posible, intentando generalizar los hallazgos de una muestra a una población más grande. De igual forma, Hernández Sampieri y Mendoza Torres (2018) mencionan que con el enfoque cualitativo se tiene una gran amplitud de ideas e interpretaciones que enriquecen el fin de la investigación. El alcance final del estudio cualitativo consiste en comprender un fenómeno social complejo, más allá de medir las variables involucradas, se busca entenderlo.

3.2 ALCANCE

Según Cortés y Iglesias (2004) este alcance se realiza cuando se va a examinar o estudiar un tema poco abordado, si es que la revisión de la literatura revela que no hay muchos estudios acerca del tema o vagamente relacionadas con el problema, o, si se desea indagar un tema desde otras áreas, perspectivas o enfoques. De acuerdo con Salinas y Cárdenas (2009) estos estudios son mucho más flexibles en su metodología a comparación de los otros alcances. Como menciona Hurtado (2010) este tipo de investigación es común en disciplinas como la ingeniería y la administración, ya que permite proponer soluciones a partir de un proceso de investigación previo.

El alcance de esta investigación es exploratorio y descriptivo. El estudio se centra en el análisis de riesgos en el software de cajeros automáticos, con el fin de proponer un plan de acción para resolver las necesidades y problemas identificados, sin llegar a ejecutar el plan propuesto.

3.3 DISEÑOS

El estudio se basa en un diseño no experimental, ya que no se manipularon las variables de estudio ni se someterá a los sujetos a condiciones experimentales. La evaluación se realizará en su contexto natural, sin alterar ninguna situación. Dentro de este diseño, se utilizará un enfoque transversal, lo que significa que la recolección de datos se llevará a cabo en un único momento.

Este enfoque es comparable a "tomar una foto o una radiografía" para su posterior análisis. El diseño transversal es adecuado para investigaciones con alcances exploratorios, descriptivos y correlacionales.

3.4 POBLACIÓN

Acerca de las poblaciones, Gregorio Rojas (2023) explica: Las unidades de análisis son los objetos o personas con ciertas características especiales que proveen la información para

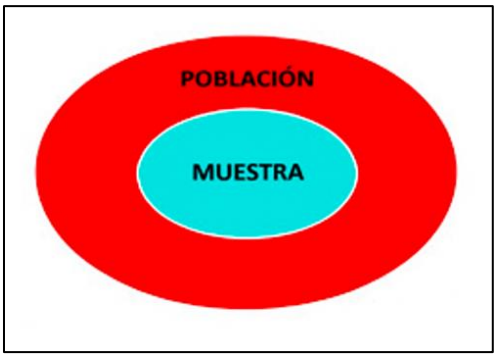
comprender el problema. Estás unidades, deben reunir ciertos requisitos para estar incluidos en el marco de elegibilidad requerido en el estudio, a fin de que puedan ser útiles en el proceso de investigación (p. 148).

En el caso particular de Banco Ficohsa, el departamento de TI cuenta con su respectiva área de Medios de Pago ATMS. Sin embargo, la investigación se centrará específicamente en el proceso para gestionar software de cajeros automáticos, pues forma parte del alcance de esta. De igual forma como población se tomarán los marcos de referencia COBIT 2019 e ITIL 4.

Lo descrito por el autor nos permite visualizar que existe un gran conjunto que engloba los elementos de un todo (población).

El siguiente diagrama ejemplifica esta relación

Figura 18: *Diagrama que ejemplifica la relación entre población y muestra.*



Fuente: Elaboración propia

3.5 MUESTRA

Podemos deducir entonces que una muestra no es otra cosa que un segmento de ese todo, Puntualizando desde una perspectiva más cualitativa Hernández Sampieri establece que: “En la ruta cualitativa, es el grupo o conjunto de personas, eventos, sucesos, comunidades, etc., sobre el cual se habrán de recolectar los datos, sin que necesariamente sea estadísticamente representativo del universo o población que se estudia” (Hernández Sampieri & Mendoza Torres, 2018, p. 447).

Como hemos detallado, en la dimensión de personas la muestra la conformaría el especialista en gestión de software de cajeros automáticos, el jefe de soporte técnico de ATMs, el Gerente de Medios de Pago ATMS y el responsable de cumplimiento normativo, en la sección de procesos, incluye los flujos de trabajo y actividades relacionadas con la gestión del software de

cajeros automáticos, y en el apartado de marcos de referencia COBIT 2019 e ITIL 4, nos enfocaremos en los estándares y framework que guían la gestión del software de cajeros automáticos para Banco Ficohsa.

Tabla 7: *Resumen de población y muestra de la investigación*

Dimensión	Población	Muestra
Personal	4	4
Procesos	1	1
Marcos de Referencia	2	2

Fuente: Elaboración propia

3.6 TÉCNICAS DE MUESTREO

El muestreo para este estudio es de tipo no probabilístico o por conveniencia. Según Hernández Sampieri y Mendoza Torres (2018), la muestra puede estar compuesta tanto por individuos como por "herramientas, servicios y procesos". Para efectos de esta investigación, la muestra coincide con la población, dado que se trata de un universo reducido y se ha decidido trabajar con su totalidad.

3.7 CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

3.7.1 PERSONAL

Banco Ficohsa cuenta con personal preparado y con experiencia en diferentes campos del conocimiento. Sin embargo, por los propósitos que persigue esta investigación se tomaran en cuenta los siguientes criterios de inclusión y exclusión:

Tabla 8: *Criterios de inclusión y exclusión del personal.*

Criterios de Inclusión	Criterios de Exclusión
Personal de Medios de Pago TI involucrado en la gestión, desarrollo, mantenimiento y operación del software de cajeros automáticos	Personal de Medios de Pago TI que no esté directamente involucrado en la gestión, desarrollo, mantenimiento u operación del software de cajeros automáticos
Personal con credenciales y autorizaciones para acceder a entornos de desarrollo, pruebas y producción relacionados con ATMs y sistemas de pago.	Personal sin autorización para acceder a entornos de desarrollo, pruebas o producción de sistemas de cajeros.
Personal con capacitación mínima en seguridad de datos, KYC/AML y estándares de protección de información sensible como PCI DSS o equivalentes	Empleados con sanciones o suspensiones administrativas, con restricciones laborales, suspensión temporal o vulneraciones a políticas de seguridad que

locales.	impidan acceso a sistemas de pagos.
Personal que dé su consentimiento informado para la participación y cuya información pueda ser manejada de forma confidencial según políticas institucionales.	Personal que no haya recibido el consentimiento informado adecuado para participar en el proyecto y cuyos datos no puedan ser manejados confidencialmente de acuerdo con las políticas institucionales.

Fuente: Elaboración propia

3.7.2 PROCESOS

Como institución financiera, Banco Ficohsa cuenta con múltiples procesos por departamento, pero, para efectos de esta investigación nos enfocaremos específicamente en aquel ligado a la Gestión de software para cajeros automáticos.

Tabla 9: *Criterios de inclusión y exclusión de procesos.*

Criterios de Inclusión	Criterios de Exclusión
Identificar y caracterizar los procesos clave involucrados en la gestión del software de cajeros automáticos, asegurando seguridad, cumplimiento y eficiencia operativa.	Procesos que no tienen impacto directo o indirecto en la gestión del software de cajeros automáticos (ATM) y/o no contribuyen a seguridad, cumplimiento o eficiencia operativa del software de ATM.
Procesos que abarcan análisis de riesgos, diseño, desarrollo, pruebas, validación, versión y despliegue en entornos de ATM (producción, staging, testing).	Procesos no vinculados a Medios de Pago ATMs, como aquellos que no impactan directa o indirectamente en el software de cajeros automáticos o en su ciclo de vida.
Procesos de detección, clasificación, escalamiento, resolución, comunicación de incidentes, pruebas de recuperación y revisión pos incidente.	Procesos sin interacción con la plataforma de ATM, que no participan en desarrollo, despliegue, seguridad o soporte del software de ATM de Banco Ficohsa.

Fuente: Elaboración propia

3.7.3 MARCOS DE REFERENCIA

La línea temática abordada en este trabajo de investigación está basada en los marcos de referencia COBIT 2019 e ITIL 4, para lo cual tomaremos los siguientes criterios de inclusión y exclusión:

Tabla 10: *Criterios de inclusión y exclusión de marcos de referencia.*

Criterios de inclusión	Criterios de exclusión
Identificar cómo los marcos de referencia COBIT 2019 e ITIL 4 se integran para apoyar la gestión del software de cajeros	Procesos, prácticas o componentes de COBIT 2019 e ITIL 4 que no aporten de forma directa o indirecta a la gobernanza, gestión de servicios,

automáticos, con énfasis en gobierno, gestión de servicios, seguridad y continuidad.	seguridad o continuidad del software de cajeros automáticos (ATM) de Banco Ficohsa.
COBIT 2019 aplicado a gobernanza y gestión del software de ATM, incluyendo objetivos de gobierno y gestión relevantes para el software de ATM (por ejemplo, gestión de riesgos, aseguramiento de la confiabilidad del software, cumplimiento, gestión de cambios, control de acceso y seguridad de la información).	Procesos, prácticas o dominios de COBIT 2019 que no aporten de forma directa o indirecta a la gobernanza y gestión del software de cajeros automáticos (ATM), o que no se alineen con los objetivos de negocio, seguridad, cumplimiento y continuidad del software de ATM.
ITIL 4 aplicado a la gestión del servicio y del ciclo de vida del software de ATM, incluyendo las prácticas de ITIL 4 relevantes para desarrollo, despliegue, operación y mejora continua del software de ATM.	Prácticas, procesos o dominios de ITIL 4 que no aporten de forma directa o indirecta a la gestión del servicio y del ciclo de vida del software de cajeros automáticos (ATM), o que no estén alineados con el desarrollo, despliegue, operación y mejora continua del software de ATM.

Fuente: Elaboración propia

3.8 ESQUEMA DE VARIABLES

A continuación, se presentan las variables que estructuran la investigación, clasificadas en dependientes e independientes según su función dentro del estudio. Las variables independientes corresponden a los marcos de referencia y al modelo propuesto (COBIT 2019 e ITIL 4), en tanto que las variables dependientes reflejan los efectos o resultados esperados en la gestión del software de cajeros automáticos de Banco Ficohsa. Asimismo, se expone la relación que cada variable mantiene con los objetivos de la investigación, lo cual permite comprender de manera clara cómo se vinculan los elementos teóricos con la realidad práctica objeto de análisis.

Tabla 11: *Esquema de variables*

Tipo de Variable	Variable	Relación en el Estudio
Variable Dependiente	Amenazas y vulnerabilidades en la gestión del software de cajeros automáticos	Permite diagnosticar la situación actual del software de cajeros, identificando los principales riesgos que afectan su operación y que justifican la necesidad de aplicar marcos de referencia como COBIT 2019 e ITIL 4.
Variable Independiente	Aplicabilidad de COBIT 2019 e ITIL 4 en el análisis de riesgos y gestión de incidentes.	Representa la propuesta de intervención del estudio, al evaluar qué principios y prácticas de los marcos de referencia son pertinentes y adaptables para mejorar la gestión de riesgos en el software de cajeros de Banco Ficohsa.

Variable Dependiente	Efectividad de estrategias de mitigación.	Refleja el impacto que tendría la aplicación de las estrategias basadas en COBIT 2019 e ITIL 4, midiendo si realmente se logra reducir incidentes, mejorar los tiempos de respuesta y garantizar un ciclo de mejora continua.
Variable Independiente	Modelo integrado de gestión	Constituye el resultado central del trabajo de investigación, ya que busca diseñar un modelo de gestión que combine ambos marcos de referencia para optimizar la administración del software de cajeros y alinearlo con los objetivos estratégicos del banco.
Variable Dependiente	Beneficios de la implementación del modelo de gestión.	Evidencia el valor agregado esperado del estudio, identificando los beneficios que Banco Ficohsa podría obtener en términos de reducción de riesgos, mayor disponibilidad de cajeros, cumplimiento regulatorio y generación de confianza en los usuarios.

Fuente: Elaboración propia

3.9 OPERACIONALIZACIÓN DE VARIABLES

En esta sección se procede a la operacionalización de las variables definidas en el estudio, con el propósito de transformar conceptos abstractos en elementos medibles y observables que permitan analizar de manera objetiva la gestión de software para cajeros automáticos. La operacionalización constituye una etapa esencial en la investigación, dado que facilita la desagregación de cada variable en dimensiones, indicadores e instrumentos que posibilitan su evaluación empírica. Según Santiesteban Naranjo (2014), “operacionalizar significa otorgar valores a los constructos principales que aparecen en ella”, lo cual reduce el sesgo y otorga rigor científico al análisis.

Para garantizar mayor claridad metodológica, la operacionalización de variables se presenta en formato tabular, donde se incluyen la definición teórica y operativa de cada variable, así como las dimensiones, indicadores e instrumentos correspondientes.

Tabla 12: *Operacionalización de variables*

Variable	Definición Teórica	Definición Operativa	Dimensiones	Indicadores	Instrumentos
Amenazas y vulnerabilidades en la gestión del software de cajeros automáticos	Según ISO 27005 (2018), una vulnerabilidad es una debilidad de un activo que puede ser explotada por una amenaza, mientras que una amenaza es un evento potencialmente dañino que compromete la confidencialidad, integridad o disponibilidad de un sistema.	Evaluación de número de incidentes reportados, frecuencia de fallos en cajeros automáticos y nivel de cumplimiento de controles establecidos.	Procesos actuales de gestión.	Número de incidentes de seguridad reportados, Frecuencia de fallos en el software de cajeros, Grado de cumplimiento de controles actuales.	Entrevista semiestructurada y matriz de análisis documental
Aplicabilidad de COBIT 2019 e ITIL 4 en el análisis de riesgos y gestión de incidentes.	COBIT 2019 (ISACA, 2018) es un marco de gobierno y gestión de TI que proporciona principios, objetivos y prácticas para alinear la tecnología	Se evaluará mediante instrumentos de COBIT 2019 e ITIL 4, y entrevistas a personal de medios de pago ATM.	Principios de gobierno (COBIT 2019), Prácticas de gestión de incidentes (ITIL 4), Adaptación a procesos internos del banco.	Nivel de alineación entre procesos actuales y buenas prácticas, Grado de adecuación de COBIT 2019 a la estructura de TI, Porcentaje de incidentes gestionados con prácticas ITIL.	Entrevista semiestructurada, COBIT performance management (CPM), Service Value Chain (SVC) ITIL 4 y Lista de verificación basada en ITIL 4.

	con los objetivos del negocio. ITIL 4 (Axelos, 2019) es un marco de gestión de servicios que promueve prácticas para gestionar incidentes, problemas y cambios en los sistemas tecnológicos.				
Efectividad de estrategias de mitigación.	La efectividad en la gestión de riesgos (ISACA, 2018) se refiere al grado en que las medidas implementadas reducen la probabilidad o impacto de los riesgos. En ITIL 4, la mejora continua se mide a través de KPIs que monitorean la calidad	Se medirá mediante KPIs como tiempo promedio de resolución de incidentes, porcentaje de incidentes recurrentes y cumplimiento de SLA.	Definición de KPIs, Seguimiento de métricas y Mejora continua.	Tiempo promedio de resolución de incidentes, Porcentaje de incidentes recurrentes y Cumplimiento de los SLA definidos.	Dashboard y análisis comparativo de indicadores, reportes de desempeño y formatos de seguimiento.

	del servicio.				
Modelo integrado de gestión	Un modelo de gestión integrado es una estructura que combina prácticas, procesos y marcos de referencia para optimizar la administración de TI. La integración de COBIT 2019 e ITIL 4 busca alinear gobierno y gestión de servicios.	Se definirá en términos de la cantidad de procesos y prácticas incorporados y el grado de coherencia del modelo con los objetivos estratégicos del banco.	Estructura del modelo, integración de prácticas COBIT 2019 e integración de prácticas ITIL 4.	Cantidad de procesos incorporados del marco COBIT 2019, número de prácticas ITIL 4 incluidas y grado de coherencia con los objetivos del área de medios de pago ATM.	Matriz de análisis documental
Beneficios de la implementación del modelo de gestión.	Según ISACA (2018), los beneficios de la gestión de TI incluyen reducción de riesgos operativos, cumplimiento normativo, eficiencia en el uso de recursos y creación de valor para el negocio.	Se medirá mediante indicadores comparativos antes y después: reducción de incidentes críticos, menor tiempo de inactividad y satisfacción de usuarios.	Reducción de riesgos operativos, mejora en eficiencia del servicio de cajeros, cumplimiento normativo y regulatorio y valor para el negocio.	Disminución de incidentes críticos, reducción del tiempo de inactividad de cajeros y nivel de satisfacción de usuarios internos y externos.	Encuesta y análisis comparativo de indicadores antes/después.

Fuente: Elaboración propia

3.10 HIPÓTESIS

En las investigaciones con enfoque cuantitativo o mixto, las hipótesis constituyen proposiciones que permiten establecer relaciones entre variables y someterlas a verificación mediante indicadores y métricas objetivas. Hernández Sampieri señala que una hipótesis es una explicación tentativa del fenómeno investigado, formulada como una proposición susceptible de ser comprobada empíricamente (Hernández Sampieri & Mendoza Torres, 2018, p. 447).

Esta investigación, al adoptar un enfoque exploratorio-descriptivo con énfasis en el diseño de una propuesta de mejora, no requiere el planteamiento de hipótesis en su formulación tradicional (es decir, relación causa y efecto entre variables). Por lo tanto, se define la hipótesis basada en el hecho de que la naturaleza del objetivo específico 3 es cualitativo, en este sentido, orientado a la definición de indicadores clave de desempeño (KPIs) y métricas de seguimiento para evaluar la efectividad de las estrategias de mitigación propuestas, se plantea la siguiente hipótesis de investigación:

La implementación de estrategias de mitigación basadas en COBIT 2019 e ITIL 4 mejora significativamente la efectividad en la gestión del software de cajeros automáticos, evidenciada por la reducción del número de incidentes críticos y la disminución del tiempo promedio de resolución de incidentes en un período de seis meses.

3.11 TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTOS Y PLAN DE ANÁLISIS

3.11.1 TÉCNICAS

Las técnicas de investigación constituyen los procedimientos específicos que permiten llevar a la práctica el método seleccionado, asegurando que la recolección de datos se realice de manera rigurosa y confiable. Estas técnicas funcionan como un puente entre la teoría y la realidad observada, ya que facilitan la identificación, análisis y comprensión de los fenómenos estudiados. En el caso de esta investigación, orientada al análisis de riesgos con COBIT 2019 e ITIL 4 en la gestión del software de cajeros automáticos de Banco Ficohsa, la selección de técnicas se fundamenta en la necesidad de obtener tanto información cualitativa como cuantitativa que respalde el planteamiento de la propuesta y la validación de sus beneficios.

Entre las técnicas a emplear para la recolección de información podemos mencionar:

Entrevista semiestructurada: Técnica de recolección de datos en la que el investigador

formula preguntas abiertas, pero con alguna guía temática estructurada, permitiendo explorar percepciones, experiencias y opiniones profundas de los participantes. (Chand, 2025).

Observación directa: Según Chand (2025) esta técnica consiste en el registro sistemático de comportamientos, interacciones y contexto en el entorno natural de los sujetos de estudio, sin intervención del investigador.

Análisis documental: Esta técnica implica la revisión, interpretación y síntesis de textos, registros, informes institucionales y otros documentos relevantes para extraer información útil para la investigación.

3.11.2 INSTRUMENTOS TEMÁTICOS

Para organizar mejor los instrumentos se categorizaron por su naturaleza en temáticos y metodológicos, esta estructura también se verá reflejada en la sección de Anexos.

- **COBIT Performance Management (CPM):** Herramienta utilizada en el marco de referencia COBIT 2019 que se basa en un sistema de niveles de capacidad que permite a las organizaciones identificar el estado actual de sus procesos. Ver Anexo 2.
- **Service Value Chain (SVC) ITIL 4:** Es un modelo operativo que define un conjunto de seis actividades interconectadas (Planificar, Mejorar, Implicar, Diseño/Transición, Obtener/Construir, y Entregar/Apoyar) que una organización combina de manera flexible y sin un orden preestablecido para crear flujos de valor. Ver Anexo 3.
- **Lista de Verificación basada en ITIL 4:** Instrumento diseñado a partir de las prácticas más relevantes de ITIL 4, orientado a evaluar de forma estructurada la existencia, nivel de aplicación y madurez de dichas prácticas en la gestión del software de cajeros automáticos. La lista permite validar prácticas relacionadas con gestión de incidentes, problemas, cambios, disponibilidad, continuidad y seguridad, entre otros, asegurando así un análisis integral en concordancia con los objetivos de la investigación. Ver Anexo 4.

3.11.3 INSTRUMENTOS METODOLÓGICOS

Los instrumentos metodológicos por utilizar son:

- **Matriz de análisis documental:** Documento que sintetiza los datos relevantes de las

fuentes consultadas para sustentar la investigación. Ver Anexo 5.

- **Cuestionario semiestructurado:** Es el instrumento correspondiente a la técnica de la entrevista y se conformará por las preguntas Ver Anexo 6.
- **Dashboard de indicadores de seguimiento:** Herramienta visual que permite consolidar y presentar de forma dinámica los indicadores de gestión definidos en la investigación. Facilita la comparación en distintos periodos de tiempo y posibilita la toma de decisiones basada en evidencia. Ver Anexo 7.
- **Reporte de desempeño:** Documento estructurado que registra los resultados obtenidos en la aplicación de procesos o estrategias. Constituye evidencia objetiva para medir avances, identificar desviaciones y evaluar el cumplimiento de los objetivos planteados. Ver Anexo 8.
- **Formatos de seguimiento:** Plantillas estandarizadas que sirven para recopilar, organizar y verificar información de manera sistemática sobre la ejecución de actividades, incidentes y acciones correctivas en la gestión del software de cajeros automáticos. Ver Anexo 9.
- **Encuesta:** Instrumento de recolección de información estructurada, aplicada a una muestra de participantes, que permite obtener datos cuantitativos y cualitativos sobre percepciones, experiencias y valoraciones en torno a los beneficios que generaría la implementación del modelo de gestión basado en COBIT 2019 e ITIL 4 Ver Anexo 10

3.12 PROCEDIMIENTO DE APLICACIÓN

A continuación, se expone brevemente el procedimiento a seguir según cada instrumento descrito en la investigación

Tabla 13*: Procedimiento de aplicación*

Instrumento	Procedimiento
COBIT PERFORMANCE MANAGEMENT (CPM) COBIT 2019	-Definir qué procesos de TI y de negocio abarcarán CPM, como ser entrega y soporte de software ATM, gestión de cambios, operaciones, continuidad, seguridad de la información. -Priorizar procesos con mayor impacto en disponibilidad, seguridad y experiencia del cliente. -Establecer objetivos de negocio y de TI alineados a la gestión

	de software de ATM. -Aplicar un modelo de madurez, por ejemplo, escalas de madurez de COBIT o propia de la organización para cada proceso CPM. -Desarrollar planes de mitigación específicos vinculados a procesos CPM.
SERVICE VALUE CHAIN (SVC) ITIL 4	-Realizar un mapeo de la cadena de valor de servicio (SVC). - Identificar las cinco actividades centrales de SVC en el contexto de la gestión de software de ATM. - Recolectar datos extrayendo métricas de cada actividad de la SVC, como tiempos de diseño, pruebas, despliegue, incidencias, disponibilidad. -Evaluar si cada actividad aporta valor y los riesgos asociados con seguridad, cumplimiento, impacto operativo entre otros. -Alinear las actividades de la SVC con los procesos de COBIT 2019 para asegurar una gestión de software integral.
Matriz de análisis documental	-Identificar fuentes clave: Documentos oficiales de COBIT 2019 e ITIL 4, políticas internas de Banco Ficohsa, manuales de software de cajeros automáticos y normativas del sector bancario. Crear una matriz con categorías como: Marco de referencia (COBIT/ITIL), procesos relacionados, riesgos identificados, controles sugeridos y brechas actuales. -Analizar los documentos y completar la matriz con información relevante. -Identifica áreas de mejora y oportunidades de optimización.
Cuestionario semiestructurado	Diseñar un cuestionario con preguntas abiertas y cerradas. Incluyendo temas como: percepción de riesgos, cumplimiento de COBIT 2019/ITIL 4, desafíos operativos y sugerencias de mejora. -Seleccionar a los participantes: personal de gestión de software, jefatura y gerente de MDP ATM. -Realizar las entrevistas o encuestas, asegurando registrar respuestas detalladas. -Analizar las respuestas para identificar patrones, problemas recurrentes y áreas de oportunidad.
Dashboard y análisis comparativo de indicadores de seguimiento	-Visualizar datos clave sobre la gestión del software y los riesgos identificados. -Definir los indicadores clave de rendimiento (KPIs) relacionados con la gestión del software, como ser tiempo de disponibilidad, tasa de errores, cumplimiento de controles. -Seleccionar una herramienta para crear el dashboard: Power BI. -Integrar los datos recopilados de la matriz documental y el cuestionario en el dashboard. -Diseña visualizaciones claras y útiles para monitorear el

	desempeño y los riesgos en tiempo real.
Reporte de desempeño	-Definir métricas clave para identificar indicadores de rendimiento (KPIs) relacionados con la disponibilidad, seguridad, eficiencia y cumplimiento del software. -Recopilar datos utilizando herramientas de monitoreo internas y registros históricos para obtener datos sobre el desempeño del software. -Comparar los datos recopilados con los estándares establecidos por COBIT 2019 e ITIL 4, y así identificar brechas y áreas de mejora. -Elaborar el reporte, presentando los hallazgos de manera clara y estructurada, incluyendo gráficos y tablas.
Formatos de seguimiento	-Diseñar el formato. -Analizar los datos recopilados en el formato para identificar retrasos o desviaciones para cada actividad relacionada con la gestión del software.

Fuente: Elaboración propia

3.13 PLAN DE ANÁLISIS DE DATOS

El presente estudio emplea un enfoque mixto, por lo que el análisis de datos se llevará a cabo en dos vertientes complementarias: cualitativa y cuantitativa. Esta integración permitirá comprender en profundidad las amenazas, vulnerabilidades y deficiencias en la gestión del software de cajeros automáticos, así como medir el impacto de las estrategias propuestas. A continuación, se plantea el plan de análisis a seguir para cada instrumento a aplicar:

COBIT Performance Management (CPM)

Permitirá evaluar el nivel de capacidad de los procesos relacionados con la gestión del software de cajeros automáticos, con el fin de identificar brechas, riesgos y oportunidades de optimización, las fases en que se realizará el análisis es el siguiente:

- Análisis descriptivo: Cálculo de promedios y porcentajes de nivel alcanzado en cada actividad de cada proceso evaluado.
- Comparación: Identificar diferencias entre procesos críticos.
- Mapeo visual: Gráficos radar o de barras para visualizar el nivel de capacidad por práctica evaluada.

Service Value Chain (SVC) ITIL 4

Permitirá evaluar la efectividad de las actividades de la cadena de valor de los servicios

relacionados con el software de cajeros automáticos, con el fin de identificar deficiencias, riesgos operativos y oportunidades de mejora, las fases en que se realizará el análisis son el siguiente:

- Análisis descriptivo: Cálculo de promedios y porcentajes de cumplimiento de cada actividad de la cadena de valor. Identificar qué tanto las prácticas actuales del software de cajeros automáticos se alinean con cada actividad.
- Comparación: Contrastar los resultados entre actividades críticas de la SVC para poder identificar en que actividades se tiene un mayor grado de madurez.
- Mapeo visual: Gráficos de barras o pastel para mostrar el nivel de desempeño y madurez por actividad de la SVC. Representación de flujos de valor: evidenciar puntos de mayor aporte y cuellos de botella en la gestión del software de cajeros automáticos.

Lista de Verificación basada en ITIL 4

Permitirá medir el grado de cumplimiento de las prácticas ITIL 4 aplicables a la gestión del software de cajeros automáticos, con el fin de detectar brechas, riesgos y áreas que requieren acciones correctivas, las fases en que se realizará el análisis son el siguiente:

- Análisis descriptivo: Cálculo de porcentajes de cumplimiento por práctica y cálculo de promedios generales de cumplimiento en la gestión del software de cajeros automáticos.
- Comparación: Identificar prácticas con mayor y menor nivel de cumplimiento y contrastar estos resultados entre prácticas críticas.
- Mapeo visual: Gráficos de barras para mostrar porcentaje de cumplimiento por práctica. Gráfico radar para representar la alineación global con ITIL 4.

Matriz de análisis documental

Permitirá analizar la literatura académica, normativa y técnica relacionada con COBIT 2019, ITIL 4 y la gestión de riesgos en software de cajeros automáticos, con el fin de identificar tendencias, vacíos de investigación y buenas prácticas aplicables, las fases en que se realizará el análisis son el siguiente:

- Análisis descriptivo: Distribución de documentos por año (tendencia de publicaciones recientes), frecuencia de aparición de temas e identificación de autores o instituciones

más citados/referentes.

- Comparación de los recursos obtenidos para contrastar enfoques.
- Obtener síntesis estructurada de la literatura más relevante para COBIT, ITIL 4.

Cuestionarios semiestructurados

Permitirá recopilar percepciones, experiencias y evidencias del personal responsable de la gestión del software de cajeros automáticos, con el fin de identificar riesgos, deficiencias y oportunidades de mejora, las fases en que se realizará el análisis son el siguiente:

- Análisis descriptivo: Cálculo de promedios, frecuencias y porcentajes para preguntas cerradas. Conteo de menciones de temas y categorías en preguntas abiertas.
- Análisis cualitativo: Codificación temática de respuestas abiertas: identificación de patrones, tendencias, riesgos y buenas prácticas. Agrupación por categorías relevantes para los objetivos de la tesis (incidentes, continuidad, seguridad, mejora continua).
- Comparación: Contrastar percepciones entre distintos roles y perfiles. Identificar discrepancias entre percepción de riesgos y cumplimiento real de procesos.
- Mapeo visual: Gráficos para mostrar percepciones cuantitativas. Nube de palabras o diagramas de categorías para representar hallazgos cualitativos.

Dashboard de indicadores de seguimiento

Para analizar los datos recopilados mediante el diseño y la creación de un Dashboard con la herramienta Power BI, comenzaremos con la transcripción y organización de la información que nos permitirá:

- Monitorear y comparar indicadores clave de gestión del software de cajeros automáticos, basado en los marcos COBIT 2019 e ITIL 4.
- Consolidar los indicadores de gestión definidos en la investigación.
- Facilitar la comparación de datos en distintos periodos de tiempo.
- Proporcionar una herramienta visual para la toma de decisiones basada en evidencia para la gestión de riesgos y la operación de software de cajeros automáticos (ATM).

Alcance y cobertura

- Indicadores de riesgo vinculados a COBIT 2019 (gobernanza y gestión de riesgos) y ITIL 4 (gestión de servicios).
- Indicadores de desempeño de software de cajeros (Uptime, disponibilidad, tiempo de inactividad, MTTR, incidentes, cambios, configuración, seguridad).
- Periodos: mensual, trimestral y anual; también comparación interanual donde aplique.
- Usuarios: PMO/único responsable de IT, operaciones de ATM.

Reporte de desempeño

Es un documento estructurado que registra y analiza los resultados obtenidos en la aplicación de procesos o estrategias relacionadas con la gestión del software de cajeros automáticos.

Este reporte sirve como evidencia objetiva para medir avances, identificar desviaciones y evaluar el cumplimiento de los objetivos planteados en la investigación.

Propósito y alcance del instrumento

- Definir claramente en el Reporte de desempeño los resultados obtenidos al aplicar procesos/estrategias (COBIT 2019 e ITIL 4) en la gestión del software de cajeros automáticos.
- Establecer el alcance temporal (p. ej., trimestre/semestre) y de sistema (p. ej., software de CAJEROS, plataformas de monitoreo, servicios de TI relacionados).
- Utilizar los principios de COBIT 2019 para definir métricas clave y los procesos de ITIL 4 para evaluar la gestión de servicios.

Identificación de Métricas y KPI

- COBIT 2019: Seleccionar métricas alineadas con los objetivos de gobierno y gestión de TI (ej.: porcentaje de tiempo de actividad, tasa de errores en transacciones).
- ITIL 4: Incorporar métricas de gestión de servicios, como tiempos de respuesta, resolución de incidentes y satisfacción del usuario.

Análisis de Resultados

- Comparación con objetivos: Evaluar si los resultados cumplen con los objetivos

planteados (ej.: disponibilidad del 99.9%).

- Identificación de desviaciones: Detectar áreas donde el desempeño no cumple con los estándares esperados.

Evaluación de Cumplimiento

- COBIT 2019: Verificar el cumplimiento de los procesos de gobierno y gestión de TI.
- ITIL 4: Evaluar si los servicios de TI están alineados con las necesidades del negocio y si se están siguiendo las mejores prácticas.
- Evidencia objetiva: Documentar hallazgos con datos concretos (ej.: gráficos, tablas, estadísticas).

Propuestas de Mejora

- Acciones correctivas: Sugerir medidas para abordar las desviaciones identificadas (ej.: actualización de software, capacitación del personal).
- Optimización de procesos: Proponer mejoras basadas en las mejores prácticas de COBIT 2019 e ITIL 4.
- Plan de implementación: Establecer un cronograma y responsables para ejecutar las mejoras.

Formatos de seguimiento

Esta plantilla está diseñada para recopilar, organizar y verificar información de manera sistemática sobre la ejecución de actividades, incidentes y acciones correctivas en la gestión del software de cajeros automáticos. Los datos recopilados mediante los formatos de seguimiento pueden analizarse para identificar tendencias, riesgos recurrentes y áreas de mejora.

- Identificación de patrones recurrentes: Analizar incidentes comunes (por ejemplo, software de cajeros que falla en una ubicación específica, o un problema frecuente de seguridad).
- Evaluación del rendimiento del software: Utilizar los incidentes reportados para evaluar la fiabilidad del software en el tiempo.
- Evaluación de la eficacia de las acciones correctivas: Determinar si las soluciones

implementadas son efectivas a largo plazo o si se requiere un cambio en el enfoque.

- Priorización de riesgos: Aplicar los principios de COBIT 2019 para clasificar los incidentes según su impacto y probabilidad, para gestionar los riesgos más críticos primero.

3.14 FUENTES DE INFORMACIÓN

3.14.1 FUENTES PRIMARIAS

Según Sampieri, R. (2006), las fuentes primarias son la base de la investigación, ya que ofrecen datos originales y no procesados por otros. En el contexto de tu estudio, los documentos del Banco Ficohsa (como manuales de políticas, procedimientos y registros de eventos críticos) se consideran fuentes primarias porque son la evidencia directa y la materia bruta de tu análisis, tales como:

- Manuales de políticas y procesos del banco.
- Manual de procedimientos de eventos críticos en sistemas ATM.
- Registros de monitoreo de incidentes y problemas en el software de cajeros automáticos.
- Entrevistas anónimas con encargados de las áreas de TI y personal responsable de los ATM.

3.14.2 FUENTES SECUNDARIAS

Para Hernández Sampieri, R. (2006), las fuentes secundarias se definen como compilaciones, resúmenes y listados de referencias que ya han sido publicadas en un área de conocimiento específica. Esencialmente, estas fuentes "reprocesan" la información de las fuentes primarias para proporcionar una visión general o resumida del tema. En esta investigación, se utilizan para fundamentar teóricamente los conceptos y metodologías aplicadas. Las principales fuentes secundarias incluyen:

- Tesis, artículos de investigación y libros especializados.
- Documentos y guías de buenas prácticas.
- Artículos y estudios académicos.

3.15 MATRIZ METODOLÓGICA

Tabla 14: *Matriz metodológica*

Preguntas de Investigación	Objetivos	Metodología	Variables	Dimensiones	Indicadores	Instrumentos
¿Cuáles son las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software de cajeros automáticos de Banco Ficohsa, considerando los procesos, métricas y prácticas vigentes?	Identificar y analizar las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software de cajeros automáticos de Banco Ficohsa, considerando los procesos, métricas y prácticas vigentes.	Cualitativa	Amenazas y vulnerabilidades en la gestión del software de cajeros automáticos	Procesos actuales de gestión.	Número de incidentes de seguridad reportados, Frecuencia de fallos en el software de cajeros, Grado de cumplimiento de controles actuales.	Entrevista semiestructurada y matriz de análisis documental
¿Cómo se pueden adaptar y aplicar los principios y prácticas de COBIT 2019 e ITIL 4 para el análisis de riesgos y gestión de incidentes en el contexto	Evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 al análisis de riesgos y gestión de incidentes en el software	Cualitativa	Aplicabilidad de COBIT 2019 e ITIL 4 en el análisis de riesgos y gestión de incidentes.	Principios de gobierno (COBIT 2019), Prácticas de gestión de incidentes (ITIL 4), Adaptación a procesos internos del banco.	Nivel de alineación entre procesos actuales y buenas prácticas, Grado de adecuación de COBIT 2019 a la estructura de TI, Porcentaje de incidentes gestionados	Entrevista semiestructurada, COBIT performance management (CPM) y Service Value Chain (SVC) ITIL 4

específico del software de cajeros automáticos de Banco Ficohsa?	de cajeros automáticos de Banco Ficohsa, con el fin de proponer acciones de mejora.				con prácticas ITIL.	
¿Qué indicadores clave de desempeño (KPIs) y métricas de seguimiento permitirán evaluar la efectividad de las estrategias de mitigación propuestas y fomentar un ciclo de mejora continua?	Definir indicadores clave de desempeño (KPIs) y métricas de seguimiento que permitan evaluar la efectividad de las estrategias de mitigación propuestas y fomenten un ciclo de mejora continua en la gestión del software de cajeros automáticos.	Cuantitativa	Efectividad de estrategias de mitigación.	Definición de KPIs, Seguimiento de métricas y Mejora continua.	Tiempo promedio de resolución de incidentes, Porcentaje de incidentes recurrentes y Cumplimiento de los SLA definidos.	Dashboard y análisis comparativo de indicadores, reportes de desempeño y formatos de seguimiento.
¿Cómo puede diseñarse un modelo de optimización que integre	Diseñar un modelo integrado de gestión basado en COBIT 2019 e ITIL 4 que	Cualitativa	Modelo integrado de gestión	Estructura del modelo, integración de prácticas COBIT 2019 e integración de prácticas ITIL 4.	Cantidad de procesos incorporados del marco COBIT 2019, número de prácticas ITIL 4	Matriz de análisis documental

COBIT 2019 e ITIL 4 para fortalecer la gestión del software de cajeros automáticos y responder a los requisitos del entorno financiero actual?	fortalezca la administración del software de cajeros automáticos y responda de manera efectiva a los requisitos del entorno financiero actual.				incluidas y grado de coherencia con los objetivos del área de medios de pago ATM.	
¿Qué beneficios obtendrá Banco Ficohsa a futuro al aplicar la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4 para optimizar la gestión del software de cajeros automáticos?	Identificar y analizar los beneficios que Banco Ficohsa podría obtener a futuro al implementar la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4 para la optimización del software de cajeros automáticos.	Cualitativa	Beneficios de la implementación del modelo de gestión.	Reducción de riesgos operativos, mejora en eficiencia del servicio de cajeros, cumplimiento normativo y regulatorio y valor para el negocio.	Disminución de incidentes críticos, reducción del tiempo de inactividad de cajeros y nivel de satisfacción de usuarios internos y externos.	Encuesta y análisis comparativo de indicadores antes/después.

Fuente: Elaboración propia

CAPÍTULO IV. RESULTADOS Y ANÁLISIS

En el presente capítulo se procede a la presentación, al análisis y a la discusión de los datos recopilados a través de la aplicación de los instrumentos metodológicos diseñados: las listas de verificación y las guías de observación. Estos instrumentos fueron construidos a partir de los indicadores de control y buenas prácticas de los marcos COBIT 2019 e ITIL 4, y aplicados a los procesos clave del personal de Tecnología de la Información de Banco Ficohsa. Esta información es crucial para dar respuesta a la pregunta de investigación general: ¿Cómo puede un análisis de riesgos basado en COBIT 2019 e ITIL 4 contribuir a la formulación de estrategias de mitigación para optimizar la gestión del software de cajeros automáticos en Banco Ficohsa, garantizando continuidad operativa, seguridad y cumplimiento regulatorio?

Mediante la realización de este análisis se permite evaluar variables específicas dentro de la investigación, tales como la identificación de las amenazas y vulnerabilidades más críticas que afectan la gestión del software de ATMs (Objetivo Específico 1), la evaluación de las brechas existentes entre las prácticas actuales y los estándares de COBIT 2019 e ITIL 4 (Objetivo Específico 2), y la validación de las necesidades para la definición de KPIs y métricas de seguimiento (Objetivo Específico 3).

Los hallazgos derivados de esta fase de investigación se estructuran de forma detallada, realizando un desglose de los resultados obtenidos en función de cada uno de los objetivos específicos planteados en el Capítulo I. Este proceso analítico permitió identificar y cuantificar los factores críticos de riesgo, las oportunidades de mejora en la gobernanza de TI y la gestión de servicios, y la viabilidad técnica para la formulación de un modelo integrado de gestión. En última instancia, este capítulo proporciona la base empírica sólida y necesaria para el diseño de la propuesta final en el Capítulo V, asegurando que las estrategias de mitigación se alineen con la realidad operativa de Banco Ficohsa.

4.1 PRINCIPALES AMENAZAS, VULNERABILIDADES Y DEFICIENCIAS EN LA GESTIÓN ACTUAL DEL SOFTWARE.

El primer objetivo busca analizar las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software de cajeros automáticos de Banco Ficohsa, considerando los procesos, métricas y prácticas vigentes. Para lograrlo, se aplicó un enfoque metodológico mixto que combinó el juicio experto del personal clave con la revisión documental, cuyos resultados se presentan a continuación.

4.1.1 INSTRUMENTOS APLICADOS

- Entrevista semiestructurada:

La recogida de información se realizó a través de la aplicación de un Cuestionario Semiestructurado al personal clave de las áreas de Tecnología de la Información (TI) y Operaciones de Cajeros Automáticos de Banco Ficohsa. Este cuestionario fue diseñado para obtener información cualitativa y cuantitativa que permitiera evaluar tres ejes centrales: 1) el estado de la gestión de incidentes y disponibilidad del software de ATMs; 2) la percepción del riesgo operativo y de seguridad; y 3) el nivel de conocimiento y aplicabilidad de los marcos de referencia COBIT 2019 e ITIL 4.

Es de destacar que la muestra obtenida es intencional y reducida (N=4), compuesta por personal altamente experimentado, centrando en la calidad de la información y el juicio experto para el análisis de riesgos, en lugar de la generalización estadística. Los resultados, por tanto, reflejan la visión de los profesionales más directamente involucrados en la gestión diaria del software de los cajeros automáticos.

Validación de Instrumento

Para asegurar la calidad metodológica del instrumento de recolección de datos utilizado en la presente investigación, se realizó un proceso de validación mediante juicio de experto y una prueba piloto aplicada a un colaborador del área de Medios de Pago - Cajeros Automáticos de Banco Ficohsa.

El objetivo de la validación fue comprobar la claridad, pertinencia y relevancia de las preguntas planteadas en relación con la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4, orientada a optimizar la gestión del software.

Como resultado del proceso de validación, el instrumento fue ajustado realizando mejora en la pregunta numero 9 cambiando a selección múltiple para la respuesta, priorizando claridad y profundidad técnica. Se determinó que la entrevista semiestructurada resultante es válida y adecuada para recabar información relevante para la identificación y análisis de riesgos asociados a la gestión del software de cajeros automáticos.

4.1.2 PARTICIPANTES Y SUS CARACTERÍSTICAS

La muestra del cuestionario semiestructurado estuvo compuesta por personal altamente experimentado, lo que confiere alta credibilidad a los hallazgos:

El 100% de los participantes cuenta con más de 10 años de experiencia en el área,

confirmando su rol como expertos en la gestión del software ATM.

La muestra se distribuye equitativamente entre Operaciones de Cajeros Automáticos y Tecnología de la Información (TI), asegurando una visión balanceada de la gestión del riesgo desde la perspectiva operativa y la perspectiva técnica.

4.1.3 ENTORNO ACTUAL DEL SOFTWARE DE CAJEROS AUTOMÁTICOS EN BANCO FICOHSA

El ecosistema de cajeros automáticos (ATM) de Banco Ficohsa opera bajo una arquitectura robusta y estandarizada, diseñada para garantizar la disponibilidad, seguridad y eficiencia transaccional. La base de este entorno es el sistema operativo Windows 10 IoT Enterprise LTSB, el cual proporciona el soporte fundamental para la ejecución de las aplicaciones del ATM. Sobre esta base, se implementan soluciones específicas según el fabricante del hardware, utilizando Diebold VCP LITE y NCR Secure Base OS Hardening para asegurar y optimizar los sistemas operativos de las terminales.

La gestión y el mantenimiento de esta infraestructura tecnológica se realizan en estrecha colaboración con proveedores especializados: D&G, encargado de la flota Diebold, y TECNASA, responsable de las unidades NCR.

Desde una perspectiva de ciberseguridad y protección de datos, el entorno incorpora componentes críticos para mitigar riesgos. La protección a nivel de endpoint se gestiona a través del antivirus Trellix, mientras que la integridad y confidencialidad de la información en tránsito se asegura mediante protocolos de encriptación TLS (Transport Layer Security) para las comunicaciones entre el switch transaccional y los cajeros automáticos.

A nivel de integraciones internas y flujo transaccional, la red de cajeros interactúa directamente con el switch BASE24, que actúa como intermediario para la autorización de operaciones contra el core bancario T24. Finalmente, para garantizar la continuidad operativa y la visibilidad en tiempo real del estado de la red, se utilizan herramientas avanzadas de monitoreo como INETCO y Outside View, permitiendo una gestión proactiva de incidencias y análisis de transacciones.

4.1.4 PROCESOS ACTUALES DE GESTION DE SOFTWARE DE CAJEROS AUTOMATICOS EN BANCO FICOHSA

La gestión del ciclo de vida del software en la red de cajeros automáticos de Banco Ficohsa se ejecuta mediante un modelo híbrido, con una fuerte dependencia de los proveedores tecnológicos para el suministro de actualizaciones y una gestión interna enfocada en la validación,

autorización y despliegue operativo. A continuación, se detallan los flujos de trabajo actuales:

GESTIÓN DE ACTUALIZACIONES Y PARCHES DE SEGURIDAD

El proceso de mantenimiento correctivo y evolutivo es reactivo y dependiente del proveedor. No existe un calendario interno autónomo de parches; en su lugar, la gestión se inicia a través de canales de comunicación directos (correo electrónico y reuniones virtuales) con los proveedores (D&G Diebold y TECNASA NCR). Estos actores notifican la disponibilidad de parches de seguridad o mejoras funcionales, actuando como el disparador del proceso de actualización.

IMPLEMENTACIÓN DE NUEVAS VERSIONES (RELEASE MANAGEMENT)

El despliegue de nuevas versiones del sistema operativo o del aplicativo del ATM sigue un flujo secuencial jerárquico:

-Notificación del Fabricante: El proveedor informa oficialmente sobre una nueva actualización del sistema operativo o firmware.

-Aprobación Gerencial: Se requiere un visto bueno explícito de la gerencia para iniciar el proyecto de actualización, evaluando la necesidad y el impacto.

-Transición al Laboratorio: Una vez aprobado, el software se traslada al entorno de pruebas para su validación técnica antes de cualquier intento de instalación en la red comercial.

