UNIVERSIDAD IBEROAMERICANA

Estudios con Reconocimiento de Validez Oficial por Decreto Presidencial
Del 3 de abril de 1981

“Propuesta Metodológica para Incidir en el Sector Financiero Ocasionado por los Ciberataques”

TESIS

Que para obtener el grado de

MAESTRÍA EN GOBIERNO DE TECNOLOGÍA DE LA INFORMACIÓN

P r e s e n t a

LIC. ALBERTO PANTOJA SOSA

DRA. LUZ MARÍA CASTAÑEDA DE LEÓN

Ciudad de México, 2025

IBERO

Contenido

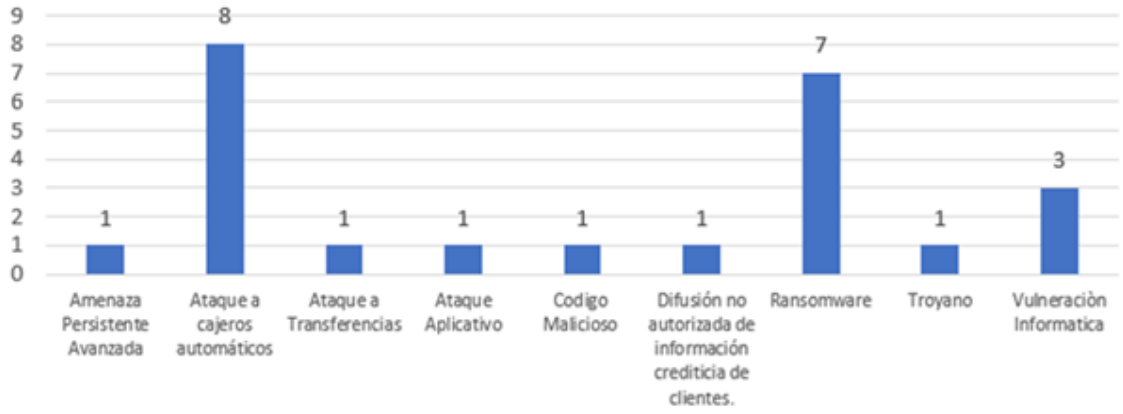
1. Descripción del problema y la situación actual

El Banco de México (BdeM) en el año 2023 reportó una creciente del doble de riesgos de ciberseguridad con respecto al año 2022 y pérdidas multimillonarias, lo cual detona una alerta en el sector financiero mexicano y motivo para el desarrollo de este trabajo de investigación. Datos obtenidos del "Banco de México. *Reporte de estabilidad financiera 2024"*

El Banco de México (BdeM) informa en: "Reporte de incidentes cibernéticos ocurridos en 2024 en el sistema financiero nacional que han sido reportados al Banco de México" se cometieron cuatro ciberataques al sistema financiero en México, tres a bancos y uno a una sociedad financiera popular (SOFIPO), que generaron pérdidas de cientos de millones de pesos. Para evitar estas afectaciones es urgente la implementación de medidas de protección en ciberseguridad y gobierno de TI que protejan a las instituciones financieras.

El informe del BdeM indica que los cuatro ciberataques NO tuvieron repercusiones para los clientes y éstos se presentaron en los meses de marzo, abril, noviembre y diciembre del 2024, respectivamente.

En el :"Reporte de incidentes cibernéticos ocurridos en 2020-2024 en el sistema financiero nacional que han sido reportados al Banco de México" encontramos que las principales amenazas de ciberseguridad son: los códigos maliciosos (malware), el secuestro de información a cambio del pago de rescates (ransomware), amenaza persistente avanzada (APT) y ataque a cajeros automáticos, tal como lo muestra la siguiente imagen:



Pantoja, A. *Principales incidentes cibernéticos relevantes en el sistema financiero mexicano en los últimos cinco años* [Imagen desarrollada a partir de datos del Banco de México].