ASEGURAMIENTO DE LA CALIDAD (QA) Y DESPLIEGUE

Para mitigar riesgos operativos, Banco Ficohsa utiliza un entorno de Laboratorio de Pruebas Físicas.

-Validación: Todas las actualizaciones se instalan y prueban exhaustivamente en cajeros automáticos de prueba que replican la configuración de producción.

-Capacitación Técnica: Posterior a la certificación en laboratorio, se programa la capacitación del personal técnico. Esta transferencia de conocimiento es un requisito previo para la instalación en campo.

-Ventana de Despliegue: La masificación de la actualización en toda la red de ATMs se planifica en un cronograma estimado de dos meses, asegurando una implementación gradual.

GESTIÓN DE INCIDENTES

La operación diaria y la respuesta ante fallos se centralizan en el Centro de Operaciones de Red (NOC) de ATMs. El flujo de gestión de incidentes se basa en:

-Detección y Registro: Los operadores del NOC monitorean el estado de la red y, ante una

alerta o reporte, proceden a la apertura de tickets en la plataforma de gestión de servicios IVANTI.

-Escalamiento: Los incidentes de software que no pueden resolverse en primer nivel son escalados a las áreas de soporte correspondientes o a los proveedores externos según la complejidad.

GESTIÓN DE LA CONFIGURACIÓN Y REPOSITORIOS

Actualmente, la custodia de la línea base de configuración y los repositorios de software no se gestiona de manera centralizada internamente. Esta responsabilidad está delegada en los proveedores tecnológicos (Diebold y Tecnasa NCR), quienes administran las versiones "master" y las configuraciones específicas del hardware, lo que implica una dependencia externa para la recuperación o auditoría de las configuraciones base.

CICLO DE VIDA DEL SOFTWARE EN EL ENTORNO ATM

El ciclo de vida actual del software se comporta de la siguiente manera:

-Identificación (Proveedor): Notificación de updates.

-Autorización (Banco): Visto bueno gerencial.

-Validación (Banco): Pruebas en laboratorio físico (QA).

-Preparación (Banco): Capacitación del personal técnico.

-Despliegue (Mixto): Instalación en red en un periodo de 2 meses.

-Operación y Soporte (Banco/NOC): Gestión de incidentes vía IVANTI.

IDENTIFICACIÓN PRELIMINAR DE RIESGOS EN LA GESTIÓN DEL SOFTWARE DE ATMS

Matriz de identificación de vulnerabilidades y amenazas potenciales derivadas del modelo operativo actual, clasificándolas según el proceso impactado y su posible consecuencia en la operación de Banco Ficohsa.

Tabla 15: *Riesgos identificados en la gestión del Software de ATMs*

ID	Proceso / Elemento Asociado	Riesgo Identificado (Descripción)	Impacto Potencial en el Negocio	Alineación de Solución (COBIT/ITIL)
R01	Gestión de Actualizaciones y Parches	Dependencia Reactiva del Proveedor: La identificación de parches depende exclusivamente de notificaciones externas (correos/reuniones) sin	Obsolescencia tecnológica y exposición prolongada a brechas de seguridad si el proveedor retrasa la comunicación o si el correo se omite.	COBIT BAI03: Gestión de soluciones. ITIL: Gestión de Seguridad de

		un monitoreo proactivo interno de vulnerabilidades del sistema operativo (Windows 10 IoT) o aplicaciones.		la Información.
R02	Implementación y Despliegue (Release Management)	Ventana de Exposición Amplia: El tiempo de despliegue de 2 meses para toda la red genera un entorno híbrido donde coexisten versiones vulnerables y actualizadas, dificultando la estandarización.	Riesgo de ataques dirigidos a los cajeros no actualizados durante el periodo de transición (ataques de día cero). Inconsistencia en la experiencia del cliente.	ITIL: Gestión de Liberaciones y Despliegue. COBIT BAI06: Gestionar los cambios de TI.
R03	Gestión de Configuración y Repositorios	Caja Negra del Proveedor (Vendor Lock-in): La custodia externa de los repositorios y configuraciones "master" (por Diebold y Tecnasa) impide al banco tener control directo o capacidad de auditoría inmediata sobre los cambios en el código base.	Incapacidad para recuperar el servicio autónomamente ante una falla crítica del proveedor o ruptura de contrato. Dificultad para auditar cambios no autorizados.	ITIL: Gestión de la Configuración del Servicio. COBIT APO10: Gestionar los proveedores.
R04	Pruebas y QA (Laboratorio)	Limitación en Pruebas de Estrés e Integración: Las pruebas físicas en laboratorio aseguran funcionalidad básica, pero pueden no replicar condiciones de red complejas o volúmenes transaccionales masivos del switch BASE24 en tiempo real.	Fallos en producción no detectados en el laboratorio que podrían causar caídas del servicio en días de alto tráfico (ej. días de pago).	ITIL: Validación y Pruebas del Servicio. COBIT BAI07: Gestionar la aceptación y el cambio.
R05	Gestión de Incidentes (IVANTI/NOC)	Resolución Reactiva vs. Proactiva: El modelo actual en IVANTI se basa en la apertura de tickets *post-evento*. No se menciona una correlación de eventos	Mayor tiempo de inactividad (Downtime) de los cajeros y afectación directa a la satisfacción del cliente y la reputación del	ITIL: Gestión de Incidentes / Gestión de Problemas. COBIT DSS02:

		predictiva basada en los logs de INETCO/Outside View para prevenir fallos de software antes de que ocurran.	banco.	Gestionar las peticiones y los incidentes del servicio.
R06	Seguridad del Endpoint (Trellix/TLS)	Riesgo de Configuración Desactualizada: Aunque se usan herramientas robustas (Trellix/TLS), la falta de gestión centralizada de configuraciones podría llevar a que ciertos ATMs tengan firmas de antivirus desactualizadas durante el ciclo de 2 meses.	Infección de malware en la red de cajeros o compromiso de datos en tránsito si los certificados TLS caducan o no se renuevan sincronizadamente.	COBIT DSS05: Gestionar los servicios de seguridad. ITIL: Gestión de Seguridad.
R07	Capacitación Técnica	Dependencia del Conocimiento Tácito: La capacitación se realiza "cada vez que hay una actualización". Si hay alta rotación de personal técnico o de proveedores, se pierde el *know-how* de la instalación.	Errores humanos durante la instalación manual en sitio, generando retrabajos y costos operativos adicionales.	COBIT APO07: Gestionar los recursos humanos. ITIL: Gestión del Conocimiento.

Fuente: Elaboración Propia

4.1.5 DESCRIPCIÓN DE LOS RESULTADOS

Resultados de Entrevista Semiestructurada

La presente sección expone los resultados obtenidos a partir de las entrevistas realizadas al personal responsable de la administración, monitoreo y soporte técnico del software de cajeros automáticos en Banco Ficohsa. El propósito del análisis fue identificar el nivel actual de madurez en la gestión de incidentes, documentación, seguridad y continuidad operativa, así como reconocer los principales riesgos y vulnerabilidades asociados al funcionamiento del software de cajeros automáticos.

Los datos recolectados permitieron obtener una visión clara sobre la frecuencia de los incidentes, los tipos de fallas más comunes, la eficacia del proceso de recuperación del servicio, el grado de ejecución de mantenimientos preventivos, la disponibilidad del sistema y la percepción sobre las prácticas actuales de gestión de riesgos y controles de seguridad. Asimismo, se analizaron

factores operativos críticos como la comunicación entre áreas, asignación de responsabilidades, aplicación de parches y efectividad del monitoreo, elementos esenciales para la optimización de la operación tecnológica en el marco de la continuidad del servicio.

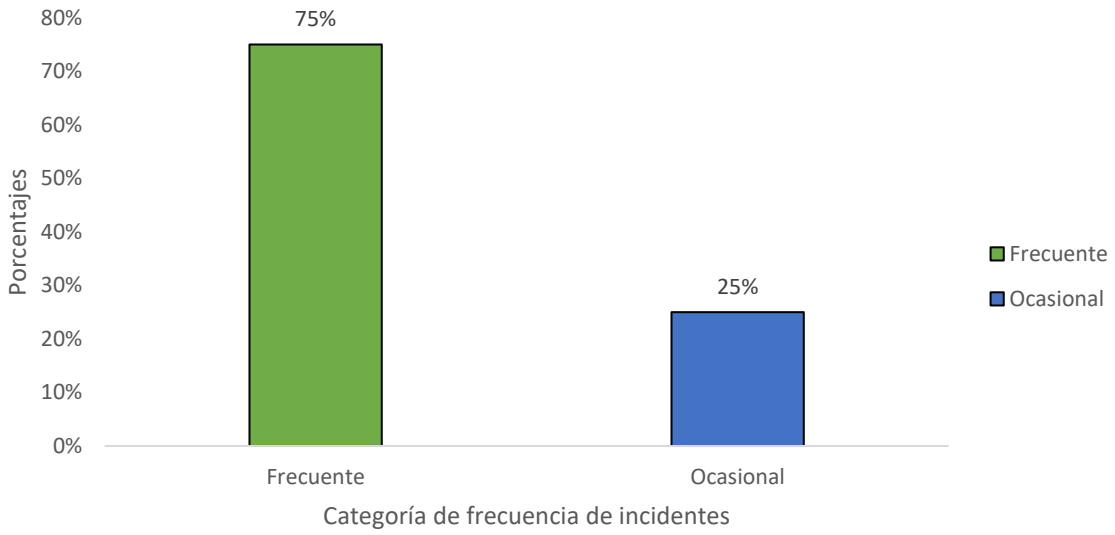
La información presentada constituye una base fundamental para sustentar la propuesta de un modelo de gestión de riesgos alineado con los marcos de referencia COBIT 2019 e ITIL 4, orientado a fortalecer la eficiencia y seguridad del software de cajeros automáticos del banco.

Las preguntas analizadas (8 a la 23) se enfocan en comprender el estado actual de la gestión del software de cajeros automáticos en Banco Ficohsa, caracterizando aspectos como riesgos percibidos, controles existentes, procesos operativos, prácticas de mantenimiento, mecanismos de monitoreo y dinámicas de comunicación entre áreas involucradas.

A continuación, presentamos los resultados obtenidos:

Pregunta: En su experiencia, ¿qué tan frecuentes son los incidentes en el software de cajeros automáticos?

Figura 19: *Frecuencia de los incidentes en el software de cajeros automáticos*



Fuente: Elaboración propia

Descripción

La figura 19 muestra que el 75 % de los encuestados percibe que los incidentes en el software de cajeros automáticos ocurren de forma frecuente, mientras que el 25 % restante los considera ocasionales. No se reportan percepciones de baja frecuencia o ausencia de incidentes, lo que evidencia que las fallas son un evento recurrente en la operación de este servicio.

Análisis

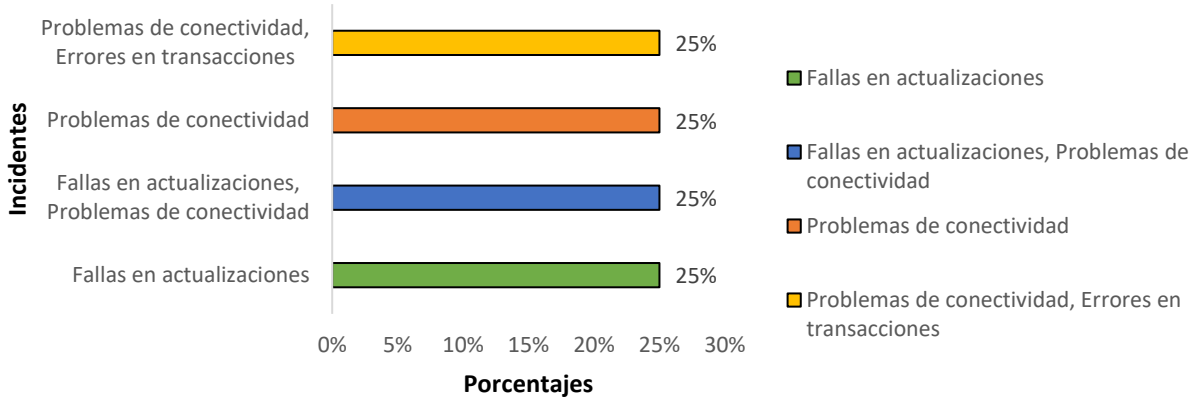
La alta frecuencia de incidentes confirma la vulnerabilidad operacional que el proyecto busca mitigar, y demanda que las acciones de mejora (Objetivo 1) se centren en estabilizar el software mediante procesos de Gestión de Problemas y Gestión de Cambios.

Hallazgo

Se confirma una alta recurrencia de incidentes en el software de cajeros automáticos, lo que evidencia debilidades en la gestión actual de la plataforma y la necesidad urgente de implementar controles y mejoras específicas para garantizar su estabilidad.

Pregunta: ¿Qué tipo de incidentes considera más comunes?

Figura 20: *Incidentes más comunes*



Fuente: Elaboración propia

Descripción

La figura 20 muestra que los tipos de incidentes señalados como más comunes se distribuyen de manera equitativa entre las cuatro categorías presentadas, cada una con un 25 %. Los encuestados mencionan con igual frecuencia: fallas en actualizaciones, problemas de conectividad, la combinación de fallas en actualizaciones con problemas de conectividad y la combinación de problemas de conectividad con errores en transacciones.

Análisis

La distribución uniforme de respuestas indica que no existe un único tipo de incidente predominante, sino un conjunto de fallas recurrentes vinculadas principalmente a la conectividad y a los procesos de actualización del software. La presencia de errores en transacciones asociados

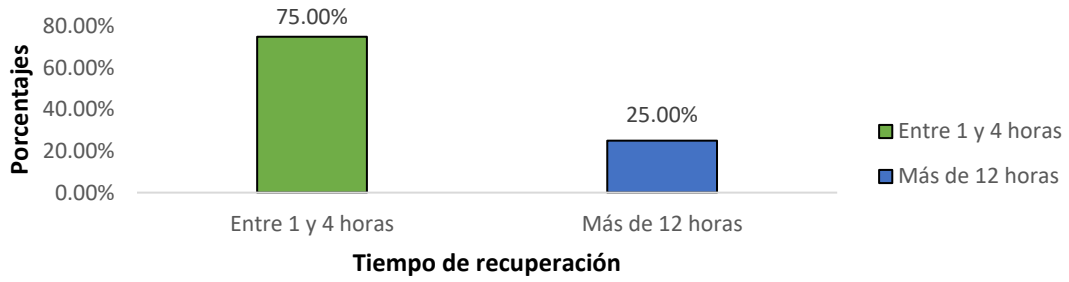
a problemas de conectividad evidencia que las incidencias técnicas impactan directamente la operación financiera y la percepción del usuario final. Estos resultados refuerzan la necesidad de fortalecer los controles sobre la infraestructura de red, los procedimientos de liberación de cambios y las pruebas previas a las actualizaciones, conforme a las prácticas recomendadas por COBIT 2019 e ITIL 4.

Hallazgo

Se identifica que los incidentes más frecuentes se concentran en problemas de conectividad y fallas en actualizaciones, los cuales en algunos casos se traducen en errores en las transacciones, afectando la continuidad y confiabilidad del servicio de cajeros automáticos.

Pregunta: Cuando ocurre un incidente en el software de cajeros, ¿qué tan rápido considera que se logra la recuperación del servicio?

Figura 21: *Tiempo de recuperación*



Fuente: Elaboración propia

Descripción

La figura 21 muestra que el 75 % de los encuestados considera que, cuando ocurre un incidente en el software de cajeros automáticos, la recuperación del servicio se logra en un intervalo de entre 1 y 4 horas. En contraste, el 25 % señala que la recuperación puede tardar más de 12 horas. No se reportan tiempos de solución menores a una hora, lo que evidencia que los incidentes siempre generan una ventana de indisponibilidad significativa.

Análisis

La concentración de respuestas en el rango de 1 a 4 horas indica que, aunque existe capacidad para restablecer el servicio en un tiempo moderado, la operación aún enfrenta periodos de indisponibilidad que pueden afectar la continuidad del negocio y la satisfacción del cliente. El hecho de que una cuarta parte de los incidentes tarde más de 12 horas en resolverse revela la

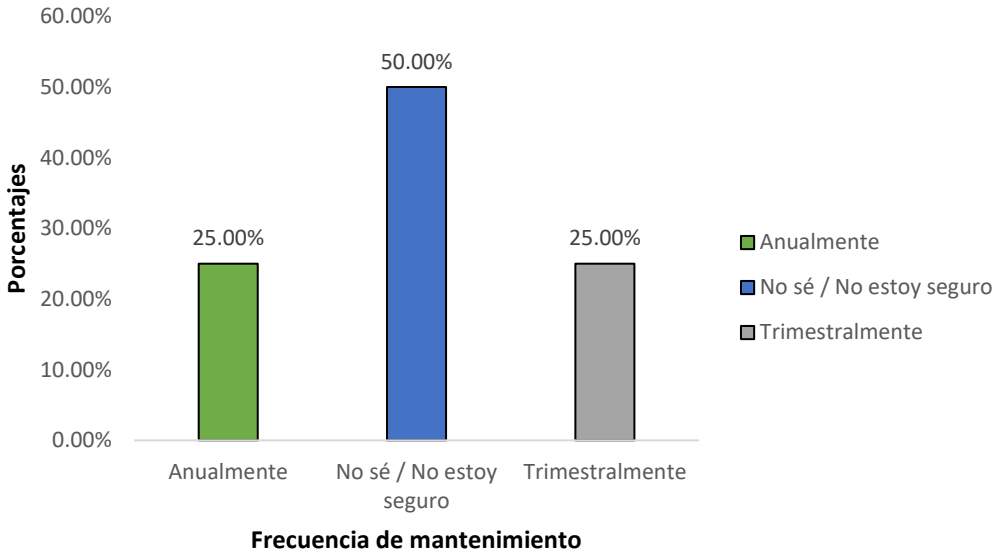
ausencia de procedimientos estandarizados y de métricas robustas de tiempo medio de resolución (MTTR), aspectos clave en los procesos de Gestión de Incidentes y Problemas. Esto refuerza la necesidad de implementar acuerdos de nivel de servicio (SLA) más exigentes y mecanismos de escalamiento alineados con las buenas prácticas de COBIT 2019 e ITIL 4.

Hallazgo

Se evidencia que los tiempos de recuperación del servicio ante incidentes en el software de cajeros son prolongados, especialmente en el 25 % de los casos que supera las 12 horas, lo que confirma debilidades en la gestión de incidentes y la urgencia de optimizar los procedimientos de atención y resolución para reducir la indisponibilidad del servicio.

Pregunta: ¿Con qué frecuencia se realizan mantenimientos preventivos al software de cajeros automáticos?

Figura 22: *Frecuencia de realización de mantenimientos preventivos*



Fuente: Elaboración propia

Descripción

La figura 22 muestra que el 50 % de los encuestados indica no saber o no estar seguro de la frecuencia con que se realizan mantenimientos preventivos al software de cajeros automáticos. El 25 % señala que estos se realizan anualmente y otro 25 % menciona que se efectúan de manera trimestral.

Análisis

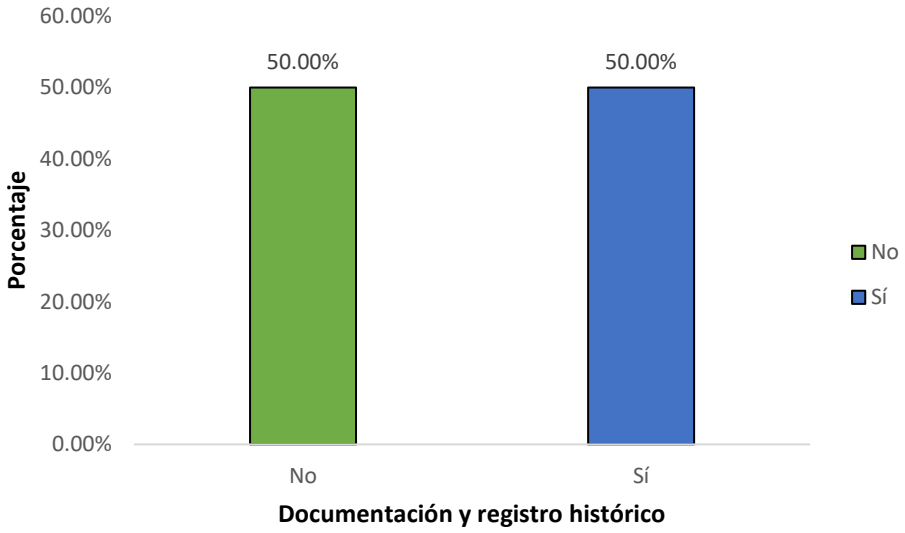
El alto porcentaje de respuestas de desconocimiento sugiere poca difusión o claridad sobre el plan de mantenimiento preventivo del software. Esto puede reflejar debilidades en la comunicación interna y en la formalización de los calendarios de mantenimiento, lo cual dificulta evaluar si la frecuencia actual es adecuada para reducir incidentes.

Hallazgo

Predomina la incertidumbre sobre la periodicidad de los mantenimientos preventivos del software de cajeros, lo que evidencia la necesidad de documentar y comunicar de forma más clara estos procesos entre los actores involucrados.

Pregunta: ¿Considera que existe suficiente documentación y registro histórico de incidentes en los cajeros automáticos?

Figura 23: *Percepción sobre la existencia de documentación y registro histórico de incidentes*



Fuente: Elaboración propia

Descripción

La figura 23 muestra que el 50 % de los encuestados considera que **no** existe suficiente documentación y registro histórico de incidentes en los cajeros automáticos, mientras que el otro 50 % opina que **sí** existe dicha documentación. La percepción se encuentra dividida en partes iguales.

Análisis

La distribución equilibrada de respuestas refleja falta de consenso sobre la gestión de la

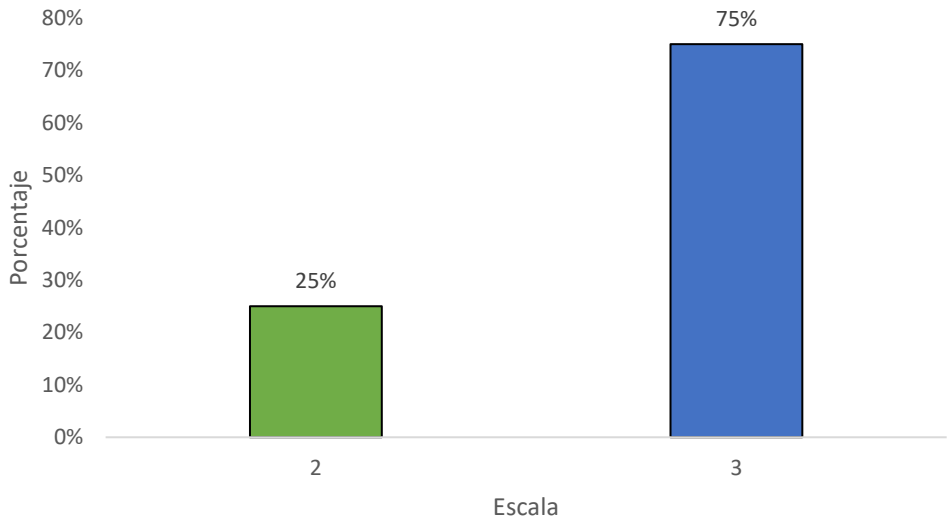
documentación de incidentes. Esto sugiere que, aunque existen registros para algunos usuarios, estos no son lo suficientemente visibles o estandarizados para todos los involucrados en la operación.

Hallazgo

Se evidencia una gestión poco homogénea de la documentación y del registro histórico de incidentes, lo que indica la necesidad de fortalecer y unificar estos procesos para asegurar trazabilidad y facilitar el análisis de causas y tendencias.

Pregunta: En una escala del 1 al 5, ¿qué tan efectivo considera el proceso de monitoreo actual del software de cajeros automáticos?

Figura 24: *Percepción sobre la efectividad del monitoreo actual del software*



Fuente: Elaboración propia

Descripción

La figura 24 muestra que el 75 % de los encuestados califica la efectividad del monitoreo actual del software de cajeros con un valor de 3 en una escala de 1 a 5, mientras que el 25 % lo valora con 2. No se registran calificaciones altas (4 o 5), ni la mínima (1).

Análisis

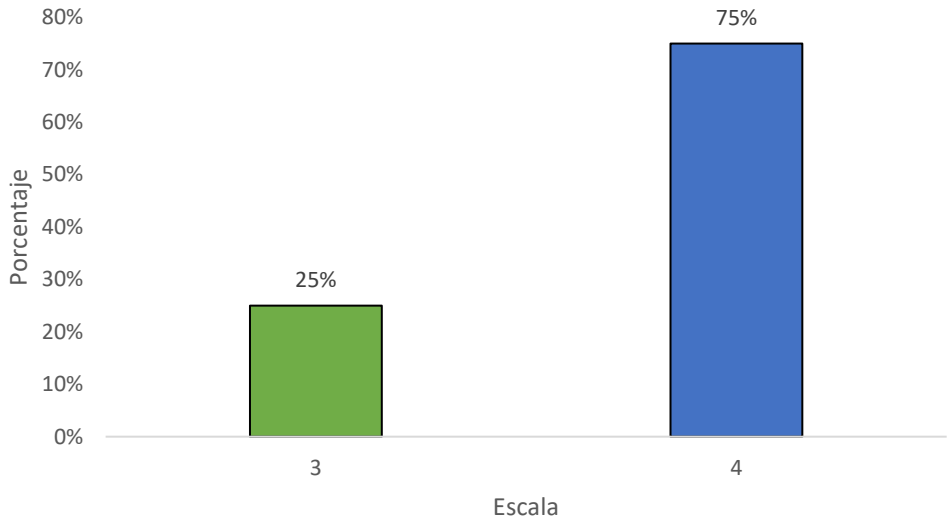
Estos resultados indican que el monitoreo del software es percibido como medianamente efectivo, pero con margen importante de mejora. La ausencia de valoraciones altas sugiere que los mecanismos actuales no garantizan una detección oportuna y completa de incidentes, lo que limita su contribución a la continuidad del servicio.

Hallazgo

Se identifica una percepción de efectividad solo moderada del monitoreo del software de cajeros, lo que refuerza la necesidad de robustecer las herramientas y procedimientos de supervisión para alcanzar niveles de control más altos.

Pregunta: En una escala del 1 al 5, ¿qué tan efectiva es la comunicación entre áreas durante la resolución de incidentes de cajeros automáticos?

Figura 25: *Percepción sobre la comunicación entre áreas*



Fuente: Elaboración propia

Descripción

La figura 25 muestra que el 75 % de los encuestados califica con 4 la efectividad de la comunicación entre áreas durante la resolución de incidentes en cajeros automáticos, mientras que el 25 % la valora con 3 en una escala de 1 a 5. No se registran percepciones bajas (1 o 2) ni la máxima (5).

Análisis

Los resultados indican que la comunicación interáreas es percibida como buena, aunque aún perfectible. Existe coordinación suficiente para atender los incidentes, pero la ausencia de calificación máxima sugiere oportunidades de mejora en la rapidez, claridad o trazabilidad de la información que se comparte durante el proceso.

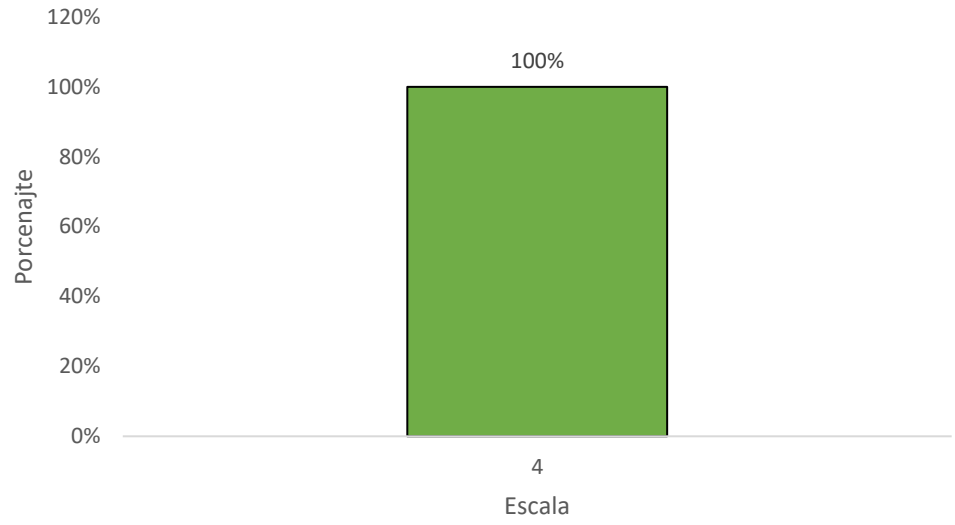
Hallazgo

Se identifica una comunicación entre áreas mayormente efectiva en la atención de

incidentes, pero con margen para fortalecer los canales y protocolos existentes a fin de alcanzar niveles óptimos de coordinación.

Pregunta: En una escala del 1 al 5, ¿qué tan clara considera la asignación de roles y responsabilidades en la gestión de incidentes de cajeros automáticos?

Figura 26: *Percepción sobre la efectiva asignación de roles*



Fuente: Elaboración propia

Descripción

La figura 26 muestra que el 100 % de los encuestados califica con 4, en una escala de 1 a 5, la claridad en la asignación de roles y responsabilidades en la gestión de incidentes de cajeros automáticos. No se registran valoraciones menores ni la máxima puntuación.

Análisis

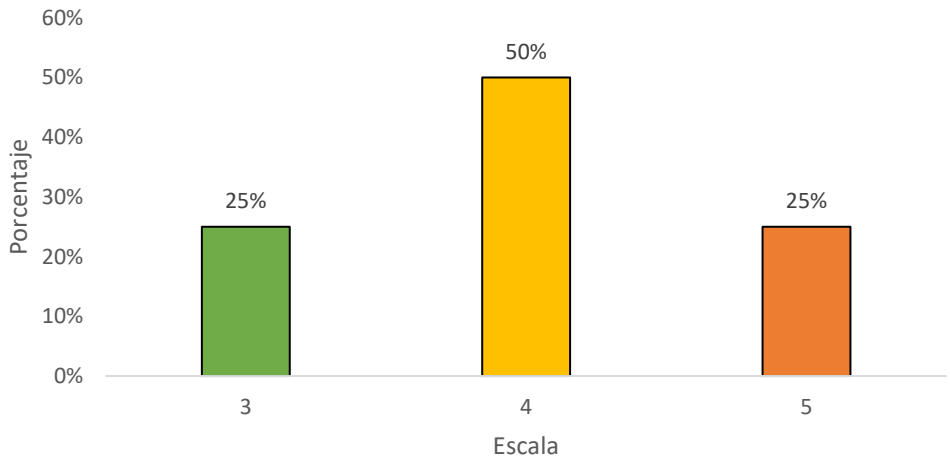
Este resultado indica que todos perciben una buena definición de roles y responsabilidades durante la atención de incidentes. Sin embargo, la ausencia de calificación 5 sugiere que aún existen pequeños aspectos por mejorar en la formalización o difusión de dichos roles para alcanzar un nivel óptimo de claridad.

Hallazgo

Se confirma una percepción generalizada de claridad en la asignación de roles y responsabilidades en la gestión de incidentes, aunque persiste un margen de mejora para robustecer la definición y documentación de estas funciones.

Pregunta: En una escala del 1 al 5, ¿cómo evalúa la disponibilidad del software de cajeros automáticos de Banco Ficohsa, entendida como la capacidad del sí continuo y accesible cuando se requiere su uso?

Figura 27: *Percepción de la disponibilidad del software de cajeros automáticos*



Fuente: Elaboración propia

Descripción

La figura 27 muestra que el 50 % de los encuestados evalúa la disponibilidad del software de cajeros automáticos con una calificación de 4 en una escala de 1 a 5. El 25 % la califica con 3 y otro 25 % con 5, por lo que la percepción se concentra entre niveles medios y altos de disponibilidad.

Análisis

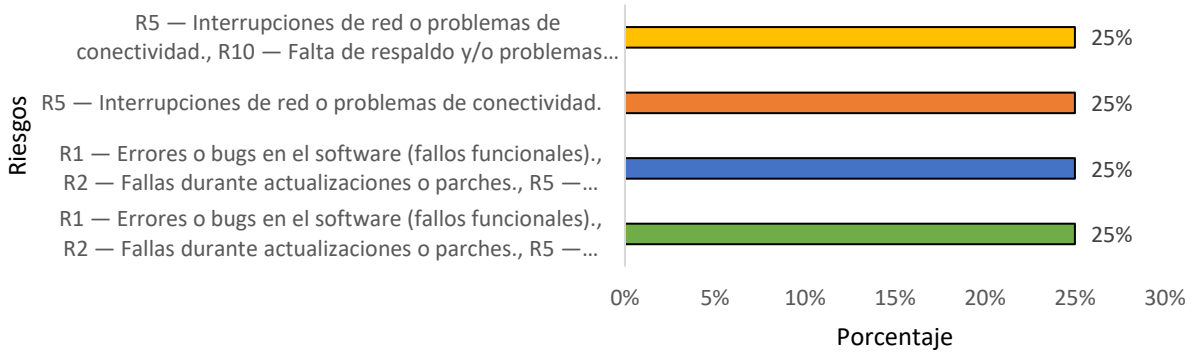
Los resultados indican que la disponibilidad del software es percibida como generalmente buena, con una proporción importante de usuarios que incluso la considera muy alta. Sin embargo, la presencia de calificaciones de 3 evidencia que persisten episodios de indisponibilidad que afectan la experiencia del usuario y que justifican reforzar los controles sobre continuidad del servicio.

Hallazgo

Se identifica una percepción mayoritariamente favorable sobre la disponibilidad del software de cajeros, aunque aún existen brechas que limitan que todos los usuarios la valoren en el nivel máximo, lo que confirma la necesidad de consolidar las acciones de mejora orientadas a la continuidad operativa.

Pregunta: ¿Cuáles son los siguientes riesgos más comunes en el software de cajeros automáticos de Banco Ficohsa?

Figura 28: *Riesgos más comunes en la gestión de software de cajeros automáticos*



Fuente: Elaboración propia

Descripción

La figura 28 muestra que los riesgos identificados como más comunes en la gestión del software de cajeros automáticos se distribuyen de manera uniforme: errores o bugs en el software (R1), fallas durante actualizaciones o parches (R2), interrupciones de red o problemas de conectividad (R5) y falta de respaldo y/o problemas en la recuperación ante desastres (R10) registran cada uno un 25 % de las respuestas.

Análisis

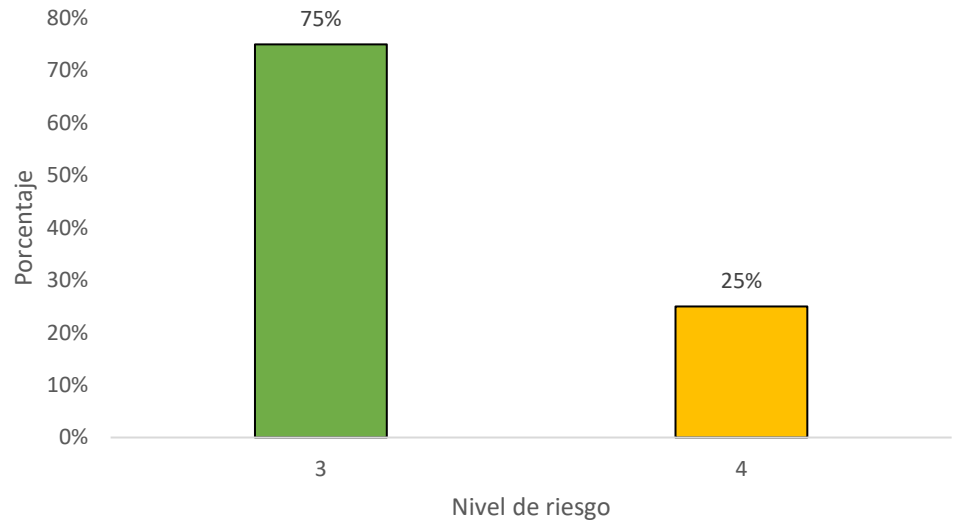
La falta de conocimiento y la percepción de revisión insuficiente de las políticas de seguridad es una vulnerabilidad de alto impacto en la Gobernanza de TI que expone al software a amenazas evolutivas. La propuesta debe corregir esta deficiencia mediante la formalización de la revisión y comunicación de las políticas, tal como lo requiere el Objetivo 2.

Hallazgo

Se identifica un conjunto de riesgos frecuentes ligados a errores de software, fallas en actualizaciones, problemas de conectividad y debilidades en respaldo y recuperación, lo que confirma la urgencia de implementar controles más robustos y coordinados en la gestión del software de cajeros automáticos.

Pregunta: En una escala del 1 al 5, ¿qué nivel de riesgo operativo percibe en la operación del software de cajeros automáticos?

Figura 29: *Nivel de riesgo operativo perceptible*



Fuente: Elaboración propia

Descripción

La figura 29 muestra que el 75 % de los encuestados percibe el nivel de riesgo operativo en la operación del software de cajeros automáticos en 3, mientras que el 25 % lo valora en 4 en una escala de 1 a 5. No se registran percepciones de riesgo bajo (1 o 2) ni de riesgo máximo (5).

Análisis

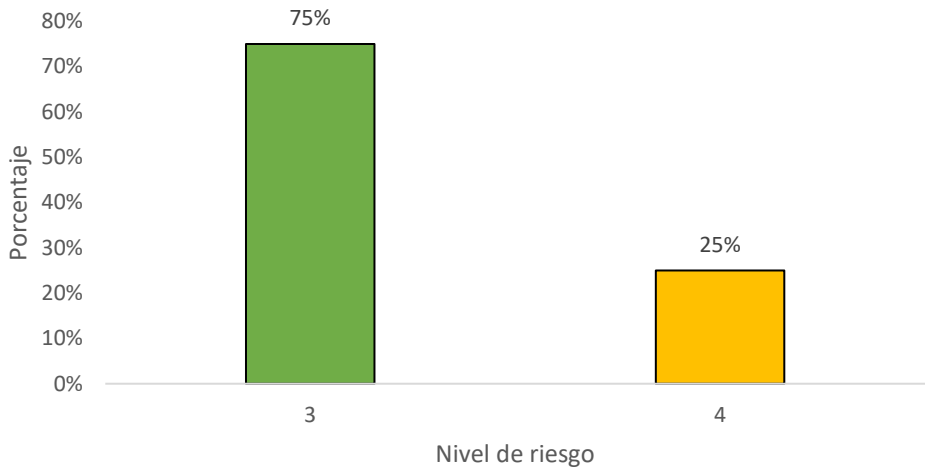
La claridad media o baja en el cumplimiento de los SLA es una deficiencia en las métricas y la gobernanza, lo que requiere que la propuesta se enfoque en formalizar, medir y comunicar de manera transparente los Acuerdos de Nivel de Servicio (incluyendo el RTO y la fiabilidad) para alcanzar la madurez en la gestión de servicios (Objetivo 2).

Hallazgo

Se evidencia una percepción predominante de riesgo operativo medio–alto en la operación del software de cajeros, lo que confirma la importancia de implementar acciones de mitigación específicas para reducir la exposición a incidentes.

Pregunta: En una escala del 1 al 5, ¿qué nivel de riesgo de seguridad informática percibe en el software de cajeros automáticos?

Figura 30: *Nivel de riesgo de seguridad informática perceptible*



Fuente: Elaboración propia

Descripción

La figura 30 muestra que el 75 % de los encuestados percibe el nivel de riesgo de seguridad informática en el software de cajeros automáticos en 3, mientras que el 25 % lo valora en 4 en una escala de 1 a 5. No se reportan percepciones de riesgo bajo (1 o 2) ni máximo (5).

Análisis

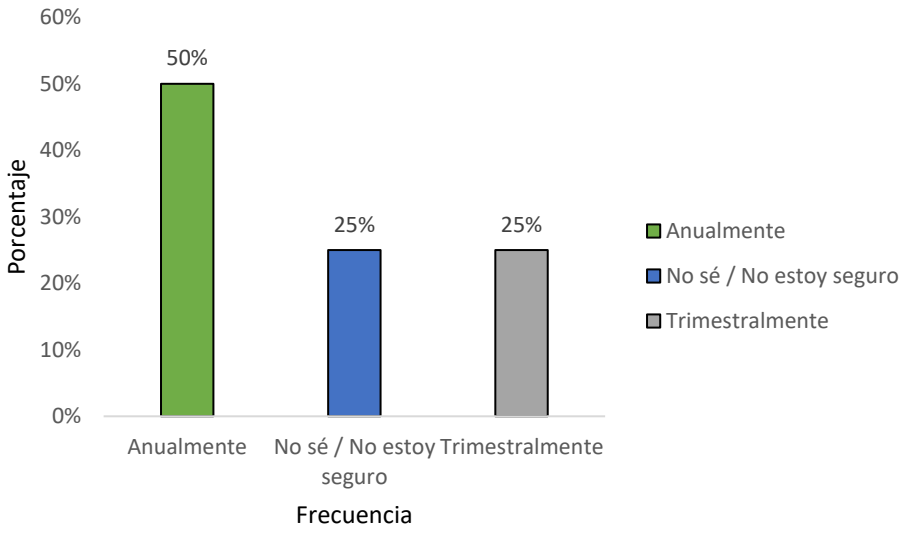
Este gráfico refuerza el hallazgo de que la gestión actual adolece de una deficiencia en la formalización de métricas, lo que requiere que el Objetivo 2 se enfoque en establecer un marco de medición de servicios claro y auditable.

Hallazgo

Se identifica una percepción de riesgo de seguridad informática medio–alto en el software de cajeros, lo que confirma la urgencia de robustecer los mecanismos de protección para reducir la exposición a amenazas y vulneraciones.

Pregunta: ¿Con qué frecuencia considera que el banco realiza evaluaciones de riesgos en el software de cajeros automáticos?

Figura 31: *Frecuencia de evaluaciones de riesgos*



Fuente: Elaboración propia

Descripción

La figura 31 muestra que el 50 % de los encuestados considera que el banco realiza evaluaciones de riesgos en el software de cajeros automáticos de forma anual. El 25 % indica que estas se llevan a cabo trimestralmente y el otro 25 % señala que no sabe o no está seguro de la frecuencia.

Análisis

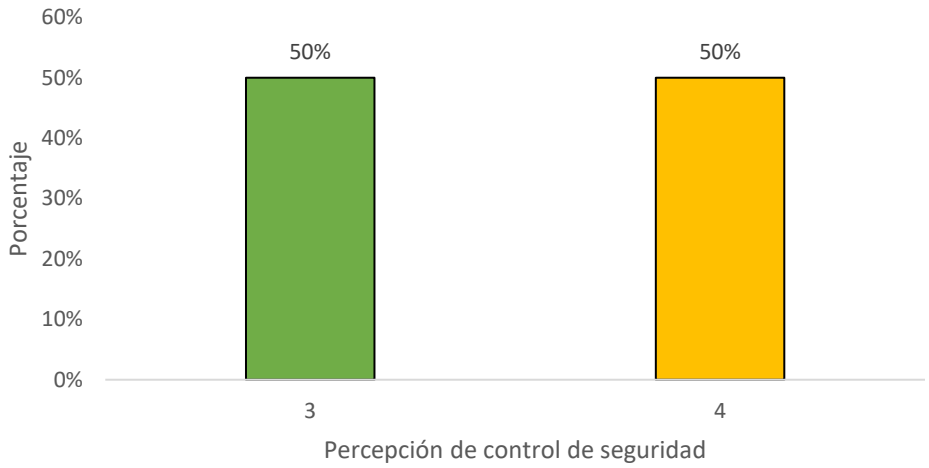
Este gráfico mapea las amenazas de mayor impacto (Conectividad y Fraude/Terceros) y valida que las vulnerabilidades y deficiencias de proceso (monitoreo, parches) están creando el entorno ideal para que estos riesgos se materialicen. El modelo propuesto debe abordarlos de manera integral.

Hallazgo

Se identifica que las evaluaciones de riesgos son percibidas como mayoritariamente anuales y poco conocidas por todos los actores, lo que confirma la necesidad de formalizar y difundir mejor el programa de gestión de riesgos en el software de cajeros automáticos.

Pregunta: En una escala del 1 al 5, ¿qué tan efectiva considera la aplicación de controles de seguridad en el software de cajeros automáticos?

Figura 32: *Efectividad perceptible en controles de seguridad*



Fuente: Elaboración propia

Descripción

La figura 32 muestra que el 50 % de los encuestados califica con 3 la efectividad de la aplicación de controles de seguridad en el software de cajeros automáticos y el otro 50 % la evalúa con 4, en una escala de 1 a 5. No se registran calificaciones bajas (1 o 2) ni la máxima (5).

Análisis

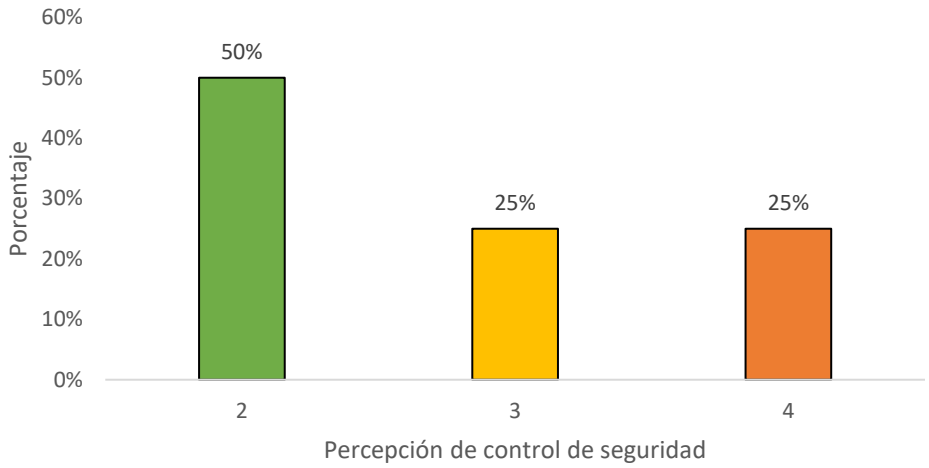
El gráfico valida que el modelo propuesto debe estar diseñado para mitigar las amenazas de conectividad y fraude/terceros (riesgos de mayor impacto) mediante la corrección de las deficiencias procesales (monitoreo y patch management) que aumentan la exposición a vulnerabilidades de software.

Hallazgo

Se identifica una efectividad media–alta en los controles de seguridad del software de cajeros, pero con oportunidades de mejora para fortalecer su implementación y lograr una percepción de seguridad más sólida entre los usuarios.

Pregunta: En escala del 1 al 5, ¿qué tan oportuna considera las actualizaciones y parches del software de cajeros automáticos?

Figura 33: *Percepción sobre las actualizaciones y parches del software*



Fuente: Elaboración propia

Descripción

La figura 33 muestra que el 50 % de los encuestados califica con 2, en una escala de 1 a 5, la oportunidad de las actualizaciones y parches del software de cajeros automáticos. El 25 % otorga una calificación de 3 y el 25 % restante una calificación de 4. No se registran valoraciones mínimas (1) ni máximas (5).

Análisis

Este gráfico es el punto culminante del Objetivo 1, ya que las respuestas abiertas identifican las deficiencias procesales (Logística de Parches y Estándares) como la vulnerabilidad principal que perpetúa los incidentes frecuentes y expone al software a amenazas de seguridad.

Hallazgo

Se evidencia una valoración mayoritariamente desfavorable respecto a la oportunidad de las actualizaciones y parches del software, lo que confirma la necesidad de fortalecer la planificación y ejecución de estos procesos para asegurar un mantenimiento más oportuno del sistema.

Pregunta: En su opinión, ¿Cuáles son las principales vulnerabilidades que afectan al software de cajeros automáticos?

Tabla 16: *Principales vulnerabilidades que afectan al software*

Respuestas de 4 Entrevistas realizadas				
Pregunta 23	**Entrevistado 1**	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**

En su opinión, ¿Cuáles son las principales vulnerabilidades que afectan al software de cajeros automáticos?	Problemas del entorno como fallas en red eléctrica problemas de comunicación y fraude físico	No realizar las actualizaciones y parches en sistema operativo, brindadas por el fabricante en tiempo y forma, así mismo actualizaciones en aplicativos.	Logística a nivel de parcheo o actualizaciones	No contar con un estándar a nivel de software.

Fuente: Elaboración propia

Descripción

La tabla 16 presenta las respuestas de cuatro entrevistados sobre las principales vulnerabilidades que afectan al software de cajeros automáticos. Se mencionan problemas del entorno como fallas en la red eléctrica y en la comunicación, riesgos de fraude físico, ausencia de actualizaciones y parches oportunos tanto del sistema operativo como de aplicativos, dificultades logísticas para aplicar dichos parches y la falta de un estándar definido a nivel de software.

Análisis

La principal deficiencia en la gestión actual es de carácter procesal y de gobierno del software. Por lo tanto, el Objetivo 2 (Evaluar la aplicabilidad) debe enfocarse con urgencia en:

- Implementar el proceso COBIT 2019 BAI08 (Gestionar Cambios) para corregir la logística y la oportunidad de parches.
- Implementar la práctica de ITIL 4 Gestión de Configuración para establecer el estándar a nivel de software que actualmente no existe.

Hallazgo

Se identifican como vulnerabilidades críticas las fallas de red y comunicación, la gestión deficiente de actualizaciones y parches, y la ausencia de un estándar de software claramente establecido, lo que incrementa el riesgo operativo y de seguridad en la operación de los cajeros automáticos.

RESULTADOS DEL INSTRUMENTO MATRIZ DE ANÁLISIS DOCUMENTAL

Los resultados del instrumento “Matriz de análisis documental” permiten sistematizar y sintetizar la información teórica y empírica relacionada con las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software. A partir de la revisión de diversas fuentes clasificadas por año, autores, tipo de recurso y referencia se identificaron patrones

recurrentes en torno a fallas de seguridad, debilidades en los procesos de control, riesgos operativos y brechas en el cumplimiento de buenas prácticas y marcos normativos.

Este análisis documental constituye una base sólida para sustentar el diagnóstico del problema, ya que ofrece una visión comparativa de cómo distintos estudios abordan la gestión del software, qué riesgos priorizan y qué vacíos señalan en la implementación de controles. De este modo, la matriz no solo organiza las fuentes consultadas, sino que también orienta la interpretación crítica de la literatura y respalda la formulación de propuestas de mejora en la gestión del software.

En la matriz de análisis documental se organizaron y sistematizaron diversas fuentes académicas, normativas y técnicas relacionadas con la gestión del software, priorizando aquellas que abordan riesgos, amenazas, vulnerabilidades y deficiencias en entornos organizacionales. Cada registro incluye el año, autores, título, tipo de recurso y referencia, lo que permite contar con un panorama estructurado de la producción científica y técnica más relevante. Esta sistematización facilita la identificación de tendencias, enfoques conceptuales y buenas prácticas recomendadas para la gestión segura y eficiente del software.

Tabla 17: *Fuentes documentales sobre amenazas, vulnerabilidades y deficiencias en la gestión actual del software*

N°	Año	Autores	Título	Tipo de recurso	Referencia
1	2021	OWASP Foundation	OWASP Top 10: 2021. The Ten Most Critical Web Application Security Risks	Guía técnica / estándar de buenas prácticas	OWASP Foundation. (2021). *OWASP Top 10: 2021. The Ten Most Critical Web Application Security Risks*. Recuperado de https://owasp.org/Top10/
2	2024	Verizon	2024 data Breach Investigations Report	Informe técnico	Verizon. (2024). *2024 Data Breach Investigations Report*. Recuperado de https://www.verizon.com/business/resources/reports/2024-data-breach-investigations-report-dbir/
3	2022	Souppaya, Murugiah; Scarfone, Karen	Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology (NIST SP 800-40 Rev. 4)	Guía técnica NIST	Souppaya, M., & Scarfone, K. (2022). *Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology (NIST Special Publication 800-40 Rev. 4)*. National Institute of Standards and Technology. Recuperado de https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final
4	2022	National Institute of Standards and Technology	Secure Software Development Framework (SSDF) Version 1.1 (NIST SP 800-218)	Guía técnica NIST / marco de desarrollo seguro	National Institute of Standards and Technology. (2022). *Secure Software Development Framework (SSDF) Version 1.1 (NIST Special Publication 800-218)*. Recuperado de https://csrc.nist.gov/publications/detail/sp/800-218/final
5	2022	International Organization for Standardization; International Electrotechnical Commission	ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Information security risk management	Norma técnica internacional	International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection. Information security risk management*. Recuperado de https://www.iso.org/standard/80585.html
6	2024	Salami, S.; et al.	A systematic review of software vulnerability detection using machine learning and deep learning models	Artículo científico	Salami, S., et al. (2024). A systematic review of software vulnerability detection using machine learning and deep learning models. *Engineering Applications of Artificial Intelligence, 130*, 107881. Recuperado de https://www.sciencedirect.com/science/article/pii/S0952197623015635 (owasp.org)
7	2020	OWASP Foundation	OWASP Software Assurance Maturity Model (SAMM)	Marco de madurez / guía de gestión de seguridad del software	OWASP Foundation. (2020). *OWASP Software Assurance Maturity Model (SAMM)*. Recuperado de https://owaspsamm.org/
8	2021	European Union	ENISA Threat Landscape for	Informe	European Union Agency for Cybersecurity. (2021). *ENISA Threat Landscape*

		Agency for Cybersecurity (ENISA)	Supply Chain Attacks	técnico sobre amenazas a la cadena de suministro de software	*for Supply Chain Attacks*. Recuperado de https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Fuente: Elaboración Propia

Análisis

A partir de la revisión de los documentos seleccionados, se realizó una evaluación crítica del contenido, contrastando los planteamientos teóricos con las prácticas descritas en los estudios de caso y lineamientos técnicos. El análisis se centró en detectar coincidencias sobre los factores que incrementan la exposición al riesgo, tales como la ausencia de políticas formales, la falta de controles de acceso, la escasa documentación de procesos y la limitada capacitación del personal. Asimismo, se identificaron discrepancias y vacíos en la aplicación de marcos de referencia, lo que permitió delimitar con mayor precisión las debilidades presentes en la gestión actual del software.

Hallazgo

Del análisis de la matriz se derivan varios hallazgos relevantes: se confirma la existencia de amenazas recurrentes asociadas a fallas de actualización, gestión inadecuada de credenciales y ausencia de monitoreo continuo; se evidencian vulnerabilidades estructurales vinculadas a la falta de estandarización de procesos y a la débil cultura de seguridad; y se observan deficiencias en la alineación de la gestión del software con marcos normativos y buenas prácticas internacionales. Estos hallazgos respaldan la necesidad de fortalecer los procedimientos internos, actualizar las políticas de gestión del software y diseñar estrategias integrales de mejora orientadas a reducir riesgos y optimizar la seguridad operativa.

4.1.5 HALLAZGOS SOBRE LAS PRINCIPALES AMENAZAS, VULNERABILIDADES Y DEFICIENCIAS EN LA GESTIÓN ACTUAL DEL SOFTWARE

Los resultados de la entrevista aplicada a cuatro colaboradores evidencian que la gestión actual del software de cajeros automáticos presenta deficiencias críticas tanto a nivel procesal como de gobernanza. Estas debilidades incrementan la exposición a incidentes operativos y a riesgos de seguridad que afectan la continuidad y confiabilidad del servicio.

Se constató que la alta frecuencia de incidentes (P8) revela una vulnerabilidad operativa significativa, asociada a fallas en los procesos de Gestión de Problemas y Gestión de Cambios, lo que impacta de forma directa en la estabilidad del software. Además, se identificó una deficiente gestión del conocimiento (P9), que restringe el aprendizaje organizacional y limita el avance hacia mayores niveles de madurez en los procesos operativos y de gobierno de TI.

También se observaron fortalezas importantes, como la buena comunicación entre áreas (P14), la claridad en roles y responsabilidades (P15) y tiempos de recuperación relativamente

ágiles ante incidentes (P16). Estos elementos culturales constituyen una base favorable para la implementación del modelo de mejora propuesto, alineado con las buenas prácticas de COBIT 2019 e ITIL 4. Sin embargo, dichas fortalezas no logran compensar las debilidades estructurales de monitoreo y gestión de actualizaciones.

En materia de riesgos, los participantes señalaron que las amenazas vinculadas con problemas de conectividad y con fraude o terceros (P20 y P21) representan el mayor impacto potencial, y que se ven agravadas por las deficiencias ya mencionadas en monitoreo y administración de parches. Finalmente, coinciden en que la principal vulnerabilidad se relaciona con fallas logísticas y falta de estandarización en la gestión de parches (P22 y P23), lo que confirma la necesidad urgente de formalizar y fortalecer los controles de gobernanza sobre el software de cajeros automáticos.

4.2 EVALUACIÓN DE COBIT 2019 E ITIL 4 EN EL ANÁLISIS DE RIESGOS Y LA GESTIÓN DE INCIDENTES DEL SOFTWARE DE CAJEROS AUTOMÁTICOS

El segundo objetivo se centra en evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 en los procesos de análisis de riesgos y gestión de incidentes del software de los cajeros automáticos de Banco Ficohsa. Para alcanzarlo, se realizó un análisis comparativo entre los marcos de referencia y la situación actual de la institución, complementado con el criterio experto del personal involucrado en la operación. Los resultados obtenidos se presentan a continuación.

4.2.1 INSTRUMENTOS APLICADOS

Para el cumplimiento del segundo objetivo se utilizó un instrumento metodológico y tres instrumentos temáticos. Estos permitieron recopilar, contrastar y validar información desde diferentes perspectivas organizacionales y técnicas. Los instrumentos empleados fueron los siguientes:

- Entrevista semiestructurada:

Se aplicó una entrevista semiestructurada a los colaboradores directamente vinculados con la operación, monitoreo y soporte del software de cajeros automáticos. Las preguntas analizadas en esta sección correspondieron a los ítems 6, 7 y 24 al 34, orientados a identificar el nivel de madurez de los procesos actuales, el grado de alineación con prácticas de COBIT 2019 e ITIL 4, la percepción del personal sobre riesgos, incidentes recurrentes, deficiencias del flujo operativo, la aplicabilidad de mejores prácticas y posibles obstáculos para su adopción.

Este instrumento permitió obtener información cualitativa de primera mano, fundamentada en la experiencia operativa de los participantes y su interacción directa con los incidentes y riesgos del sistema ATM.

- COBIT performance management (CPM):

Se utilizó el instrumento COBIT Performance Management (CPM) para evaluar el nivel de capacidad de las prácticas relevantes de gobierno y gestión vinculadas al análisis de riesgos, la continuidad del negocio y la gestión de incidentes del software de cajeros. Este instrumento permitió identificar el nivel actual de capacidad de las prácticas (niveles 0 a 5), reconocer brechas entre la situación actual y el nivel de capacidad recomendado para garantizar una gestión efectiva del riesgo, analizar la aplicabilidad de prácticas específicas de dominios como EDM, APO, DSS y MEA relevantes para el control y respuesta de incidentes en plataformas críticas como ATMs.

- Service Value Chain (SVC) ITIL 4

La cadena de valor de servicio (Service Value Chain – SVC) se utilizó para mapear las actividades clave involucradas en el ciclo de vida del software de cajeros automáticos, analizando su coherencia con las prácticas recomendadas de ITIL 4. El análisis se centró en actividades como Planificación, Mejora, Participación, Diseño y Transición, Obtención/Construcción, Entrega y Soporte. La SVC permitió identificar qué etapas presentan mayor riesgo operativo, qué actividades no se encuentran adecuadamente integradas y dónde existen oportunidades para fortalecer la gestión de incidentes y la respuesta a fallas.

- Lista de verificación ITIL 4

Finalmente, se aplicó una lista de verificación basada en las prácticas esenciales de ITIL 4, con énfasis en: gestión de incidentes, gestión de cambios, gestión de problemas, gestión de disponibilidad, gestión de riesgos, gestión de continuidad del servicio y monitoreo de eventos. Esta herramienta permitió evaluar el nivel de cumplimiento y adopción de cada práctica dentro del entorno operativo de los cajeros automáticos, facilitando la identificación de desviaciones, brechas de madurez y oportunidades de mejora.

En conjunto, los instrumentos empleados brindaron una visión integral del estado actual de la gestión del software de cajeros automáticos en Banco Ficohsa.

4.2.2 PARTICIPANTES Y SUS CARACTERÍSTICAS

Los participantes de la entrevista semiestructurada correspondieron al mismo grupo descrito en la sección 4.1.2. Esto garantiza consistencia en la evaluación y un análisis transversal

de los procesos relacionados tanto con riesgos como con incidentes. El 100% de los entrevistados cuenta con más de 10 años de experiencia en funciones asociadas al software y operación de cajeros automáticos, lo que fortalece la confiabilidad de las percepciones y valoraciones obtenidas. La muestra se mantiene equilibrada entre Operaciones de Cajeros Automáticos y Tecnología de la Información (TI), asegurando una visión integral que combina la perspectiva operativa y la técnica. Este grupo permitió profundizar en la aplicabilidad práctica de COBIT 2019 e ITIL 4 desde la experiencia acumulada en el entorno ATM.

Los tres instrumentos temáticos (COBIT Performance Management, análisis mediante la Cadena de Valor del Servicio e instrumentos de verificación ITIL 4) fueron aplicados a un grupo especializado compuesto por dos participantes clave, un jefe de área, responsable de la coordinación estratégica y operativa del sistema ATM, con amplia experiencia en gestión de riesgos, continuidad operativa y toma de decisiones relacionadas con la infraestructura tecnológica del banco y un especialista técnico, encargado del soporte y mantenimiento del software de cajeros automáticos, con experiencia directa en resolución de incidentes, monitoreo de eventos y ejecución de actividades de operación diaria.

Este grupo permitió realizar un análisis más profundo y técnico, al estar conformado por personal con responsabilidades directas en la operación del sistema y en la evaluación del desempeño de los procesos TI. Su experiencia y rol dentro del área brindaron información detallada sobre el nivel de madurez, la aplicabilidad de las prácticas y las brechas existentes en comparación con los marcos COBIT 2019 e ITIL 4.

4.2.3 DESCRIPCIÓN DE LOS RESULTADOS

- Resultados de Entrevista Semiestructurada

Con el propósito de evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 en el análisis de riesgos y la gestión de incidentes asociados al software de cajeros automáticos de Banco Ficohsa, se aplicó un cuestionario semiestructurado dirigido a colaboradores con amplia experiencia en la operación y soporte de la plataforma ATM. Este instrumento permitió recopilar información cualitativa y cuantitativa sobre la percepción del personal respecto al nivel de madurez de los procesos actuales, los riesgos operativos más relevantes, la efectividad de la gestión de incidentes, así como la factibilidad de implementar marcos de buenas prácticas dentro del entorno operativo del banco.

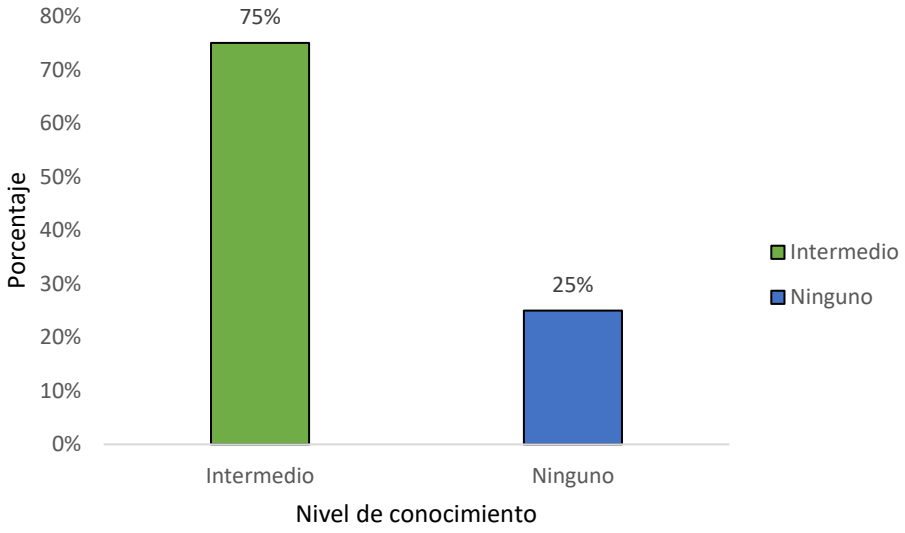
Las preguntas analizadas en esta sección (correspondientes a los ítems 6, 7 y 24 a 34) se

enfocaron específicamente en elementos clave para comprender la situación actual del sistema ATM desde dos dimensiones, La gestión del riesgo y de incidentes, según la experiencia directa de los colaboradores, y el grado de alineación con los principios y prácticas de COBIT 2019 e ITIL 4. Los resultados presentados a continuación constituyen la base para identificar tendencias, brechas y oportunidades de mejora, sirviendo como insumo para el análisis comparativo desarrollado en las siguientes secciones del capítulo.

A continuación, presentamos los resultados obtenidos:

Pregunta: Nivel de conocimiento en marcos de referencia de gestión y gobierno de TI (COBIT, ITIL, ISO, etc.)

Figura 34: *Nivel de conocimiento en marcos de referencia de gestión y gobierno de TI (COBIT, ITIL, ISO, etc.)*



Fuente: Elaboración propia

Descripción

La figura 34 muestra que el 75 % de los encuestados declara tener un nivel intermedio de conocimiento sobre marcos de referencia de gestión y gobierno de TI (COBIT, ITIL, ISO, etc.), mientras que el 25 % señala no tener ningún conocimiento. No se reportan niveles avanzados.

Análisis

El análisis muestra que los participantes poseen un nivel de conocimiento principalmente intermedio sobre marcos de referencia de gestión y gobierno de TI. Esta percepción indica que, aunque existe familiaridad general con estos modelos, el grado de dominio no es uniforme y puede

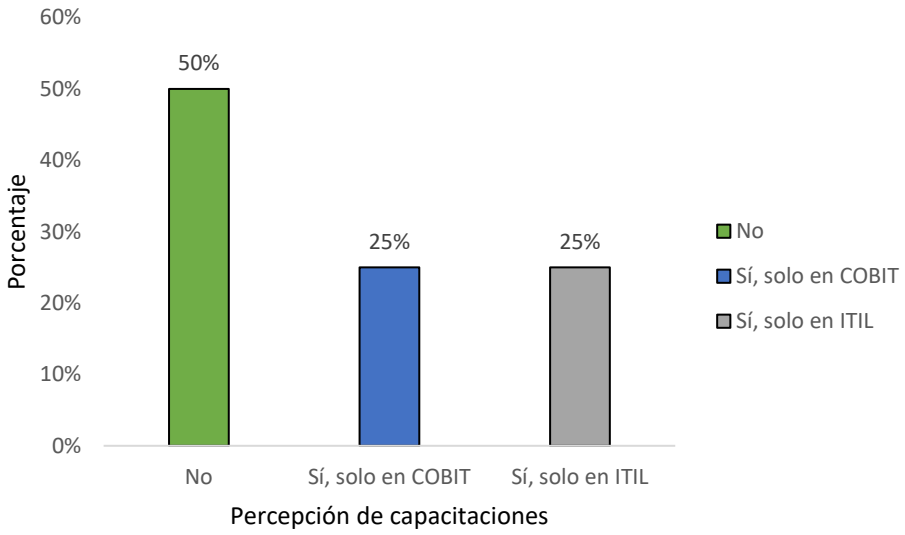
influir en la adopción efectiva de COBIT 2019 e ITIL 4 dentro del contexto operativo del software ATM.

Hallazgo

Predomina un nivel de conocimiento intermedio sobre marcos de referencia de gestión y gobierno de TI, pero persiste una brecha formativa en una parte del personal, lo que refuerza la importancia de fortalecer la capacitación en COBIT, ITIL e ISO.

Pregunta: ¿Ha recibido capacitaciones formales en COBIT 2019 o ITIL 4?

Figura 35: *Capacitaciones formales en COBIT 2019 o ITIL 4*



Fuente: Elaboración propia

Descripción

La figura 35 muestra que el 50 % de los encuestados no ha recibido capacitaciones formales en COBIT 2019 ni en ITIL 4. El 25 % indica haber sido capacitado solo en COBIT 2019 y otro 25 % señala haber recibido capacitación únicamente en ITIL 4. No se registran participantes con formación en ambos marcos.

Análisis

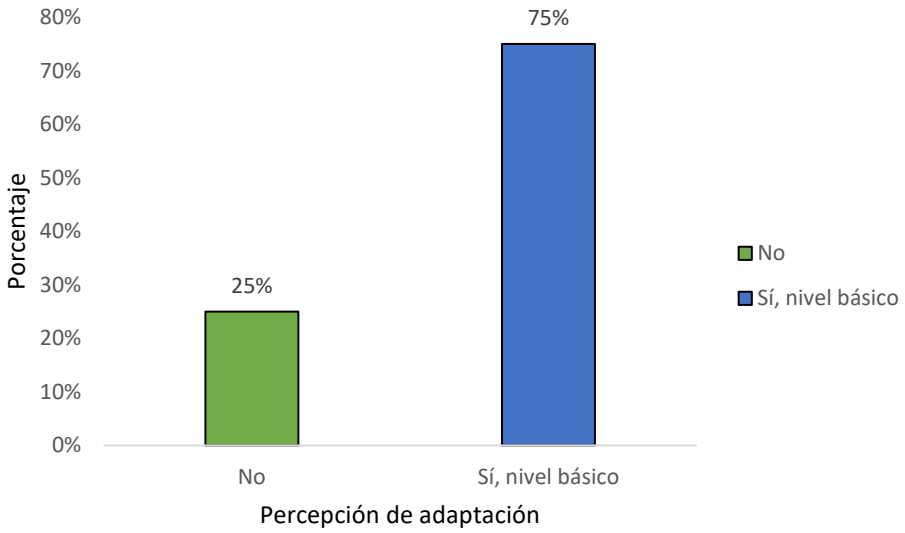
Los resultados evidencian una baja exposición a capacitaciones formales en COBIT 2019 e ITIL 4. Esta situación sugiere que el personal ha desarrollado conocimiento principalmente empírico, lo que limita la aplicabilidad plena de las prácticas requeridas por ambos marcos en procesos críticos como la gestión de incidentes y el análisis de riesgos del software ATM.

Hallazgo

Se identifica una brecha importante de capacitación formal en COBIT 2019 e ITIL 4 y una formación parcial entre quienes sí han recibido entrenamiento, lo que refuerza la necesidad de implementar un programa sistemático de formación para apoyar la adopción efectiva del modelo propuesto.

Pregunta: ¿Está familiarizado(a) con los principios de COBIT 2019?

Figura 36: *Percepción de adaptación a los principios COBIT 2019*



Fuente: Elaboración propia

Descripción

La figura 36 muestra que el 75 % de los encuestados indica estar familiarizado con los principios de COBIT 2019 a un nivel básico, mientras que el 25 % restante señala no estar familiarizado. No se reportan niveles intermedios ni avanzados de familiaridad.

Análisis

Se identifica un nivel de familiaridad moderado con los principios de COBIT 2019. Este hallazgo indica que, si bien los participantes reconocen el marco, su dominio conceptual no es integral, lo que podría afectar la integración de prácticas de gobernanza formal en los procesos actuales del software ATM.

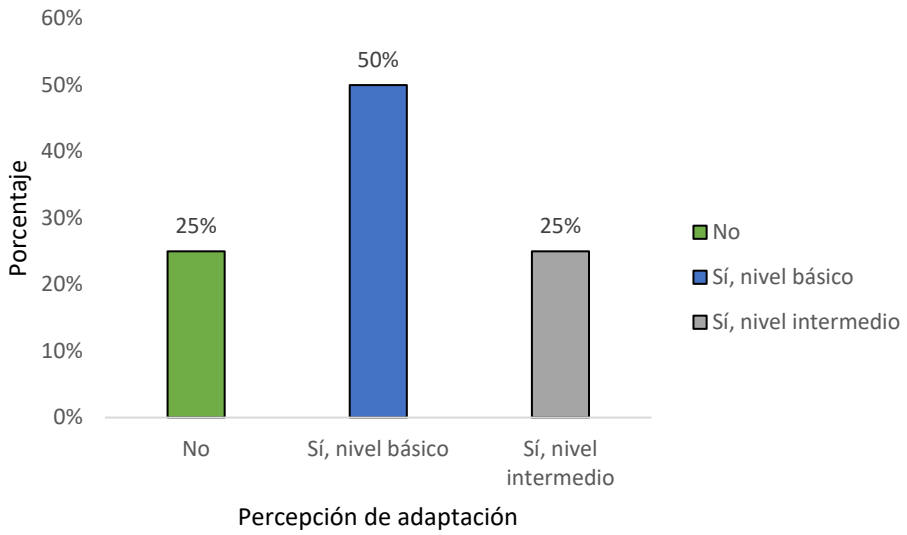
Hallazgo

Predomina una familiaridad solo básica con los principios de COBIT 2019, acompañada de un segmento sin conocimiento del marco, lo que confirma la importancia de implementar procesos de formación más estructurados para apoyar la adopción del modelo de gobernanza

propuesto.

Pregunta: ¿Está familiarizado con las prácticas de ITIL 4?

Figura 37: *Percepción de adaptación a las prácticas ITIL 4*



Fuente: Elaboración propia

Descripción

La figura 37 muestra que el 50 % de los encuestados afirma estar familiarizado con las prácticas de ITIL 4 a un nivel básico, el 25 % reporta un nivel intermedio y el 25 % indica no tener familiaridad. No se registran niveles avanzados.

Análisis

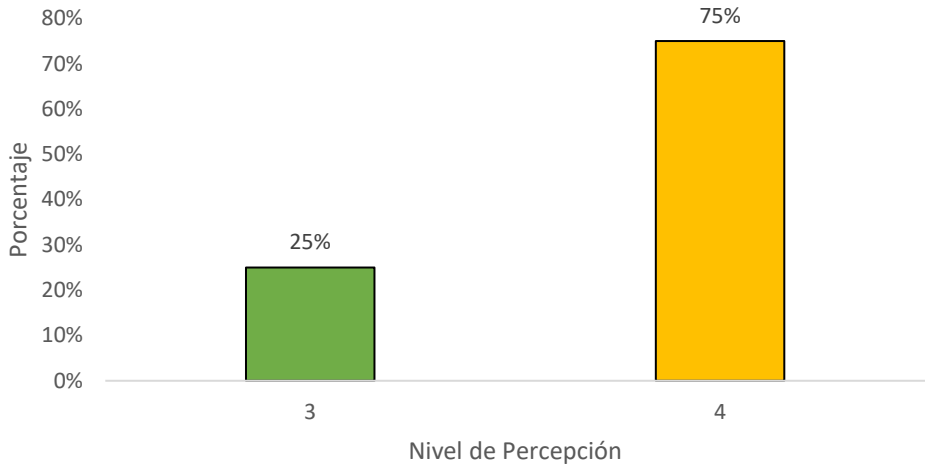
Los participantes reportan un nivel de familiaridad intermedio con las prácticas de ITIL 4. Este nivel de conocimiento parcial sugiere que la adopción de ITIL 4 como guía metodológica aún no es plena, especialmente en áreas como gestión de cambios, monitoreo y mejora continua, que son esenciales para el contexto ATM.

Hallazgo

Predomina un conocimiento básico a intermedio de ITIL 4, pero persiste una brecha de especialización y de cobertura formativa que debe atenderse para consolidar la adopción efectiva de sus prácticas en la gestión del software de cajeros automáticos.

Pregunta: En una escala del 1 al 5, ¿qué tan útil considera COBIT 2019 para el análisis de riesgos en cajeros automáticos?

Figura 38: *Percepción sobre la utilidad de COBIT 2019 para el análisis de riesgos en cajeros automáticos*



Fuente: Elaboración propia

Descripción

La figura 38 muestra que el 75 % de los encuestados califica con 4, en una escala de 1 a 5, la utilidad de COBIT 2019 para el análisis de riesgos en cajeros automáticos, mientras que el 25 % le asigna una calificación de 3. No se registran valoraciones extremas (1, 2 o 5).

Análisis

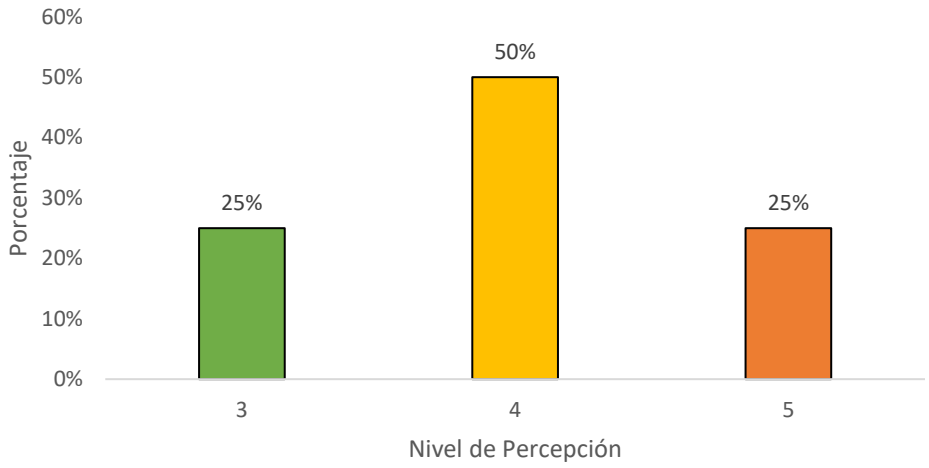
El gráfico muestra que los participantes consideran COBIT 2019 como un marco significativamente útil para el análisis de riesgos, con predominio de calificaciones altas. Esto evidencia que el personal reconoce la pertinencia del marco en actividades relacionadas con gobernanza, control y aseguramiento del software ATM.

Hallazgo

Se identifica una percepción favorable sobre la utilidad de COBIT 2019 en el análisis de riesgos de cajeros automáticos, lo que respalda su selección como marco de referencia para el modelo de gobernanza propuesto, pero también evidencia la necesidad de fortalecer su implementación y uso cotidiano.

Pregunta: En una escala del 1 al 5, ¿qué tan útil considera ITIL 4 para la gestión de incidentes en cajeros automáticos?

Figura 39: *Percepción sobre la utilidad de ITIL 4 para el análisis de riesgos en cajeros automáticos*



Fuente: Elaboración propia

Descripción

La figura 39 muestra que el 50 % de los encuestados califica con 4, en una escala de 1 a 5, la utilidad de ITIL 4 para la gestión de incidentes en cajeros automáticos. El 25 % le asigna una calificación de 3 y el 25 % restante la evalúa con 5.

Análisis

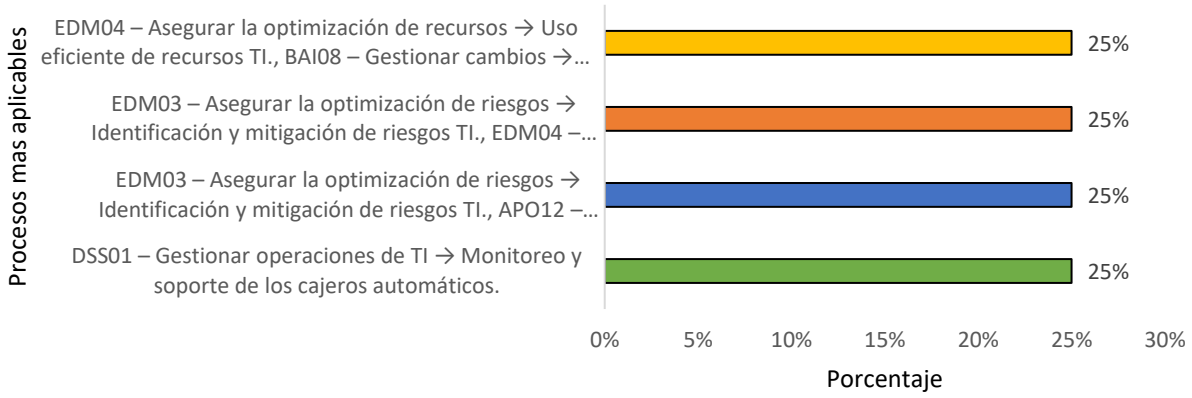
La mayoría de los participantes calificó ITIL 4 como útil o muy útil para la gestión de incidentes. Este hallazgo refuerza la percepción de que las prácticas de ITSM pueden mejorar sustancialmente la eficiencia del proceso de atención de fallas y la recuperación del servicio en los cajeros automáticos.

Hallazgo

Se confirma una percepción positiva sobre la utilidad de ITIL 4 en la gestión de incidentes y riesgos de cajeros automáticos, lo que respalda su incorporación como marco de referencia en la propuesta, aunque es necesario fortalecer su implementación para aprovechar todo su potencial.

Pregunta: ¿Qué procesos de COBIT 2019 cree más aplicables a la gestión de software de cajeros automáticos de Banco Ficohsa?

Figura 40: *Procesos COBIT 2019 más aplicables a la gestión de software de cajeros automáticos*



Fuente: Elaboración propia

Descripción

La figura 40 muestra que las combinaciones de procesos de COBIT 2019 consideradas más aplicables a la gestión del software de cajeros automáticos se distribuyen de forma uniforme, cada una con un 25 %. En todas las respuestas aparecen procesos vinculados con la gestión de operaciones de TI, la optimización de recursos, la gestión de cambios, la identificación y tratamiento de riesgos y la seguridad de la información.

Análisis

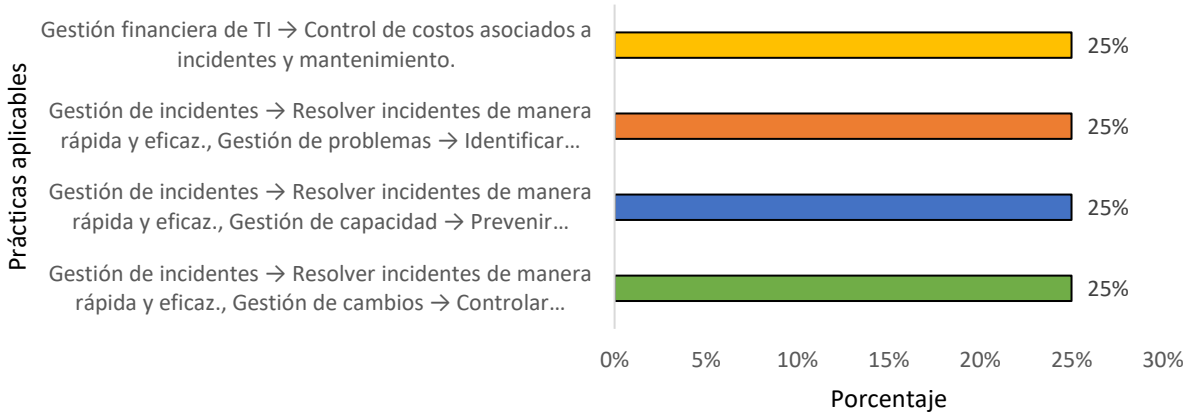
Los participantes identifican que los procesos más aplicables son aquellos asociados a entrega de servicios, monitoreo y gestión de riesgos. Esto coincide con las necesidades operativas del sistema ATM, evidenciadas en el cuestionario, en cuanto a control, supervisión y continuidad del servicio.

Hallazgo

Se identifica un grupo de procesos COBIT 2019 relacionados con operaciones, cambios, riesgos, seguridad y optimización de recursos como los más aplicables a la gestión del software de cajeros, lo que orienta la propuesta a priorizar estos dominios en el diseño del modelo de gobernanza y control.

Pregunta: ¿Qué prácticas de ITIL 4 considera más relevantes para mejorar la gestión de incidentes en el software de cajeros automáticos de Banco Ficohsa?

Figura 41: *Prácticas ITIL 4 más aplicables a la gestión de software de cajeros automáticos*



Fuente: Elaboración propia

Descripción

La figura 41 muestra que las combinaciones de prácticas de ITIL 4 consideradas más relevantes para mejorar la gestión de incidentes en el software de cajeros automáticos se distribuyen de forma uniforme, cada una con un 25 %. Entre ellas destacan la gestión de incidentes, gestión de problemas, gestión de cambios, gestión de disponibilidad, gestión de capacidad, gestión de nivel de servicio y gestión financiera de TI, enfocadas en asegurar la operación continua y el control de costos.

Análisis

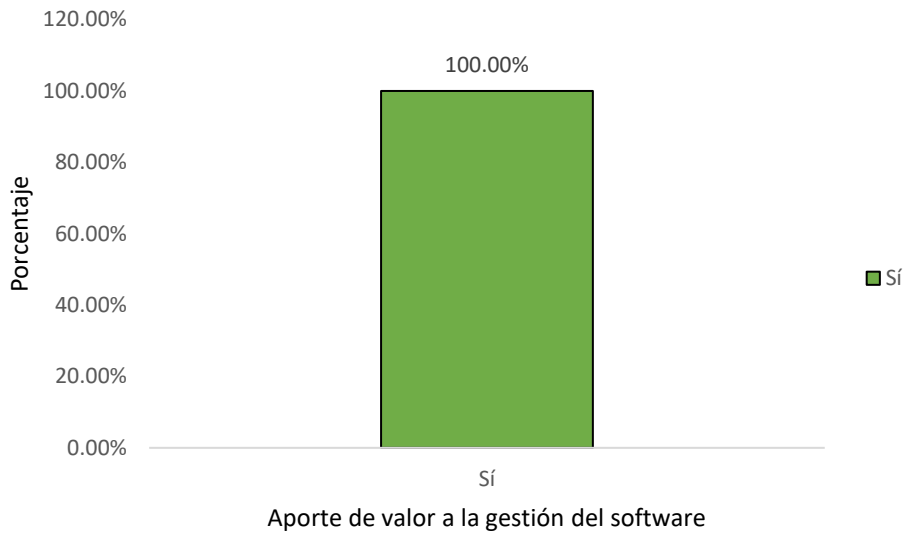
Los participantes priorizan prácticas como Gestión de incidentes, Gestión de cambios, Gestión de disponibilidad y Gestión de monitoreo y eventos como las más relevantes. Esto refleja una comprensión clara de las áreas críticas necesarias para optimizar la operación del software ATM.

Hallazgo

Se identifica un conjunto de prácticas de ITIL 4 especialmente gestión de incidentes, problemas, cambios, disponibilidad, capacidad, nivel de servicio y gestión financiera de TI como las más aplicables para fortalecer la gestión del software de cajeros, lo que orienta la propuesta a priorizar estas áreas en el diseño del modelo de gestión de servicios.

Pregunta: ¿Cree que la integración de COBIT 2019 e ITIL 4 aportaría valor a la gestión del software de cajeros automáticos?

Figura 42: *Percepción sobre la aportación de valor de los marcos de referencia*



Fuente: Elaboración propia

Descripción

La figura 42 muestra que el 100 % de los encuestados considera que la integración de COBIT 2019 e ITIL 4 aportaría valor a la gestión del software de cajeros automáticos. No se registran respuestas en desacuerdo.

Análisis

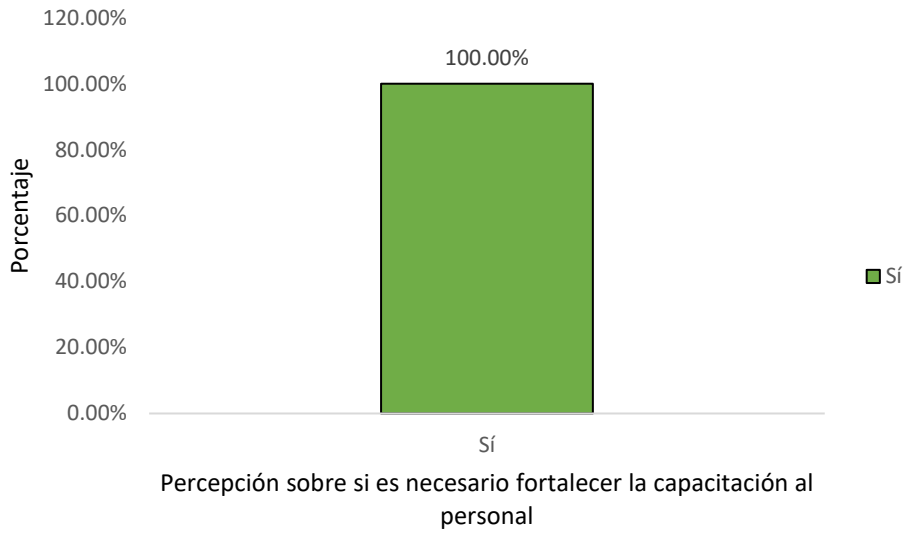
Existe consenso entre los participantes respecto a que la integración de ambos marcos aportaría un valor significativo a la gestión del software ATM. Se reconoce que COBIT 2019 proporcionaría la estructura de gobernanza necesaria, mientras ITIL 4 fortalecería los procesos operativos y de atención de incidentes.

Hallazgo

Se confirma una aceptación unánime respecto a que la integración de COBIT 2019 e ITIL 4 generaría valor en la gestión del software de cajeros, lo que respalda la viabilidad y legitimidad de la propuesta planteada en el proyecto.

Pregunta: ¿Considera necesario fortalecer la capacitación del personal en COBIT 2019 e ITIL 4 para gestionar correctamente los cajeros automáticos en Banco Ficohsa?

Figura 43: *Percepción de la necesidad de capacitaciones sobre marcos de referencia COBIT 2019 e ITIL 4*



Fuente: Elaboración propia

Descripción

La figura 43 muestra que el 100 % de los encuestados considera necesario fortalecer la capacitación del personal en COBIT 2019 e ITIL 4 para gestionar correctamente los cajeros automáticos en Banco Ficohsa. No se registran respuestas en desacuerdo.

Análisis

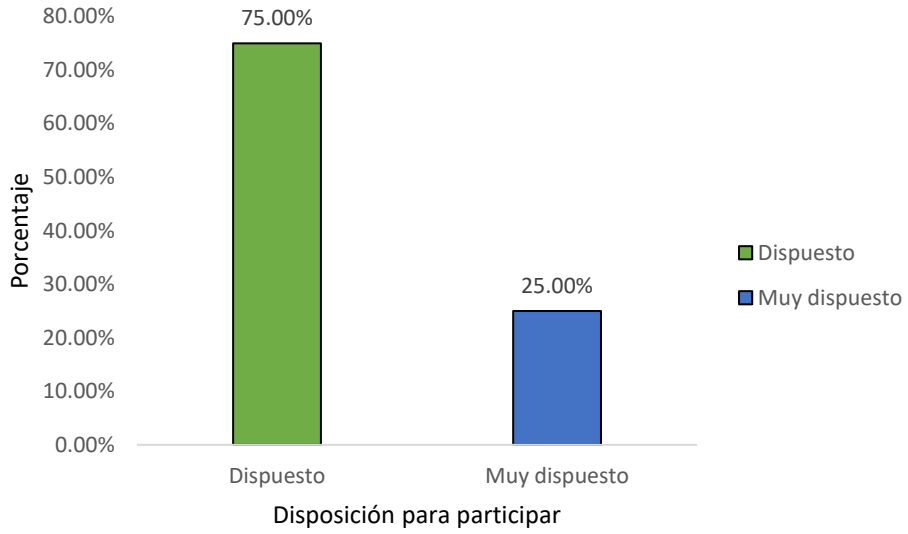
Los resultados muestran un acuerdo fuerte en la necesidad de reforzar la capacitación formal del personal en COBIT 2019 e ITIL 4. Esto evidencia una brecha de formación que limita la implementación efectiva de buenas prácticas en la operación de cajeros automáticos.

Hallazgo

Se confirma una necesidad unánimemente reconocida de fortalecer la capacitación del personal en COBIT 2019 e ITIL 4, lo que respalda la inclusión de un componente formativo explícito dentro de la propuesta de mejora.

Pregunta: ¿Qué tan dispuesto estaría a participar en programas de mejora continúa relacionados con la gestión de cajeros automáticos?

Figura 44: *Disposición para participar en programas de mejora continua*



Fuente: Elaboración propia

Descripción

La figura 44 muestra que el 75 % de los encuestados se declara dispuesto a participar en programas de mejora continua relacionados con la gestión de cajeros automáticos y el 25 % restante se declara muy dispuesto. No se registran respuestas de indiferencia o rechazo.

Análisis

La mayoría de los participantes expresó alta disposición a involucrarse en iniciativas de mejora continua. Esto indica un entorno favorable para procesos formales de implementación, capacitación o adopción de marcos de referencia.

Hallazgo

Se identifica una alta disposición del personal para involucrarse en programas de mejora continua vinculados a la gestión de cajeros automáticos, lo que constituye un factor facilitador clave para la implementación y sostenibilidad de la propuesta de gobernanza y gestión de servicios.

Pregunta: En su opinión, ¿cuáles son las acciones prioritarias de mejora para la gestión del software de cajeros automáticos?

Tabla 18: *Resultados pregunta 33*

Respuestas de 4 Entrevistas realizadas				
Pregunta 33	**Entrevistado 1**	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
En su opinión, ¿cuáles son las acciones prioritarias de mejora para la gestión del software de cajeros automáticos?	Implementación de software para configuración remotas	Monitorear, evaluar e implementar, y así abordar las mejoras en atenciones de soporte y sistema operativo, así como en seguridad de la información.	Mejora de los procesos	Introducir un estándar a nivel de software.

Fuente: Elaboración propia

Descripción

La tabla 18 presenta las respuestas de cuatro entrevistados sobre las acciones prioritarias de mejora para la gestión del software de cajeros automáticos. Entre las propuestas destacan la implementación de software para configuraciones remotas, el monitoreo, evaluación e implementación de mejoras en atenciones de soporte, sistema operativo y seguridad de la información, la mejora integral de los procesos y la introducción de un estándar a nivel de software.

Análisis

Las respuestas convergen en cuatro prioridades:

- Implementación de herramientas que permitan mayor control y configuración del software ATM.
- Fortalecimiento del monitoreo y evaluación continua.
- Estandarización de procesos.
- Optimización de atención de soporte y seguridad.

Esto muestra una clara percepción de que la madurez operativa puede elevarse mediante estandarización y automatización.

Hallazgo

Se identifica que las acciones de mejora consideradas más urgentes se relacionan con el

incremento de capacidades técnicas (configuración remota y soporte), la mejora de procesos y la adopción de un estándar de software, lo que confirma la necesidad de un modelo de gestión y gobernanza más estructurado para el software de cajeros automáticos.

Pregunta: ¿Qué beneficios concretos espera que se logren al aplicar COBIT 2019 e ITIL 4 en este contexto?

Tabla 19: *Resultados pregunta 34*

Respuestas de 4 Entrevistas realizadas				
Pregunta 34	**Entrevistado 1**	**Entrevistado 2**	**Entrevistado 3**	**Entrevistado 4**
¿Qué beneficios concretos espera que se logren al aplicar COBIT 2019 e ITIL 4 en este contexto? automáticos?	Optimizar el tiempo de respuesta en fallas	Tener una red más segura y mejorar los procesos en el área.	Mejora en los procesos	Lograr que cumplan con un estándar.