La imagen nos muestra que el ataque a los cajeros automáticos tiene la mayor cantidad de ataques registrados y el Ransomware ocupa el segundo lugar, estos datos nos indican una tendencia que podemos considerar para priorizar los esfuerzos para minimizar y/o mitigar las afectaciones por este tipo de ciberataques.

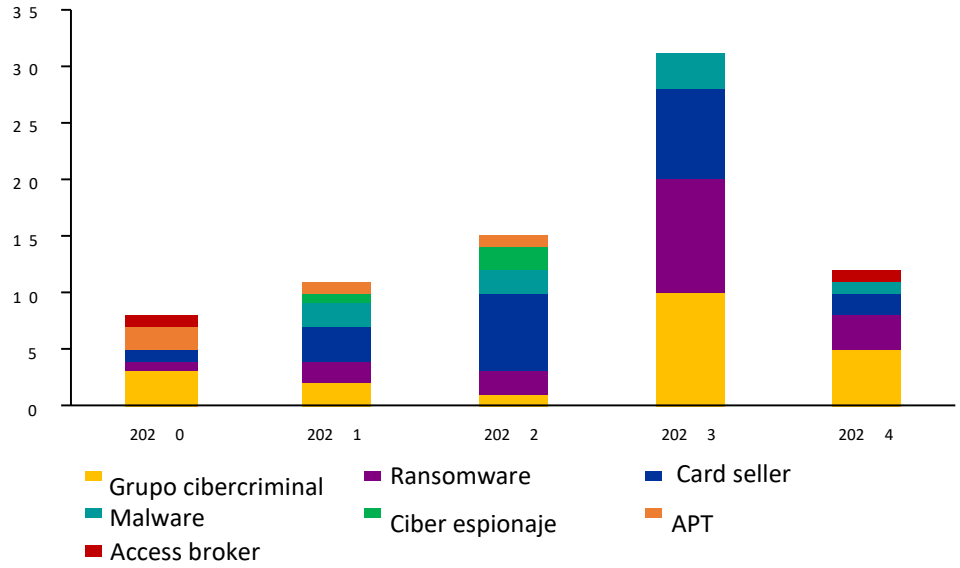
Tal como se muestra documentado en los "Reporte de Incidentes cibernéticos ocurridos en 2020-2024 en el sistema financiero nacional que han sido reportados al Banco de México" encontramos que los principales ciberataques que han generado impacto en los últimos cinco años son los siguientes:

- 2020-Ransomware identificados en los incidentes fueron: MedusaLocker, Sodinokibi, Crysis/Phobos y Emotet
- 2021- Ransomware identificado en el incidente fue: Revil, también conocido como Sodinokibi.
- 2022- Amenaza persistente avanzada.
- 2023 -Vulneración informática del servicio de transferencias a través de un código malicioso no identificado.
- Vulneración informática a través de un código malicioso de tipo troyano identificado perteneciente a la familia "Prometei".
- Vulneración informática a través de un código malicioso de tipo ransomware identificado fue "BlackCat".
- 2024-Vulneración informática del servicio de transferencias a través de un código malicioso "Akira".

Otro dato importante que encontramos en los "Reporte de Incidentes cibernéticos ocurridos en 2020-2024 en el sistema financiero nacional que han sido reportados al Banco

de México" es la cuantificación de $1,168.98 millones de pesos de afectación a las instituciones financieras en México y cabe destacar que hay ataques de los cuales no se cuenta con el dato preciso del monto de la afectación, por lo tanto, la cuantificación del monto es aún mayor.

En base a la información del Banco de México "Banco de México. (2024). *Reporte de estabilidad financiera 2024"* muestra la siguiente gráfica con respecto a los riesgos de ciberataques en los últimos cinco años:



Banco de México. (2024). *Reporte de estabilidad financiera 2024* [Imagen del índice de riesgo de ciberataques en México]. https://www.banxico.org.mx

La gráfica muestra un crecimiento importante de los riesgos en el año 2023 por lo que se deben de tomar acciones inmediatas para evitar que esto siga teniendo una tendencia de crecimiento continuo, en el año 2024 se identifica una baja de estas amenazas.

la disminución observada en las amenazas de ciberseguridad durante 2024 se explica principalmente por diferentes factores estratégicos y operativos que fortalecieron la postura del sistema financiero mexicano frente a estos riesgos como fueron:

1. Fortalecimiento de capacidades de inteligencia y monitoreo. El Banco de México y las instituciones financieras promovieron la maduración de sus capacidades de inteligencia, incluyendo el intercambio continuo de información sobre amenazas, vulnerabilidades e incidentes. Este esfuerzo sistemático permitió anticipar ataques y robustecer los mecanismos de prevención y contención.

2. Incremento en la concientización del personal y alta dirección. Se reforzaron las estrategias de formación y sensibilización, integrando a la alta dirección en la cultura de

ciberseguridad. Esto facilitó una respuesta más efectiva ante eventos y mayor alineación organizacional.

3. Simulacros y ejercicios de validación. Durante 2024, se llevaron a cabo ejercicios de simulación de incidentes cibernéticos, incluyendo escenarios de interrupción de servicios y ataques complejos. Estos simulacros contribuyeron a mejorar la capacidad de reacción y la preparación de los equipos responsables.

4. Protocolos de respuesta activados oportunamente. Aunque se reportaron dos incidentes relevantes, la activación de protocolos de respuesta por parte del Grupo de Respuesta a Incidentes Sensibles de Seguridad de la Información (GRI) evitó impactos económicos significativos y redujo la exposición de los clientes.

5. Regulación y vigilancia permanente. El cumplimiento regulatorio y la vigilancia digital constante, incluso en el contexto de conflictos geopolíticos, ayudaron a contener amenazas que en otros países tuvieron más incidencia. México mantuvo un nivel de alerta “Amarillo”, sin afectaciones sistémicas atribuibles a estos conflictos.

6. Disminución en la visibilidad mediática de eventos. El índice de riesgo se construye parcialmente con base en publicaciones y reportes especializados; la baja en incidentes notables y la mejora en prevención contribuyeron a una menor presencia mediática de ciberataques.

Sin embargo, las amenazas y ciberataques hoy son un problema que tiene diferentes dimensiones, por ejemplo:

- La utilización de los sistemas financieros es parte de nuestro día a día, pagamos desde una bebida en una tienda de conveniencia, hasta el pago de un activo o una transacción bancaria importante y relevante en nuestras vidas.
- La falta de disponibilidad puede generar distintas problemáticas sociales y afectar nuestra vida cotidiana, por lo que es muy importante contar con alta disponibilidad que garantice la seguridad y confianza a los usuarios.
- El sistema financiero depende de los sistemas de tecnología integrado por componentes de hardware, software y telecomunicaciones, los cuales enlistamos de manera general: CORE, SPEI, SPID, ATM, Mibile Banking, Net Banking, OpenBancking, Plataforma Transaccional, Manejador de Tarjetas, Servicios y Productos Financieros.
- Los ciberataques afectan el sistema de tecnología de la información en sus diferentes componentes de las instituciones financieras, estos sistemas se encuentran regulados por organizaciones como el Banco de México y la Comisión Nacional Bancaria y de Valores.

Existen otras fuentes informales de las cuales no se puede tomar la información para una investigación, pero si pueden ser consideradas como canales de información de las afectaciones o vulnerabilidad de la seguridad de una institución financiera. Estas fuentes puedes ser noticias, redes sociales u otras formas de divulgación de información.

Las afectaciones a los servicios del sector financiero se encuentran monitoreadas por la Comisión Nacional Bancaria y de Valores (CNBV), la cual tiene documentado en su página https://www.gob.mx/cnbv como parte de sus objetivos el supervisar y regular las entidades financieras , dar la estabilidad y el buen funcionamiento del sistema financiero, promover el desarrollo del sistema financiero, proteger los intereses de los usuarios y contribuir a la construcción de un México próspero.