Fuente: Elaboración propia

Descripción

La tabla 19 presenta las respuestas de cuatro entrevistados sobre los beneficios concretos que esperan obtener al aplicar COBIT 2019 e ITIL 4 en la gestión del software de cajeros automáticos. Entre las expectativas destacan la optimización del tiempo de respuesta ante fallas, contar con una red más segura, mejorar los procesos del área y lograr que la gestión del software se alinee con un estándar definido.

Análisis

Los participantes coinciden en que la aplicación de los marcos permitirá:

- Optimizar tiempos de respuesta.
- Mejorar la seguridad.
- Aumentar la calidad de los procesos.
- Estandarizar la operación del software ATM.

Existe consenso en que ambos marcos representan una mejora significativa frente a los

métodos actuales.

Hallazgo

Se identifica que los beneficios más esperados de aplicar COBIT 2019 e ITIL 4 son la mejora en la rapidez de respuesta, el aumento de la seguridad y la estandarización de los procesos, lo que confirma la pertinencia de estos marcos como base para optimizar la gestión del software de cajeros automáticos.

- RESULTADOS DEL INSTRUMENTO COBIT PERFORMANCE MANAGEMENT (CPM)

El análisis mediante COBIT Performance Management (CPM) permitió evaluar el nivel de capacidad de las prácticas de gobierno y gestión relacionadas con la identificación, tratamiento y monitoreo de riesgos, así como con la atención de incidentes en el software de cajeros automáticos de Banco Ficohsa. Este instrumento, alineado al objetivo de evaluar la aplicabilidad de los principios de COBIT 2019 al contexto operativo del sistema ATM, ofrece una visión estructurada del grado de formalización, eficiencia y consistencia de los procesos actuales. Los resultados que se presentan a continuación permiten identificar brechas entre el estado actual y el nivel de capacidad recomendado, proporcionando evidencia clave para determinar oportunidades de mejora y reforzar la gestión del riesgo en un servicio crítico para la institución.

A continuación, se presenta el resultado de la aplicación del instrumento CPM:

Tabla 20: *Aplicación del instrumento CPM*

Práctica	Actividad	Nivel de Capacidad COBIT	Nivel de Capacidad BANCO FICOHSA	JUSTIFICACIÓN (Breve comentario que explica por qué asignó ese nivel de capacidad)
APO12 - Gestionar Riesgos	Identificar, analizar y evaluar riesgos tecnológicos asociados al software de cajeros automáticos.	3	2	Existen procedimientos de identificación de riesgos operativos y tecnológicos, pero no se aplican de forma estandarizada en todos los sistemas de software de ATM.
	Implementar controles de mitigación y planes de respuesta ante incidentes de software.	3	3	Se ejecutan planes de respuesta ante fallos de software y vulnerabilidades; sin embargo, no se miden formalmente los indicadores de efectividad.
BAI06 - Gestionar Cambios	Controlar cambios en versiones del software de cajeros.	4	3	Existe un proceso formal de aprobación de cambios con documentación y pruebas; falta la automatización de métricas de rendimiento post-cambio.
	Realizar pruebas previas a la liberación de nuevas versiones.	4	4	El banco realiza pruebas controladas en entornos aislados, garantizando estabilidad antes de producción.
DSS02 - Gestionar Servicios	Monitorear disponibilidad del software de cajeros y servicios relacionados.	4	3	Se cuenta con monitoreo centralizado, pero los indicadores de desempeño no están totalmente integrados en un cuadro de mando de TI.
	Implementar gestión de incidentes	3	4	La mesa de ayuda y soporte de TI usa ITIL 4 para

	y solicitudes.			seguimiento y resolución de incidentes con trazabilidad completa.
MEA01 - Monitorear, Evaluar y Valorar el Desempeño y Conformidad	Evaluar periódicamente el cumplimiento de controles de TI relacionados con software ATM.	3	2	Se realizan auditorías internas, pero sin un marco de indicadores continúo alineado a COBIT.
	Generar reportes de desempeño de los sistemas críticos.	4	3	Se reportan métricas, aunque no todas están automatizadas o integradas con sistemas de monitoreo.
APO11 - Gestionar la Calidad	Definir métricas de calidad del software de cajeros (tiempo de respuesta, fallos, integridad).	3	2	Aún no existe un marco de calidad formal; se mide de manera reactiva tras incidencias.
	Realizar revisiones de mejora continua.	4	3	Se aplican revisiones periódicas de mejora, aunque sin indicadores de madurez formalizados.

Fuente: Elaboración Propia

Descripción

La tabla 18 presenta la aplicación del instrumento CPM a diferentes prácticas de COBIT 2019 en Banco Ficohsa. Se comparan los niveles de capacidad de referencia con los niveles alcanzados por el banco en gestión de riesgos (APO12), cambios (BAI06), servicios (DSS02), monitoreo y evaluación (MEA01) y calidad (APO11), acompañados de una breve justificación para cada actividad evaluada.

Análisis

En general, los niveles de capacidad del banco se ubican uno o dos puntos por debajo del nivel COBIT esperado, lo que refleja procesos implementados, pero con limitaciones en estandarización, medición y automatización. Destacan como fortalezas la realización de pruebas en entornos controlados antes de liberar nuevas versiones y la gestión de incidentes basada en ITIL 4, donde el nivel de capacidad del banco iguala o supera el de referencia. Sin embargo, la gestión de riesgos, el monitoreo de controles, la definición de métricas de calidad y la integración de indicadores en tableros de mando aún presentan brechas significativas.

Hallazgo

El análisis del instrumento CPM muestra que el nivel de capacidad del Banco Ficohsa presenta madurez moderada, con puntajes mayoritariamente ubicados en niveles 2 y 3. Aunque existen prácticas estructuradas, estas no se encuentran totalmente estandarizadas ni alineadas a los requerimientos de COBIT 2019. Las capacidades actuales permiten operar el software ATM de manera funcional, pero aún existen brechas en la medición, control y mejora continua de los procesos evaluados.

Áreas de fortaleza según CPM:

Los resultados evidencian fortalezas significativas en las siguientes prácticas:

- Pruebas previas a liberaciones (BAI06): nivel 4, demostrando procesos maduros de QA, entornos controlados y validación previa antes de producción.
- Gestión de incidentes y solicitudes (DSS02): nivel 4, reflejando una mesa de ayuda basada en ITIL 4 con trazabilidad y control efectivamente implementados.
- Revisiones de mejora continua (APO11): nivel 3, mostrando mecanismos de retroalimentación y mejora, aunque sin estructura formal de madurez.

Brechas relevantes:

Asimismo, el instrumento identifica brechas importantes que limitan la madurez general

del proceso:

- Gestión de riesgos tecnológicos (APO12): nivel 2. No existe un proceso estandarizado de análisis y evaluación aplicado de forma consistente en todo el ciclo de vida del software ATM.
- Monitoreo del desempeño y conformidad (MEA01): nivel 2. Las auditorías se realizan, pero no bajo un marco continuo de indicadores alineados a COBIT.
- Gestión de calidad del software (APO11): nivel 2. No existe un marco formal de métricas; el control se realiza mayormente de forma reactiva.
- Integración de indicadores en monitoreo (DSS02): nivel 3. Aunque el monitoreo existe, no se encuentra completamente automatizado ni vinculado a un cuadro de mando.

Los hallazgos del CPM permiten concluir que:

- El banco opera con un nivel de madurez suficiente para mantener el servicio, pero insuficiente para garantizar gobernanza completa, gestión proactiva del riesgo y monitoreo integral del software ATM.
- Las brechas identificadas incrementan la probabilidad de riesgos operativos y de seguridad, ya que no todos los controles se ejecutan con consistencia o bajo métricas formales.
- La incorporación estructurada de COBIT 2019 permitiría elevar el nivel de madurez hacia capacidades más estables, medibles y alineadas con las necesidades críticas del servicio ATM.
- RESULTADOS DEL INSTRUMENTO SERVICE VALUE CHAIN (SVC) ITIL 4

El análisis basado en la Cadena de Valor del Servicio (Service Value Chain – SVC) de ITIL 4 permitió mapear las principales actividades involucradas en el ciclo de vida del software de cajeros automáticos y valorar su grado de alineación con las prácticas esenciales de gestión de servicios. En coherencia con el segundo objetivo de la investigación, este instrumento facilita la identificación de puntos críticos, áreas de mejora y oportunidades para optimizar el manejo de riesgos e incidentes mediante una integración más efectiva de actividades como Planificación, Mejora, Participación, Diseño y Transición, Obtención/Construcción y Entrega y Soporte. Los resultados expuestos a continuación ofrecen una visión clara del desempeño actual de la cadena de valor y de la aplicabilidad de ITIL 4 en el entorno operativo del sistema ATM.

A continuación, se presenta el resultado de la aplicación del instrumento CPM:

Tabla 21: *Aplicación del instrumento Cadena de Valor de Servicio ITIL 4 (SVC)*

Entada/Salida	Actividad Clave (SVC)	Práctica(s)	Rol	Actividad
Demanda	Obtener y construir	Gestión y Desarrollo de Software	Equipo de Desarrollo TI	Construir, adaptar o integrar módulos de software ATM según requerimientos y parches críticos.
	Diseño y transición	Gestión de Liberaciones, Validación y Pruebas del Servicio	Equipo de QA / Project Manager	Preparar releases, ejecutar pruebas funcionales, de regresión y de seguridad antes de desplegar a los ATMs.
	Transición	Gestión de Implementaciones, Gestión de Cambios	Change Manager / Operaciones TI	Coordinar despliegue de software en ATMs, asegurando aprobaciones de los involucrados en la gestión de cambios y planes de rollback.
	Entrega y soporte	Gestión de Incidentes, Gestión de Problemas, Gestión de Disponibilidad, Gestión de Monitorización y Eventos	Mesa de Servicio / Soporte TI	Monitorear ATMs, atender incidentes, analizar causas raíz y restaurar servicio ante fallas de software.
	Producto y servicio	Gestión de Activos de TI, Gestión de Versiones	Operaciones TI / Administrador de Sistemas	Mantener inventario de software, versiones instaladas y disponibilidad del servicio,

				entregando valor continuo al cliente.
Valor				Garantizar software funcional, seguro y disponible en todos los ATMs, generando valor para el banco y los clientes.

Fuente: Elaboración Propia

Descripción

La tabla 19 presenta la aplicación del instrumento de la Cadena de Valor del Servicio (SVC) de ITIL 4 al ciclo de vida del software de cajeros automáticos. Se detallan las entradas y salidas, las actividades clave (Obtener y construir, Diseño y transición, Transición, Entrega y soporte), las prácticas asociadas y los roles responsables, desde el desarrollo y las pruebas hasta el despliegue, monitoreo, gestión de incidentes y administración de activos y versiones.

Análisis

Los resultados muestran que el banco cuenta con actividades claramente definidas a lo largo de la SVC, especialmente en las etapas de construcción, pruebas, implementación y soporte del software de cajeros. La articulación entre Desarrollo, QA, Gestión de Cambios, Mesa de Servicio y Operaciones TI evidencia una base organizativa que permite aplicar las prácticas de ITIL 4 para garantizar continuidad y disponibilidad del servicio. No obstante, se observa que la cadena de valor se centra en la operación y el soporte, por lo que existe oportunidad de fortalecer explícitamente las actividades de planificación y mejora continua para lograr un ciclo más maduro y proactivo en la gestión del software ATM.

Hallazgo

El mapeo del flujo de valor demuestra que todas las actividades clave del SVC están presentes, aunque el grado de formalización y coordinación varía entre fases. El flujo funciona, pero existen puntos donde el proceso depende en exceso de acciones reactivas o manuales.

Hallazgos por actividad del SVC:

Planificación: Se evidencia planificación funcional pero fragmentada. No existe una articulación formalizada que conecte estrategias, análisis de riesgo y definición de capacidades necesarias para el software ATM.

Mejora: La mejora continua está presente de manera reactiva, impulsada principalmente por incidencias y auditorías. Carece de métricas formales y ciclos estructurados.

Participación: Los roles están definidos y existe comunicación entre equipos, pero la participación aún depende de solicitudes y no de mecanismos colaborativos automatizados.

Diseño y Transición: Esta actividad muestra uno de los niveles más altos de madurez. QA y Gestión de Liberaciones están bien integradas, con ejecución de pruebas funcionales y de seguridad antes del despliegue.

Obtención/Construcción: El desarrollo y mantenimiento del software se encuentra activo y

estructurado, con roles definidos, aunque falta integración completa con el control de versiones y el catálogo de activos.

Entrega y Soporte: La entrega y soporte funcionan adecuadamente, especialmente en atención de incidentes. Sin embargo, el monitoreo presenta brechas de automatización que afectan la capacidad preventiva.

Identificación de cuellos de botella:

- Ausencia de monitoreo automatizado limita la anticipación a fallas.
- Falta de integración entre activos, versiones y configuración afecta la trazabilidad.
- La planificación y la mejora continua carecen de mecanismos formales que permitan retroalimentación sistemática.
- RESULTADOS DEL INSTRUMENTO LISTA DE VERIFICACIÓN ITIL

La aplicación de la Lista de Verificación ITIL 4 permitió evaluar el grado de cumplimiento y adopción de las prácticas esenciales relacionadas con la gestión de incidentes, la gestión de riesgos y la operación del software de cajeros automáticos. Este instrumento, alineado al objetivo de determinar la adaptación de las prácticas de ITIL 4 al contexto de Banco Ficohsa, permitió identificar fortalezas, debilidades y áreas donde la madurez de los procesos aún no es suficiente para garantizar una gestión eficaz y robusta del servicio ATM. Los resultados que se presentan a continuación constituyen una base fundamental para comprender el nivel de adopción de las buenas prácticas y para orientar acciones concretas de mejora.

A continuación, se presenta el resultado de la aplicación del instrumento CPM:

Tabla 22: *Aplicación del instrumento lista de verificación ITIL 4*

N°	Práctica ITIL 4	Descripción	Cumple (Sí/No)	Observaciones
1	Gestión y Desarrollo de Software	Garantiza el diseño, codificación, mantenimiento y mejora del software que opera en los cajeros automáticos, asegurando cumplimiento normativo bancario, seguridad transaccional, compatibilidad con hardware ATM y alineación con las políticas del banco.	Si	
2	Gestión de Implementaciones (Deployment Management)	Asegura que las nuevas versiones, parches y actualizaciones del software ATM se desplieguen de forma coordinada, controlada y con mínima interrupción del servicio. Incluye ventanas de mantenimiento, pruebas previas y planes de reversión.	Si	
3	Gestión de Cambios (Change Enablement)	Controla los cambios al software de ATMs como actualizaciones de seguridad, cambios regulatorios o nuevas funcionalidades; Evaluando riesgos, impactos en las transacciones, dependencia de dispositivos y aprobación del CAB.	No	La práctica no se aplica de forma completa debido a que los cambios en el software ATM no siguen un proceso formalizado de evaluación de riesgos, categorización y aprobación estructurada. No existe un CAB plenamente operativo ni un flujo documentado que garantice la trazabilidad y gobierno del cambio según ITIL 4.
4	Gestión de Liberaciones (Release Management)	Gestiona el empaquetado de versiones finales del software ATM, asegurando que contengan configuraciones correctas, certificación QA, validación de integridad y documentación requerida antes de su distribución a la red de cajeros.	Si	
5	Gestión de Incidentes	Permite la resolución rápida de fallas en el software de ATMs, como errores de comunicación, fallas en módulos transaccionales, bloqueos de interfaz o caídas del servicio, asegurando la restauración oportuna del ATM.	Si	

6	Gestión de Problemas	Analiza fallas recurrentes en el software ATM (timeouts, errores EMV, cuelgues del kernel del ATM, fallas en la comunicación con switch bancario), identifica causas raíz y propone soluciones definitivas.	Si	
7	Gestión de la Disponibilidad	Se enfoca en asegurar que el software ATM cumpla los niveles de disponibilidad comprometidos, minimizando caídas de servicio, definiendo métricas de uptime, monitoreo proactivo y análisis de puntos de falla.	Si	
8	Gestión de Monitorización y Eventos	Supervisa en tiempo real el estado del software ATM y detecta eventos como errores de módulos, desconexiones, reinicios inesperados o anomalías operativas, permitiendo alertas tempranas y acciones automáticas.	No	No se aplica conforme a ITIL 4 porque la monitorización del software ATM no está centralizada ni automatizada, y no existe un tratamiento formal del ciclo de vida de eventos. La identificación, correlación y priorización de alertas se realiza de forma reactiva, sin un marco definido de reglas o umbrales de referencia.
9	Gestión de Activos de TI	Controla inventario de software ATM (versiones instaladas, licencias, parches), permitiendo rastrear configuraciones por cajero, ciclo de vida y cumplimiento normativo del software.	No	La práctica no está implementada según ITIL 4, ya que no existe un inventario consolidado, actualizado y trazable del software ATM. Las versiones, licencias y configuraciones no se gestionan mediante un repositorio formal (CMS/CMDB), lo que limita la visibilidad y control del ciclo de vida de los activos lógicos.
10	Validación y Pruebas del Servicio	Asegura pruebas funcionales, de regresión, seguridad, desempeño y certificación con switch bancario antes de desplegar nuevas versiones del software ATM. Garantiza que el software cumpla estándares bancarios y regulatorios.	Si	

11	Gestión de Infraestructura y Plataformas	Asegura que la infraestructura y plataformas tecnológicas que soportan el software de los cajeros automáticos (sistemas operativos, middleware, versiones certificadas y tecnologías asociadas) se gestionen de forma estandarizada y controlada, garantizando compatibilidad, soporte del proveedor, seguridad operativa y continuidad del servicio ATM.	No	La gestión de infraestructura y plataforma no se encuentra formalizada conforme a ITIL 4, ya que no existe un control centralizado de versiones, configuraciones y dependencias tecnológicas del entorno ATM. La falta de estandarización y documentación limita la trazabilidad del ciclo de vida del software y dificulta la evaluación de impactos ante cambios, despliegues o incidentes.

Fuente: Elaboración Propia

Descripción

La tabla 20 presenta la aplicación de la Lista de Verificación ITIL 4 para el software de cajeros automáticos, evaluando diez prácticas clave. Se observa cumplimiento en Gestión y Desarrollo de Software, Gestión de Implementaciones, Gestión de Liberaciones, Gestión de Incidentes, Gestión de Problemas, Gestión de la Disponibilidad y Validación y Pruebas del Servicio. En contraste, no cumplen plenamente las prácticas de Gestión de Cambios, Gestión de Monitorización y Eventos y Gestión de Activos de TI, donde se señalan observaciones específicas sobre debilidades en formalización, automatización e inventario.

Análisis

Los resultados evidencian que el banco cuenta con una base importante de prácticas ITIL 4 orientadas a operación y soporte del software ATM, especialmente en la atención de incidentes, problemas, disponibilidad y pruebas, lo que favorece la continuidad del servicio. Sin embargo, las brechas en Gestión de Cambios, Monitorización y Eventos y Gestión de Activos de TI muestran que aún no se dispone de un gobierno completo del ciclo de vida del software: faltan procesos formalizados de cambio, monitoreo centralizado y un inventario consolidado de activos lógicos, lo que limita la trazabilidad, la prevención de fallas y el control de riesgos.

Hallazgo

La ausencia de control formal de cambios y activos incrementa los riesgos de fallas, inconsistencias y vulnerabilidades, la falta de monitoreo automatizado perpetúa el modelo reactivo, afectando disponibilidad y aumentando incidentes. De igual forma, las prácticas aplicadas correctamente son una base sólida, pero no logran compensar las brechas en control, trazabilidad y prevención. Esto confirma la necesidad de adoptar ITIL 4 de forma más completa y estandarizada.

Cuatro prácticas no se aplican según los lineamientos de ITIL 4:

- Gestión de Cambios: falta un CAB operativo y un proceso formalizado para analizar riesgos, impacto y categorización.
- Gestión de Monitorización y Eventos: ausencia de monitoreo automatizado y correlación de alertas.
- Gestión de Activos de TI: no existe inventario consolidado del software, versiones o licencias.
- Gestión de Infraestructura y Plataformas: no existe un estándar para el manejo de

versiones, configuraciones y dependencias tecnológicas.

RESULTADOS DEL INSTRUMENTO MATRIZ DE ANÁLISIS DOCUMENTAL

Los resultados del instrumento matriz de análisis documental permiten identificar de forma sistemática cómo la literatura especializada y los marcos de referencia internacionales aportan a la comprensión y mejora de la gestión de riesgos e incidentes en el software de cajeros automáticos. A través de la revisión de normas, guías de buenas prácticas y estudios empíricos, se evidencian los elementos de COBIT 2019 e ITIL 4 que pueden ser adaptados al contexto de la institución bancaria, especialmente en lo relativo al gobierno de TI, la gestión de servicios y el tratamiento de incidentes operativos. La matriz sintetiza dichos aportes y sirve de base para la propuesta de fortalecimiento del modelo de gestión actual.

Descripción

La matriz de análisis documental recopila fuentes normativas y académicas que desarrollan los principios, procesos y prácticas de COBIT 2019 e ITIL 4 vinculados con el gobierno de TI, la gestión de riesgos y el manejo de incidentes. Cada registro incluye año, autores, tipo de recurso y referencia, lo que permite ubicar los documentos clave que orientan el diseño de controles, flujos de atención y mecanismos de respuesta ante fallos del software de cajeros automáticos. En conjunto, las fuentes revisadas cubren tanto la fundamentación teórica como aplicaciones prácticas en organizaciones financieras y de servicios.

Tabla 23: *Resultados del análisis documental sobre la aplicabilidad de COBIT 2019 e ITIL 4 en la gestión de riesgos e incidentes del software de cajeros automáticos*

N°	Año	Autores	Título	Tipo de recurso	Referencia
1	2018	ISACA	COBIT 2019 Framework: Introduction and Methodology	Marco de referencia / libro	ISACA. (2018). *COBIT 2019 framework: Introduction and methodology*. Schaumburg, IL: ISACA. (community.mis.temple.edu)
2	2018	ISACA	COBIT 2019 Governance and Management Objectives	Marco de referencia / libro	ISACA. (2018). *COBIT 2019: Governance and management objectives*. Schaumburg, IL: ISACA. (ISACA)
3	2019	AXELOS	ITIL Foundation: ITIL 4 Edition	Manual oficial de buenas prácticas	AXELOS. (2019). *ITIL foundation: ITIL 4 edition*. London: TSO for AXELOS. (abim.go.ug)
4	2020	AXELOS	ITIL 4: Incident Management Practice	Guía de práctica ITIL 4	AXELOS. (2020). *ITIL 4: Incident management practice*. London: AXELOS.
5	2023	IT Process Maps GmbH	ITIL 4 Incident Management	Artículo técnico en línea	IT Process Maps. (2023). *ITIL 4 incident management*. IT Process Wiki.
6	2025	Alloy Software Inc.	The Role of Incident Management in ITIL 4	Artículo web aplicado al sector TI	Alloy. (2025). *The role of incident management in ITIL 4*. Alloy Software Blog. (ManageEngine)
7	2022	Santoso, Y.; otros	Information System Audit Using COBIT 2019 on Multi Finance Company	Artículo científico	Santoso, Y., et al. (2022). Information system audit using COBIT 2019 on multi finance company. *Tanesa Journal of Information Technology*. (ISACA)
8	2023	Hidayat, R.; otros	IT Governance Analysis Using COBIT 2019 Framework at BMKG	Artículo de conferencia	Hidayat, R., et al. (2023). IT governance analysis using COBIT 2019 framework at BMKG. En *Proceedings on information system governance*. (ejournal.uniks.ac.id)
9	2025	Al Qatanani, K. M.	The Impact of Implementing Information Technology Governance Based on the COBIT 2019 Framework on Institutional Performance	Artículo científico	Al Qatanani, K. M. (2025). The impact of implementing information technology governance based on the COBIT 2019 framework on institutional performance. *Learning Gate*, 2(4). (learning-gate.com)
10	2023	Hidayah, N.; otros	Mapping COBIT 2019 Processes to ITIL 4 Practices for Integrated IT Governance and Service Management	Artículo técnico / académico	Hidayah, N., et al. (2023). Mapping COBIT 2019 processes to ITIL 4 practices for integrated IT governance and service management. *IT Service Management Review*. (Cybiant)

Fuente: Elaboración Propia

Análisis

Del análisis comparativo de los documentos se desprende que COBIT 2019 ofrece un marco sólido para alinear la gestión de riesgos tecnológicos con los objetivos de negocio, mientras que ITIL 4 aporta directrices específicas para estructurar procesos de gestión de incidentes, problemas y continuidad del servicio. La convergencia de ambos enfoques permite identificar brechas entre las buenas prácticas internacionales y la realidad operativa del software de cajeros automáticos, especialmente en aspectos de gobernanza, definición de roles, trazabilidad de incidentes y mejora continua. Esto evidencia oportunidades claras de estandarización y optimización del modelo actual.

Hallazgo

El principal hallazgo derivado de la matriz es que la aplicabilidad conjunta de COBIT 2019 e ITIL 4 resulta pertinente y viable para robustecer el análisis de riesgos y la gestión de incidentes del software de cajeros automáticos. Los documentos revisados muestran que la adopción estructurada de estos marcos contribuye a reducir la ocurrencia de fallos, mejorar los tiempos de respuesta y fortalecer la confiabilidad del servicio hacia los usuarios. Asimismo, se constata que la institución carece de una integración formal de estos lineamientos, lo que justifica la necesidad de una propuesta que incorpore procesos, controles e indicadores alineados con dichos estándares.

4.2.4 HALLAZGOS SOBRE LA EVALUACIÓN DE COBIT 2019 E ITIL 4 EN EL ANÁLISIS DE RIESGOS Y LA GESTIÓN DE INCIDENTES DEL SOFTWARE DE CAJEROS AUTOMÁTICOS

El análisis cualitativo aplicado al Objetivo 2 evidencia que la gestión actual del software de cajeros automáticos en Banco Ficohsa dispone de prácticas operativas funcionales, pero presenta brechas relevantes en materia de gobernanza, estandarización y control preventivo. En términos generales, los tres instrumentos utilizados (COBIT Performance Management, Service Value Chain de ITIL 4 y la Lista de Verificación ITIL 4) coinciden en señalar la coexistencia de procesos bien ejecutados en el nivel operativo con carencias importantes en actividades estratégicas y de control.

Desde la perspectiva de COBIT Performance Management, el nivel de capacidad organizacional se sitúa en un rango medio, con fortalezas claras en las actividades de pruebas, gestión de incidentes y liberaciones. Sin embargo, persisten brechas en la gestión de riesgos, el monitoreo del desempeño y la gobernanza del ciclo de vida del software. Estas debilidades reducen

la capacidad de anticiparse a fallas y exponen el servicio de cajeros automáticos a riesgos tecnológicos y operativos que no se gestionan de manera sistemática.

En la Cadena de Valor del Servicio, el flujo de valor se observa completo y en funcionamiento, especialmente en las actividades de Diseño y Transición, Entrega y Soporte, y Obtención o Construcción. No obstante, se mantienen debilidades en las actividades de Planificación, Participación y Mejora, donde la ausencia de mecanismos formales, de retroalimentación estructurada y de automatización genera ineficiencias y una alta dependencia de respuestas reactivas. Estas interrupciones del flujo incrementan la probabilidad de fallas y disminuyen la estabilidad operativa del sistema.

La Lista de Verificación ITIL 4 refuerza este patrón: aunque varias prácticas se ejecutan adecuadamente (desarrollo, liberaciones, incidentes, problemas, disponibilidad y validación), tres prácticas críticas no se aplican conforme al marco de referencia. Se trata de la gestión de cambios, la gestión de monitorización y eventos, y la gestión de activos de TI. Su ausencia limita la trazabilidad de las decisiones, retrasa la detección temprana de fallas y dificulta la prevención de inconsistencias en versiones y configuraciones del software.

En conjunto, los hallazgos describen una organización con experiencia operativa y procesos funcionales, pero con un nivel de madurez insuficiente en gobernanza, monitoreo, gestión de riesgos y control del ciclo de vida del software. Esta situación confirma la pertinencia del Objetivo 2 y respalda la necesidad de implementar de manera integrada COBIT 2019 e ITIL 4. La adopción articulada de ambos marcos permitiría elevar el nivel de madurez, fortalecer la gobernanza del software de cajeros automáticos, optimizar la gestión de incidentes y consolidar controles preventivos mediante procesos estandarizados, medibles y con mayor grado de automatización.

4.3 INDICADORES CLAVE Y MÉTRICAS PARA LA MEJORA CONTINUA DEL SOFTWARE DE CAJEROS AUTOMÁTICOS

La presente sección se enfocará en el diseño de indicadores clave de desempeño (KPIs) y métricas de seguimiento orientadas a evaluar de manera sistemática la efectividad de la gestión del software de cajeros automáticos. A partir de los hallazgos obtenidos en el análisis de riesgos, vulnerabilidades e incidentes, se establecerán parámetros cuantificables que permitirán medir el nivel de cumplimiento de los controles, la oportunidad en la atención de fallos y la estabilidad operativa de la plataforma. Estos indicadores se vincularán con los objetivos estratégicos de la institución y con las buenas prácticas propuestas por marcos como COBIT 2019 e ITIL 4, de modo

que la medición del desempeño no sea aislada, sino parte de una visión integral de gobierno y gestión de TI.

Asimismo, se propondrá un esquema de monitoreo continuo que facilitará la identificación temprana de desviaciones, la retroalimentación de los procesos y la toma de decisiones basada en evidencia. De este modo, los KPIs y métricas definidas no solo servirán para verificar resultados, sino que se convertirán en herramientas clave para impulsar un ciclo de mejora continua en la gestión del software de cajeros automáticos, favoreciendo la reducción de riesgos, el incremento de la disponibilidad del servicio y el fortalecimiento de la confianza de los usuarios internos y externos.

4.3.1 ALINEACIÓN METODOLÓGICA CON COBIT 2019 E ITIL 4

Antes de presentar los indicadores numéricos y las métricas específicas, se establecerá el marco de referencia que los sustenta, integrando las buenas prácticas de ITIL 4 y COBIT 2019. Esta alineación permitirá que los KPIs no solo midan el desempeño operativo del software de cajeros automáticos, sino también su contribución al control de riesgos, al cumplimiento normativo y a la mejora continua de la gestión de TI en la institución financiera.

- **Enfoque ITIL 4:** Se tomará como referencia principalmente las prácticas de Gestión de Disponibilidad y Gestión de Liberación de Software. Bajo este enfoque, los indicadores estarán orientados a garantizar que el software de los cajeros automáticos aporte valor al cliente, asegurando que el servicio esté disponible cuando el usuario lo requiere, que las actualizaciones se apliquen de forma controlada y que las interrupciones se reduzcan al mínimo posible. Los KPIs derivados de ITIL 4 se enfocarán en tiempos de disponibilidad, frecuencia de incidentes, tiempos de resolución y éxito en las liberaciones.
- **Enfoque COBIT 2019:** Se priorizarán los objetivos de gobierno y gestión vinculados al dominio MEA (Monitorizar, Evaluar y Valorar), con énfasis en la supervisión del desempeño de TI y la gestión de riesgos lógicos asociados al software de cajeros automáticos. Desde esta perspectiva, los indicadores buscarán evidenciar el grado de cumplimiento de las regulaciones establecidas por la Comisión Nacional de Bancos y Seguros en Honduras, así como la eficacia de los controles implementados. Los KPIs derivados de COBIT 2019 se orientarán a la detección de vulnerabilidades, el registro y análisis de incidentes, el seguimiento de acciones correctivas y la evaluación periódica del nivel de riesgo residual.

4.3.2 MATRIZ DE INDICADORES CLAVE DE DESEMPEÑO (KPIS)

En este apartado se presentará la matriz de indicadores clave de desempeño diseñada específicamente para evaluar la gestión del software de cajeros automáticos. La construcción de esta matriz se realizará tomando como base la alineación metodológica previamente descrita con COBIT 2019 e ITIL 4, de manera que cada KPI responda a objetivos concretos de disponibilidad, continuidad del servicio, seguridad lógica, cumplimiento normativo y control de riesgos.

La matriz permitirá visualizar de forma estructurada los indicadores propuestos, incluyendo su definición, fórmula de cálculo, frecuencia de medición, unidad de análisis, fuente de datos y responsable de monitoreo. De esta forma, se facilitará la toma de decisiones fundamentadas, se promoverá la trazabilidad de las acciones correctivas y se fomentará un ciclo de mejora continua en la gestión del software de cajeros automáticos dentro de la institución financiera.

4.3.2.1 KPIS DE DISPONIBILIDAD Y OPERACIÓN DEL SOFTWARE ATM (ENFOQUE ITIL 4)

En este subapartado se presentarán los indicadores clave de desempeño orientados a medir la disponibilidad y operación del software de cajeros automáticos, bajo el enfoque de ITIL 4. Estos KPIs permitirán evaluar, de forma objetiva y periódica, la continuidad del servicio, la frecuencia y duración de las caídas, el cumplimiento de los acuerdos de nivel de servicio y la capacidad de respuesta ante incidencias operativas. Su definición y seguimiento contribuirán a garantizar que el software del ATM se mantenga funcional cuando el cliente lo requiere, reduciendo tiempos de inactividad, mejorando la experiencia del usuario y fortaleciendo la eficiencia operativa de la institución financiera.

Tabla 24: *KPIs de Disponibilidad y Operación (Enfoque ITIL 4 - SVS)*

Indicador (KPI)	Descripción	Fórmula / Cálculo	Frecuencia	Meta Sugerida
% Disponibilidad del Software ATM	Tiempo total que el software está operativo y capaz de transaccionar.	Tiempo Total - Tiempo Inactividad por Software / Tiempo Total x 100	Mensual	> 97 %
MTTR (Mean Time to Restore) de Software	Tiempo promedio para restaurar el servicio tras una falla de software.	Tiempo Total de Inactividad / Número de Incidentes	Mensual	< 30 min
Tasa de Éxito en Despliegues Remotos	Porcentaje de cajeros actualizados exitosamente sin intervención física.	Actualizaciones Exitosas / Total de Intentos x100	Por Release	> 98 %

Fuente: Elaboración Propia

La Tabla 23 presenta los indicadores clave de desempeño orientados a monitorear la disponibilidad y operación del software de cajeros automáticos bajo el enfoque de ITIL 4. El indicador de % de Disponibilidad del Software ATM mide la proporción de tiempo en que el sistema permanece operativo y apto para procesar transacciones, siendo su meta superior al 97 %, lo que asegura continuidad del servicio para los usuarios. El MTTR (Mean Time to Restore) de Software permite conocer el tiempo promedio que se tarda en restablecer el servicio después de una falla; una meta menor a 30 minutos refleja una capacidad de respuesta oportuna del equipo técnico. Finalmente, la Tasa de Éxito en Despliegues Remotos evalúa el porcentaje de actualizaciones de software realizadas correctamente sin requerir intervención física en los cajeros, con una meta superior al 98 %, lo que contribuye a minimizar interrupciones y optimizar los procesos de mantenimiento y mejora continua del servicio.

4.3.2.2 KPIS DE RIESGO Y SEGURIDAD LÓGICA (ENFOQUE COBIT 2019)

Los KPIs de riesgo y seguridad lógica presentados en este apartado se diseñarán con base en los objetivos de gobierno y gestión propuestos por COBIT 2019, especialmente aquellos vinculados al monitoreo, evaluación y valoración del desempeño y la conformidad. Estos indicadores permitirán medir la exposición del software de cajeros automáticos a incidentes de seguridad, vulnerabilidades y fallos de control, así como el grado de cumplimiento de las políticas internas y de la normativa emitida por la CNBS y otros entes reguladores. De esta forma, los KPIs de riesgo y seguridad lógica servirán como insumo estratégico para identificar desviaciones, priorizar acciones de mitigación y fortalecer el marco de control interno asociado al ciclo de vida del software ATM.

Tabla 25: *KPIs de Riesgo y Seguridad (Enfoque COBIT 2019 - EDM/DSS)*

Indicador (KPI)	Descripción	Fórmula / Cálculo	Frecuencia	Meta Sugerida
% Vulnerabilidades Críticas Mitigadas	Porcentaje de parches de seguridad aplicados dentro del tiempo establecido (SLA).	Parches Críticos Aplicados Total Parches Críticos Liberados x 100	Quincenal	100%
Incidentes de Fraude Lógico (Software)	Intentos de manipulación del software (ej. Jackpotting) detectados/bloqueados.	Conteo Simple de Eventos	Semanal	0
Índice de Cumplimiento	Adherencia a los controles de software exigidos por la CNBS	Controles Cumplidos / Total	Trimestral	100%

Normativo (CNBS)	(Honduras).	Controles CNBS x 100		

Fuente: Elaboración Propia

4.3.3 DISEÑO DEL DASHBOARD DE GESTIÓN DEL SOFTWARE ATM

Para materializar la supervisión de los riesgos identificados se ha diseñado un cuadro de mando integral en formato de dashboard. Este instrumento no solo permite visualizar el estado actual de la red de cajeros automáticos, sino que también funciona como detonante principal del ciclo de mejora continua propuesto a partir de COBIT 2019 e ITIL 4, al transformar datos operativos en información útil para la toma de decisiones estratégicas en Banco Ficohsa.

Para cumplir con el objetivo, se propone el diseño visual de un tablero de control que permita a la Gerencia de Medios de Pago TI de Banco Ficohsa monitorear, en tiempo casi real, la salud y los riesgos del software de cajeros automáticos. Este dashboard debe facilitar una toma de decisiones ágil y alimentar el ciclo de mejora continua en la gestión del software ATM.

Tabla 26: *Resumen del diseño del dashboard de gestión del software ATM*

Componente del dashboard	Contenido principal	Propósito en la gestión del software ATM	Relación con COBIT 2019 e ITIL 4
Visión general del dashboard	Cuadro de mando integral en formato de panel visual que consolida datos operativos de la red de cajeros automáticos y los convierte en información para la toma de decisiones.	Materializar la supervisión de los riesgos identificados y la salud de la red de ATMs, integrando en una sola vista el estado actual del servicio y los principales indicadores de desempeño y riesgo.	COBIT 2019 aporta el enfoque de gobierno y gestión del riesgo. ITIL 4 proporciona la lógica de cadena de valor y operación del servicio sobre la que se apoya el monitoreo.
Zona 1. Encabezado y estado general	Título “Monitor de Salud y Riesgos de Software ATMs, Banco Ficohsa”, semáforo general de riesgo (rojo, ámbar, verde) y filtros dinámicos por zona geográfica, tipo de ATM y versión de software.	Proporcionar una vista ejecutiva inmediata del estado global de la red y permitir segmentar el análisis para identificar con rapidez escenarios de mayor criticidad y priorizar la atención.	COBIT 2019 respalda la supervisión de desempeño y riesgo. ITIL 4 se refleja en la operación del servicio y en la gestión de la disponibilidad.
Zona 2. Tarjetas de KPIs operativos	Tarjetas con disponibilidad actual, número de cajeros fuera de servicio por software y	Facilitar el seguimiento continuo de los indicadores operativos críticos, detectar	COBIT 2019 alinea los KPIs con objetivos de negocio y continuidad. ITIL 4

	MTTR promedio de restauración, con valores numéricos y tendencias para lectura rápida.	desviaciones respecto a los SLA y orientar decisiones ágiles de soporte y mantenimiento.	articula estos indicadores con la gestión de incidentes y de la disponibilidad.
Zona 3. Gráficas de tendencia y análisis	Gráfico de líneas sobre tendencia de fallos de software frente a actualizaciones y gráfico de barras apiladas sobre estado de parches de seguridad (instalado, pendiente de reinicio, fallido).	Analizar la evolución de incidentes en el tiempo, correlacionar fallos con despliegues de parches y evaluar el avance de las tareas de endurecimiento del sistema para ajustar la estrategia de actualización.	COBIT 2019 se vincula con la medición y evaluación del rendimiento. ITIL 4 se refleja en la gestión de cambios, versiones y mejora continua del servicio.
Zona 4. Matriz dinámica de riesgos	Mapa de calor de tres por tres que muestra riesgos residuales por probabilidad e impacto y lista de "Top 5 ATMs con incidentes recurrentes de software".	Visualizar de forma sintética los riesgos más críticos, focalizar la mitigación y dirigir el mantenimiento preventivo y correctivo hacia los cajeros con mayor reincidencia de fallos de software.	COBIT 2019 guía la gestión y seguimiento del riesgo residual. ITIL 4 apoya la gestión de problemas y la priorización de incidentes.
Estrategia de mejora continua asociada	Secuencia de pasos: monitoreo del desempeño, evaluación de evidencias, acción correctiva sobre procesos y resultados y retroalimentación para el siguiente ciclo de medición.	Integrar el dashboard en un ciclo de mejora continua que use las desviaciones de los KPIs para ajustar pruebas, despliegues y métricas, reduciendo de forma progresiva la incidencia de fallos y el riesgo residual.	COBIT 2019 se concreta en el dominio de medición, evaluación y auditoría. ITIL 4 aporta la práctica de mejora continúa aplicada a la gestión del software ATM.

Fuente: Elaboración Propia

4.3.4. FICHAS TÉCNICAS DE INDICADORES SELECCIONADOS

El presente apartado desarrolla la ficha técnica del indicador Índice de disponibilidad operativa del software de cajeros automáticos (KPI-ATM-001), concebido como uno de los principales mecanismos de seguimiento del desempeño del sistema. A partir de la alineación con COBIT 2019 e ITIL 4, se define su propósito, fórmula de cálculo, fuentes de información, frecuencia de medición y umbrales de referencia. Con ello se busca contar con un indicador claramente delimitado, técnicamente robusto y vinculado a la gestión de riesgos, que permita evaluar de forma objetiva la continuidad del servicio transaccional en la red de ATMs de Banco

Ficohsa.

4.3.4.1 FICHA TÉCNICA DEL INDICADOR KPI-ATM-001

Nombre del indicador: Índice de disponibilidad operativa del software de cajeros automáticos

1. Identificación y alineación estratégica

- **Código:** KPI-ATM-001
- **Perspectiva COBIT 2019:** Alineado con los objetivos de gestión DSS01 (Gestionar las operaciones) y MEA01 (Supervisar, evaluar y valorar el rendimiento).
- **Prácticas ITIL 4 relacionadas:** Gestión de la disponibilidad y Gestión de incidentes.
- **Objetivo de negocio:** Garantizar la continuidad del servicio transaccional en los canales electrónicos de Banco Ficohsa.

2. Definición operativa

- **Descripción:** Mide el porcentaje de tiempo durante el cual el software del cajero automático, tanto la capa aplicativa como el sistema operativo, se mantiene funcionando correctamente y habilitado para procesar transacciones de clientes.
- **Alcance:** Considera exclusivamente incidentes atribuibles al software. Se excluyen fallas de hardware (atascos de papel, fallas de dispensador, etc.) y problemas de telecomunicaciones (caída de enlaces, pérdida de señal).

3. Cálculo matemático

Para obtener el porcentaje de disponibilidad se utiliza la fórmula:

$$\text{Disponibilidad}(\%) = \frac{\text{Tiempo total programado} - \text{Tiempo de inactividad por software}}{\text{Tiempo total programado}} \times 100$$

Donde:

- **Tiempo total programado:** Horario de servicio definido para el ATM, generalmente 24/7, equivalente a un promedio mensual cercano a 720 horas.
- **Tiempo de inactividad por software:** Suma de las horas o minutos en que el cajero estuvo fuera de servicio por errores de aplicación, pantallas azules, reinicios forzados o

actualizaciones fallidas.

4. Fuente de datos y recolección

- **Fuente de información:** Registros del switch transaccional y de la herramienta de monitoreo de ATMs (por ejemplo, Vynamic View, NCR Aptra Vision o la solución utilizada por el banco).
- **Responsable de la medición:** Coordinador de canales electrónicos, oficial de monitoreo TI o especialista de medios de pago.
- **Frecuencia de medición:** Mensual, con seguimiento diario a través del dashboard de monitoreo.

5. Umbrales de desempeño

Los rangos de referencia permiten evaluar la efectividad de las estrategias de mitigación propuestas en la investigación.

Tabla 27: *Umbrales de Desempeño*

Estado	Rango de disponibilidad	Interpretación y acción sugerida
Óptimo (verde)	mayor o igual a 97 %	La estrategia de gestión de software es efectiva. El riesgo operativo es bajo.
Alerta (amarillo)	entre 96 % y 95 %	Se observa degradación del servicio. Requiere revisión de parches recientes y análisis de logs.
Crítico (rojo)	menor a 95 %	Nivel inaceptable según estándares bancarios y de la CNBS. Se activa plan de contingencia y reversión de cambios.

Fuente: Elaboración Propia

6. Relación con la gestión de riesgos

- **Riesgo principal mitigado:** Interrupción del negocio por fallos lógicos del software de los cajeros automáticos.
- **Impacto asociado:** Si el indicador disminuye, aumenta el riesgo reputacional y el riesgo financiero por comisiones no percibidas y operaciones no ejecutadas.

4.3.4.2 FICHA TÉCNICA DEL INDICADOR KPI-ATM-002

Nombre del indicador: MTTR (Mean Time to Restore) de software de cajeros

automáticos

1. Identificación y alineación estratégica

Código: KPI-ATM-002

Perspectiva COBIT 2019: Alineado con los objetivos de gestión DSS02 (Gestionar solicitudes e incidentes de servicio), DSS03 (Gestionar problemas) y MEA01 (Supervisar, evaluar y valorar el rendimiento).

Prácticas ITIL 4 relacionadas: Gestión de incidentes, Gestión de la disponibilidad y Gestión de problemas.

Objetivo de negocio: Reducir el tiempo promedio de recuperación del servicio de los cajeros automáticos ante fallas de software, a fin de limitar el impacto operativo y reputacional asociado a la indisponibilidad del canal.

2. Definición operativa

Descripción: Mide el tiempo promedio que transcurre desde que se registra un incidente de indisponibilidad del cajero automático causado por software hasta que el servicio queda restaurado y validado como operativo para los clientes.

Alcance: Considera únicamente incidentes cuya causa raíz esté asociada a errores de aplicación, sistema operativo, conflictos de parches o configuraciones lógicas. Se excluyen interrupciones planificadas por mantenimiento y eventos originados por fallas de hardware o telecomunicaciones.

3. Cálculo matemático

Para obtener el MTTR de software se utiliza la fórmula:

$$MTTR\ de\ Software = \sigma\ \frac{Tiempo\ de\ restauración\ de\ incidentes\ de\ software}{Número\ de\ incidentes\ de\ software\ en\ el\ periodo}$$

Donde: Tiempo de restauración de incidentes de software: Diferencia, medida en minutos, entre la hora de registro del incidente en la herramienta ITSM y la hora en que el cajero vuelve a estar disponible para operar transacciones, según el sistema de monitoreo.

Número de incidentes de software en el periodo: Total de incidentes de indisponibilidad por software registrados en el intervalo de análisis (por ejemplo, un mes).

4. Fuente de datos y recolección

Fuente de información: Registros de la herramienta de gestión de servicios (ITSM, por ejemplo, IVANTI), bitácoras del Centro de Operaciones de Red (NOC) y registros de la herramienta de monitoreo de ATMs y del switch transaccional.

Responsable de la medición: Coordinador de canales electrónicos, analista de monitoreo TI o responsable de gestión de incidentes en Medios de Pago.

Frecuencia de medición: Mensual, con seguimiento operativo diario o semanal mediante el dashboard de monitoreo.

5. Umbrales de desempeño

Los rangos de referencia permiten evaluar la efectividad de las estrategias de respuesta y restauración del servicio.

Tabla 28: *Umbrales de desempeño del MTTR de software*

Estado	Rango de MTTR	Interpretación y acción sugerida
Óptimo	menor o igual a 20 minutos	El tiempo de recuperación es adecuado y consistente con los objetivos de continuidad del servicio. Se mantienen los procedimientos vigentes.
Alerta	mayor de 20 a 40 minutos	El tiempo de restauración muestra degradación. Requiere revisar la coordinación entre NOC, soporte de software y proveedores, así como la efectividad de los procedimientos de resolución.
Crítico	mayor a 40 minutos	Tiempo promedio de recuperación inaceptable para un canal crítico. Debe activarse un plan de mejora, revisar recursos asignados y optimizar los flujos de atención de incidentes.

Fuente: Elaboración Propia

6. Relación con la gestión de riesgos

Riesgo principal mitigado: Prolongación de la interrupción del negocio por fallas de software en cajeros automáticos, con impacto en la satisfacción del cliente y en los ingresos por comisiones.

Impacto asociado: Si el MTTR aumenta de forma sostenida, se incrementa el riesgo operativo y reputacional, ya que los clientes encuentran con mayor frecuencia cajeros inoperativos o fuera de servicio. La reducción progresiva del MTTR contribuye a limitar la duración de los eventos de indisponibilidad y a reforzar la resiliencia del canal ATM dentro del marco de gestión

de riesgos definido por COBIT 2019 y las prácticas de ITIL 4.

4.3.4.3 FICHA TÉCNICA DEL INDICADOR KPI-ATM-003

Nombre del indicador: Tasa de éxito en despliegues remotos de software de cajeros automáticos

1. Identificación y alineación estratégica

Código: KPI-ATM-003

Perspectiva COBIT 2019: Alineado con los objetivos de gestión BAI07 (Gestionar la aceptación y transición de cambios), BAI08 (Gestionar cambios) y MEA01 (Supervisar, evaluar y valorar el rendimiento).

Prácticas ITIL 4 relacionadas: Gestión de cambios, Gestión de despliegues, Gestión de versiones y Mejora continua.

Objetivo de negocio: Asegurar que las actualizaciones y cambios de software ejecutados de forma remota sobre la red de cajeros automáticos se completen correctamente, minimizando fallos en producción y evitando impactos negativos en la disponibilidad del canal ATM.

2. Definición operativa

Descripción: Mide el porcentaje de despliegues remotos de software de cajeros automáticos que se ejecutan de manera exitosa en un periodo determinado, es decir, que concluyen conforme al plan y no generan incidentes de indisponibilidad atribuibles al cambio dentro de la ventana de estabilización definida.

Alcance: Considera únicamente cambios y despliegues remotos en el software de los cajeros automáticos, incluyendo parches de seguridad, actualizaciones de versión y ajustes de configuración lógica. Se excluyen actividades de mantenimiento planificado que no impliquen modificación del software y cambios en infraestructura o telecomunicaciones ajenos al ATM.

3. Cálculo matemático

Para obtener la tasa de éxito en despliegues remotos se utiliza la fórmula:

$$Tasa\ de\ éxito\ en\ despliegues\ remotos\ (\%) = \left(\frac{Número\ de\ despliegues\ remotos\ exitosos\ en\ el\ periodo}{Número\ total\ de\ despliegues\ remotos\ en\ el\ periodo}\right) \times 100$$

Donde:

Número de despliegues remotos exitosos en el periodo: Cantidad de despliegues que finalizaron según lo programado y que no originaron incidentes de severidad alta o crítica por fallas de software en la ventana de estabilización definida por el banco.

Número total de despliegues remotos en el periodo: Conjunto de todos los cambios y actualizaciones remotas realizados sobre el software de los cajeros en el intervalo de análisis, independientemente de su resultado.

4. Fuente de datos y recolección

Fuente de información: Registros de la herramienta de gestión de servicios (ITSM) y del módulo de Gestión de Cambios, bitácoras de despliegue de software, reportes del Centro de Operaciones de Red y registros de incidentes vinculados a cambios.

Responsable de la medición: Gestor de cambios de TI, coordinador de canales electrónicos o responsable de la gestión de versiones de software de ATMs.

Frecuencia de medición: Mensual, con revisión posterior a cada ventana de despliegue para actualizar el resultado de los cambios ejecutados.

5. Umbrales de desempeño

Los rangos de referencia permiten evaluar la madurez del proceso de despliegue remoto y su contribución a la estabilidad del servicio.

Tabla 29: *Umbrales de desempeño de la tasa de éxito en despliegues remotos*

Estado	Rango de tasa de éxito	Interpretación y acción sugerida
Óptimo	mayor o igual a 98 %	El proceso de despliegue remoto es altamente confiable y rara vez genera incidentes. Se mantienen procedimientos y se documentan buenas prácticas.
Alerta	entre 95 % y 97,99 %	Se observa presencia de fallos asociados a cambios. Requiere revisar planificación, pruebas previas y criterios de aprobación de despliegues.
Crítico	menor a 95 %	Nivel de fallos inaceptable en cambios sobre un canal crítico. Se deben reforzar controles de cambio, ampliar pruebas en entornos de calidad y limitar despliegues masivos hasta estabilizar el proceso.

Fuente: Elaboración Propia

6. Relación con la gestión de riesgos

Riesgo principal mitigado: Fallos de software derivados de cambios y despliegues defectuosos que provoquen indisponibilidad del servicio, errores transaccionales o vulnerabilidades de seguridad en la red de cajeros automáticos.

Impacto asociado: Una tasa baja de éxito en los despliegues remotos incrementa el riesgo operativo y reputacional, ya que los cambios se convierten en una fuente recurrente de incidentes. La mejora progresiva de este indicador reduce la probabilidad de interrupciones causadas por actualizaciones, refuerza la confianza en el proceso de cambio y contribuye a mantener el riesgo residual dentro de los niveles definidos por el marco de gobierno COBIT 2019 y las prácticas de ITIL 4.

4.3.4.4 FICHA TÉCNICA DEL INDICADOR KPI-ATM-004

Nombre del indicador: Porcentaje de vulnerabilidades críticas mitigadas en el software de cajeros automáticos

1. Identificación y alineación estratégica

Código: KPI-ATM-004

Perspectiva COBIT 2019: Alineado con los objetivos de gestión APO12 (Gestionar el riesgo), DSS05 (Gestionar servicios de seguridad) y MEA01 (Supervisar, evaluar y valorar el rendimiento).

Prácticas ITIL 4 relacionadas: Gestión de la seguridad de la información, Gestión de vulnerabilidades, Gestión de cambios.

Objetivo de negocio: Reducir la exposición a riesgos de seguridad asociados a vulnerabilidades críticas en el software de los cajeros automáticos, garantizando que estas se atiendan y mitiguen dentro de los plazos definidos por la organización y la normativa aplicable.

2. Definición operativa

Descripción: Mide el porcentaje de vulnerabilidades clasificadas como críticas en el software de cajeros automáticos que han sido mitigadas o remediadas efectivamente en un periodo determinado, de acuerdo con los tiempos objetivo de tratamiento establecidos por el banco. Alcance: Considera únicamente vulnerabilidades críticas identificadas en la capa de software de

los ATMs (sistema operativo, middleware, aplicación de cajero y componentes relacionados). Se excluyen vulnerabilidades de infraestructura general que no impacten directamente al software del ATM y aquellas catalogadas como medias o bajas.

3. Cálculo matemático

Para obtener el porcentaje de vulnerabilidades críticas mitigadas se utiliza la fórmula:

$$\%\ de\ vulnerabilidades\ críticas\ mitigadas = \left(\frac{Número\ de\ vulnerabilidades\ críticas\ mitigadas\ en\ el\ periodo}{Número\ total\ de\ vulnerabilidades\ críticas\ identificadas\ en\ el\ periodo}\right) \times 100$$

Donde:

Número de vulnerabilidades críticas mitigadas en el periodo: Cantidad de vulnerabilidades catalogadas como críticas para el software de cajeros automáticos que han sido corregidas o controladas dentro del periodo de análisis, cumpliendo los plazos de tratamiento definidos (por ejemplo, 30 días calendario).

Número total de vulnerabilidades críticas identificadas en el periodo: Total de vulnerabilidades críticas detectadas en el software de los ATMs por herramientas de escaneo, auditorías o pruebas de seguridad durante el mismo periodo.

4. Fuente de datos y recolección

Fuente de información: Reportes de herramientas de gestión de vulnerabilidades y escaneo de seguridad, informes de auditoría de seguridad, registros del área de Seguridad de la Información y documentación de cambios aplicados al software de cajeros.

Responsable de la medición: Responsable de seguridad de la información, oficial de ciberseguridad o administrador de la plataforma de gestión de vulnerabilidades en coordinación con el área de Medios de Pago.

Frecuencia de medición: Mensual o trimestral, según la periodicidad de los ciclos de escaneo de vulnerabilidades y de los planes de remediación establecidos por el banco.

5. Umbrales de desempeño

Los rangos de referencia permiten evaluar la efectividad del proceso de tratamiento de vulnerabilidades críticas.

Tabla 30: *Umbrales de desempeño del porcentaje de vulnerabilidades críticas mitigadas*

Estado	Rango de mitigación	Interpretación y acción sugerida
Óptimo	mayor o igual a 95 %	La mayoría de las vulnerabilidades críticas se mitigan dentro de los plazos definidos. El riesgo de exposición es controlado. Se mantienen procesos y se documentan lecciones aprendidas.
Alerta	entre 80 % y 94,99 %	Existen vulnerabilidades críticas pendientes que incrementan la ventana de exposición. Requiere priorizar recursos, acelerar planes de remediación y revisar la coordinación entre seguridad y desarrollo.
Crítico	menor a 80 %	Nivel de vulnerabilidades críticas no mitigadas considerado inaceptable. Es necesario activar planes de respuesta, revisar la estrategia de gestión de vulnerabilidades y escalar el riesgo a la alta dirección.

Fuente: Elaboración Propia

6. Relación con la gestión de riesgos

Riesgo principal mitigado: Explotación de vulnerabilidades críticas en el software de cajeros automáticos que puedan derivar en fraudes lógicos, accesos no autorizados, interrupción del servicio o compromisos de información sensible.

Impacto asociado: Un porcentaje bajo de vulnerabilidades críticas mitigadas incrementa de forma directa el riesgo de materialización de incidentes de seguridad de alto impacto financiero y reputacional. La mejora de este indicador contribuye a reducir la superficie de ataque, fortalecer el cumplimiento de estándares y regulaciones, y mantener el riesgo residual dentro de los niveles aceptables definidos por COBIT 2019 y las prácticas de seguridad de ITIL 4.

4.3.4.5 FICHA TÉCNICA DEL INDICADOR KPI-ATM-005

Nombre del indicador: Incidentes de fraude lógico (software) en cajeros automáticos

1. Identificación y alineación estratégica

Código: KPI-ATM-005

Perspectiva COBIT 2019: Alineado con los objetivos de gestión APO12 (Gestionar el riesgo), DSS05 (Gestionar servicios de seguridad) y MEA01 (Supervisar, evaluar y valorar el rendimiento).

Prácticas ITIL 4 relacionadas: Gestión de incidentes, Gestión de seguridad de la información, Detección y respuesta ante eventos.

Objetivo de negocio: Detectar y minimizar los intentos de fraude lógico que buscan manipular el software de los cajeros automáticos, garantizando la integridad de las transacciones y protegiendo los activos del banco y de los clientes.

2. Definición operativa

Descripción: Mide el número de incidentes de fraude lógico relacionados con el software de los cajeros automáticos, tales como intentos de manipulación de la lógica de la aplicación, ataques de tipo *jackpotting* o ejecución de código malicioso, que hayan sido detectados y/o bloqueados por los controles de seguridad implementados.

Alcance: Incluye todos los eventos de seguridad clasificados como fraude lógico que afecten directamente al software del ATM (sistema operativo, aplicación de cajero, middleware, módulos de seguridad). Se excluyen fraudes puramente físicos (por ejemplo, *skimming* sin modificación del software) y fraudes en otros canales (banca en línea, POS, etc.).

3. Cálculo matemático

De acuerdo con la definición establecida en la matriz de KPIs, el indicador se calcula mediante un conteo simple:

Incidentes de fraude lógico (software) = Número total de eventos de fraude lógico detectados en el periodo

Donde:

Incidentes de fraude lógico: Eventos registrados por los sistemas de monitoreo y seguridad (SIEM, herramientas de detección de malware, logs de ATM, etc.) en los que se ha intentado manipular la lógica del software del cajero, independientemente de que el ataque haya sido exitoso o bloqueado.

Periodo: Intervalo de análisis definido por el banco (por ejemplo, una semana para seguimiento operativo y un mes para análisis de tendencia).

4. Fuente de datos y recolección

Fuente de información: Registros de las herramientas de monitoreo de seguridad (SIEM), logs de los cajeros automáticos, reportes del área de Seguridad de la Información, informes del Centro de Operaciones de Seguridad (SOC) y reportes de investigación de incidentes.

Responsable de la medición: Oficial de ciberseguridad, responsable de seguridad de la información o equipo del SOC en coordinación con Medios de Pago y el área de Riesgos Operativos.

Frecuencia de medición: Semanal, con consolidación mensual para análisis de tendencias y reportes de riesgo.

5. Umbrales de desempeño

Los rangos de referencia se definen para un periodo de análisis (por ejemplo, un mes), tomando como meta ideal cero incidentes:

Tabla 31: *Umbrales de desempeño del indicador Incidentes de fraude lógico (software)*

Estado	Rango de incidentes en el periodo	Interpretación y acción sugerida
Óptimo	0 incidentes	No se han registrado intentos de fraude lógico en el periodo. Se mantienen los controles actuales y se continúa con la vigilancia preventiva.
Alerta	1–2 incidentes	Se identifican intentos puntuales de fraude lógico. Requiere análisis detallado, revisión de controles y actualización de reglas de detección.
Crítico	3 o más incidentes	Actividad de amenaza elevada o controles insuficientes. Debe activarse plan de respuesta, reforzar medidas de seguridad, revisar configuraciones y escalar el riesgo a la alta dirección.

Fuente: Elaboración Propia

6. Relación con la gestión de riesgos

Riesgo principal mitigado: Materialización de fraudes lógicos sobre el software de cajeros automáticos que provoquen dispensa no autorizada de efectivo (jackpotting), alteración de saldos, transacciones fraudulentas o exposición de datos sensibles.

Impacto asociado: El incremento en el número de incidentes de fraude lógico eleva de manera directa el riesgo operativo, financiero y reputacional del banco. Mantener este indicador en cero o en niveles mínimos, junto con un análisis oportuno de cada evento, contribuye a disminuir la superficie de ataque, fortalecer el cumplimiento de la normativa de la CNBS y alinear la gestión de seguridad con los principios de COBIT 2019 e ITIL 4.

4.3.4.6 FICHA TÉCNICA DEL INDICADOR KPI-ATM-006

Nombre del indicador: Índice de Cumplimiento Normativo (CNBS)

1. Identificación y alineación estratégica

Código: KPI-ATM-006

Perspectiva COBIT 2019: Alineado con los objetivos de gestión APO12 (Gestionar el riesgo), APO01 (Gestionar el marco de gestión de TI) y MEA03 (Supervisar, evaluar y valorar el cumplimiento).

Prácticas ITIL 4 relacionadas: Gestión de la seguridad de la información, Gestión de riesgos, Mejora continua.

Objetivo de negocio: Asegurar que la gestión del software de cajeros automáticos cumpla con los controles y requisitos establecidos por la Comisión Nacional de Bancos y Seguros (CNBS), reduciendo el riesgo de sanciones, observaciones regulatorias y afectaciones a la reputación institucional.

2. Definición operativa

Descripción: Mide el porcentaje de controles y obligaciones normativas emitidas por la CNBS, aplicables al software y a la operación de cajeros automáticos, que se encuentran implementados y en cumplimiento efectivo dentro de Banco Ficohsa.

Alcance: Incluye controles relacionados con seguridad lógica, continuidad del negocio, gestión de riesgos tecnológicos, registros y monitoreo de transacciones en canales electrónicos. Se excluyen disposiciones de carácter estrictamente contable o financiero que no tengan relación directa con el canal ATM.

3. Cálculo matemático

Para obtener el índice de cumplimiento normativo se utiliza la fórmula definida en la matriz de KPIs:

$$Índice\ de\ Cumplimiento\ Normativo\ (CNBS) = \left(\frac{Controles\ CNBS\ cumplidos}{Total\ de\ controles\ CNBS\ aplicables}\right) \times 100$$

Donde:

Controles CNBS cumplidos: Número de controles y requisitos normativos aplicables al

software y operación de cajeros automáticos que el banco tiene implementados, documentados y en funcionamiento verificable.

Total, de controles CNBS aplicables: Total de controles identificados como obligatorios para el canal ATM según las normas vigentes de la CNBS en materia de tecnología, seguridad y continuidad de negocio.

4. Fuente de datos y recolección

Fuente de información: Matrices de cumplimiento normativo de Riesgos y Cumplimiento, informes de auditoría interna y externa, reportes de la unidad de Seguridad de la Información y documentación de políticas, procedimientos y controles asociados al canal ATM.

Responsable de la medición: Unidad de Cumplimiento, en coordinación con Riesgos Operativos, Seguridad de la Información y el área de Medios de Pago.

Frecuencia de medición: Trimestral, con actualizaciones adicionales cuando se emitan nuevas disposiciones de la CNBS o se modifiquen las existentes.

5. Umbrales de desempeño

Los rangos de referencia se definen considerando que la meta estratégica es alcanzar el 100 por ciento de cumplimiento.

Tabla 32: *Umbrales de desempeño del Índice de Cumplimiento Normativo (CNBS)*

Estado	Rango de cumplimiento	Interpretación y acción sugerida
Óptimo	100 %	Todos los controles CNBS aplicables se encuentran implementados y en cumplimiento. Se mantiene el esquema actual y se da seguimiento a cambios normativos.
Alerta	90 % a 99,99 %	Existen controles pendientes o parcialmente implementados. Requiere plan de acción priorizado y seguimiento cercano por parte de Cumplimiento y Riesgos.
Crítico	Menor a 90 %	Nivel de cumplimiento insuficiente frente al ente regulador. Debe elaborarse un plan de remediación urgente, escalar el riesgo a la alta dirección y revisar la gobernanza de TI y de riesgos.

Fuente: Elaboración Propia

6. Relación con la gestión de riesgos

Riesgo principal mitigado: Incumplimiento de disposiciones regulatorias de la CNBS

relacionadas con tecnología y seguridad del canal ATM, que pueda derivar en sanciones, requerimientos correctivos, restricciones operativas o pérdida de confianza por parte de clientes y regulador.

Impacto asociado: Un índice de cumplimiento normativo bajo incrementa el riesgo legal, regulatorio y reputacional del banco. La mejora continua de este indicador contribuye a mantener el riesgo dentro del apetito definido por la organización, alinear la gestión de TI con las exigencias de la CNBS y demostrar, ante auditorías y supervisiones, la efectividad de los controles implementados sobre el software de cajeros automáticos.

4.3.5 PROTOCOLO DE ACTUACIÓN Y CICLO DE MEJORA CONTINUA

Para complementar el desarrollo de los indicadores y del dashboard propuesto, se establece un Plan de Respuesta orientado a actuar cuando el Índice de Disponibilidad Operativa del Software de Cajeros Automáticos desciende por debajo de los niveles de servicio acordados. Este plan tiene como propósito restablecer oportunamente los SLA comprometidos con las áreas de negocio y con los clientes, activando de forma coordinada los mecanismos de la cadena de valor del servicio descritos por ITIL 4, en armonía con los principios de gobierno y gestión del riesgo de COBIT 2019.

A través de fases claramente definidas que abarcan la detección, contención, análisis de causa raíz y solución definitiva, el plan convierte los desvíos del KPI en oportunidades de aprendizaje organizacional, fortaleciendo tanto la estabilidad operativa del software de los cajeros automáticos como la madurez del gobierno de TI en Banco Ficohsa.

4.4 BENEFICIOS ESTRATÉGICOS DE IMPLEMENTAR EL ANÁLISIS DE RIESGOS CON COBIT 2019 E ITIL 4 EN EL SOFTWARE DE CAJEROS AUTOMÁTICOS

En este apartado se identificarán y analizarán los beneficios estratégicos que Banco Ficohsa podrá obtener al implementar la propuesta de análisis de riesgos sustentada en COBIT 2019 e ITIL 4 para la gestión del software de cajeros automáticos. Se valorarán impactos esperados en la continuidad del servicio, la reducción de incidentes lógicos, el cumplimiento regulatorio, la eficiencia operativa y la experiencia del cliente, articulando estos resultados con los objetivos de negocio y de TI de la institución. Asimismo, se destacará cómo la adopción de estos marcos fortalecerá la cultura de gestión de riesgos y el ciclo de mejora continua en los canales electrónicos.

4.4.1 INSTRUMENTOS APLICADOS

Para identificar los beneficios estratégicos esperados de la implementación del análisis de riesgos basado en COBIT 2019 e ITIL 4, se aplicó un único instrumento de recolección de datos: una encuesta estructurada dirigida al personal involucrado en la gestión, operación y soporte del software de cajeros automáticos en Banco Ficohsa.

Este instrumento permitió obtener información cuantitativa sobre el nivel de conocimiento de los colaboradores respecto a los marcos de referencia, su percepción sobre la efectividad de los procesos actuales, la identificación de riesgos operativos y tecnológicos, así como su criterio sobre el valor que aportaría la adopción de COBIT 2019 e ITIL 4 en la optimización del software ATM.

La encuesta también facilitó evaluar el nivel de madurez organizacional en áreas clave como gestión de incidentes, monitoreo, gestión de cambios, disponibilidad y seguridad lógica, permitiendo proyectar de manera fundamentada los beneficios estratégicos que se derivarían de la implementación de un enfoque integrado de análisis de riesgos.

En conjunto, este instrumento proporcionó una base empírica sólida para comprender las expectativas del personal y sustentar la identificación de los beneficios esperados para la institución.

4.4.2 PARTICIPANTES Y SUS CARACTERÍSTICAS

El instrumento de encuesta fue aplicado a un grupo de colaboradores directamente vinculados con la operación, mantenimiento y soporte del software de cajeros automáticos en Banco Ficohsa. La muestra estuvo conformada principalmente por personal técnico y operativo con amplia experiencia en la gestión de la red ATM, lo que permitió obtener percepciones fundamentadas y alineadas a las condiciones reales del entorno tecnológico del banco.

En términos de edad, la mayoría de los participantes se concentró en los rangos de 30 a 39 años y 40 a 49 años, reflejando un grupo de colaboradores con trayectoria consolidada en el sector. Respecto al género, la muestra estuvo compuesta exclusivamente por personal masculino, lo cual concuerda con la composición actual de los equipos encargados de la operación de cajeros automáticos en la institución.

En cuanto al área de trabajo, los participantes se distribuyeron principalmente entre Operaciones de Cajeros Automáticos y Tecnología de la Información (TI), dos unidades críticas

para el funcionamiento y supervisión del software ATM. Los roles desempeñados abarcaron posiciones como técnicos, personal de soporte, analistas, especialistas y un gerente o líder del área, permitiendo obtener una visión integral del proceso operativo y de gestión.

Finalmente, la variable años de experiencia evidenció un alto nivel de madurez profesional en la muestra, ya que la mayoría de los encuestados reportó entre 7 y más de 10 años de experiencia en su puesto actual. Esto contribuye a que los resultados del estudio estén respaldados por la opinión de colaboradores con conocimiento profundo de los riesgos, incidentes y desafíos asociados al software de cajeros automáticos.

4.4.3 DESCRIPCIÓN DE LOS RESULTADOS

La presente sección expone los resultados obtenidos a partir de la aplicación del instrumento de encuesta dirigido a los colaboradores involucrados en la gestión, soporte y operación del software de cajeros automáticos. Los hallazgos permiten identificar las percepciones, experiencias y valoraciones del personal respecto a las amenazas, vulnerabilidades y debilidades actuales del sistema, así como su posible alineación con los marcos de COBIT 2019 e ITIL 4.

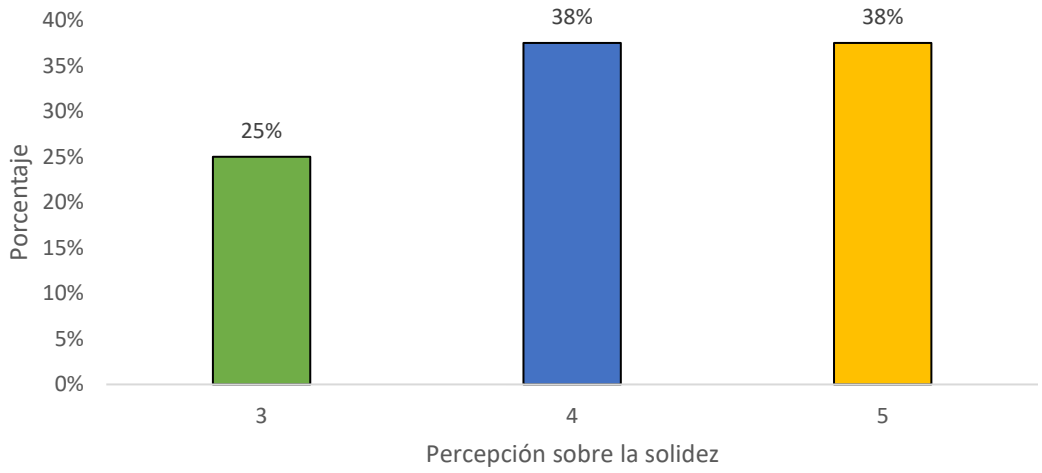
El análisis de estos datos constituye la base para comprender el nivel de madurez operativa, el grado de implementación de controles y la efectividad de los procesos utilizados en la administración del software ATM. Asimismo, estos resultados permiten proyectar los beneficios estratégicos que el banco podría obtener al implementar un modelo integral de análisis de riesgos y gestión de incidentes fundamentado en buenas prácticas internacionales.

A continuación, presentamos los resultados obtenidos:

6. Según su experiencia, COBIT 2019 aporta un marco sólido para la gobernanza de TI y gestión de riesgos en entornos bancarios.

Figura 45: *Percepción sobre la solidez de COBIT 2019 como marco de gobernanza y gestión de*

riesgos en banca



Fuente: Elaboración propia

Descripción

La figura anterior muestra la percepción del personal encuestado acerca de la solidez de COBIT 2019 como marco de referencia para la gobernanza de TI y la gestión de riesgos en entornos bancarios. Los resultados se distribuyen en tres niveles: 3 (25 %), 4 (38 %) y 5 (38 %), evidenciando una valoración mayoritariamente positiva respecto al aporte de COBIT 2019.

Análisis

Los datos revelan que el 76 % de los participantes (niveles 4 y 5) considera que COBIT 2019 constituye un marco robusto y útil para estructurar los procesos de control, auditoría y gobernanza del software de cajeros automáticos. Esta percepción coincide con las buenas prácticas del sector financiero, donde COBIT es ampliamente utilizado para garantizar cumplimiento regulatorio, trazabilidad y gestión efectiva del riesgo TI. El 25 % restante, ubicado en el nivel 3, sugiere la necesidad de reforzar la capacitación del personal para comprender plenamente la aplicabilidad del marco.

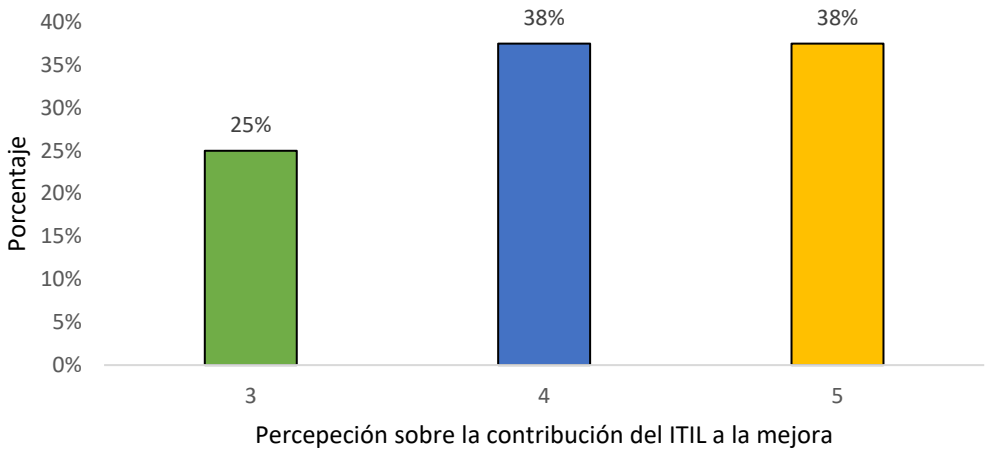
Hallazgo

La evidencia indica que existe una aceptación significativa de COBIT 2019 dentro del equipo operativo y técnico de Banco Ficohsa, lo cual constituye un facilitador clave para su implementación. Esta percepción favorable reduce la resistencia al cambio, aumenta la disposición

a adoptar controles más rigurosos y valida la pertinencia del modelo propuesto en la investigación para fortalecer la gobernanza del software ATM.

7. ITIL 4 mejora la gestión de servicios de TI, incluyendo servicios críticos como el software de cajeros automáticos.

Figura 46: *Percepción sobre la contribución de ITIL 4 a la mejora de los servicios de TI en el software de cajeros automáticos*



Fuente: Elaboración propia

Descripción

La gráfica presenta la valoración del personal encuestado sobre el impacto de ITIL 4 en la mejora de los servicios de TI, específicamente en componentes críticos como el software de cajeros automáticos. Los resultados se distribuyen en tres niveles: 3 (25 %), 4 (38 %) y 5 (38 %), reflejando una tendencia mayoritaria hacia una percepción positiva del marco ITIL 4.

Análisis

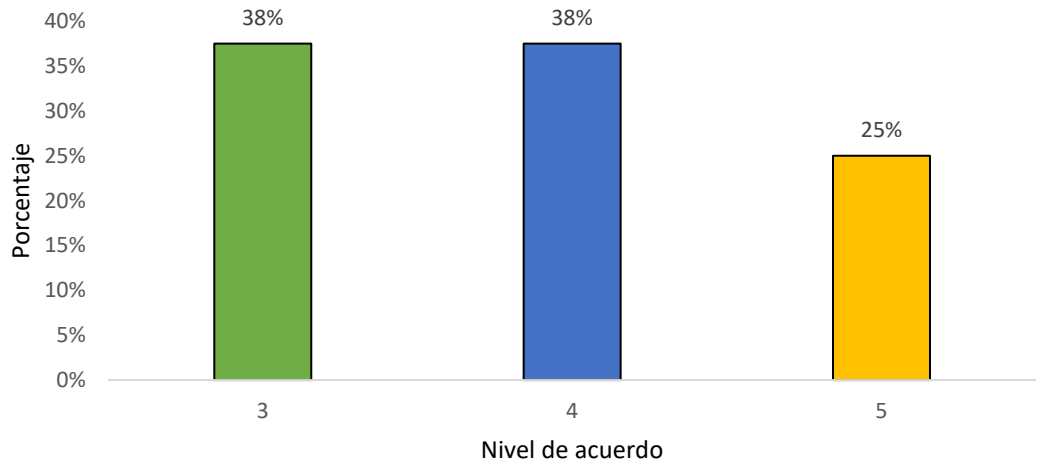
Los datos muestran que el 76 % de los participantes considera que ITIL 4 contribuye significativamente a mejorar la gestión del software ATM, especialmente en prácticas como gestión de incidentes, gestión de disponibilidad, gestión de cambios y liberaciones. Esto indica que el personal reconoce el valor práctico del marco, particularmente en procesos operativos que requieren respuesta rápida, coordinación entre áreas y estandarización de procedimientos. El 25 % que asignó una calificación intermedia sugiere que, aunque ITIL 4 es percibido como útil, aún puede fortalecerse su adopción mediante procesos más estructurados o capacitación adicional.

Hallazgo

El principal hallazgo es que ITIL 4 es visto como un marco altamente beneficioso para la operación y mantenimiento del software de cajeros automáticos. Esta percepción favorable valida la pertinencia de su integración en la propuesta de análisis de riesgos de la investigación. Además, confirma que la adopción de ITIL 4 puede mejorar la eficiencia operativa, reducir tiempos de indisponibilidad y estandarizar la respuesta ante incidentes, factores clave para la continuidad del servicio ATM.

8. La combinación de COBIT 2019 e ITIL 4 ofrece una visión integral de riesgos y operación de software de cajeros.

Figura 47: *Percepción sobre la integración de COBIT 2019 e ITIL 4 para una visión integral de riesgos y operación del software ATM*



Fuente: Elaboración propia

Descripción

La gráfica muestra la percepción del personal encuestado sobre si la combinación de COBIT 2019 e ITIL 4 brinda una visión integral y complementaria para gestionar riesgos y la operación del software de cajeros automáticos. Los resultados se distribuyen de la siguiente forma: nivel 3 (38 %), nivel 4 (38 %) y nivel 5 (25 %), evidenciando una valoración principalmente favorable respecto a la sinergia entre ambos marcos.

Análisis

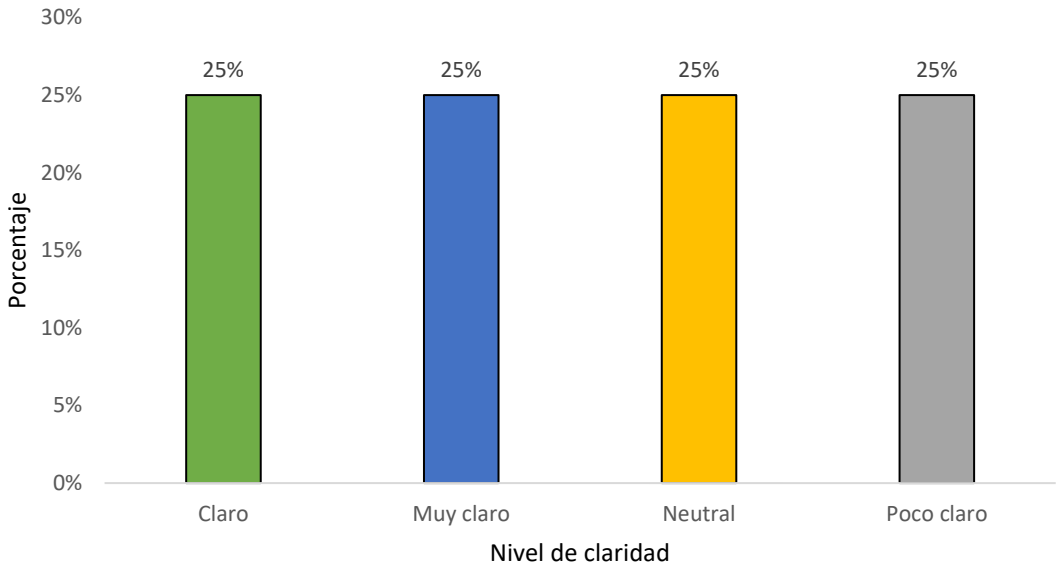
El 76 % de los participantes (niveles 4 y 3) considera que la integración de COBIT 2019 e ITIL 4 permite fortalecer la gobernanza, estandarizar procesos, mejorar la respuesta ante incidentes y reducir riesgos en el ciclo de vida del software ATM. Esta percepción señala que el personal reconoce cómo ambos marcos se complementan: mientras COBIT aporta estructura, control y gestión de riesgos, ITIL enfoca la operación diaria, la calidad del servicio y la mejora continua. La calificación del 25 % en el nivel 5 indica que un segmento del personal percibe una compatibilidad altamente beneficiosa entre ambos marcos.

Hallazgo

El hallazgo clave es que existe una percepción sólida a favor de combinar COBIT 2019 e ITIL 4 como enfoque integral para gestionar riesgos y la operación del software de cajeros automáticos. Esta aceptación respalda la viabilidad del modelo propuesto en la investigación, demostrando que la integración de ambos marcos no solo es pertinente, sino también reconocida internamente como una estrategia capaz de mejorar la eficiencia, trazabilidad y estabilidad del servicio ATM.

9. ¿Qué tan claro considera el alineamiento entre la propuesta y los objetivos estratégicos del banco (p. ej., disponibilidad, continuidad, seguridad)?

Figura 48: *Nivel de claridad del alineamiento entre la propuesta y los objetivos estratégicos del banco*



Fuente: Elaboración propia

Descripción

La gráfica presenta la percepción del personal encuestado respecto al nivel de claridad del alineamiento entre la propuesta de análisis de riesgos y los objetivos estratégicos del banco, tales como disponibilidad, continuidad operativa y seguridad. Las respuestas se distribuyen equitativamente entre las cuatro categorías evaluadas: Claro (25%), Muy claro (25%), Neutral (25%) y Poco claro (25%).

Análisis

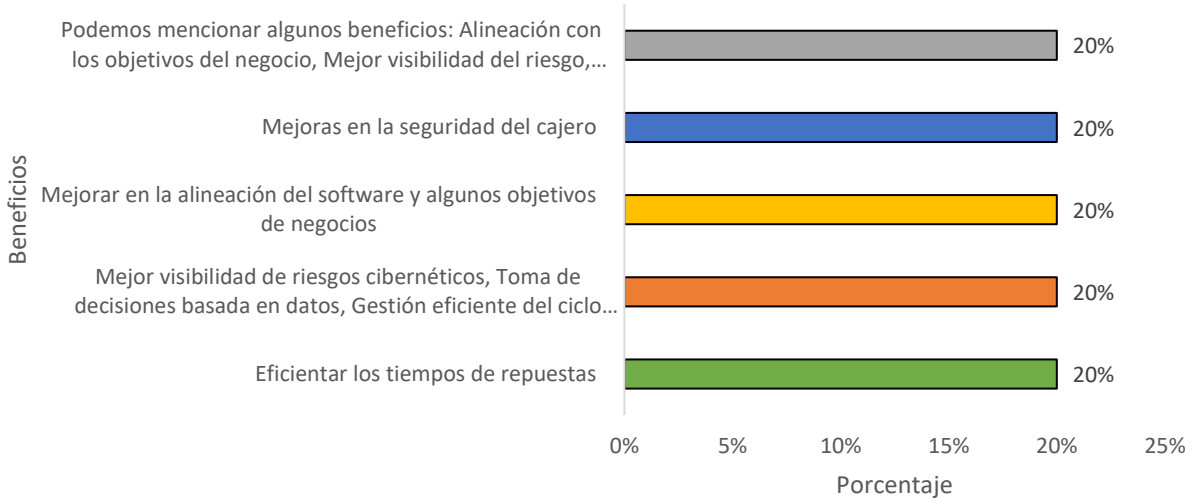
Los resultados muestran una dispersión uniforme, lo que indica que no existe una percepción dominante acerca del grado de alineamiento estratégico de la propuesta. Mientras un 50% del personal considera que el alineamiento es claro o muy claro, otro 25% se mantiene neutral y un 25% lo percibe como poco claro. Esta distribución puede reflejar variaciones en el nivel de conocimiento del personal respecto a los objetivos estratégicos institucionales o a los marcos de referencia utilizados (COBIT 2019 e ITIL 4). Asimismo, evidencia que algunos equipos pueden requerir mayor sensibilización o comunicación sobre cómo la propuesta contribuye directamente a la disponibilidad, continuidad del servicio y seguridad lógica del software ATM.

Hallazgo

El hallazgo central es que, aunque la mitad de los participantes reconoce claramente el alineamiento estratégico de la propuesta, existe un 50% que aún no lo percibe con la misma claridad o mantiene una postura neutral. Esto sugiere la necesidad de fortalecer los procesos de divulgación interna, capacitación y alineación conceptual para asegurar que todo el personal entienda cómo la propuesta contribuye a los objetivos institucionales de continuidad, disponibilidad y seguridad, reforzando su aceptación y viabilidad operativa.

10. ¿Cuáles serían los beneficios estratégicos más relevantes de implementar esta propuesta? (pregunta abierta)

Figura 49: *Beneficios estratégicos esperados al implementar la propuesta*



Fuente: Elaboración propia

Descripción

La gráfica presenta la distribución de las respuestas obtenidas en la pregunta abierta sobre cuáles serían los beneficios estratégicos más relevantes derivados de la implementación de la propuesta basada en COBIT 2019 e ITIL 4. Cada categoría reporta un 20% de frecuencia, reflejando una diversificación homogénea de opiniones. Entre los beneficios mencionados se destacan: alineación con los objetivos del negocio, mejora en la seguridad del cajero, mayor visibilidad del riesgo, eficiencia en los tiempos de respuesta, cumplimiento normativo y madurez operativa del ciclo de vida del software.

Análisis

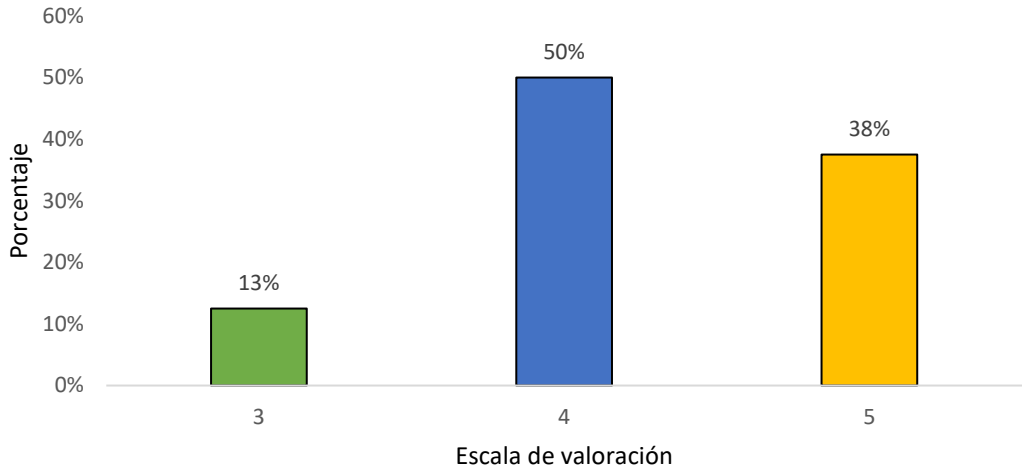
Los resultados revelan que los participantes identifican una variedad de beneficios estratégicos, todos considerados igualmente relevantes. La recurrencia de temas como seguridad, visibilidad del riesgo, eficiencia operativa y alineamiento con objetivos del negocio sugiere que el personal reconoce la propuesta como una oportunidad para fortalecer tanto la gobernanza de TI como la operación del software de cajeros automáticos. La igualdad en porcentajes indica que la propuesta no es vista como una solución aislada, sino como un mecanismo integral capaz de generar mejoras en múltiples áreas críticas del banco, desde la continuidad operativa hasta la toma de decisiones basada en datos.

Hallazgo

El principal hallazgo es que la totalidad de los encuestados coincide en que la propuesta generaría beneficios estratégicos significativos, distribuidos en cinco áreas clave: seguridad, eficiencia, alineación institucional, gobernanza del software y gestión de riesgos. Esta convergencia de percepciones valida la pertinencia del marco propuesto y demuestra que su implementación podría generar valor transversal para el banco, fortaleciendo la confiabilidad del servicio ATM y consolidando prácticas de gobernanza alineadas con estándares internacionales.

11. Mayor disponibilidad de cajeros automáticos (uptime) y reducción de fallas críticas.

Figura 50: *Percepción sobre la mejora en disponibilidad del software ATM y reducción de fallas críticas*



Fuente: Elaboración propia

Descripción

La gráfica muestra las respuestas de los participantes respecto al beneficio estratégico relacionado con el incremento del uptime de los cajeros automáticos y la disminución de fallas críticas del software. Los resultados evidencian que el 50% de los encuestados seleccionó el valor 4 (de acuerdo), seguido por un 38% que seleccionó el valor 5 (totalmente de acuerdo). Únicamente un 13% eligió el valor 3, lo que indica opiniones moderadamente positivas. No se registraron calificaciones bajas.

Análisis

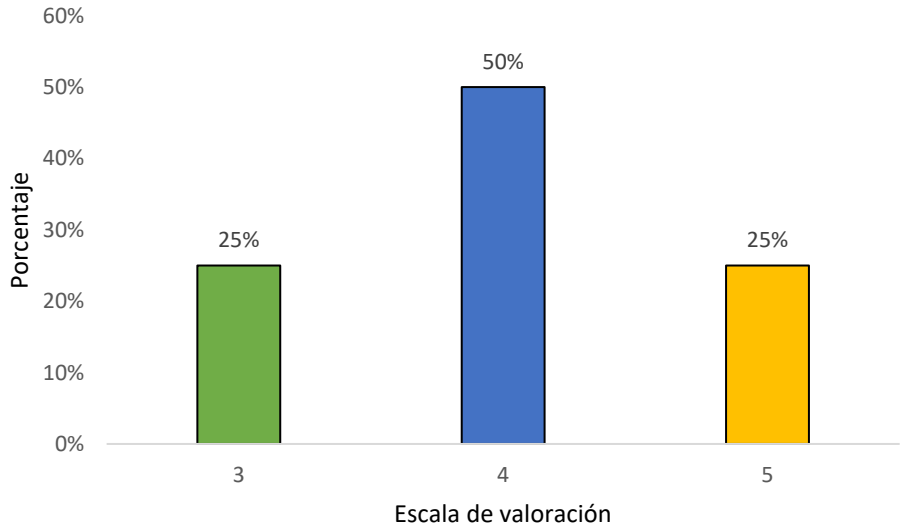
Los datos reflejan una percepción ampliamente favorable hacia la capacidad de la propuesta basada en COBIT 2019 e ITIL 4 para mejorar la disponibilidad operativa del software ATM. Este resultado es coherente con la crítica importancia que el uptime tiene para los servicios financieros, especialmente en una red de cajeros que opera 24/7. La concentración del 88% de respuestas entre los niveles 4 y 5 sugiere que el personal técnico y operativo reconoce que la implementación de controles, métricas y procesos estandarizados contribuiría a minimizar fallas críticas, optimizar el rendimiento del software y garantizar continuidad del servicio para los usuarios finales.

Hallazgo

El hallazgo principal indica un consenso sólido en torno a que la propuesta generará una mejora tangible en la disponibilidad del servicio ATM. La alta valoración obtenida evidencia que el personal identifica este beneficio como una expectativa realista y directamente alcanzable mediante la adopción de prácticas formales de gestión de riesgos, incidentes y disponibilidad. Esto confirma que el aumento del uptime es percibido como uno de los beneficios más inmediatos y de mayor impacto para el banco.

12. Mejora en la detección y gestión proactiva de riesgos de software de cajeros (ransomware, malware, fallos de software, etc.).

Figura 51: *Evaluación del beneficio: mejora en la eficiencia de tiempos de respuesta del software ATM*



Fuente: Elaboración propia

Descripción

La gráfica presenta la percepción de los participantes respecto a si la propuesta basada en COBIT 2019 e ITIL 4 contribuirá a mejorar los tiempos de respuesta del software de cajeros automáticos. Los resultados muestran que un 50% de los encuestados calificó con "4", mientras que un 25% seleccionó "3" y otro 25% marcó "5". Esto evidencia una distribución positiva, sin respuestas negativas o de desacuerdo.