La Comisión Nacional Bancaria y de Valores (CNBV) se encarga de monitorear, auditar, revisar y validar a los sistemas de tecnología que son utilizados para el funcionamiento del sistema financiero, el resultado de estas actividades de la CNBV es entregada a cada una de las instituciones por lo que no es pública.

A partir de la información obtenida del Banco de México se definió trabajar en la propuesta para incidir en las afectaciones que los ciberataques presentados en el sistema financiero mexicano, tomando diferentes marcos de referencia que permiten hacer una implementación de sistemas de gestión de tecnología que se encarguen de atender las necesidades de crecimiento, actualización, capacidad, auditoría, mantenimiento, redundancia y flexibilidad para los distintos sistemas que se utilizan en una institución financiera.

A pesar de la regulación existente del (BdeM y CNBV) y la conciencia sobre los ciberataques, las Instituciones financieras en México continúan experimentando incidentes con pérdidas millonarias. El problema central radica en la aparente falta de modelos de gobierno que prioricen la inversión y esfuerzos de mitigación basándose en el impacto financiero y operativo real de las amenazas, partiendo de las mas altas como son el ransomware y APT hasta las de menor impacto como son los ataques a cajeros automáticos. Esta desalineación en la priorización de recursos impide la reducción efectiva del riesgo de alto impacto, comprometiendo la estabilidad financiera y la continuidad operativa.

2. Objetivo

Desarrollar una propuesta de fortalecimiento de gobierno de TI, basada en marcos de referencia como en ITIL , COBIT , ISO 38500 orientada a mejorar la resiliencia cibernética de instituciones del sistema financiero mexicano, con énfasis en la reducción de la

indisponibilidad de servicios y la mitigación de las pérdidas financieras derivadas de ciberataques.

3. Justificación

La importancia del sector financiero. El sector financiero es una de las infraestructuras críticas más relevantes para el desarrollo económico, la estabilidad social y el funcionamiento cotidiano del país. Las instituciones bancarias, de ahorro, inversión y pago operan plataformas tecnológicas que permiten transacciones por montos millonarios cada día, soportan los sistemas de pagos interbancarios, la dispersión de nóminas, la inversión y el ahorro de millones de personas. Su adecuada operación es fundamental para mantener la confianza pública, evitar crisis de liquidez y asegurar la continuidad económica. En México, este sector representa un pilar estratégico que interconecta con otras industrias y servicios esenciales.

Presentación del problema. En los últimos años, la frecuencia y sofisticación de los ciberataques dirigidos contra el sector financiero mexicano se han incrementado de manera significativa, comprometiendo la disponibilidad de sistemas críticos como SPEI, banca móvil, cajeros automáticos y plataformas de pagos digitales. Aunque se han fortalecido capacidades de vigilancia y respuesta, los incidentes de indisponibilidad operativa continúan representando un riesgo alto, pues incluso breves interrupciones pueden generar pérdidas económicas, afectación a la reputación institucional y desconfianza generalizada entre los usuarios.

Detalle de las consecuencias. La indisponibilidad provocada por ciberataques produce impactos multidimensionales que pueden incluir:

- Pérdidas económicas directas derivadas de interrupciones de servicios, fraudes y operaciones fallidas.
- Afectación reputacional por percepción pública de vulnerabilidad.
- Costos regulatorios y sanciones por incumplimiento de normas de seguridad y continuidad.
- Daño en la confianza de los clientes y contrapartes, con consecuencias en la atracción y retención de usuarios.
- Efectos sistémicos si la indisponibilidad afecta plataformas de uso generalizado como SPEI.

Vulnerabilidad del sector y relación con la necesidad de Gobierno de TI. El sector financiero es **particularmente vulnerable** por diversas razones:

- Alta interconexión digital y dependencia tecnológica.
- Volúmenes elevados de transacciones en tiempo real.
- Incentivos económicos para actores maliciosos.
- Exposición a amenazas sofisticadas (phishing avanzado, ransomware, ataques de denegación de servicio).