Análisis

Los datos reflejan que la mitad de los participantes considera "muy probable" que la propuesta reduzca los tiempos de respuesta del software ATM, mientras que un 25% adicional estima que el beneficio es "totalmente alcanzable". Esta expectativa coincide con los principios de ITIL 4 relacionados con la mejora del flujo de valor y la gestión eficiente de incidentes, así como con los objetivos de COBIT 2019 orientados a optimizar el desempeño del servicio y mitigar riesgos operativos. El 25% restante que seleccionó la opción intermedia indica una percepción moderada, pero no negativa, lo cual reafirma la solidez del beneficio esperado.

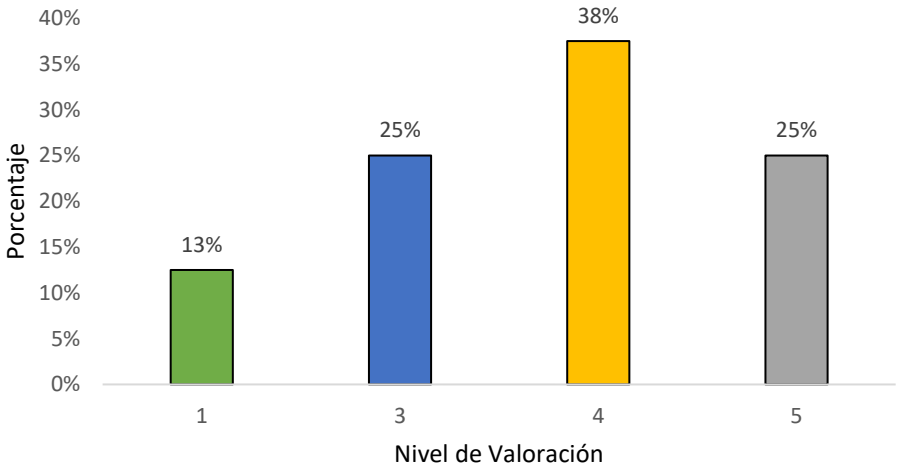
Hallazgo

El hallazgo clave evidencia que existe una alta confianza en que la propuesta permitirá mejorar significativamente los tiempos de respuesta del software ATM. Con un 75% de preferencias entre los niveles 4 y 5, queda claro que los usuarios técnicos anticipan un impacto directo en la eficiencia operativa, lo cual fortalece la viabilidad del enfoque planteado y confirma que la optimización del rendimiento es un beneficio estratégico relevante para Banco Ficohsa.

13. Optimización del ciclo de vida del software de cajeros (despliegues, parches, actualizaciones) con menores tiempos de inactividad.

Figura 52: *Evaluación del beneficio: optimización del ciclo de vida del software ATM y reducción*

de inactividad



Fuente: Elaboración propia

Descripción

La gráfica muestra la percepción de los participantes sobre el impacto que tendría la propuesta basada en COBIT 2019 e ITIL 4 en la optimización del ciclo de vida del software de cajeros automáticos (despliegues, parches y actualizaciones), así como en la reducción de tiempos de inactividad. Los resultados indican que el 38% de los encuestados seleccionó la opción “4”, un 25% eligió “3”, otro 25% marcó “5”, y un 13% escogió la opción “1”.

Análisis

Los datos reflejan una tendencia predominantemente favorable hacia la idea de que la propuesta mejoraría la gestión del ciclo de vida del software ATM. La mayor concentración en el valor “4” (38%) y la presencia significativa de respuestas en “5” (25%) refuerzan la percepción de que los procesos de actualización y despliegue serían más eficientes si se aplica el enfoque combinado COBIT–ITIL. Aunque existe un 13% que considera que el beneficio sería limitado (opción “1”), este grupo minoritario no altera la tendencia general positiva. La presencia del 25% en el nivel “3” sugiere que algunos participantes reconocen el potencial, pero estiman que su efectividad dependerá del grado real de implementación y automatización.

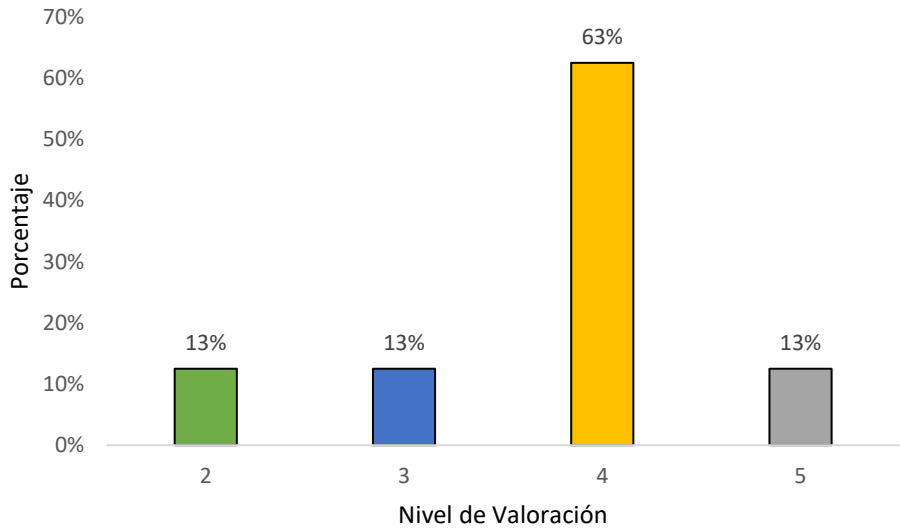
Hallazgo

El hallazgo central indica que más de dos tercios de los participantes (63%) perciben que

la propuesta permitirá optimizar de manera significativa el ciclo de vida del software ATM y disminuir los tiempos de inactividad asociados a despliegues y parches. Esto confirma que, desde la perspectiva operativa, existe una expectativa clara de mejora en la estabilidad del servicio, sustentada en prácticas clave de ITIL 4 como Gestión de Cambios, Gestión de Implementaciones y Gestión de Disponibilidad, junto con los mecanismos de control y supervisión que propone COBIT 2019.

14. Reducción de costos operativos a través de procesos estandarizados y automatización de controles.

Figura 53: *Percepción sobre la reducción de costos operativos mediante procesos estandarizados y automatización de controles*



Fuente: Elaboración propia

Descripción

La gráfica presenta la valoración de los participantes respecto al beneficio potencial de reducir costos operativos a través de la estandarización de procesos y la automatización de controles en la gestión del software de cajeros automáticos. Los resultados muestran que el 63% de los encuestados seleccionó la opción “4”, mientras que las opciones “2”, “3” y “5” registran cada una un 13%.

Análisis

Los datos evidencian una clara tendencia favorable hacia la idea de que la adopción de prácticas alineadas con COBIT 2019 e ITIL 4 contribuiría significativamente a reducir costos operativos. El valor más alto (63% en la opción "4") indica que la mayoría percibe una mejora sustancial, aunque no absoluta, lo cual refleja una visión pragmática por parte del personal: se reconoce el potencial de eficiencia, pero también se entiende que este dependerá del nivel de automatización, la madurez de los procesos actuales y la correcta implementación del marco propuesto.

Los porcentajes en los valores "2" y "3" (13% cada uno) muestran que un grupo minoritario mantiene expectativas moderadas, posiblemente debido a limitaciones previas en la adopción de prácticas de gobernanza. Entretanto, el 13% que seleccionó "5" aunque bajo confirma que existe un sector que considera que el impacto positivo podría ser incluso mayor.

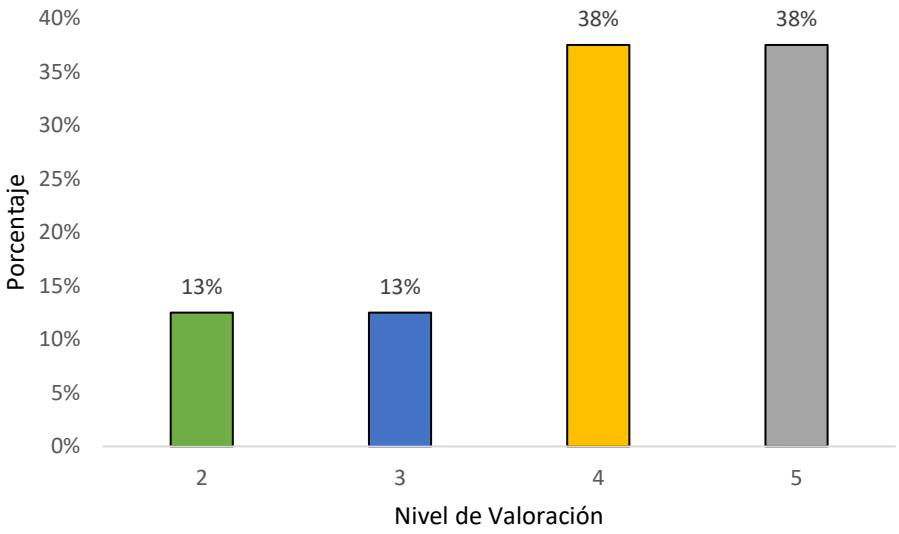
Hallazgo

El hallazgo principal indica que casi dos tercios de los participantes (63%) consideran que la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4 permitiría una reducción significativa de costos operativos mediante procesos más estandarizados, mayor trazabilidad y automatización de controles. Esto respalda la premisa de que la optimización del ciclo de vida del software ATM no solo mejora la disponibilidad y seguridad del servicio, sino que también genera eficiencias económicas relevantes para el banco, alineadas con los objetivos estratégicos de continuidad, calidad y sostenibilidad operativa.

15. Mayor visibilidad y trazabilidad de riesgos y decisiones a nivel gerencial.

Figura 54: *Percepción sobre la visibilidad y trazabilidad de riesgos para la toma de decisiones*

gerenciales



Fuente: Elaboración propia

Descripción

La gráfica muestra la valoración de los participantes respecto al beneficio de obtener una mayor visibilidad y trazabilidad de los riesgos del software de cajeros automáticos, con impacto directo en la toma de decisiones a nivel gerencial. Los resultados evidencian que el 38% seleccionó la opción “4” y otro 38% la opción “5”, mientras que las categorías “2” y “3” obtuvieron cada una un 13%.

Análisis

Los datos reflejan un consenso mayoritario acerca de la relevancia estratégica de contar con información más clara, accesible y estructurada sobre la operación y riesgos del software ATM. La suma de las opciones “4” y “5” (76%) indica que los encuestados reconocen que marcos como COBIT 2019 e ITIL 4 no solo fortalecen la operación técnica, sino que también proporcionan una capa robusta de gobernanza y trazabilidad que es indispensable para las decisiones ejecutivas.

El 13% que eligió “2” y otro 13% que seleccionó “3” sugieren la existencia de percepciones moderadas, posiblemente asociadas a experiencias previas con sistemas de monitoreo fragmentados o procesos de reporte manual, que históricamente limitan la visibilidad para la gerencia. Sin embargo, la tendencia general señala una valoración altamente positiva del beneficio

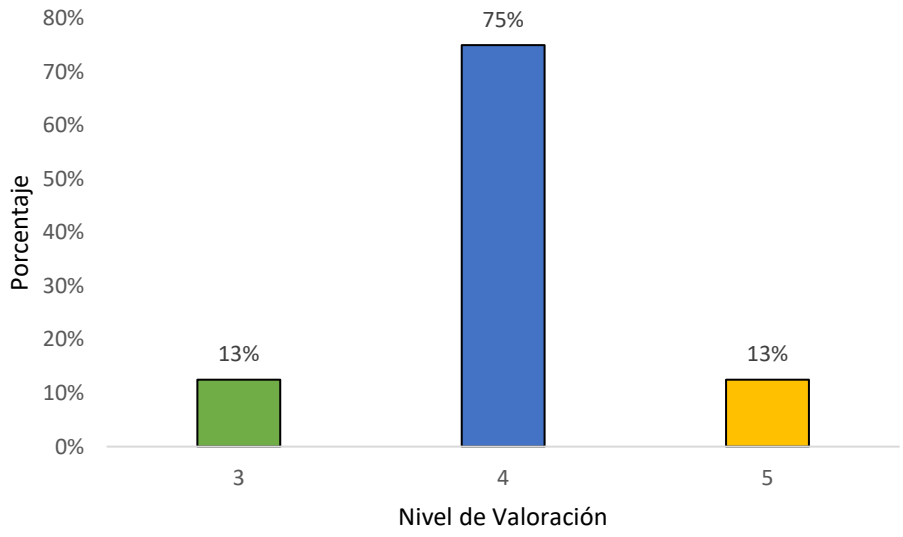
esperado.

Hallazgo

El hallazgo principal revela que tres cuartas partes de los encuestados (76%) consideran que la implementación del análisis de riesgos basado en COBIT 2019 e ITIL 4 proporcionará una mejora significativa en la visibilidad y trazabilidad de riesgos para la gerencia. Esta percepción valida la importancia de contar con indicadores, dashboards integrados y flujos de información estandarizados, elementos que permiten decisiones más oportunas, basadas en evidencia y alineadas con los objetivos estratégicos del banco.

16. Mejora en la satisfacción de clientes internos (operadores, analistas) por procesos más consistentes.

Figura 55: *Percepción sobre la mejora en la satisfacción de clientes internos mediante procesos más consistentes*



Fuente: Elaboración propia

Descripción

La gráfica presenta la evaluación de los participantes sobre el beneficio relacionado con el aumento de la satisfacción de los clientes internos operadores y analistas como resultado de procesos más consistentes en la gestión del software de cajeros automáticos. Los resultados muestran que el 75% seleccionó la opción “4”, mientras que un 13% eligió “3” y otro 13%

seleccionó “5”.

Análisis

Los datos reflejan una fuerte convergencia hacia la opción “4”, lo cual indica que la mayoría percibe mejoras importantes en la satisfacción interna derivadas de la estandarización, automatización y control del ciclo de vida del software ATM. Este comportamiento sugiere que los procesos actuales presentan variabilidad operativa que afecta el trabajo diario de técnicos y analistas, por lo que la adopción de marcos como ITIL 4 y COBIT 2019 se considera una vía viable para reducir inconsistencias y fortalecer la experiencia del personal interno.

El 13% que seleccionó valores “3” y “5” representa percepciones ligeramente divergentes: por un lado, un grupo identifica beneficios moderados, posiblemente por experiencias previas con sistemas heterogéneos; y por otro, un grupo más reducido ve beneficios aún mayores. Aunque minoritarios, estos extremos aportan una lectura equilibrada sobre distintas expectativas respecto a los impactos operativos.

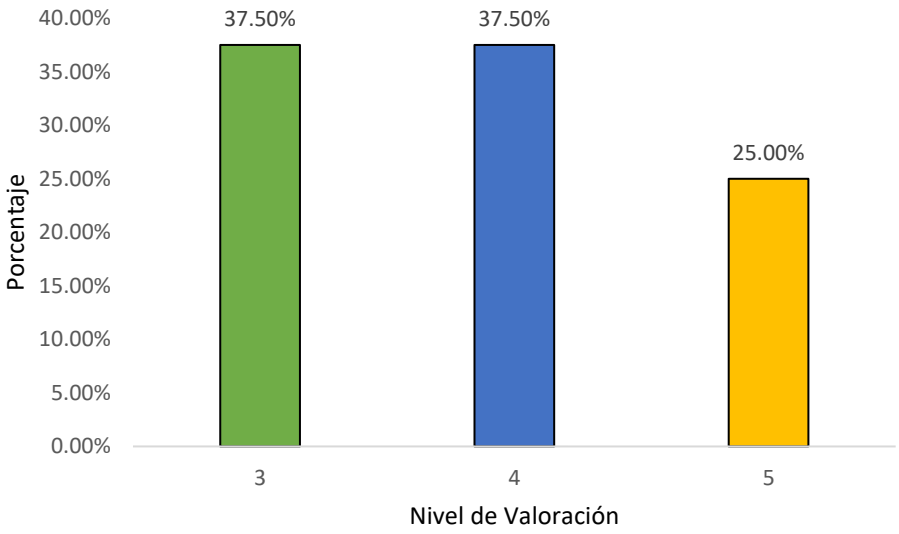
Hallazgo

El hallazgo principal indica que el 75% de los encuestados reconoce claramente que la implementación de procesos más consistentes, basados en COBIT 2019 e ITIL 4, mejorará la satisfacción de los usuarios internos. Esto valida la importancia estratégica de la estandarización y la mejora continua, ya que procesos más predecibles y eficientes reducen retrabajos, agilizan la resolución de incidentes y generan una percepción positiva del área de TI entre los equipos que dependen del correcto funcionamiento del software ATM.

17. Cumplimiento normativo y más robusto, (Ej.: regulaciones bancarias)

Figura 56: *Percepción sobre el fortalecimiento del cumplimiento normativo mediante la*

propuesta basada en COBIT 2019 e ITIL 4



Fuente: Elaboración propia

Descripción

La gráfica muestra la valoración de los encuestados respecto al beneficio vinculado con la mejora del cumplimiento normativo, particularmente en relación con las regulaciones bancarias aplicables al software de cajeros automáticos. Los resultados se distribuyen entre las opciones 3 (37.5%), 4 (37.5%) y 5 (25%), sin respuestas en niveles inferiores.

Análisis

Los datos evidencian una percepción predominantemente positiva en torno al aporte de la propuesta para fortalecer la adherencia normativa. Tanto la opción “3” como “4” comparten el mayor porcentaje (37.5%), lo que refleja una visión moderada a alta sobre la capacidad de COBIT 2019 e ITIL 4 para robustecer los mecanismos de control regulatorio, estandarizar procesos y asegurar trazabilidad documental en la gestión del software ATM.

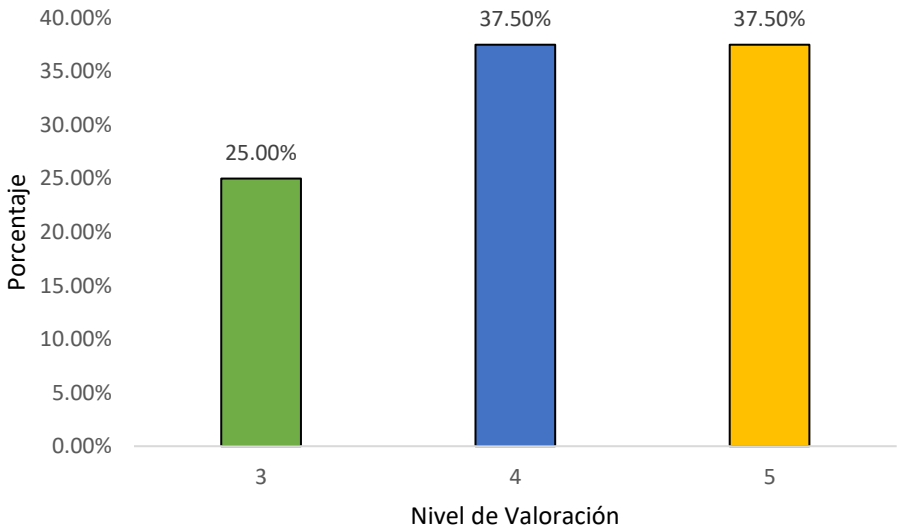
El 25% que seleccionó la opción “5” indica que una parte menor de los participantes considera que el impacto podría ser aún más significativo, especialmente en aspectos como continuidad del negocio, seguridad lógica, auditorías y cumplimiento de lineamientos de la CNBS. La ausencia de valores bajos confirma que ningún encuestado percibe que la propuesta genere poco o nulo fortalecimiento regulatorio, lo cual refuerza su validez en términos de gobierno de TI.

Hallazgo

El principal hallazgo señala que el 100% de los encuestados reconoce que la propuesta contribuye al fortalecimiento del cumplimiento normativo, situando las respuestas entre niveles de percepción media-alta y alta. Esto demuestra que la adopción de prácticas integradas de COBIT 2019 e ITIL 4 no solo mejora la operación técnica del software ATM, sino que también optimiza los controles regulatorios y facilita la alineación con marcos exigidos por el entorno bancario hondureño.

18. Mayor claridad sobre roles y responsabilidades en la gestión de software de cajeros.

Figura 57: *Percepción sobre la claridad de roles y responsabilidades en la gestión del software de cajeros automáticos*



Fuente: Elaboración propia

Descripción

La gráfica presenta la distribución de respuestas relacionadas con el beneficio esperado de una mayor claridad en los roles y responsabilidades dentro de la gestión del software de cajeros automáticos. Los porcentajes se concentran en tres niveles de valoración: 25% en la opción 3, 37.5% en la opción 4, y 37.5% en la opción 5, sin registros en niveles inferiores.

Análisis

Los resultados reflejan una percepción mayoritariamente positiva respecto al impacto de

la propuesta basada en COBIT 2019 e ITIL 4 para mejorar la definición y asignación de roles. La concentración de respuestas en los niveles 4 y 5 (75% en conjunto) indica que los participantes reconocen que ambos marcos fortalecerían los procesos de gobernanza mediante la estandarización de responsabilidades, la formalización de flujos de trabajo y la reducción de ambigüedades en la operación del software ATM.

El 25% ubicado en el nivel 3 sugiere que algunos colaboradores perciben el beneficio como moderado, posiblemente debido a la ausencia actual de documentos normativos, matrices RACI o procedimientos oficialmente actualizados. No obstante, la ausencia total de valoraciones bajas evidencia que la propuesta es vista de manera favorable en términos de organización interna y eficiencia operativa.

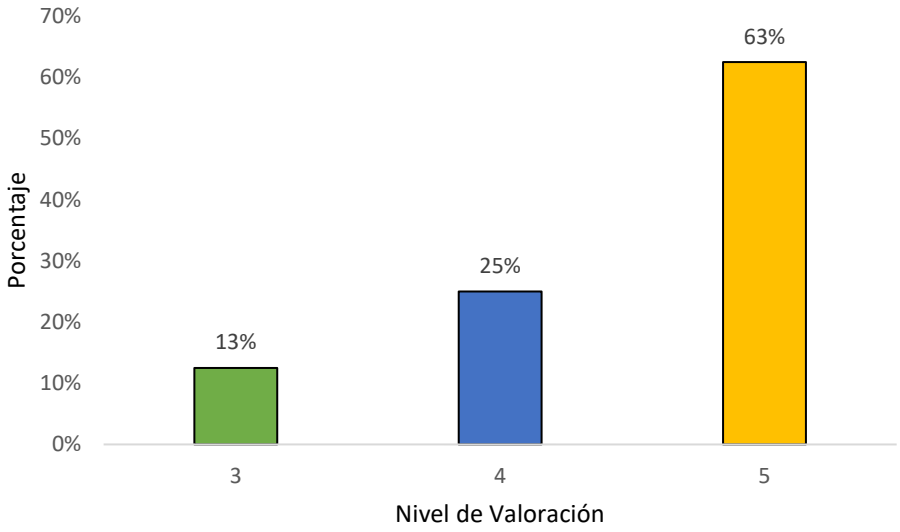
Hallazgo

Se identifica que el 100% de los encuestados considera que la propuesta contribuirá a mejorar la claridad de roles y responsabilidades, situándose entre niveles medios y altos. Esto demuestra que la adopción de COBIT 2019 e ITIL 4 permitiría fortalecer la estructura de gobernanza y asegurar un entendimiento uniforme de las funciones, algo esencial para reducir errores operativos, mejorar la trazabilidad y fortalecer la responsabilidad colectiva en la gestión del software de cajeros automáticos.

19. Mejor control de cambios y gestión de configuración del software de cajeros

Figura 58: *Percepción sobre la mejora del control de cambios y la gestión de configuración del*

software de cajeros automáticos



Fuente: Elaboración propia

Descripción

La gráfica muestra el nivel de acuerdo de los participantes respecto a que la propuesta basada en COBIT 2019 e ITIL 4 contribuiría a mejorar el control de cambios y la gestión de configuración del software de los cajeros automáticos. Los resultados indican que 13% se ubicó en el nivel 3, 25% en el nivel 4 y 63% en el nivel 5, evidenciando una tendencia fuerte hacia evaluaciones altamente favorables.

Análisis

El predominio del nivel 5 (63%) evidencia una percepción robusta de que la integración de los marcos COBIT e ITIL puede resolver las deficiencias actuales en el gobierno del cambio, especialmente considerando que la gestión de cambios fue uno de los puntos críticos identificados en los instrumentos previos (COBIT Performance Management y Lista de Verificación ITIL).

El apoyo del 25% en la categoría 4 refuerza la idea de que los colaboradores perciben beneficios concretos como: mayor trazabilidad, reducción de errores en despliegues, estabilidad de versiones y disminución de riesgos operativos asociados a configuraciones inconsistentes.

El bajo porcentaje en nivel 3 (13%) sugiere que, aunque existe reconocimiento del beneficio, algunos participantes consideran que aún sería necesario fortalecer capacidades internas

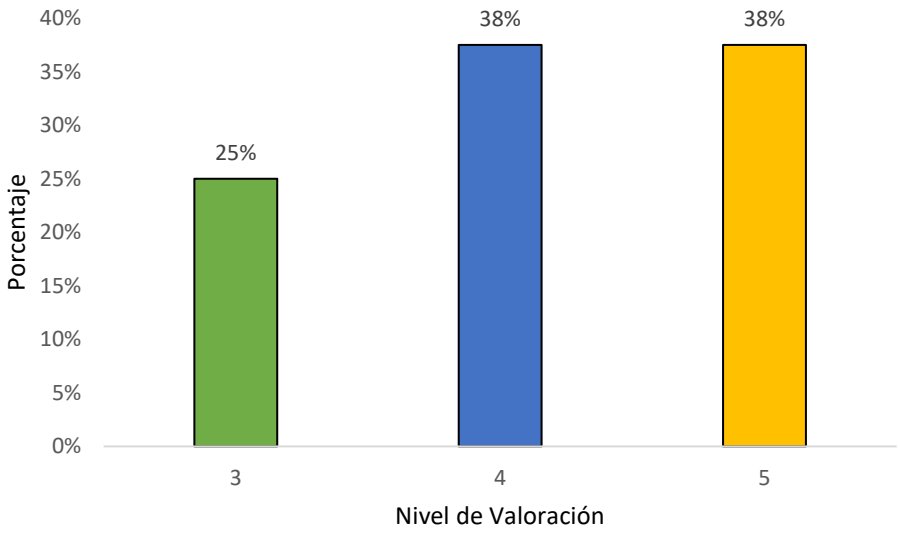
o automatizar herramientas para lograr una implementación integral de estas prácticas.

Hallazgo

El 88% de los encuestados (niveles 4 y 5) considera que la propuesta mejoraría significativamente el control de cambios y la gestión de configuración, consolidando uno de los beneficios estratégicos más sólidos identificados. Esto confirma que la adopción de COBIT 2019 e ITIL 4 atendería directamente una de las principales debilidades actuales del banco, permitiendo establecer procedimientos formales, métricas de seguimiento y una gobernanza más rigurosa sobre el ciclo de vida del software ATM.

20. Mayor capacidad de auditoría y cumplimiento (normativas, políticas internas).

Figura 59: *Percepción sobre el fortalecimiento de auditoría y cumplimiento normativo mediante la propuesta*



Fuente: Elaboración propia

Descripción

La gráfica presenta la valoración de los participantes respecto a si la propuesta basada en COBIT 2019 e ITIL 4 aumentaría la capacidad de auditoría y cumplimiento normativo en la gestión del software de cajeros automáticos. Los resultados muestran que 25% calificó el beneficio en nivel 3, mientras que 38% se ubicó en nivel 4 y otro 38% en nivel 5, reflejando una percepción predominantemente positiva.

Análisis

Los resultados revelan que los colaboradores identifican una relación directa entre la adopción de marcos de gobierno de TI y el fortalecimiento de los procesos de auditoría, conformidad regulatoria y cumplimiento de políticas internas. La suma del 76% en niveles 4 y 5 subraya que la propuesta es vista como un mecanismo eficaz para estandarizar procedimientos, mejorar la trazabilidad, consolidar evidencias de control y facilitar revisiones futuras por entes regulatorios como la CNBS.

El 25% que se ubica en nivel 3 indica que aún persisten percepciones de que el cumplimiento normativo requiere inversiones adicionales en herramientas, automatización y actualización de políticas internas para lograr niveles óptimos de madurez. Sin embargo, ninguna respuesta se coloca en niveles bajos, evidenciando confianza generalizada en los beneficios de la propuesta.

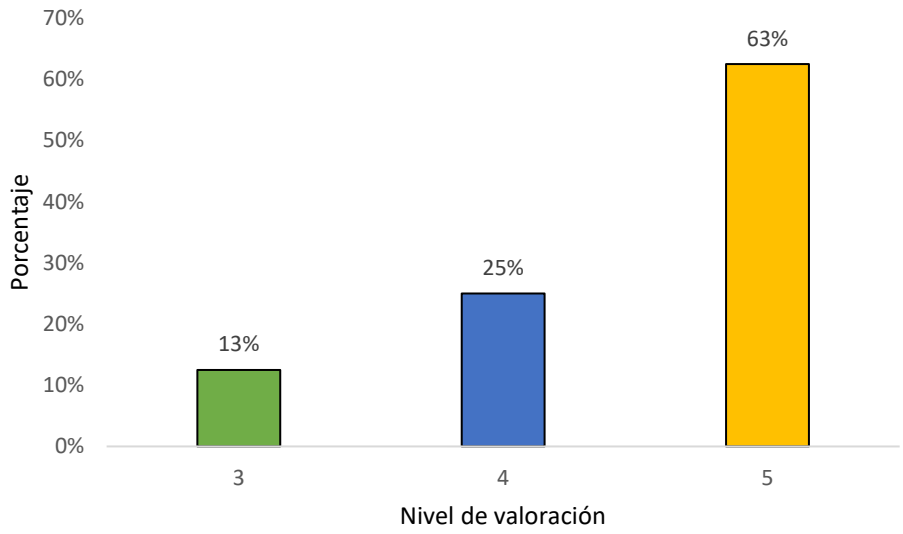
Hallazgo

El 76% de los encuestados considera que la implementación del análisis de riesgos basado en COBIT 2019 e ITIL 4 incrementará significativamente la capacidad de auditoría y cumplimiento normativo del banco. Este hallazgo confirma que la propuesta no solo mejora la operación técnica del software ATM, sino que también fortalece dimensiones estratégicas vinculadas a gobierno, control interno y exigencias regulatorias del sector financiero.

21. Mayor capacidad de respuesta ante incidentes y tiempos de recuperación (RTO/RPO)

Figura 60: *Percepción sobre la mejora en la capacidad de respuesta ante incidentes y tiempos*

de recuperación (RTO/RPO)



Fuente: Elaboración propia

Descripción

La gráfica presenta la valoración de los participantes respecto al impacto potencial de la propuesta basada en COBIT 2019 e ITIL 4 en la mejora de la capacidad de respuesta ante incidentes y la reducción de los tiempos de recuperación (RTO/RPO). Los resultados muestran que 13% calificó el beneficio en nivel 3, 25% lo ubicó en nivel 4 y la mayoría, 63%, lo valoró con nivel 5.

Análisis

Los resultados reflejan una percepción ampliamente favorable por parte de los encuestados, quienes reconocen que la integración de marcos como COBIT 2019 e ITIL 4 permitiría agilizar la detección, contención y resolución de incidentes relacionados con el software de cajeros automáticos. El 63% que seleccionó el nivel más alto indica una fuerte confianza en que la propuesta fortalecerá elementos clave como la coordinación operativa, la trazabilidad, la estandarización de respuestas y la capacidad de recuperar servicios críticos en menor tiempo.

El 25% en nivel 4 complementa este panorama, sugiriendo que la propuesta se percibe como un mecanismo robusto para reducir interrupciones transaccionales y mejorar indicadores de continuidad del negocio. El porcentaje menor en nivel 3 (13%) evidencia que algunos participantes

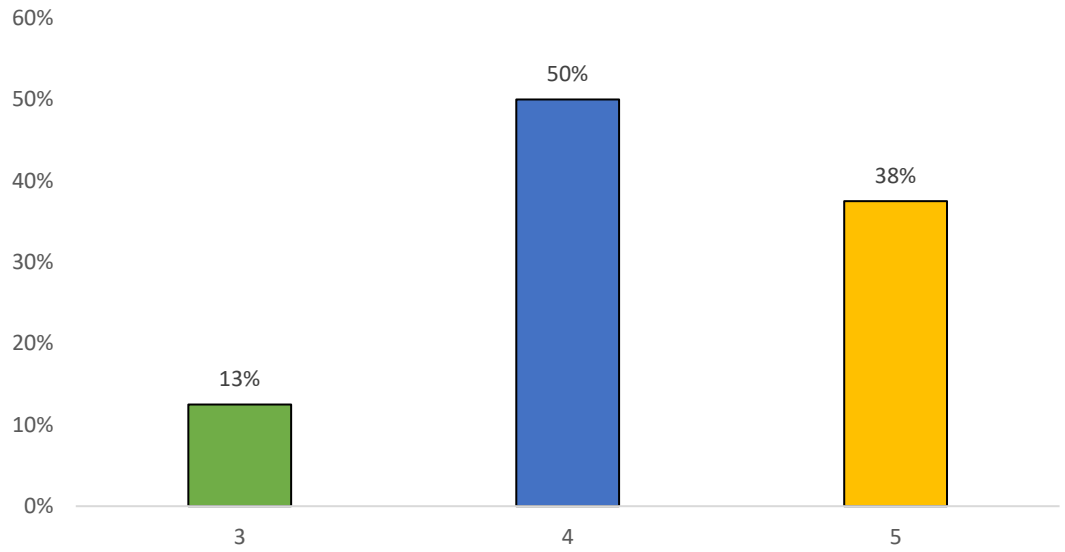
consideran que la reducción de RTO/RPO también depende de factores externos como infraestructura, proveedores y automatización, aunque sin cuestionar la utilidad de la propuesta.

Hallazgo

El 88% de los encuestados (niveles 4 y 5) considera que la implementación del análisis de riesgos basado en COBIT 2019 e ITIL 4 fortalecerá significativamente la capacidad de respuesta ante incidentes y disminuirá los tiempos de recuperación del servicio ATM. Este hallazgo valida la pertinencia del enfoque propuesto para mejorar la continuidad operativa y la resiliencia tecnológica del banco.

22. ¿Integración entre COBIT 2019 e ITIL 4 facilita la gobernanza de servicios críticos?

Figura 61: *Percepción sobre si la integración entre COBIT 2019 e ITIL 4 facilita la gobernanza de servicios críticos*



Fuente: Elaboración propia

Descripción

La gráfica muestra la valoración de los participantes respecto a la contribución de la integración entre COBIT 2019 e ITIL 4 para fortalecer la gobernanza de servicios críticos, incluyendo el software de cajeros automáticos. Los resultados reflejan que 13% asignó una calificación de 3, mientras que 50% seleccionó el nivel 4 y el 38% restante optó por el nivel 5.

Análisis

Los datos evidencian una percepción positiva y consistente sobre la utilidad de combinar ambos marcos de referencia para mejorar la gobernanza en la operación de servicios críticos. Que el 88% de los encuestados ubique su valoración en niveles altos (4 y 5) muestra que los profesionales reconocen los aportes estructurales de COBIT 2019 en materia de control, alineación estratégica, cumplimiento y gestión del riesgo, complementados con el enfoque operativo de ITIL 4 orientado al ciclo de valor del servicio.

Esta valoración indica que la mayor parte del personal técnico y de TI observa que la integración propuesta permitiría mejorar la toma de decisiones, estandarizar procesos, fortalecer la coordinación interdepartamental y establecer un gobierno más claro y medible sobre los servicios tecnológicos esenciales del banco.

Hallazgo

Los resultados permiten concluir que la mayoría de los encuestados (88%) considera que la integración COBIT 2019 + ITIL 4 facilitaría significativamente la gobernanza de servicios críticos, lo que respalda la pertinencia de la propuesta y reafirma la necesidad de adoptar un enfoque unificado de gestión y control en el software de cajeros automáticos.

4.4.4 HALLAZGOS SOBRE LOS BENEFICIOS ESTRATÉGICOS DE IMPLEMENTAR EL ANÁLISIS DE RIESGOS CON COBIT 2019 E ITIL 4 EN EL SOFTWARE DE CAJEROS AUTOMÁTICOS

El análisis de los resultados obtenidos mediante la encuesta aplicada al personal técnico y de TI de Banco Ficohsa evidencia una percepción ampliamente favorable respecto a la implementación de un modelo de análisis de riesgos basado en COBIT 2019 e ITIL 4 para optimizar la gestión del software de cajeros automáticos. En términos generales, los participantes manifestaron niveles altos de acuerdo respecto al impacto estratégico, operativo y de gobernanza que tendría la propuesta institucional.

En primer lugar, los hallazgos muestran que la mayoría de los encuestados reconoce el valor de COBIT 2019 como marco de gobernanza y gestión del riesgo, especialmente en la estandarización de procesos, cumplimiento normativo y visibilidad de riesgos. Simultáneamente, se identifica una fuerte aceptación de ITIL 4 como marco operativo clave para mejorar la continuidad del servicio, la atención de incidentes, el diseño del ciclo de vida del software y la gestión de disponibilidad.

Asimismo, los resultados indican que la integración de ambos marcos es vista como una estrategia sólida para mejorar la disponibilidad del software ATM, reducir fallas críticas, optimizar tiempos de respuesta y fortalecer los mecanismos de recuperación ante incidentes. De manera consistente, los participantes subrayan que una adopción conjunta de COBIT 2019 e ITIL 4 permitiría incrementar la eficiencia de los despliegues, mejorar la trazabilidad de cambios y aumentar la transparencia y claridad en los roles y responsabilidades asociados a la operación del software.

Finalmente, los encuestados destacan beneficios estratégicos como el cumplimiento regulatorio, la madurez organizacional, la mejora en la satisfacción de clientes internos, la consolidación de una cultura de datos para la toma de decisiones y la creación de un entorno de TI más seguro, controlado y alineado a los objetivos del negocio. En conjunto, los hallazgos evidencian que la propuesta tiene un alto potencial de impacto positivo en la operación del sistema de cajeros automáticos del banco, respaldando la pertinencia del modelo planteado en esta investigación.

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

A continuación, se engloban los hallazgos críticos obtenidos en el diagnóstico de la gestión del software de cajeros automáticos en Banco Ficohsa, el cual se basó en la percepción de expertos con experiencia en el área. Las conclusiones formuladas responden directamente al objetivo de la investigación: en la que se pretenden identificar las deficiencias que exponen al sistema a riesgos y justificar la necesidad de una transformación basada en los marcos de COBIT 2019 e ITIL 4. Finalmente, se proponen las recomendaciones clave para mitigar las vulnerabilidades encontradas y lograr un modelo de gestión proactivo y seguro.

5.1 CONCLUSIONES

1. En coherencia con el objetivo general de desarrollar un análisis de riesgos basado en COBIT 2019 e ITIL 4 para proponer estrategias de mitigación en la gestión del software de cajeros automáticos, se concluye que la situación actual del software ATM en Banco Ficohsa presenta una exposición de riesgo inaceptable, evidenciada en un Riesgo de Fraude Muy Alto (Media 4.75) y un Riesgo de Seguridad Informática Alto (Media 4.00). Este diagnóstico da cumplimiento al primer objetivo específico, al identificar de manera clara las principales amenazas, vulnerabilidades y deficiencias que afectan al sistema, y pone de manifiesto la urgencia de adoptar un marco de gobernanza sólido como COBIT 2019 que priorice la seguridad, estandarice los controles y reduzca la probabilidad de pérdidas financieras y daños reputacionales.

2. En relación con el segundo objetivo específico, orientado a evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 al análisis de riesgos y gestión de incidentes, los resultados muestran que la causa raíz de la alta exposición y de la elevada frecuencia de incidentes (Media 3.75) es la inmadurez de los procesos de gestión de servicios, que operan bajo un enfoque predominantemente reactivo. La baja oportunidad en la aplicación de parches (Media 2.50) y la baja efectividad del monitoreo (Media 2.50) confirman que las vulnerabilidades no se previenen ni se detectan con la rapidez requerida, lo cual demuestra que COBIT 2019 e ITIL 4 resultan plenamente pertinentes para formalizar procesos, establecer controles estructurados y transformar el modelo actual hacia una gestión más disciplinada y orientada al riesgo.

3. Vinculado con el tercer objetivo específico, que busca definir indicadores clave de desempeño y métricas de seguimiento para evaluar la efectividad de las estrategias de mitigación,

los hallazgos evidencian una falla sistémica en el control y la gestión del conocimiento, expresada en la ausencia de un estándar definido de software, la carencia de una logística clara para el patch management y la falta de documentación histórica de incidentes (75 por ciento de respuestas negativas o inciertas). Esta situación limita la capacidad del banco para medir con precisión la disponibilidad, la frecuencia de incidentes, la oportunidad en la aplicación de parches y la efectividad del monitoreo, lo que refuerza la necesidad de implementar KPIs de riesgo y desempeño alineados con COBIT 2019 e ITIL 4 que permitan alimentar un ciclo de mejora continua en la gestión del software ATM.

4. Finalmente, en correspondencia con el cuarto y quinto objetivos específicos, relacionados con el diseño de un modelo integrado de gestión basado en COBIT 2019 e ITIL 4 y con la identificación de los beneficios que obtendría Banco Ficohsa al implementar la propuesta, se concluye que la integración de ambos marcos se encuentra plenamente validada por el personal experto consultado. Las demandas reiteradas de “mejora en los procesos”, “lograr que cumplan con un estándar” y la necesidad de automatizar la “configuración remota” muestran que la solución estratégica reside en articular COBIT 2019 para la gobernanza y los estándares, e ITIL 4 para la formalización de las prácticas operacionales. Con ello se confirma que el modelo propuesto contribuye a optimizar la continuidad del servicio, fortalecer la resiliencia operativa, mejorar el cumplimiento regulatorio y generar beneficios tangibles para la gestión del software de cajeros automáticos en Banco Ficohsa.

5.2 RECOMENDACIONES

1. En coherencia con el objetivo general y con el primer y segundo objetivos específicos, la primera recomendación es fortalecer la gobernanza de riesgos y seguridad mediante la implementación prioritaria de los procesos COBIT 2019 EDM03 (Optimización de Riesgos) y APO13 (Gestionar Seguridad). Con ello se busca establecer formalmente el apetito de riesgo de fraude y seguridad informática, definir políticas claras de control de vulnerabilidades y alinear la gestión del software ATM con las exigencias regulatorias y estratégicas del banco. Esta acción permite responder de forma directa a la exposición de riesgo inaceptable identificada en el análisis, asegurando que la gestión del software sea conducida bajo un marco de gobierno que oriente las decisiones a la continuidad del servicio, la protección de la información y la resiliencia operativa.

2. En relación con el primer, segundo y tercer objetivos específicos, se recomienda

formalizar la Gestión de Cambios y Configuración apoyándose en la combinación de COBIT 2019, particularmente el proceso BAI08 (Gestionar Cambios), y las prácticas de ITIL 4 asociadas a la gestión de cambios y la gestión de configuración. Esta recomendación implica definir una Línea Base del software ATM en una base de datos de gestión de la configuración (CMDB) sencilla pero funcional, establecer un estándar de software claramente documentado y diseñar una logística robusta para el patch management que priorice los parches de seguridad. Al estructurar este proceso, se corrige la inoportunidad en la aplicación de parches y se habilita la definición de KPIs específicos sobre tiempos de despliegue, cumplimiento de ventanas de mantenimiento y niveles de estabilidad, contribuyendo a un seguimiento sistemático de las estrategias de mitigación.

3. Finalmente, en alineación con el tercer, cuarto y quinto objetivos específicos, se recomienda transformar el modelo de operación de reactivo a proactivo mediante el fortalecimiento de la Detección y Eliminación de Fallas con las prácticas de ITIL 4 de Gestión de Monitoreo y Eventos y Gestión de Problemas. La implementación de herramientas de monitoreo en tiempo real sobre parámetros críticos de conectividad, rendimiento y registros de seguridad permitirá superar la baja efectividad del monitoreo y anticipar fallas antes de que generen interrupciones severas. De forma complementaria, activar de manera sistemática la Gestión de Problemas posibilitará realizar análisis de causa raíz de los incidentes de mayor frecuencia, documentar las soluciones permanentes y alimentar los KPIs definidos para la toma de decisiones gerenciales. Con ello se consolida el modelo integrado basado en COBIT 2019 e ITIL 4 y se maximizan los beneficios esperados en términos de reducción de incidentes, mejora en los tiempos de respuesta y aumento de la confianza en la red de cajeros automáticos del banco.

4. Se recomienda institucionalizar un modelo integrado de gobernanza y operación para la gestión del software ATM, mediante la formalización de un esquema de coordinación entre las áreas clave (Tecnología, Seguridad de la Información, Operaciones y Mesa de Servicio), con comités de seguimiento, responsables definidos y un calendario de revisión periódica. Esta medida permitirá sostener la integración entre COBIT 2019 e ITIL 4 en el tiempo, asegurar la trazabilidad de decisiones, fortalecer la rendición de cuentas y consolidar una adopción gradual sin depender de esfuerzos aislados. Asimismo, se sugiere incorporar un plan de capacitación y gestión del cambio (roles, procedimientos, uso de registros y lectura de indicadores) y ejecutar evaluaciones periódicas de cumplimiento y efectividad, de forma que el modelo se mantenga vigente ante cambios tecnológicos, incidentes recurrentes y exigencias regulatorias

CAPÍTULO VI APLICABILIDAD

6.1 PROPUESTA DE FORTALECIMIENTO DE LA GESTIÓN DE RIESGOS DEL SOFTWARE DE CAJEROS AUTOMÁTICOS MEDIANTE LA INTEGRACIÓN DE COBIT 2019 E ITIL 4

El presente capítulo desarrolla la propuesta de aplicabilidad de una solución articulada en los marcos COBIT 2019 e ITIL 4. COBIT 2019 proporcionará el marco de gobernanza necesario para alinear la gestión de riesgos de TI con los objetivos del negocio y establecer estándares de control para el software de cajeros automáticos. Por su parte, ITIL 4 aportará las prácticas detalladas de gestión de servicios en particular, gestión de incidentes, de cambios y de configuración requeridas para transformar el modelo operativo actual, predominantemente reactivo, en un modelo proactivo orientado a la prevención y a la mejora continua. Las secciones siguientes detallan la estructuración de esta propuesta y muestran cómo cada componente se fundamenta directamente en la mitigación de los hallazgos críticos identificados por los expertos.

La solución propuesta para optimizar la gestión del software de cajeros automáticos se basa en la aplicación complementaria y articulada de COBIT 2019 e ITIL 4, de manera que cada marco aborde un nivel específico de las necesidades de mejora identificadas en el diagnóstico. COBIT 2019 se orienta a la gobernanza, la definición de estándares y el control gerencial, mientras que ITIL 4 se enfoca en la operación cotidiana del servicio, a través de prácticas de gestión de servicios que permiten ejecutar en la práctica las directrices de gobernanza definidas.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

La presente propuesta se justifica a partir de la necesidad estratégica de fortalecer la gestión del software de cajeros automáticos (ATM) en Banco Ficohsa, considerando que este canal constituye uno de los principales medios de interacción entre la institución financiera y sus clientes. La alta dependencia operativa de los cajeros automáticos, sumada al incremento de amenazas tecnológicas, fallas operativas y exigencias regulatorias, hace indispensable la implementación de un modelo estructurado que permita identificar, evaluar y mitigar los riesgos asociados a este tipo de software crítico.