Estos factores hacen indispensable contar con un Gobierno de TI sólido, capaz de alinear estrategias de negocio con la gestión de riesgos tecnológicos, la operación segura y la continuidad operativa. El gobierno de TI permite asignar responsabilidades, establecer procesos de control, medir el desempeño y fomentar una cultura de seguridad transversal a toda la organización.

Justificación del enfoque del trabajo. Frente a este panorama, el presente trabajo propone un modelo híbrido que integra los marcos COBIT, ITIL e ISO/IEC 38500 como una solución adaptada al contexto mexicano, con el propósito de:

- Articular la gobernanza estratégica con la gestión operativa y el aseguramiento de la disponibilidad.
- Fortalecer la capacidad institucional de prevención y respuesta ante ciberataques.
- Generar un esquema escalable que pueda adaptarse a distintos niveles de madurez tecnológica.

Este enfoque se justifica porque ningún marco por sí solo cubre la totalidad de necesidades del sector; su integración permite construir un modelo más robusto y alineado con las mejores prácticas internacionales.

Aportaciones del trabajo. Las principales aportaciones de este proyecto son:

- La propuesta de un modelo metodológico híbrido contextualizado al sector financiero mexicano, con fases, roles, indicadores y mecanismos de validación.
- La identificación de factores críticos de éxito, condiciones mínimas de aplicación y recomendaciones para su replicabilidad.
- El desarrollo de un caso de simulación que muestra la aplicabilidad práctica del modelo.

- La generación de un marco conceptual que puede servir como referencia para otras instituciones con necesidades similares de fortalecer su gobierno de TI

La resolución de este problema es crítica para garantizar la **resiliencia operativa** de las instituciones financieras mexicanas. No atender esta amenaza puede derivar en **pérdida de confianza del usuario, afectaciones económicas masivas, impacto reputacional** y **sanciones regulatorias**.

El Congreso Mexicano de Protección de Infraestructuras Críticas (PIC) de la **Ciudad de México** considera crítica la infraestructura del sector financiero para el país, por lo tanto, es importante proteger la operación, disponibilidad, seguridad de los sistemas, datos y resiliencia de los bancos y toma una gran relevancia el reducir los impactos provocados por ciberataques en el sector.

Proponer soluciones para minimizar las afectaciones de los ciberataques utilizando los marcos de referencia que existen y que se utilizan para la gestión de infraestructura de TI que permite minimizar, mitigar, prevenir las afectaciones, así como predecir las capacidades los sistemas TI y la estrategia de ciberseguridad que se busca implementar para la prevención de estos incidentes cibernéticos.

La estabilidad y resiliencia del sistema financiero mexicano son pilares fundamentales para la economía nacional y la confianza pública. Sin embargo, este sector enfrenta una amenaza persistente y crecientes, los ciberataques en el año 2024 generaron pedidas millonarias y afectaron a múltiples instituciones , según el **Reporte de incidentes cibernéticos ocurridos en 2024 en el sistema financiero nacional que han sido reportados al Banco de México.** La presente investigación se justifica por la urgente necesidad de fortalecer las defensas del sector financiero ante este panorama.

No abordar proactivamente la vulnerabilidad de los ciberataques acarrea consecuencias. Estas van desde perdidas económica masiva directa e indirecta, hasta un cebero impacto reputacional que puede erosionar la confianza de los usuarios en las instituciones e incluso en el sistema en su conjunto.

Adicionalmente las fallas en la ciberseguridad pueden derivar en sanciones regulatorias de gran impacto. La criticidad del sector financiero es reconocida a nivel nacional, como lo subraya el **Congreso Mexicano de protección de Infraestructuras críticas**, Enfatizando la importancia de proteger su operación, disponibilidad, seguridad y resiliencia. Por tanto , reducir los impactos provocados por los ciberataques adquiere una relevancia estratégica para el país.