Los resultados obtenidos en el desarrollo de la investigación evidencian la existencia de vulnerabilidades, deficiencias operativas y brechas metodológicas en la gestión actual del software ATM, especialmente en aspectos relacionados con la gestión de incidentes, la continuidad del

servicio, el control de cambios, la trazabilidad de eventos y la medición del desempeño. Estas debilidades incrementan la exposición del banco a riesgos operativos, financieros, reputacionales y de cumplimiento normativo, lo cual justifica la formulación de una propuesta orientada a fortalecer la gobernanza y la gestión de los servicios tecnológicos.

La integración de los marcos de referencia COBIT 2019 e ITIL 4 se justifica por su complementariedad y aplicabilidad en entornos financieros altamente regulados. COBIT 2019 proporciona una estructura sólida para la gobernanza de tecnologías de la información, permitiendo alinear los objetivos estratégicos del negocio con la gestión de riesgos, el control interno y el cumplimiento normativo. Por su parte, ITIL 4 aporta un enfoque práctico y operativo orientado a la gestión eficiente de servicios, la mejora continua, la optimización de tiempos de respuesta y la creación de valor para los usuarios internos y externos.

Desde una perspectiva operativa, la propuesta permite pasar de un modelo reactivo de atención de incidentes a un enfoque preventivo y proactivo, basado en la identificación temprana de riesgos, la estandarización de procesos, la definición clara de roles y responsabilidades, y el uso de indicadores clave de desempeño (KPIs y KRIs). Esto contribuye a mejorar la disponibilidad del software ATM, reducir los tiempos de recuperación ante fallas, minimizar interrupciones del servicio y fortalecer la experiencia del cliente.

Asimismo, la propuesta se justifica por su alineación con las exigencias regulatorias del sector financiero hondureño y los estándares internacionales de seguridad y gestión de TI. Al estructurar controles, métricas y procedimientos basados en buenas prácticas reconocidas, Banco Ficohsa podrá fortalecer sus procesos de auditoría, supervisión y cumplimiento, reduciendo el riesgo de sanciones y mejorando la transparencia en la gestión tecnológica.

Finalmente, la viabilidad de la propuesta se sustenta en que los marcos COBIT 2019 e ITIL 4 son flexibles, escalables y adaptables al contexto organizacional del banco, permitiendo su implementación progresiva sin afectar la operación diaria. De esta manera, la propuesta no solo responde a las problemáticas identificadas en la investigación, sino que constituye una herramienta práctica y sostenible para fortalecer la resiliencia operativa, la seguridad del software de cajeros automáticos y la toma de decisiones estratégicas en Banco Ficohsa.

El diagnóstico de la gestión del software de cajeros automáticos en Banco Ficohsa, realizado a partir de los hallazgos del Capítulo IV, confirmó la existencia de un riesgo crítico de

fraude (media 4.75) y de un riesgo alto de seguridad informática (media 4.00). Estos niveles de exposición se explican por deficiencias procesales y de gobernanza, entre las que destacan la baja efectividad del monitoreo (media 2.50), la inoportunidad en la aplicación de parches (media 2.50) y la ausencia de un estándar de software y de una logística claramente definida para las actualizaciones (ítem P23). De forma complementaria, la percepción de baja satisfacción con los procesos actuales (media 2.75) y la alta frecuencia de incidentes (media 3.75) refuerzan la urgencia de una intervención estructural sobre la gestión del software ATM.

6.2.1 ROL DE COBIT 2019: GOBERNANZA Y ESTÁNDARES

COBIT 2019 se utilizará para establecer la gobernanza de TI sobre el software de cajeros automáticos y asegurar su alineación con los objetivos estratégicos del banco. Considerando la alta percepción de riesgo identificada en los ítems P24 y P19, el énfasis se centrará en los procesos de Evaluación, Dirección y Monitoreo (EDM) y de Alineación, Planificación y Organización (APO), con el propósito de fortalecer el control gerencial y reducir la exposición a riesgos de fraude y seguridad lógica.

Tabla 33: *Procesos de COBIT 2019 seleccionados para gobernanza y control*

Proceso COBIT 2019	Justificación basada en hallazgos	Objetivo a mitigar
EDM03: Asegurar la optimización de riesgos	La media de riesgo de fraude (4.75) y de seguridad informática (4.00) resulta inaceptablemente alta para un canal crítico como el ATM.	Establecer el apetito de riesgo, definir controles y monitorear sistemáticamente el riesgo de fraude y seguridad.
APO01: Gestionar el marco de gestión de TI	Responde a la necesidad de "lograr que cumplan con un estándar" (P34) y a la ausencia de un estándar a nivel de software (P23).	Formalizar la estructura organizativa, los roles y las responsabilidades para la gestión del software ATM.
APO13: Gestionar seguridad	Orientado a mitigar la alta exposición a malware (P17) y la falta de revisión periódica de políticas de seguridad (P20).	Definir y comunicar políticas de seguridad para el software, integrando los controles de patch management.
MEA01: Monitorizar, evaluar y valorar el rendimiento y la conformidad	Necesario para corregir la falta de claridad en el cumplimiento de los SLA (P21, media 3.00) y fortalecer la supervisión del servicio.	Establecer métricas e indicadores de rendimiento y cumplimiento del servicio de software ATM.

Fuente: Elaboración propia

6.2.2 ROL DE ITIL 4: GESTIÓN DE SERVICIOS Y HABILITACIÓN

ITIL 4 se aplicará para definir y mejorar las prácticas operacionales requeridas para

ejecutar las directrices de COBIT 2019 en el día a día. El foco se sitúa en transformar la gestión predominantemente reactiva, evidenciada por la frecuencia de incidentes (Q8, media 3.75), en un servicio proactivo y controlado que utilice los datos de operación para prevenir fallas y reducir la recurrencia de problemas.

Tabla 34: *Prácticas de ITIL 4 seleccionadas para la gestión operacional*

Práctica ITIL 4	Justificación basada en hallazgos	Objetivo a corregir
Gestión de configuración	Responde a la necesidad de "introducir un estándar a nivel de software" (P33) y a la ausencia de una línea base de configuración.	Crear una línea base y una base de datos de gestión de la configuración (CMDB) sencilla para documentar el estándar del software ATM.
Gestión de cambios	Atiende la inoportunidad en la aplicación de parches (P22, media 2.50) y la logística deficiente de actualizaciones (P23).	Formalizar el proceso de patch management, incluyendo la evaluación de riesgos y el despliegue controlado de actualizaciones de seguridad.
Gestión de problemas	Orientada a la alta frecuencia de incidentes (P8, media 3.75) y a la falta de documentación histórica de fallas (P12).	Analizar las causas raíz de la inestabilidad, por ejemplo, la conectividad, para implementar soluciones permanentes y preventivas.
Gestión de monitoreo y eventos	Busca corregir la baja efectividad del monitoreo (P13, media 2.50) y asegurar una supervisión continua del servicio.	Implementar herramientas y umbrales de detección temprana que contribuyan a la estabilidad y seguridad del software ATM.

Fuente: Elaboración propia

6.3 ALCANCE DE LA PROPUESTA

La propuesta se formula con el propósito de mitigar las vulnerabilidades y riesgos identificados en el Capítulo IV, de manera que la gestión del software de cajeros automáticos alcance un nivel de madurez proactivo, estandarizado y alineado con los marcos COBIT 2019 e ITIL 4. En este sentido, el objetivo específico de la propuesta se orienta a reducir la exposición al riesgo de fraude y seguridad lógica, fortalecer el control sobre el ciclo de vida de parches y consolidar un modelo de operación respaldado por procesos formales de gestión de servicios y de gobernanza de TI.

Objetivo 4, Diseñar un modelo integrado de gestión basado en COBIT 2019 e ITIL 4 que fortalezca la administración del software de cajeros automáticos y responda de manera efectiva a los requisitos del entorno financiero actual.

La presente propuesta tiene como alcance el diseño y aplicación de un modelo integrado de gestión del software de cajeros automáticos de Banco Ficohsa, fundamentado en los marcos de referencia COBIT 2019 e ITIL 4, con el propósito de fortalecer la administración del canal ATM y responder de manera efectiva a los riesgos, vulnerabilidades y deficiencias identificadas en el análisis desarrollado en los capítulos previos. El alcance de la propuesta se orienta a la mitigación de los riesgos críticos asociados a la seguridad lógica, el fraude, la gestión de cambios y la operación reactiva del software, promoviendo una transición hacia un modelo de gestión proactivo, estandarizado y alineado con las buenas prácticas de gobierno y gestión de TI.

En este contexto, la propuesta establece como objetivos específicos del plan de acción la reducción de la exposición al riesgo de fraude y seguridad informática mediante la implementación de controles formales de gestión de cambios y parches; el fortalecimiento del monitoreo del software ATM y de la gestión de incidentes con el fin de disminuir la frecuencia de interrupciones y optimizar los tiempos de respuesta del servicio; y la formalización de un estándar de configuración del software que permita asegurar la trazabilidad, la documentación histórica y la consistencia operativa en la red de cajeros automáticos. Estos objetivos se materializan a través de la aplicación integrada de procesos y prácticas tales como la Gestión de Cambios, Gestión de Configuración, Gestión de Monitoreo y Eventos, Gestión de Incidentes y Gestión de Problemas, enmarcados principalmente en los dominios BAI, DSS y MEA de COBIT 2019 y en las prácticas correspondientes de ITIL 4.

El alcance de la propuesta se centra específicamente en la gestión del ciclo de vida del software de los cajeros automáticos, incluyendo el sistema operativo base, el middleware bancario y las aplicaciones propietarias del ATM, considerados como activos lógicos críticos del canal. Asimismo, contempla su articulación operativa con las áreas de Operaciones de Cajeros Automáticos, Soporte de TI y Seguridad de la Información, responsables de la ejecución de cambios, aplicación de parches, monitoreo continuo y atención de incidentes relacionados con el software y la seguridad lógica del canal ATM. Como parte del alcance, se incluyen actividades de definición de indicadores clave de desempeño y métricas de seguimiento que permitan evaluar la efectividad de las acciones de mitigación propuestas y apoyar un enfoque de mejora continua.

La propuesta delimita su aplicabilidad al software y a los procesos de soporte asociados al canal ATM, excluyendo de su alcance la gestión del hardware físico de los cajeros automáticos, la

mejora de la infraestructura de red externa al punto de conexión del ATM y los sistemas centrales de core banking o liquidación financiera. No obstante, se considera el monitoreo de la disponibilidad de la conectividad como un elemento de medición relevante, en la medida en que impacta directamente en la operación del software de cajeros automáticos. De igual forma, la propuesta no aborda la investigación ni recuperación financiera de fraudes consumados, enfocándose exclusivamente en la prevención mediante controles de TI, en coherencia con el enfoque de gestión de riesgos adoptado.

6.4 DESCRIPCIÓN Y DESARROLLO A DETALLE DE LA PROPUESTA

6.4.1. DESCRIPCIÓN

La propuesta consiste en un modelo integral de análisis de riesgos orientado a fortalecer la gestión del software de cajeros automáticos de Banco Ficohsa, fundamentado en los marcos de referencia COBIT 2019 e ITIL 4. Esta propuesta atiende el problema de la ausencia de un enfoque estructurado y estandarizado para la identificación, evaluación y control de los riesgos tecnológicos asociados a la operación del software ATM, situación que genera vulnerabilidades operativas, riesgos de seguridad, deficiencias en la continuidad del servicio y limitaciones en el cumplimiento normativo. A través de este modelo, se busca responder a las necesidades de gobernanza, control y calidad del servicio, alineando la gestión tecnológica con los objetivos institucionales y las exigencias del entorno financiero.1 párrafo: qué es la propuesta y qué problema atiende (sin "cómo").

Tabla 35: *Componentes de la propuesta y propósito*

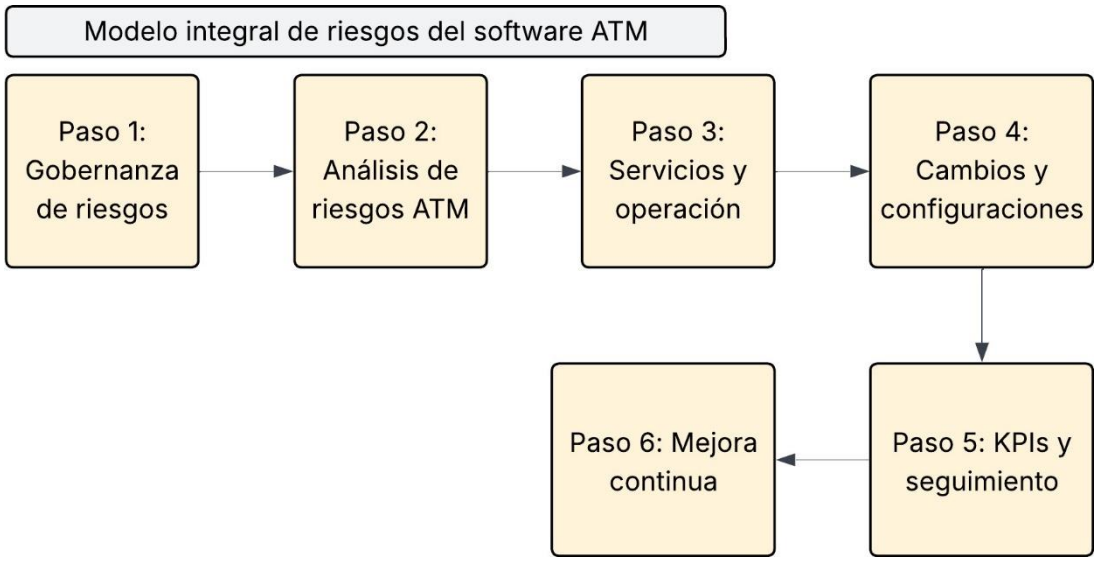
Componente	Qué incluye	Propósito	Hallazgo que atiende
Marco de gobernanza de riesgos	Principios y objetivos de gobierno de COBIT 2019, definición de roles, responsabilidades y políticas de control	Alinear la gestión del software ATM con los objetivos estratégicos y regulatorios del banco	Falta de un enfoque formal de gobernanza y alineación estratégica en la gestión del software ATM
Análisis de riesgos del software ATM	Identificación de amenazas, vulnerabilidades y riesgos operativos y de seguridad asociados al software de cajeros automáticos	Priorizar los riesgos críticos que afectan la continuidad, seguridad y confiabilidad del servicio	Ausencia de un análisis sistemático de riesgos tecnológicos específicos del software ATM

Gestión de servicios y operación	Prácticas de ITIL 4 relacionadas con operación, monitoreo, gestión de incidentes y soporte del servicio	Mejorar la disponibilidad del software ATM y la respuesta ante incidentes	Deficiencias en la gestión reactiva de incidentes y tiempos prolongados de recuperación
Gestión de cambios y control de configuraciones	Procedimientos estandarizados para actualizaciones, parches y cambios al software ATM	Reducir fallos derivados de cambios no controlados y asegurar la estabilidad del servicio	Falta de controles formales en la gestión de cambios del software de cajeros automáticos
Indicadores de desempeño y seguimiento	KPIs de disponibilidad, tiempos de respuesta, riesgo y cumplimiento normativo	Medir la efectividad de la gestión del software ATM y apoyar la toma de decisiones	Carencia de métricas e indicadores para evaluar el desempeño y la mejora continua
Mejora continua y control	Mecanismos de evaluación periódica, retroalimentación y ajustes al modelo	Asegurar la sostenibilidad y adaptación del modelo frente a cambios tecnológicos y regulatorios	Inexistencia de un ciclo estructurado de mejora continua en la gestión del software ATM

Fuente: Elaboración Propia

Los componentes de la propuesta se integran de manera coherente y complementaria, permitiendo abordar la gestión del software de cajeros automáticos desde una perspectiva estratégica y operativa. La descripción de cada componente establece una base estructural que facilita el desarrollo detallado de la propuesta, ya que define claramente su alcance, finalidad y relación con los hallazgos identificados en la investigación. Esta articulación asegura que el desarrollo posterior no sea fragmentado, sino que responda a un modelo integral orientado a la mitigación de riesgos, la continuidad del servicio y la mejora continua en Banco Ficohsa.

Figura 62: *Modelo integral de riesgos del software ATM (COBIT 2019 + ITIL 4)*



Fuente: Elaboración Propia

6.4.2 DESARROLLO

El desarrollo de la propuesta se estructura mediante un esquema de implementación por fases, en el cual se definen responsables claros, productos de salida y criterios de cierre para cada etapa, garantizando una ejecución ordenada y controlada. Cada fase contempla actividades específicas asociadas a la gobernanza, gestión de riesgos y operación del software de cajeros automáticos, con la participación de las áreas de tecnología, seguridad de la información y gestión operativa. Asimismo, se establecen evidencias verificables que permiten validar el cumplimiento de los objetivos de cada fase, así como criterios de salida que aseguran la correcta transición hacia las etapas siguientes y la alineación del proceso con los principios de COBIT 2019 e ITIL 4.

6.4.2.1 FASES DE IMPLEMENTACIÓN Y ENTREGABLES

La implementación de la propuesta se estructura por fases con el propósito de asegurar un orden lógico, controlado y alineado con la criticidad del software de cajeros automáticos. Este enfoque permite avanzar de manera progresiva desde la planificación y el diagnóstico hasta la operación y mejora continua, reduciendo riesgos asociados a cambios no controlados y facilitando la asignación clara de responsabilidades y recursos en cada etapa.

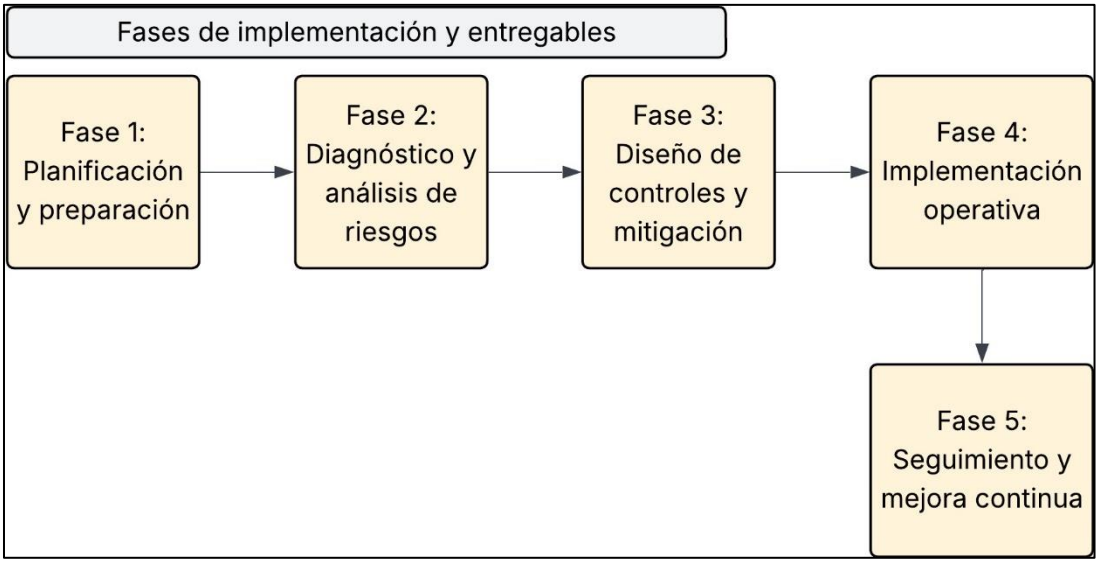
Tabla 36: *Fases de implementación y entregables*

Fase	Objetivo	Actividades	Entregables	Criterio de

		clave		cierre
Fase 1. Planificación y preparación	Establecer las bases organizativas y metodológicas de la propuesta	Conformación del equipo responsable, revisión de políticas y procesos existentes, definición de roles y alcance	Plan de implementación, matriz de roles y responsabilidades, alcance definido	Aprobación formal del plan y del equipo responsable
Fase 2. Diagnóstico y análisis de riesgos	Identificar amenazas, vulnerabilidades y deficiencias del software ATM	Aplicación de instrumentos de análisis, revisión documental, evaluación de riesgos y madurez de procesos	Matriz de riesgos, informe de diagnóstico, priorización de riesgos	Validación del diagnóstico y riesgos críticos identificados
Fase 3. Diseño de controles y estrategias de mitigación	Definir controles y acciones para reducir riesgos prioritarios	Diseño de controles COBIT 2019, estandarización de prácticas ITIL 4, definición de procedimientos operativos	Controles definidos, procedimientos documentados, flujos de gestión	Aprobación de controles y procedimientos por las áreas responsables
Fase 4. Implementación operativa	Aplicar los controles y prácticas definidos en la gestión del software ATM	Implementación de procedimientos, ajustes operativos, capacitación básica al personal	Controles operativos en ejecución, registros de capacitación	Evidencia de aplicación efectiva de controles
Fase 5. Seguimiento y mejora continua	Evaluar el desempeño y ajustar la propuesta	Monitoreo de KPIs, análisis de resultados, retroalimentación y ajustes	Reportes de desempeño, acciones de mejora documentadas	Resultados evaluados y ajustes implementados

Fuente*:* Elaboración propia

Figura 63: *Fases de implementación y entregables*



Fuente: Elaboración propia

La estructuración por fases permite asegurar el control del proceso de implementación y disminuir el riesgo operativo asociado a la gestión del software de cajeros automáticos, al establecer puntos de verificación y criterios claros de cierre en cada etapa. Este enfoque facilita la trazabilidad de las acciones, la validación de resultados y la corrección oportuna de desviaciones, contribuyendo a una adopción gradual, segura y alineada con los principios de COBIT 2019 e ITIL 4.

6.4.2.2 ROLES Y RESPONSABILIDADES OPERATIVAS

La asignación clara de roles y responsabilidades operativas es fundamental para asegurar la trazabilidad, el control y la efectividad en la gestión del software de cajeros automáticos. La definición formal de funciones permite establecer líneas de responsabilidad, facilitar la coordinación entre áreas y garantizar que las actividades relacionadas con la gestión de riesgos, incidentes y operación del servicio se ejecuten de manera consistente y verificable.

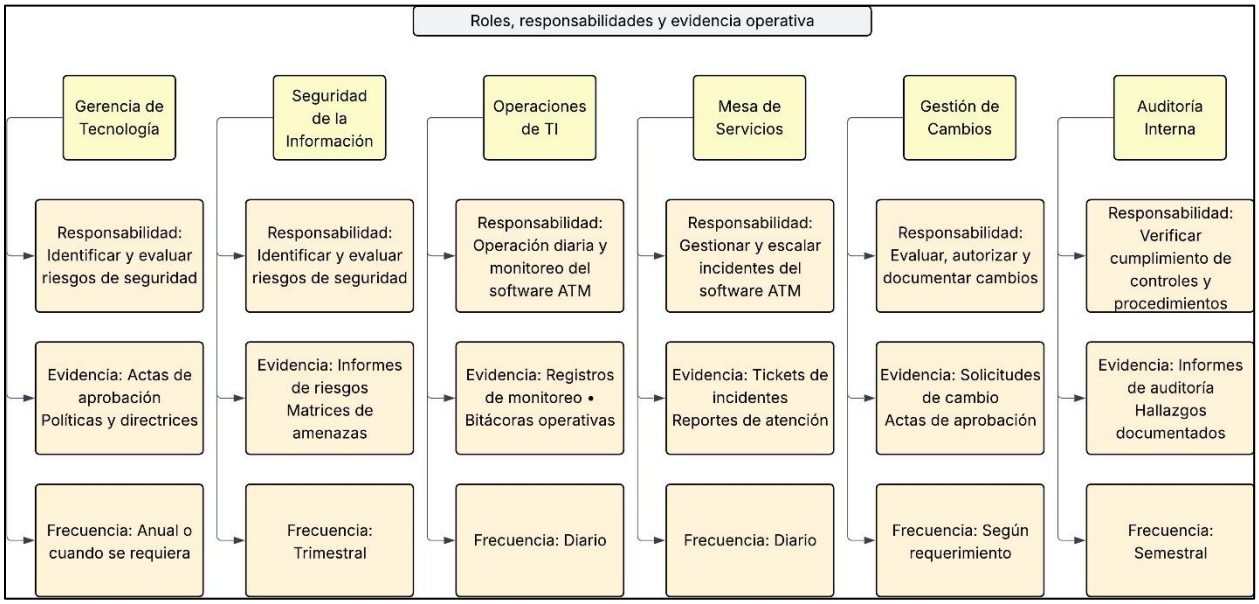
Tabla 37: *Roles, responsabilidades y evidencia*

Rol / Área	Responsabilidad	Evidencia / Registro	Frecuencia
Gerencia de Tecnología	Aprobar lineamientos, recursos y prioridades para la gestión del software ATM	Actas de aprobación, políticas y directrices	Anual o cuando se requiera
Área de Seguridad de la	Identificar y evaluar riesgos de seguridad asociados al software	Informes de riesgos, matrices de amenazas	Trimestral

Información	ATM		
Área de Operaciones de TI	Ejecutar la operación diaria y el monitoreo del software ATM	Registros de monitoreo, bitácoras operativas	Diario
Mesa de Servicios	Gestionar y escalar incidentes del software ATM	Tickets de incidentes, reportes de atención	Diario
Gestión de Cambios	Evaluar, autorizar y documentar cambios al software ATM	Solicitudes de cambio, actas de aprobación	Según requerimiento
Auditoría Interna	Verificar el cumplimiento de controles y procedimientos definidos	Informes de auditoría, hallazgos documentados	Semestral

Fuente: Elaboración Propia

Figura 64: *Roles, responsabilidades y evidencia operativa*



Fuente: Elaboración Propia

Esta asignación de roles y responsabilidades operativas reduce la existencia de vacíos de control y solapamientos funcionales, al tiempo que acelera la respuesta ante incidentes y eventos críticos del software de cajeros automáticos. Al contar con responsables claramente definidos y evidencias verificables, se fortalece la trazabilidad de las acciones, se mejora la coordinación interáreas y se facilita la supervisión y la toma de decisiones en la gestión del servicio.

6.4.2.3 PROCEDIMIENTOS OPERATIVOS PRINCIPALES (CAMBIOS Y PARCHES)

La formalización de los procedimientos de gestión de cambios y parches del software de

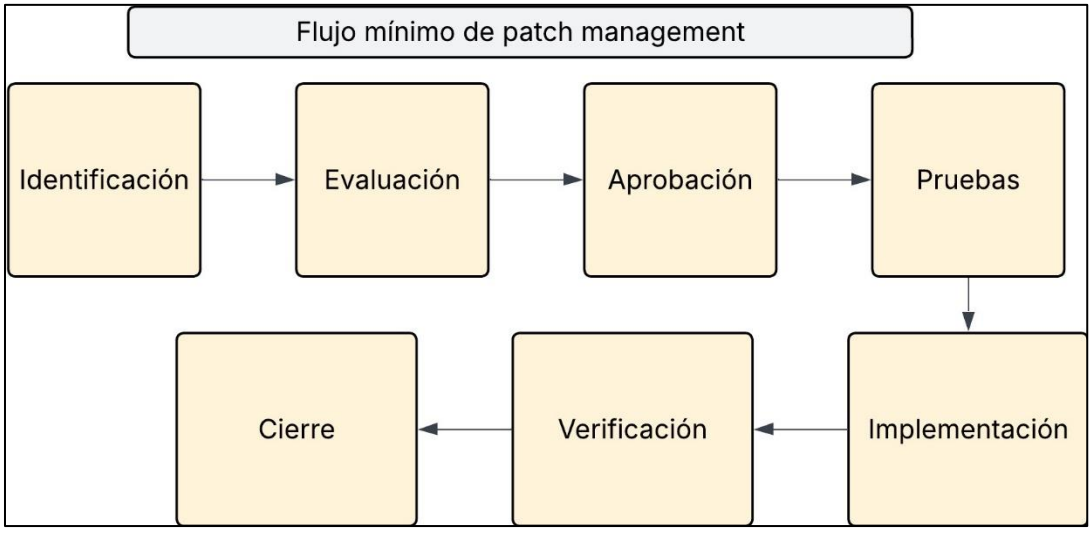
cajeros automáticos es crítica para mitigar riesgos de fraude, vulnerabilidades de seguridad y fallos operativos. Un control inadecuado de modificaciones al software ATM puede introducir errores, abrir brechas de seguridad o afectar la continuidad del servicio; por ello, establecer un flujo mínimo y estandarizado permite asegurar que toda intervención sea evaluada, autorizada y documentada conforme a criterios técnicos y de riesgo.

Tabla 38: *Flujo mínimo de patch management*

Etapa	Entrada	Actividad clave	Salida / Evidencia	Responsable
Identificación	Notificación de vulnerabilidad o necesidad de cambio	Análisis preliminar del impacto y urgencia	Registro de solicitud de cambio	Área de Seguridad de la Información
Evaluación	Solicitud de cambio registrada	Evaluación técnica y de riesgo del parche o cambio	Informe de evaluación y recomendación	Gestión de Cambios
Aprobación	Informe de evaluación	Revisión y autorización del cambio	Acta o registro de aprobación	Comité o responsable autorizado
Pruebas	Cambio aprobado	Ejecución de pruebas en ambiente controlado	Resultados de pruebas documentados	Área de Operaciones de TI
Implementación	Pruebas exitosas	Despliegue del parche o cambio en producción	Registro de implementación	Área de Operaciones de TI
Verificación	Cambio implementado	Validación de funcionamiento y monitoreo inicial	Evidencia de verificación y cierre	Mesa de Servicios
Cierre	Verificación realizada	Documentación final y actualización de registros	Ticket cerrado y bitácora actualizada	Gestión de Cambios

Fuente: Elaboración propia

Figura 65: *Flujo mínimo de patch management*



Fuente: Elaboración Propia

El flujo mínimo de gestión de cambios y parches garantiza el control, la aprobación formal y la generación de evidencias en cada etapa del proceso, reduciendo la probabilidad de fallos operativos y riesgos de seguridad asociados al software de cajeros automáticos. Al establecer responsables claros y salidas verificables, este procedimiento fortalece la trazabilidad, facilita auditorías internas y contribuye a una gestión más segura, ordenada y alineada con las buenas prácticas de COBIT 2019 e ITIL 4.

6.4.2.4 REGISTROS, HERRAMIENTAS Y CONTROL DOCUMENTAL

La adecuada gestión de registros y del control documental es fundamental para asegurar la trazabilidad de las actividades, el cumplimiento normativo y el aprendizaje organizacional en la gestión del software de cajeros automáticos. La generación sistemática de evidencias permite respaldar las decisiones operativas y de gobierno, facilitar los procesos de auditoría interna y externa, y fortalecer la capacidad del banco para analizar incidentes, evaluar riesgos y prevenir recurrencias.

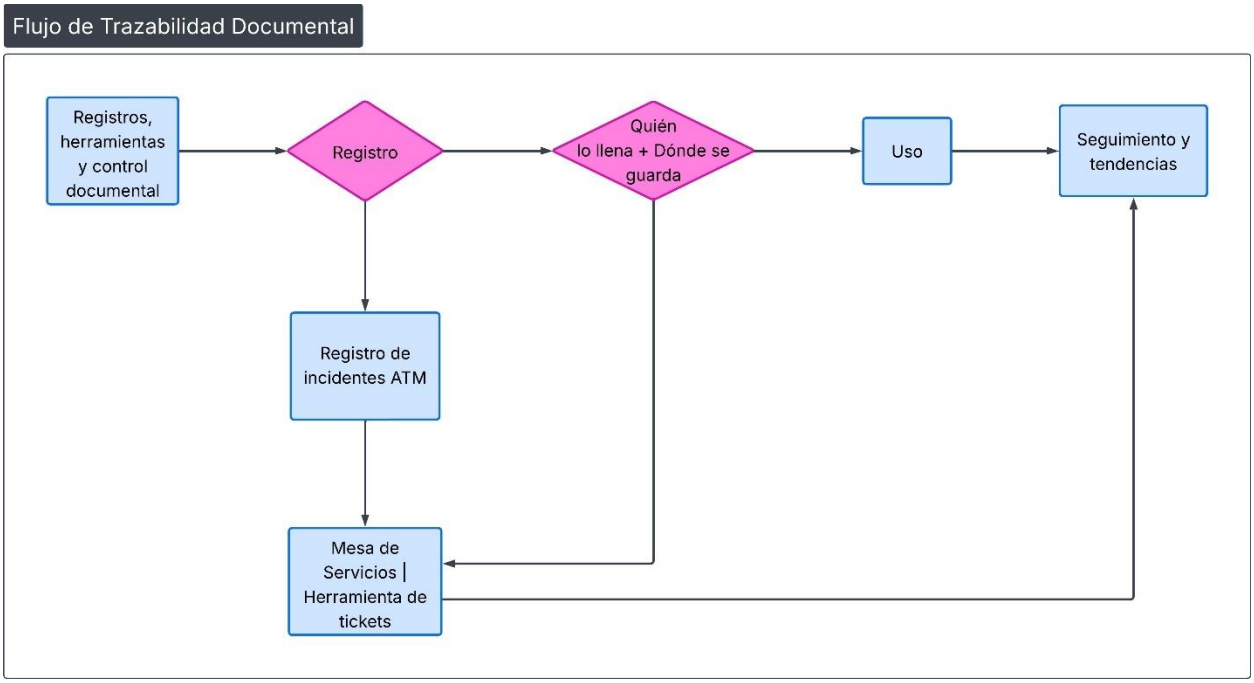
Tabla 39: *Registros y control documental*

Registro	Qué contiene	Quién lo llena	Dónde se guarda	Uso
Registro de incidentes ATM	Descripción del incidente, fecha, impacto, tiempo de	Mesa de Servicios	Herramienta de gestión de tickets	Seguimiento de incidentes y análisis de

	respuesta y solución			tendencias
Matriz de riesgos del software ATM	Riesgos identificados, probabilidad, impacto y controles asociados	Seguridad de la Información	Repositorio documental de TI	Evaluación y priorización de riesgos
Registro de cambios y parches	Detalle de cambios, parches aplicados, fechas y aprobaciones	Gestión de Cambios	Sistema de gestión de cambios	Control y trazabilidad de modificaciones
Reportes de monitoreo	Métricas de disponibilidad, alertas y eventos relevantes	Operaciones de TI	Plataforma de monitoreo	Detección temprana y control operativo
Informes de auditoría	Hallazgos, observaciones y recomendaciones	Auditoría Interna	Archivo institucional / repositorio seguro	Cumplimiento y mejora de controles

Fuente: Elaboración propia

Figura 66: *Registros, herramientas y control documental*



Fuente: Elaboración Propia

Los registros y el control documental constituyen la base para la medición del desempeño y la implementación de la mejora continua, ya que proporcionan información confiable para la definición y seguimiento de los indicadores clave de desempeño. Al alimentar los KPIs y los procesos de revisión periódica, estos registros permiten identificar patrones, evaluar la efectividad

de los controles y tomar decisiones informadas que contribuyen a optimizar la gestión del software de cajeros automáticos de manera sostenida.

6.4.2.5 PRIORIZACIÓN Y CRITICIDAD (INCIDENTES Y PARCHES)

La clasificación de la criticidad de incidentes y parches permite eliminar la improvisación en la toma de decisiones y reducir de forma significativa el riesgo operativo y de seguridad en la gestión del software de cajeros automáticos. Al contar con criterios predefinidos de priorización, la organización puede responder de manera oportuna y proporcional al impacto del evento, garantizando la continuidad del servicio y el uso eficiente de los recursos técnicos.

Tabla 40: *Matriz de criticidad para parches e incidentes*

Nivel	Definición	Tiempo objetivo	Acción requerida	Escalamiento
Crítico	Incidente o vulnerabilidad que afecta la disponibilidad total del servicio o compromete la seguridad	Atención inmediata	Contención, corrección urgente y monitoreo continuo	Gerencia de TI y Seguridad de la Información
Alto	Afectación parcial del servicio o riesgo elevado de impacto operativo o de seguridad	Corto plazo	Análisis prioritario, aplicación de parche o solución temporal	Coordinador de Operaciones
Medio	Impacto moderado sin interrupción total del servicio	Mediano plazo	Programación de corrección y seguimiento	Área de Operaciones
Bajo	Impacto mínimo o preventivo	Según planificación	Registro, evaluación y resolución planificada	Sin escalamiento inmediato

Fuente: Elaboración propia

La matriz de criticidad se integra directamente con los acuerdos de nivel de servicio, los mecanismos de monitoreo y los comités de control, permitiendo una gestión coherente y alineada con los objetivos operativos del banco. Este esquema facilita la priorización adecuada de incidentes y parches, fortalece la toma de decisiones basada en impacto y urgencia, y contribuye a una respuesta estructurada y controlada conforme a las buenas prácticas de COBIT 2019 e ITIL 4.

6.5 MEDIDAS DE CONTROL

Las medidas de control se establecen con el propósito de evaluar la eficacia y eficiencia de las acciones implementadas para mitigar los riesgos asociados a la gestión del software de cajeros

automáticos, así como verificar el cumplimiento de los objetivos definidos en la propuesta. Estas medidas permiten monitorear de forma sistemática el desempeño de los procesos, confirmar que los controles reducen efectivamente los riesgos operativos y de seguridad, y proporcionar evidencia objetiva para la supervisión, la auditoría y la toma de decisiones orientadas a la mejora continua.

6.5.1 INDICADORES KPI/KRI DE CONTROL

Los indicadores KPI y KRI constituyen herramientas fundamentales para medir el desempeño y el nivel de riesgo en la gestión del software de cajeros automáticos, ya que permiten traducir los controles implementados en información cuantificable para la toma de decisiones. Su lógica se basa en monitorear tanto la eficiencia operativa como la exposición al riesgo, facilitando la identificación temprana de desviaciones y la evaluación objetiva de la efectividad de las medidas de control.

Tabla 41: *Indicadores con límites y metas*

Indicador	**Definición**	**Fórmula**	**Frecuencia**	**Fuente**	**Responsable**	**Mínimo**	**Meta**	**Máximo**
Disponibilidad del software ATM (KPI)	Porcentaje de tiempo en que el software ATM se mantiene operativo	(Tiempo operativo / Tiempo total) × 100	Mensual	Plataforma de monitoreo	Operaciones de TI	95%	98 %	100%
Tiempo medio de resolución de incidentes – MTTR (KPI)	Promedio de tiempo requerido para resolver incidentes del software ATM	Suma de tiempos de resolución / Nº de incidentes	Mensual	Mesa de Servicios	Operaciones de TI	≤ 8 h	≤ 4 h	> 8 h
Incidentes críticos de seguridad (KRI)	Número de incidentes críticos relacionados con seguridad	Conteo de incidentes críticos	Mensual	Registro de incidentes	Seguridad de la Información	0	0–1	> 1

	del software ATM							
Cumplimiento de parches críticos (KRI)	Porcentaje de parches críticos aplicados dentro del tiempo definido	(Parches aplicados / Parches requeridos) × 100	Trimestral	Gestión de Cambios	Seguridad de la Información	85%	95 %	< 85%
Cambios no autorizados detectados (KRI)	Número de cambios al software ATM sin aprobación formal	Conteo de eventos	Trimestral	Auditoría / Registros de cambio	Auditoría Interna	0	0	≥ 1

Fuente: Elaboración propia

Estos indicadores se integran directamente con los procesos de revisión periódica y los mecanismos de control, permitiendo activar acciones correctivas cuando los valores se desvían de los límites establecidos. Al vincular los resultados de los KPI y KRI con comités de control, auditorías internas y ciclos de mejora continua, se fortalece la capacidad del banco para anticipar riesgos, corregir deficiencias operativas y asegurar una gestión del software de cajeros automáticos alineada con los principios de COBIT 2019 e ITIL 4.

6.5.2 MECANISMOS DE EVALUACIÓN Y SEGUIMIENTO

La evaluación y el seguimiento de las medidas de control permiten verificar de manera sistemática el cumplimiento de los lineamientos definidos, así como la efectividad de las acciones implementadas para mitigar los riesgos asociados al software de cajeros automáticos. Estos mecanismos se apoyan en reuniones periódicas, procesos de auditoría y revisión de evidencias documentales, asegurando que la información utilizada para la toma de decisiones sea confiable, oportuna y verificable.

Tabla 42: *Mecanismos de evaluación*

Mecanismo	Frecuencia	Responsable	Evidencia	Resultado esperado
Reunión de seguimiento	Mensual	Operaciones de TI	Actas de reunión, reportes de KPIs	Identificación de desviaciones

operativo				operativas
Revisión de indicadores KPI/KRI	Mensual	Gerencia de TI	Tablero de indicadores, reportes consolidados	Validación del desempeño y nivel de riesgo
Auditoría interna de controles	Semestral	Auditoría Interna	Informes de auditoría y hallazgos	Verificación del cumplimiento de controles
Revisión de gestión de cambios	Trimestral	Gestión de Cambios	Registros de cambios y aprobaciones	Control de modificaciones al software ATM
Evaluación de riesgos tecnológicos	Trimestral	Seguridad de la Información	Matriz de riesgos actualizada	Actualización y priorización de riesgos

Fuente: Elaboración propia

El seguimiento continuo de estos mecanismos permite cerrar de forma efectiva el ciclo de mejora continua, al transformar los resultados de la evaluación en acciones correctivas y preventivas. Esta retroalimentación sistemática fortalece la gobernanza, optimiza la gestión del software de cajeros automáticos y asegura la adaptación permanente de los controles frente a cambios tecnológicos, operativos y regulatorios.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN

El cronograma de implementación se establece con el propósito de organizar, secuenciar y controlar la ejecución de la propuesta mediante hitos claramente definidos, asegurando una adopción ordenada y verificable del modelo de gestión del software de cajeros automáticos. A través de este cronograma se facilita el seguimiento del avance, la asignación eficiente de responsabilidades y la validación del cumplimiento de cada etapa, reduciendo desviaciones y fortaleciendo el control del proceso de implementación.

6.6.1 CRONOGRAMA TIPO GANTT

El cronograma tipo Gantt se construye considerando criterios de dependencia entre actividades, nivel de criticidad del proceso y secuencia lógica de implementación, permitiendo ordenar las acciones de forma coherente y controlada. Este enfoque facilita priorizar las actividades más sensibles para la continuidad del software de cajeros automáticos y asegurar que cada fase se ejecute una vez cumplidos los requisitos de la etapa anterior.

Tabla 43: *Gantt semanal/mensual*

Actividad detallada	Ene	Feb	Mar	Abr	May	Jun
1. Conformación del equipo y patrocinio	X					
2. Definición de alcance, activos ATM y dependencias	X					
3. Levantamiento de procesos/políticas existentes y brechas	X	X				
4. Definir criterios de riesgo y criticidad (umbral/impacto)		X				
5. Aplicación CPM/SVC/checklist y consolidación de hallazgos		X				
6. Matriz de riesgos + priorización + validación con áreas		X				
7. Diseño de controles COBIT + procedimientos ITIL (incidentes)			X			
8. Diseño del flujo de cambios y patch management			X			
9. Definir registros, plantillas, repositorio y control documental			X	X		
10. Definición KPI/KRI, límites/metas y esquema de reporteo			X	X		
11. Configuración de monitoreo/alertas y pruebas operativas				X		
12. Capacitaciones (roles, procedimientos, uso de registros)				X		
13. Piloto controlado (parches/incidentes/monitoreo)					X	
14. Ajustes + despliegue ampliado + cierre con evidencias					X	X
15. Evaluación final + plan de mejora continua						X

Fuente: Elaboración Propia

El cronograma tipo Gantt facilita el seguimiento y control del avance de la propuesta al ofrecer una visión clara de las actividades, su duración y su relación temporal. Esta herramienta permite a los responsables identificar retrasos, validar el cumplimiento de hitos y tomar decisiones oportunas para garantizar una implementación ordenada y alineada con los objetivos de control y mejora de la gestión del software de cajeros automáticos.

6.6.2 HITOS Y RESPONSABLES

La definición de hitos verificables y criterios de aceptación es necesaria para asegurar el control del avance y la correcta ejecución del cronograma de implementación. Los hitos permiten validar resultados parciales, confirmar el cumplimiento de objetivos por etapa y establecer puntos formales de decisión antes de avanzar a la siguiente fase, reduciendo riesgos de desviación y reprocesos.

Tabla 44: *Hitos, entregables y responsables*

Hito	Entregable	Responsable	Fecha	Criterio de aceptación
Aprobación del plan de implementación	Plan de implementación validado	Gerencia de TI	Mes 1	Plan aprobado y comunicado a las áreas involucradas
Diagnóstico de riesgos completado	Informe de diagnóstico y matriz de riesgos	Seguridad de la Información	Mes 2	Riesgos priorizados y validados por las áreas técnicas
Controles y procedimientos definidos	Documentación de controles y procedimientos	Gestión de Cambios	Mes 3	Procedimientos aprobados y documentados
Controles operativos implementados	Evidencia de controles en operación	Operaciones de TI	Mes 4	Controles aplicados y registrados
KPIs y KRIs en seguimiento	Tablero de indicadores activo	Operaciones de TI	Mes 5	Indicadores generando reportes periódicos
Evaluación inicial y ajustes	Informe de evaluación y mejoras	Gerencia de TI	Mes 6	Resultados evaluados y acciones correctivas definidas

Fuente: Elaboración propia

Los hitos definidos aseguran el cumplimiento del plan al establecer entregables claros, responsables identificados y criterios objetivos de aceptación para cada etapa. Este esquema facilita el seguimiento del cronograma, la validación del avance y la toma de decisiones oportunas, contribuyendo a una implementación controlada y alineada con los objetivos de la propuesta.

6.7 PRESUPUESTO E IMPACTO DEL PRESUPUESTO

6.7.1 PRESUPUESTO

El presupuesto de la propuesta se plantea bajo un enfoque realista y sostenible, orientado a optimizar los recursos existentes de Banco Ficohsa y priorizar inversiones directamente relacionadas con la mitigación de riesgos, la mejora operativa y el fortalecimiento del control del software de cajeros automáticos. Este enfoque busca asegurar la viabilidad financiera de la implementación sin generar cargas innecesarias, alineando los costos con los beneficios esperados en cada fase del proyecto.

Tabla 45: *Presupuesto por rubro*

Rubro	Descripción	Cantidad	Costo unitario (USD)	Subtotal (USD)	Moneda Nacional LPS
Capacitación	Examen COBIT Foundation (personal clave) Ver Anexo 11	3	175	525	13,912.50
Análisis de riesgos	Licencia Intruder Essential (12 meses) Ver Anexo 12	12	149	1,788	47,382.00
Documentación de procesos	Elaboración y actualización de procedimientos y controles	1	1,200	1,200	31,800.00
Herramientas de monitoreo	PRTG 500 (12 meses) Ver Anexo 13	12	179	2,148	56,922.00
Seguimiento y evaluación	Actividades de seguimiento, revisión y mejora continua	1	1,000	1,000	26,500.00
			Total	**6,661.00**	**176,516.50**

Fuente: Elaboración propia

El presupuesto total de la propuesta asciende a $6,661.00 USD, lo que equivale a 176,516.50 LPS en moneda nacional. Este plan de inversión se ha diseñado bajo una premisa de eficiencia operativa, priorizando el fortalecimiento de las capacidades internas y la implementación de herramientas clave para el control del entorno de cajeros automáticos (ATM).

Beneficios estratégicos de acorde al presupuesto por rubro de la tabla 45:

- Mediante la propuesta se pretende internalizar conocimientos y reducir la dependencia de consultores externos.

- Identificar vulnerabilidades de seguridad de forma proactiva.

- Asegurar que el conocimiento sea institucional y no dependa de personas.

- Atacar directamente las caídas de servicio (uptime) de los ATM.

- Garantizar la mejora continua alineada con ITIL 4.

Análisis de valor y sostenibilidad:

Este presupuesto no representa solo un gasto, sino una inversión estratégica por las siguientes razones:

-Optimización de Recursos Existentes: Al capacitar al personal interno (3 exámenes de COBIT), el banco reduce la dependencia de consultorías externas a largo plazo, creando un centro de conocimiento interno.

-Mitigación de Riesgos Críticos: La inclusión de herramientas como Intruder y PRTG ataca directamente los puntos de falla más comunes en la gestión de software de cajeros: las vulnerabilidades de seguridad y las caídas de servicio (uptime).

-Bajo Impacto Financiero, Alto Impacto Operativo: Con una inversión cercana a los 180,000 LPS, el banco protege activos financieros y reputacionales críticos. La documentación de procesos (el rubro de inversión individual con 31,800.00 LPS) asegura que el conocimiento sea institucional y no dependa de personas específicas.

-Alineación con ITIL 4: El enfoque en "Seguimiento y evaluación" refleja el principio de Mejora Continua de ITIL, asegurando que los controles de riesgos para los cajeros automáticos se mantengan vigentes ante nuevas amenazas.

El presupuesto propuesto respalda la implementación por fases al asignar recursos específicos a cada etapa del cronograma, garantizando que las actividades críticas cuenten con el soporte necesario para su ejecución. Esta distribución permite controlar el gasto, evaluar el impacto de cada rubro y asegurar que la inversión contribuya de manera directa a la reducción de riesgos, la continuidad operativa y la sostenibilidad de la gestión del software de cajeros automáticos.

Evaluación de retorno de inversión:

La evaluación del Retorno de Inversión (ROI) se plantea como un mecanismo para determinar la conveniencia de mantener, renovar o escalar las soluciones implementadas. Dado que la propuesta está orientada a la reducción de riesgos, el ROI se analiza principalmente desde la perspectiva de costos evitados y mejoras operativas.

De forma conceptual, el ROI puede expresarse mediante la siguiente fórmula:

ROI (%) = (Beneficios obtenidos – Inversión total) / Inversión total × 100

En este contexto, los beneficios se reflejan en:

- Reducción de pérdidas económicas asociadas a indisponibilidad de cajeros automáticos.
- Disminución de incidentes de seguridad y posibles sanciones regulatorias.
- Ahorro en costos de atención de incidentes y soporte correctivo.
- Reducción de dependencia de servicios externos gracias al fortalecimiento del conocimiento interno.

Considerando que una sola interrupción significativa del servicio ATM o un incidente de seguridad puede generar pérdidas superiores al monto total de la inversión propuesta, el presupuesto de USD 6,661.00 se justifica ampliamente. Si la implementación logra evitar al menos un evento crítico anual o reducir de manera sostenida los tiempos de indisponibilidad, el retorno de inversión se vuelve positivo en el corto plazo, además de generar beneficios intangibles como mejora reputacional, confianza del cliente y madurez en la gestión de TI.

En consecuencia, el ROI de la propuesta no solo se mide en términos financieros directos, sino también en valor estratégico, resiliencia operativa y alineación con las mejores prácticas de COBIT 2019 e ITIL 4, consolidando una gestión del software de cajeros automáticos más segura, eficiente y sostenible para Banco Ficohsa.

6.7.2 IMPACTO DEL PRESUPUESTO

El impacto del presupuesto se analiza en función de su contribución directa a la mejora operativa, el fortalecimiento de la seguridad, el cumplimiento normativo y el aumento de la eficiencia en la gestión del software de cajeros automáticos. La inversión propuesta se orienta a generar resultados medibles que reduzcan riesgos críticos, optimicen la continuidad del servicio y respalden la toma de decisiones basada en evidencias.

Tabla 46: *Impacto esperado por área*

Área	Situación actual	Mejora esperada	Cómo se medirá	Indicador asociado
Operaciones de TI	Incidentes recurrentes y tiempos de recuperación elevados	Reducción de interrupciones y mejora en tiempos de respuesta	Seguimiento mensual de desempeño	MTTR del software ATM

Seguridad de la Información	Exposición a vulnerabilidades y parches tardíos	Disminución de riesgos críticos y mayor cobertura de parches	Revisión trimestral de controles	Cumplimiento de parches críticos
Cumplimiento normativo	Evidencias dispersas y controles no estandarizados	Mayor trazabilidad y soporte para auditorías	Resultados de auditoría interna	Índice de cumplimiento normativo
Gestión de servicios	Falta de métricas consolidadas para decisiones	Mejora en la visibilidad del desempeño del servicio	Análisis de reportes periódicos	Disponibilidad del software ATM
Dirección / Gerencia	Decisiones reactivas ante eventos críticos	Toma de decisiones preventiva y basada en indicadores	Revisión de tableros ejecutivos	KPIs/KRIs consolidados

Fuente: Elaboración propia

El costo de la propuesta se justifica por la reducción del riesgo operativo y de seguridad, así como por el incremento en la estabilidad y confiabilidad del software de cajeros automáticos. Al traducirse en mejoras medibles y sostenibles, la inversión permite disminuir pérdidas asociadas a incidentes, fortalecer el cumplimiento regulatorio y consolidar una gestión más eficiente y resiliente, alineada con los objetivos estratégicos del banco.

6.8 CONCORDANCIA DE LOS SEGMENTOS DE LA TESIS CON LA PROPUESTA

Tabla 47: *Concordancia De Los Segmentos De La Tesis Con La Propuesta*

Capítulo I			Capítulo II	Capítulo III			Capítulo V	Capítulo VI
Título de la Investigación	**Objetivo General**	**Objetivo Específicos**	**Teorías/Metodologías de sustento**	**Variables**	**Poblaciones**	**Técnicas**	**Conclusiones**	**Nombre de la Propuesta**
Propuesta De Análisis De Riesgos Con COBIT 2019 E ITIL 4 Para Optimizar La Gestión Del Software De Cajeros Automáticos En Banco Ficohsa	Desarrollar un análisis de riesgos basado en COBIT 2019 e ITIL 4 para proponer estrategias de mitigación en la gestión de software de cajeros automáticos optimizando la continuidad del servicio, asegurando el cumplimiento normativo y fortaleciendo la resiliencia operativa en Banco Ficohsa.	. Identificar las principales amenazas, vulnerabilidades y deficiencias en la gestión actual del software de cajeros automáticos de Banco Ficohsa, considerando los procesos, métricas y prácticas vigentes.	Teoría De La Cuarta Revolución Industrial	Amenazas y vulnerabilidades en la gestión del software de cajeros automáticos	Personal	Entrevista semiestructurada	En coherencia con el objetivo general de desarrollar un análisis de riesgos basado en COBIT 2019 e ITIL 4 para proponer estrategias de mitigación en la gestión del software de cajeros automáticos, se concluye que la situación actual del software ATM en Banco Ficohsa presenta una exposición de riesgo inaceptable, evidenciada en un Riesgo de Fraude Muy Alto (Media 4.75) y un Riesgo de Seguridad Informática Alto (Media 4.00). Este diagnóstico da cumplimiento al primer objetivo	Propuesta de fortalecimiento de la gestión de riesgos del software de cajeros automáticos mediante la integración de COBIT 2019 e ITIL 4

							específico, al identificar de manera clara las principales amenazas, vulnerabilidades y deficiencias que afectan al sistema, y pone de manifiesto la urgencia de adoptar un marco de gobernanza sólido como COBIT 2019 que priorice la seguridad, estandarice los controles y reduzca la probabilidad de pérdidas financieras y daños reputacionales	
		Evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 al análisis de riesgos y gestión de incidentes en el software de cajeros automáticos de Banco	Teoría general de sistemas	Aplicabilidad de COBIT 2019 e ITIL 4 en el análisis de riesgos y gestión de incidentes	Procesos	Observación directa	En relación con el segundo objetivo específico, orientado a evaluar la aplicabilidad y adaptación de los principios y prácticas de COBIT 2019 e ITIL 4 al análisis de riesgos y gestión de incidentes, los resultados	

		Ficohsa, con el fin de proponer acciones de mejora.					muestran que la causa raíz de la alta exposición y de la elevada frecuencia de incidentes (Media 3.75) es la inmadurez de los procesos de gestión de servicios, que operan bajo un enfoque predominantemente reactivo. La baja oportunidad en la aplicación de parches (Media 2.50) y la baja efectividad del monitoreo (Media 2.50) confirman que las vulnerabilidades no se previenen ni se detectan con la rapidez requerida, lo cual demuestra que COBIT 2019 e ITIL 4 resultan plenamente pertinentes para formalizar procesos, establecer controles estructurados y transformar el modelo actual hacia una gestión	

							más disciplinada y orientada al riesgo	
		Definir indicadores clave de desempeño (KPIs) y métricas de seguimiento que permitan evaluar la efectividad de las estrategias de mitigación propuestas y fomenten un ciclo de mejora continua en la gestión del software de cajeros automáticos.	Teoría De Alineación Estratégica Y Su Relación con COBIT 2019 e ITIL 4	Efectividad de estrategias de mitigación	Marcos de Referencia	Análisis documental	Vinculado con el tercer objetivo específico, que busca definir indicadores clave de desempeño y métricas de seguimiento para evaluar la efectividad de las estrategias de mitigación, los hallazgos evidencian una falla sistémica en el control y la gestión del conocimiento, expresada en la ausencia de un estándar definido de software, la carencia de una logística clara para el patch management y la falta de documentación histórica de incidentes (75 por ciento de respuestas negativas o inciertas). Esta situación limita la capacidad del banco para medir	
		Diseñar un modelo integrado de gestión basado en COBIT 2019 e ITIL 4 que fortalezca la administración del software de cajeros automáticos y responda de manera efectiva a los requisitos del		Modelo integrado de gestión				

		entorno financiero actual.					con precisión la disponibilidad, la frecuencia de incidentes, la oportunidad en la aplicación de parches y la efectividad del monitoreo, lo que refuerza la necesidad de implementar KPIs de riesgo y desempeño alineados con COBIT 2019 e ITIL 4 que permitan alimentar un ciclo de mejora continua en la gestión del software ATM	
		Identificar y analizar los beneficios que Banco Ficohsa podría obtener a futuro al implementar la propuesta de análisis de riesgos basada en COBIT 2019 e ITIL 4 para la optimización del software de cajeros automáticos.		Beneficios de la implementación del modelo de gestión.			Finalmente, en correspondencia con el cuarto y quinto objetivos específicos, relacionados con el diseño de un modelo integrado de gestión basado en COBIT 2019 e ITIL 4 y con la identificación de los beneficios que obtendría Banco Ficohsa al implementar la propuesta, se	

							concluye que la integración de ambos marcos se encuentra plenamente validada por el personal experto consultado. Las demandas reiteradas de "mejora en los procesos", "lograr que cumplan con un estándar" y la necesidad de automatizar la "configuración remota" muestran que la solución estratégica reside en articular COBIT 2019 para la gobernanza y los estándares, e ITIL 4 para la formalización de las prácticas operacionales. Con ello se confirma que el modelo propuesto contribuye a optimizar la continuidad del servicio, fortalecer la resiliencia operativa, mejorar el cumplimiento regulatorio y	

							generar beneficios tangibles para la gestión del software de cajeros automáticos en Banco Ficohsa	

Fuente: Elaboración propia

REFERENCIAS BIBLIOGRÁFICAS

Adame, H., Popoola, O., Akinoso, A., & Okeke, C. (2024). Marcos Teóricos Que Respaldan La Alineación De La Estrategia De Ti Y La Estrategia Empresarial Para Una Ventaja Competitiva Sostenida. Revista Internacional de Investigación en Gestión y Emprendimiento, 6(4), 1273-1287. doi:https://doi.org/10.51594/ijmer.v6i4.1058

Adane, M., Wale, T., & Meried, E. (2021). Factores determinantes del despliegue de cajeros automáticos en los bancos comerciales de Etiopía. Heliyon, 7(8), 1-20. doi:https://doi.org/10.1016/j.heliyon.2021.e07712

Al-Bassam, S., & Al-Alawi, A. (2022). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. Reserchgate, 2(5), 1-20. doi:https://www.researchgate.net/publication/337086201_The_Significance_of_Cybersecurity_System_in_Helping_Managing_Risk_in_Banking_and_Financial_Sector

Alonge, E., Eyo, N., & Ubanadu, B. (2021). Digital Transformation in Retail Banking to Enhance Customer Experience and Profitability. Iconic Research And Engineering Journals, 4(9), 169-188. doi:https://www.researchgate.net/publication/390111527_Digital_Transformation_in_Retail_Banking_to_Enhance_Customer_Experience_and_Profitability

Arnold, M., & Osorio, F. (2022). Introducción a los Conceptos Básicos de la Teoría General de Sistemas. ResearchGate, 1(8), 1-20. doi:https://www.researchgate.net/publication/28060003_Introduccion_a_los_Conceptos_Basicos_de_la_Teoria_General_de_Sistemas

AXELOS. (2019). ITIL 4 Foundation. TSO.

Ballesteros, L., Vera, R., & Román, F. (2024). Teoría General De Sistemas, . Uleam Magazine, 5(2), 1-9. doi:https://doi.org/10.56124/ubm.v5i9.010

Banco Central de Honduras. (2024). Informe de Estabilidad Financiera. Retrieved from https://www.bch.hn/estadisticos/EF/LIBINFORMEEF/IEF%20diciembre%202024.pdf

Banco Ficohsa. (Diciembre de 2025). Obtenido de https://ficohsamundocorporativo.com/ficohsa-consolida-su-liderazgo-en-honduras-al-cierre-de-2025/

Basel Committee on Banking Supervision. (2022). International Convergence of Capital Measurement and Capital Standards: A Revised Framework. . Bank for International Settlements.

Batiz, B., Bautista, M., & González, I. (2021). La transformación en el uso de efectivo y pagos digitales durante la pandemia de la Covid-19. Papeles De Economía Española, 5(2), 1-20. doi:https://www.researchgate.net/publication/358621938_La_transformacion_en_el_uso_de_efectivo_y_pagos_digitales_durante_la_pandemia_de_la_Covid-19

Bujalance, S., & Trillo, M. (2025). El declive del dinero en efectivo: perspectivas y desafíos. Revista de Estudios Andaluces, 5(2), 1-20. doi:https://doi.org/10.12795/rea.2025.i49.03

Cabrera, H., Rodríguez, B., González, L., & Medina, A. (2020). Ideas y conceptos básicos para la comprensión de las industrias 4.0. Revista Universidad y Sociedad, 12(4), 1-20. doi:http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202020000400008

CNBS. (2020). Sistema Financiero Hondureño. Obtenido de https://www.cnbs.gob.hn/sitios-relacionados-enlaces-de-interes/

CNBS. (2021, Mayo). Reporte de Inclusión Financiera en Honduras. Retrieved from CNBS: https://www.cnbs.gob.hn/inclusion-financiera/wp-content/uploads/2023/05/Reporte-de-Inclusion-Financiera-2021.pdf

CNBS. (2024). Promoviendo un entorno Fintech seguro e inclusivo. Retrieved from https://www.cnbs.gob.hn/hub-de-innovacion-financiera-de-honduras/

Comisión Europea. (2025). Directiva SRI 2: asegurar las redes y los sistemas de información. Retrieved

from Comisión Europea: https://digital-strategy.ec.europa.eu/es/policies/nis2-directive
Cortés, F., & Iglesias, M. (2004). Metodología de la investigación: fundamentos y aplicaciones. Editorial Trillas.
Dapp, T. (2022). Fintech: The Digital Transformation in the Financial Sector. ResearchGate, 5(3), 189-199. doi:https://doi.org/10.1007/978-3-319-54603-2_16
De Haes, S., van Grembergen, W., Joshi, A., & Huygh, T. (2019). Enterprise Governance of Information Technology: Achieving Alignment and Value in Digital Organizations. Springer. doi:https://doi.org/10.1007/978-3-030-25918-1
Deming, W. E. (2000). The New Economics for Industry, Government, Education. MIT Press.
Federal Bureau of Investigation. (2020). Biometric Identification and Security.
Federal Reserve Bank of Atlanta. (2020). Payments Research: What Is an ATM?
FELABAN. (2018, Octubre 18). Los Servicios Financieros Digitales en América Latina. Retrieved from FELABAN: https://felaban.com/los-servicios-financieros-digitales-en-america-latina/
Gaol, F., Prabowo, H., & Purwandari, B. (2022). Digital Banking: Challenges, Emerging Technology Trends, and Future Research Agenda. International Journal of E-Business Research, 18(1), 1-20. doi:https://doi.org/10.4018/IJEBR.309398
Gartner, I. (2020). Gartner Glossary: Digitalization.
Gil, A., Gamboa, P., & De los Santos, A. (2025). La gestión de servicios de TI como determinante en la experiencia del cliente en e-Business. Ingeniería Investiga , 5(2), 1-20. doi:https://doi.org/10.47796/ing.v7i00.1216
Graglia, I. (2024, agosto 6). COBIT e ITIL: una comparación exhaustiva de los marcos más famosos de IT. Retrieved from Invgate: https://blog.invgate.com/es/cobit-e-itil
Gregorio Rojas, J. (2023). Metodología de la investigación: fundamentos, procesos y aplicaciones. Editorial Académica.
Gutiérrez, M. (2023). Impacto de las fintech en la banca tradicional. Retrieved from Facultad de Ciencias Económicas y Empresariales : https://repositorio.comillas.edu/rest/bitstreams/619310/retrieve
Hernández Sampieri, R., & Mendoza Torres, C. (2018). Metodología de la investigación. Mcgraw-Hill Interamericana Editores, S.A. de C. V. doi:ISBN: 978-1-4562-6096-5
Hernández, J. (2021). El sector financiero en África. Boletín económico de ICE, 5(2), 53-67. doi:https://dialnet.unirioja.es/servlet/articulo?codigo=7954542
Hurtado, J. (2010). Metodología de la investigación: guía para la comprensión holística. Editorial Quirón.
IFC. (2020). Análisis De Datos Y Servicios financieros Digitales. Obtenido de https://documents1.worldbank.org/curated/en/428771531296328405/pdf/Data-analytics-and-digital-financial-services-handbook.pdf
Ilori, O., Naiho, H., & Nwosu, N. (2024). Una revisión exhaustiva de la gobernanza de TI: Implementación efectiva de los marcos COBIT e ITIL en instituciones financieras. Revista de Investigación en Ciencias de la Computación y Tecnologías de la Información, 5(6), 1391-1407. doi:https://doi.org/10.51594/csitrj.v5i6.1224
Innowise. (2025). La banca digital en 2025: 12 tendencias para adelantarse. Innowise, 5(2), 1-20. doi:https://innowise.com/es/blog/digital-banking-trends/
ISACA. (2019). Framework: Introduction and Methodology. ISACA.
ISO/IEC. (2018). ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.
Josepht, W., & Fred, T. (2025). Cybersecurity in Digital Transactions. Retrieved from ResearchGate: https://www.researchgate.net/publication/389376591_Cybersecurity_in_Digital_Transactions
Kalms, M. (2018). ATM Software: The Next Generation. RBR.
Kaplan, R. S., & Norton, D. P. (1996). The Balanced Scorecard: Translating Strategy into Action. Harvard Business Press.

Kaspersky News. (2024). El malware de los cajeros automáticos de la UE ataca los cajeros automáticos. Obtenido de https://b2b-cyber-security.de/es/eu-atm-malware-greift-geldautomaten-an/
Mordor Intelligence. (2024). Tamaño y participación del mercado de bancos retadores en Asia-Pacífico. Retrieved from https://www.mordorintelligence.ar/industry-reports/challenger-banks-in-asia-pacific
Muñiz, L., Loor, V., & Cedeño, J. (2021). El Aporte De Los Corresponsales No Bancarios (CNB) A La Inclusión Financiera. Revista Publicando, 8(31), 303-319. doi:https://doi.org/10.51528/rp.vol8.id2252
National Institute of Standards and Technology . (2020). SP 800-207: Zero Trust Architecture.
NFC Forum. (2020). What Is NFC?
NIST. (2018). Glossary of Key Information Security Terms. NISTIR .
NQA. (2024). ISO 27001:2022 Guía De Implementación De Sistemas De Gestión De Seguridad De La Información. Retrieved from https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf
Nwoke, J. (2024). Digital Transformation in Financial Services and FinTech: Trends, Innovations and Emerging Technologies. International Journal of Finance, 9(6), 1-24. doi:https://doi.org/10.47941/ijf.2224
Ojeda, F., Moreno, V., & Torres, M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología, 6(2), 192-219. doi:10.35381/cm.v6i2.366
Ortega, F., Ramírez, T., & Zúgiña, G. (2022). El sistema financiero y el rol en el desarrollo económico y social del Ecuador. Digital Publisher, 7(6), 49-64. doi:doi.org/10.33386/593dp.2022.6.1367
Peña-Casanova, M., & Anias-Calderón, C. (2020). Integración de marcos de referencia para gestión de Tecnologías de la Información. Ingeniería Industria, 52(3), 1-13. doi:https://www.redalyc.org/journal/3604/360464918003/360464918003.pdf
Rivera, C., Rivera, J., & Estévez, I. (2022). La cuarta revolución industrial: una revisión teóricaThe fourth industrial revolution: a theoretical revision. Revista Interdisciplinaria de Ingeniería Sustentable y Desarrollo Social, 3(1), 250-257. doi:https://doi.org/10.63728/riisds.v3i1.314
Rodríguez, E., Espinosa, I., Mendoza, V., & Quirós, D. (2023). Factores de riesgo asociados a trastornos temporomandibulares. Revista Cubana de Estomatología, 50(4), 1-20. doi:http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0034-75072013000400004
Salinas, R., & Cárdenas, J. (2009). Enfoques y alcances de la investigación científica. Universidad Autónoma de Nuevo León.
Sommerville, I. (2016). Ingeniería de software.
Sundas, A., Contreras, I., Mujahid, O., Beneyto, A., & Vehi, J. (2024). Efectos de los factores ambientales en la salud humana general: una revisión exploratoria. Healthcare, 12(21), 1-20. doi:https://doi.org/10.3390/healthcare12212123
The Open Group. (2011). The TOGAF® Standard, Version 9.2: A Pocket Guide. Van Haren Publishing.
Valora Analitik. (2024, Febrero 25). Ciberdelitos financieros han aumentado 400 %: ¿cómo enfrentarlos? Retrieved from Valora Analitik: https://es-us.finanzas.yahoo.com/noticias/ciberdelitos-financieros-aumentado-400-enfrentarlos-010000108.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAHRZb6IXejvb7JrENQOrQqXYfXsEsoh-JJ9vzU5ZBUmWk7Mpk50akdqHhoq3jGm_P
Vargas, A. (2021). La banca digital: Innovación tecnológica en la inclusión financiera en el Perú. Producción y Gestión, 5(2), 1-20. doi:https://doi.org/10.15381/idata.v24i2.20351
Vergara, E., & Diao, H. (2024, Noviembre 28). De la ficción a la realidad: cómo América Latina se convirtió en el campo de batalla cibernético más crítico del mundo. Retrieved from América

Latina y El Caribe: https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe
Whtiman, M., & Mattord, H. (2022). Principios de seguridad de la información. Information Security.
Wolrd Bank . (2020). Creando Mercados En Honduras. Retrieved from Wolrd Bank Group: https://documents1.worldbank.org/curated/en/099047208052233600/pdf/IDU-4380ac03-8c9a-4143-81cf-12a62abf1bbb.pdf
Yarosh, D. (2023, febrero 2). Cybersecurity en la banca: importancia, amenazas y desafíos. Retrieved from Innowise: https://innowise.com/es/blog/cybersecurity-in-banking/

ANEXOS

SECCIÓN 1: AUTORIZACIONES

ANEXO 1: CARTA DE AUTORIZACIÓN DE LA EMPRESA O INSTITUCIÓN

unitec
Facultad de Postgrado

unitec

CARTA DE AUTORIZACIÓN DE LA EMPRESA O INSTITUCIÓN

Nombre y apellido del Director o Gerente: Arlex Reyes Castro
Puesto Laboral: Gerente General Medios de Pago
Empresa o Institución: Banco Ficohsa
Dirección principal de la Empresa o Institución:
Bulevard Francia, Colonia Las Colinas, Contiguo a Diunsa.
Ciudad: Tegucigalpa Departamento: Francisco Morazán Día: 07 Mes: 08 Año: 2025

Estimado Señor(a): Arlex Reyes Castro

Reciba un cordial y atento saludo. Por medio de la presente deseamos solicitar su apoyo, dado que somos alumnos de UNITEC y nos encontramos desarrollando el Trabajo de Tesis previo a obtener nuestro título de maestría en Gestión de Tecnologías de la Información
Hemos seleccionado como tema Propuesta de Analisis de Riesgos con COBIT 2019 E ITIL4 Para Optimizar la Gestion de Soft por lo que estaríamos muy agradecidos de contar con el apoyo de la empresa que usted representa para poder desarrollar nuestra investigación. En particular, dicha solicitud se circunscribe a peticionar que se nos autorice a realizar: Entrevistas, encuestas a personal seleccionado del area medios de Pago.
(encuestas, sondeos, etc).

A la espera de su aprobación, me suscribo de Usted.

Atentamente,

- Jaime Oscar Molina Ordoñez
Firma, nombre y apellidos
No. de cuenta: 12413232

- Jean Carlo Núñez Ramirez
Firma, nombre y apellidos
No. de cuenta: 12413160

Por este medio, Banco Ficohsa
(empresa / institución),
Autoriza la realización dentro de sus instalaciones o del uso de información de la empresa en el proyecto de investigación de Tesis de Postgrado antes mencionado.

Arlex Reyes Castro
(Nombre y sello del Director / Gerente)

Vo Bo

arlex.reyes@ficohsa.com
Correo electrónico de Director/Gerente

SECCIÓN 2: INSTRUMENTOS TEMÁTICOS

ANEXO 2: COBIT PERFORMANCE MANAGEMENT (CPM)

Práctica	Actividad	Nivel de Capacidad COBIT	Nivel de Capacidad BANCO FICOHSA	JUSTIFICACIÓN (Breve comentario que explica por qué asignó ese nivel de capacidad)

ANEXO 3: SERVICE VALUE CHAIN (SVC) ITIL 4

Flujo de Valor: “Nombre del proceso que se evaluará”

Entada/Salida	Actividad Clave (SVC)	Práctica(s)	Rol	Actividad
Demanda	Obtener y construir			
	Diseño y transición			
	Transición			
	Entrega y soporte			
	Producto y servicio			
Valor				

ANEXO 4: LISTA DE VERIFICACIÓN ITIL 4

CHECKLIST DE PRACTICAS ITIL 4 – GESTIÓN DE SOFTWARE CAJEROS AUTOMÁTICOS

N°	Práctica ITIL 4	Descripción	Cumple (Sí/No)	Observaciones

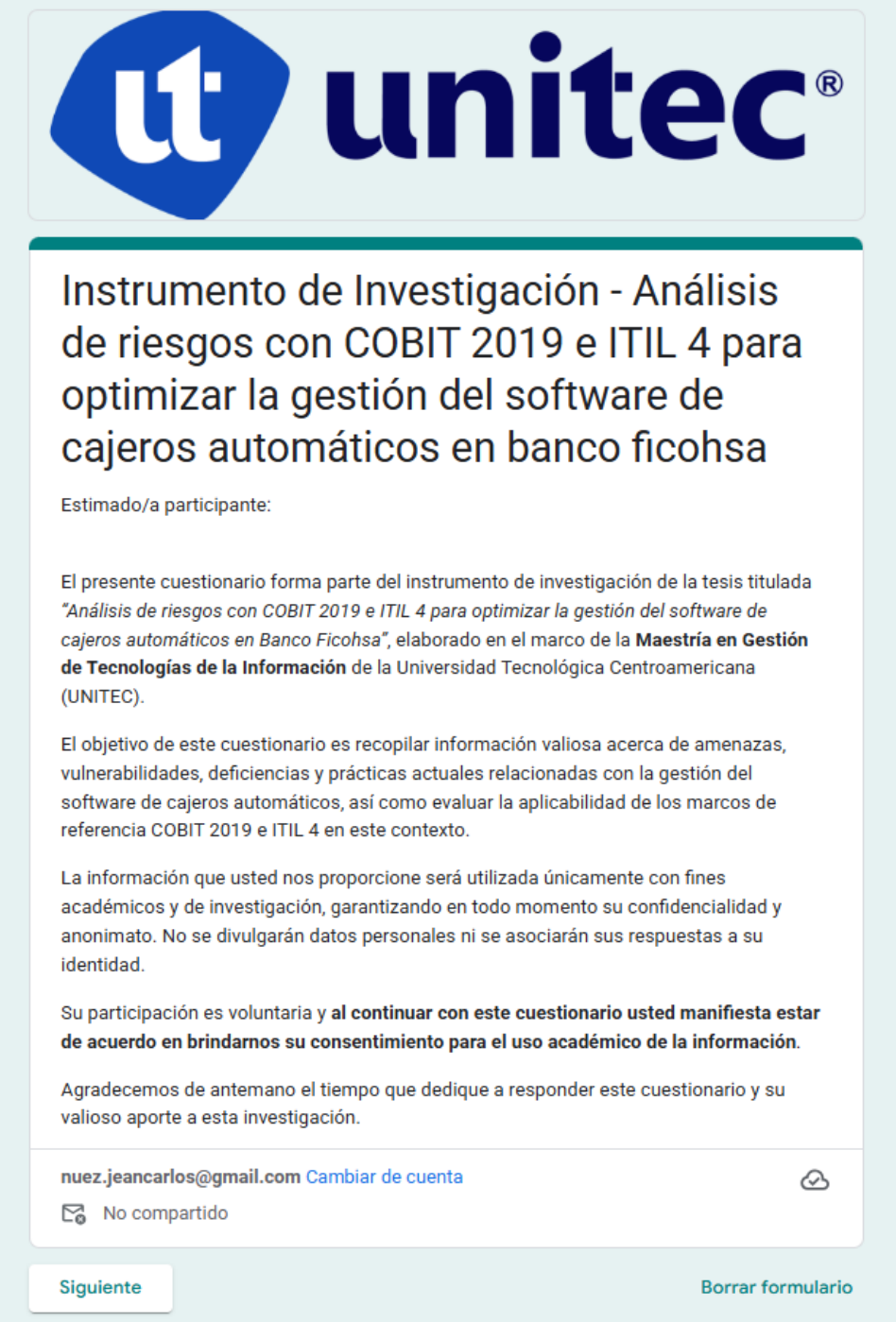
SECCIÓN 3: INSTRUMENTOS METODOLÓGICOS

ANEXO 5: MATRIZ DE ANÁLISIS DOCUMENTAL

N°	Año	Autores	Título	Tipo de recurso	Referencia

ANEXO 6: CUESTIONARIO SEMIESTRUCTURADO

Para acceder al cuestionario puede ingresar a la siguiente dirección https://docs.google.com/forms/d/e/1FAIpQLSe76B4LnGKDbvsez5TXD8ye83PF6FRwj2WBcb9fgRoCNWN_SA/viewform?usp=header



unitec®

Instrumento de Investigación - Análisis de riesgos con COBIT 2019 e ITIL 4 para optimizar la gestión del software de cajeros automáticos en banco ficohsa

Estimado/a participante:

El presente cuestionario forma parte del instrumento de investigación de la tesis titulada *"Análisis de riesgos con COBIT 2019 e ITIL 4 para optimizar la gestión del software de cajeros automáticos en Banco Ficohsa"*, elaborado en el marco de la **Maestría en Gestión de Tecnologías de la Información** de la Universidad Tecnológica Centroamericana (UNITEC).

El objetivo de este cuestionario es recopilar información valiosa acerca de amenazas, vulnerabilidades, deficiencias y prácticas actuales relacionadas con la gestión del software de cajeros automáticos, así como evaluar la aplicabilidad de los marcos de referencia COBIT 2019 e ITIL 4 en este contexto.

La información que usted nos proporcione será utilizada únicamente con fines académicos y de investigación, garantizando en todo momento su confidencialidad y anonimato. No se divulgarán datos personales ni se asociarán sus respuestas a su identidad.

Su participación es voluntaria y **al continuar con este cuestionario usted manifiesta estar de acuerdo en brindarnos su consentimiento para el uso académico de la información**.

Agradecemos de antemano el tiempo que dedique a responder este cuestionario y su valioso aporte a esta investigación.

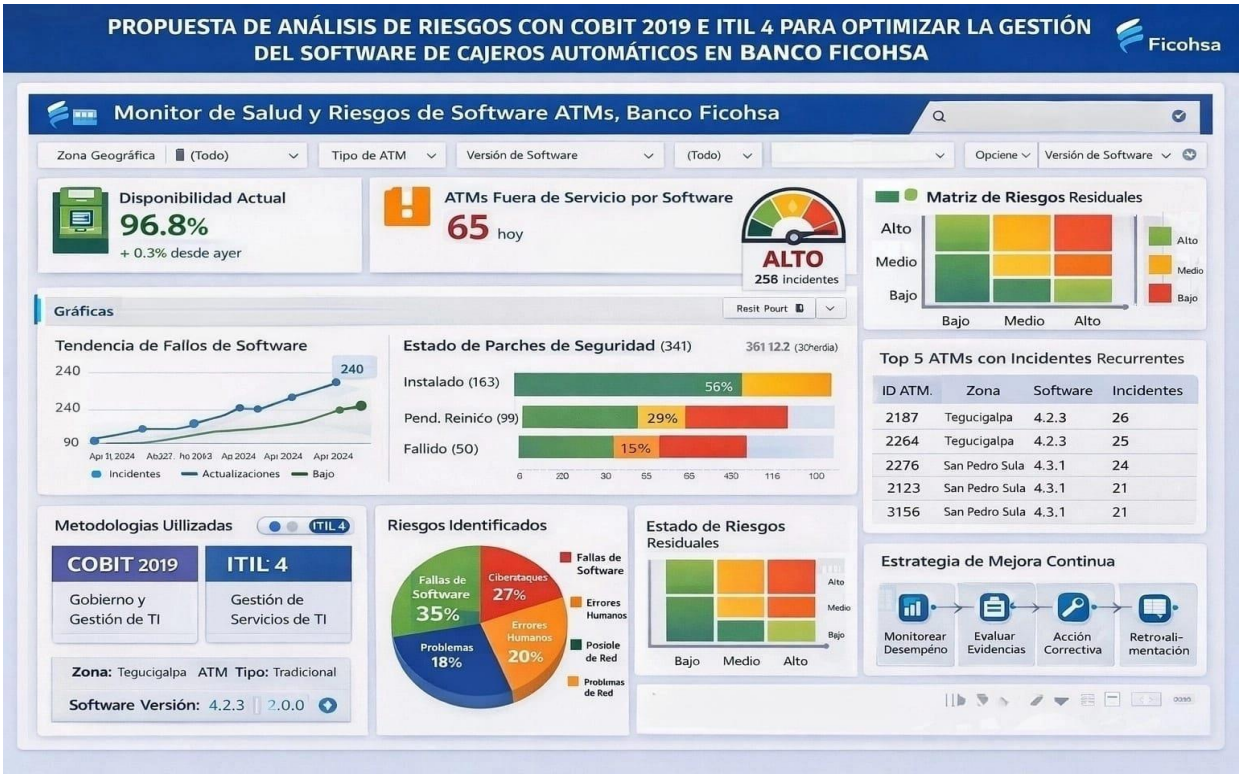
nuez.jeancarlos@gmail.com Cambiar de cuenta

No compartido

Siguiente

Borrar formulario

ANEXO 7: DASHBOARD DE INDICADORES DE SEGUIMIENTO



ANEXO 8: REPORTE DE DESEMPEÑO

Reporte de Desempeño del Software de Cajeros Automáticos
Banco Ficohsa
Periodo de evaluación:
Responsable:
Fecha de Generación:
Indicadores de Rendimiento (KPIs)

Categoría	KPI	Descripción	Valor Actual	Meta	Desviación	Acciones Correctivas
Disponibilidad	Tiempo de actividad (Uptime)					
	Tiempo de inactividad (Downtime)					
Seguridad	Incidentes de seguridad reportados					
	Vulnerabilidades críticas resueltas					
Eficiencia	Tiempo promedio de transacción					
	Tasa de errores en transacciones					
Cumplimiento	Cumplimiento de normativas internas					
	Cumplimiento de regulaciones externas					

ANEXO 9: FORMATOS DE SEGUIMIENTO

Formatos de Seguimiento - Gestión de Software de Cajeros Automáticos
Instrucciones de Uso:

1. Registro de Actividades: Utiliza esta hoja para documentar todas las actividades relacionadas con la gestión del software (actualizaciones, mantenimiento, etc.).
2. Registro de Incidentes: Aquí se registran los problemas o fallos detectados en los cajeros automáticos, junto con su seguimiento.
3. Acciones Correctivas: Documenta las acciones tomadas para resolver incidentes o mejorar procesos.
4. Indicadores de Gestión: Mide el desempeño de la gestión del software utilizando métricas clave (por ejemplo, tiempo de resolución de incidentes, disponibilidad del sistema, etc.).

Registro de Actividades

Banco Ficohsa
Periodo de seguimiento:
Responsable:
Versión:
Última actualización:

ID Actividad	Descripción de la Actividad	Fecha de Ejecución	Responsable	Estado (Completada/ En Proceso/Pendiente)	Observaciones

Registro de Incidentes

Banco Ficohsa
Periodo de seguimiento:
Responsable:
Versión:
Ultima actualización:

ID Incide	Descripción del Incidente	Fecha de Reporte	Prioridad (Alta/Med	Estado (Resuelto/En	Acciones Tomadas	Responsable	Fecha de Resolución

nte			ia/Baja)	Proceso/Pendiente)			

Acciones Correctivas

Banco Ficohsa
Periodo de seguimiento:
Responsable:
Versión:
Ultima actualización:

ID Acción	Descripción de la Acción Correctiva	Fecha de Implementación	Responsable	Estado (Completada/En Proceso/Pendiente)	Resultado Esperado	Observaciones

Indicadores de Gestión

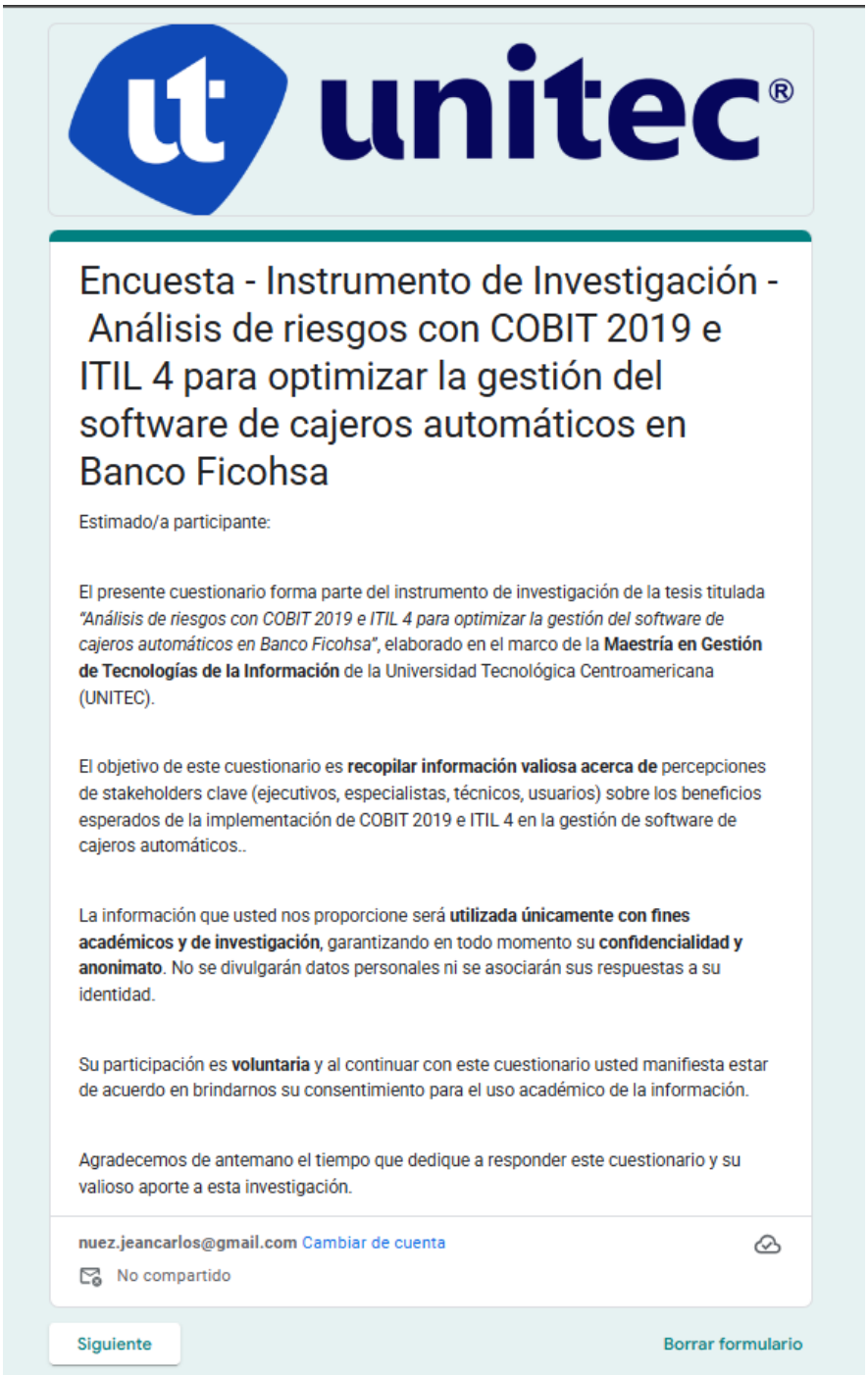
Banco Ficohsa
Periodo de seguimiento:
Responsable:
Versión:

Indicador	Descripción	Fecha de Medición	Valor Obtenido	Meta	Desviación	Acciones de Mejora

Ultima actualización:

ANEXO 10: ENCUESTA

Para acceder a la encuesta puede ingresar a la siguiente dirección https://docs.google.com/forms/d/e/1FAIpQLSf7xR4VNhSGopqdbmQ6vMXqR4v4xFyYTaluQsX8fkaACyLCOA/viewform?usp=header



unitec®

Encuesta - Instrumento de Investigación - Análisis de riesgos con COBIT 2019 e ITIL 4 para optimizar la gestión del software de cajeros automáticos en Banco Ficohsa

Estimado/a participante:

El presente cuestionario forma parte del instrumento de investigación de la tesis titulada *"Análisis de riesgos con COBIT 2019 e ITIL 4 para optimizar la gestión del software de cajeros automáticos en Banco Ficohsa"*, elaborado en el marco de la **Maestría en Gestión de Tecnologías de la Información** de la Universidad Tecnológica Centroamericana (UNITEC).

El objetivo de este cuestionario es **recopilar información valiosa acerca de** percepciones de stakeholders clave (ejecutivos, especialistas, técnicos, usuarios) sobre los beneficios esperados de la implementación de COBIT 2019 e ITIL 4 en la gestión de software de cajeros automáticos..

La información que usted nos proporcione será **utilizada únicamente con fines académicos y de investigación**, garantizando en todo momento su **confidencialidad y anonimato**. No se divulgarán datos personales ni se asociarán sus respuestas a su identidad.

Su participación es **voluntaria** y al continuar con este cuestionario usted manifiesta estar de acuerdo en brindarnos su consentimiento para el uso académico de la información.

Agradecemos de antemano el tiempo que dedique a responder este cuestionario y su valioso aporte a esta investigación.

nuez.jeancarlos@gmail.com Cambiar de cuenta

No compartido

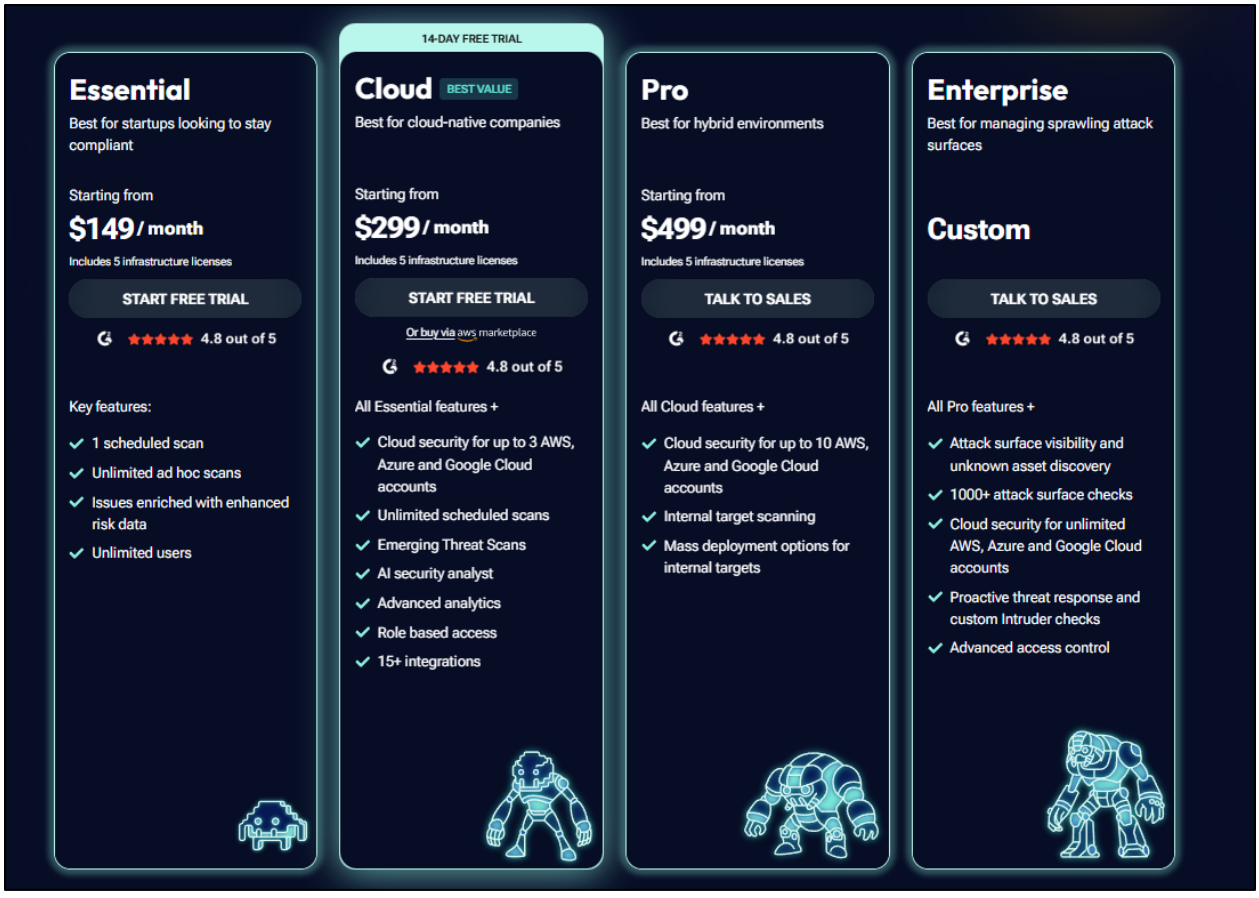
Siguiente

Borrar formulario

SECCIÓN 4: COTIZACIONES

ANEXO 11: CAPACITACIÓN COBIT 2019 E ITIL 4

ANEXO 12: ANÁLISIS DE RIESGOS



ANEXO 13: HERRAMIENTAS DE MONITOREO