El sector financiero mexicano presenta características intrínsecas que lo hacen particularmente susceptible y que justifican un enfoque robusto en gobernanza de TI como los que mencionamos a continuación:

Alta interconexión digital. Las instituciones financieras en México están altamente interconectadas a través de plataformas como SPEI, SPID y banca móvil. Esto significa que un ataque exitoso en un punto puede propagarse rápidamente a otros sistemas.

Dependencia de infraestructura crítica. Los sistemas financieros dependen de infraestructura tecnológica crítica, como cajeros automáticos (ATM), plataformas transaccionales y sistemas de banca en línea. Cualquier interrupción en estos sistemas puede tener un impacto significativo en los usuarios y la economía.

Falta de cultura de ciberseguridad. Muchas instituciones y usuarios finales carecen de una cultura sólida de ciberseguridad, lo que aumenta la probabilidad de errores humanos, como contraseñas débiles o clics en enlaces maliciosos.

Ataques sofisticados y persistentes. Los ciberdelincuentes utilizan técnicas avanzadas como ransomware, phishing y amenazas persistentes avanzadas (APT). Por ejemplo, en 2024 se reportaron ataques con ransomware como "akira", que afectaron plataformas transaccionales.

Regulación y cumplimiento limitados. Aunque existen regulaciones como las emitidas por la Comisión Nacional Bancaria y de Valores (CNBV) y el Banco de México, la implementación y supervisión de estas medidas no siempre es uniforme.

Errores humanos y fallas sistémicas. La falta de capacitación y protocolos claros puede llevar a errores humanos que faciliten los ataques. Además, fallas en componentes clave o sobrecarga de sistemas pueden agravar la situación.

Aumento de la banca digital. La creciente adopción de la banca digital y móvil ha ampliado la superficie de ataque, exponiendo a las instituciones a nuevas vulnerabilidades.

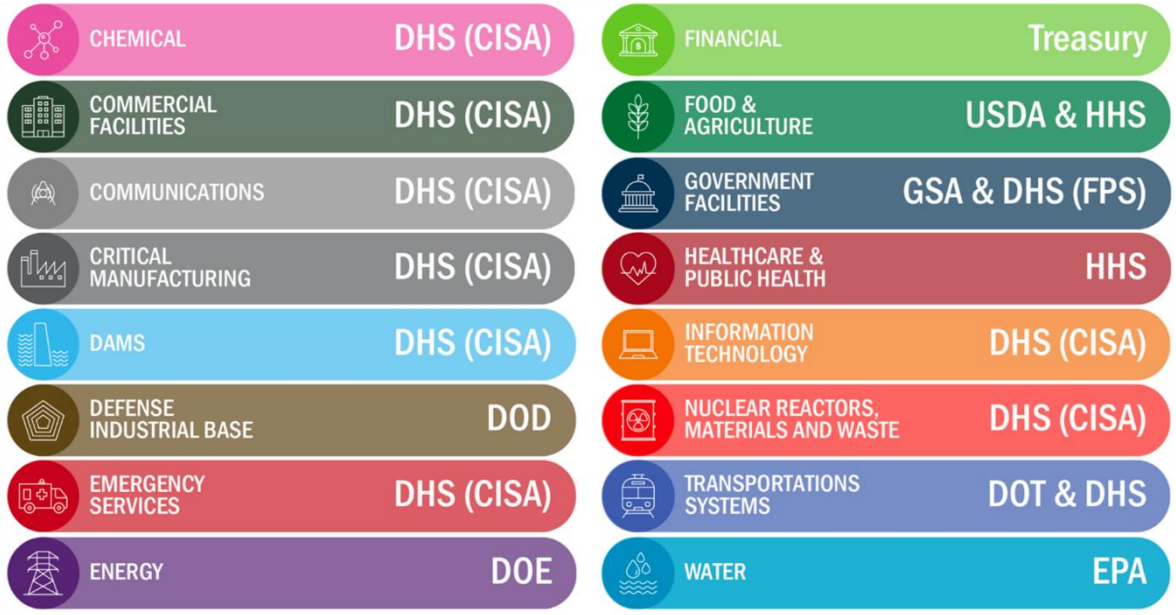
Este trabajo se justifica por su potencial para:

- **Contribuir a la resiliencia operativa y la escalabilidad del sistema financiero mexicano**, asegurando continuidad en la prestación de servicios financieros críticos.
- **Ofrecer una solución estructurada y adaptable**, adecuada para instituciones con diferentes niveles de madurez tecnológica y de gobernanza.
- **Aportar al cumplimiento normativo y la mejora continua** en materia de seguridad de la información, fortaleciendo la supervisión de CNBV y Banxico.
- **Fortalecer la confianza pública y la estabilidad sistémica**, mitigando la percepción de riesgo en los usuarios y garantizando la integridad del sistema financiero.

- **Promover una cultura organizacional de ciberseguridad y gestión del cambio**, integrando la participación de la alta dirección, áreas operativas y usuarios finales.
- **Incorporar innovación tecnológica en la gobernanza**, vinculando prácticas tradicionales con elementos como la madurez digital y la transformación organizacional.
- **Asegurar la competitividad internacional del sistema financiero mexicano**, alinear sus prácticas con estándares globales (NIST, ISO/IEC, COBIT) y fortalecer su posición en un mercado global interconectado.
- **Optimizar el uso de recursos financieros y humanos**, maximizando la eficiencia de las inversiones en seguridad y evitando duplicidades en procesos de control.
- **Generar lineamientos aplicables y replicables** para otras instituciones financieras y sectores críticos, contribuyendo al desarrollo de políticas públicas y mejores prácticas en el ámbito nacional.

4. Contexto externo

El sistema financiero de los países es catalogado como infraestructura critica tal como lo indica Dreamlamb en su publicación del año 2022 donde se documentan las distintas infraestructuras críticas de un país, tal como se muestra la siguiente imagen:



Dreamlamb(2022). *Infraestructura crítica y ciberespacio* [Imagen de infraestructura crítica]. Recuperado el 8 de abril de 2022, de https://www.dreamlamb.com

Todas las infraestructuras críticas de un país son reguladas. En el caso de las infraestructuras relacionadas con el sector financiero de México se tiene la CNBV que se encarga de hacer la regulación de todas esas entidades financieras, Banco de México y Banco Mundial que marcan la pauta para la implementación de diferentes parámetros, entre los cuales encontramos; normas de seguridad, protección y disponibilidad.

Es por esta razón que toma como una fuente formal y confiable la información proporcionada por del Banco de México en relación con los ciberataques y las afectaciones.

En otros países como Chile o EE.UU. se han adoptado marcos como NIST (National Institute of Standards and Technology) y la norma de continuidad del negocio del Banco Central de Chile. Esto permitirá comparar buenas prácticas internacionales y evaluar su posible adopción en México.

En el contexto de la creciente amenaza de ciberataques al sector financiero, es útil revisar experiencias internacionales documentadas que han dado origen a respuestas

estructuradas de gobierno de TI y ciberseguridad. A continuación, se presentan tres casos relevantes que ilustran distintas formas de enfrentar estos desafíos:

Caso de Referencia Banco de Chile (2018)

Ataque SWIFT y fortalecimiento estructural en mayo de 2018, el Banco de Chile fue víctima de un ciberataque dirigido a su red de mensajería financiera SWIFT, inicialmente percibido como una falla técnica, implicó el uso de un *malware wiper* para encubrir movimientos fraudulentos, logrando el desvío de aproximadamente 10 millones de dólares a cuentas en Asia (FireEye, 2019).

Las acciones del banco fueron las siguientes:

- Desconexión parcial de la red para contener el malware.
- Activación de una investigación forense digital con firmas especializadas (Mandiant y Microsoft).
- Reforzamiento del sistema SWIFT mediante autenticación multifactor y cifrado.
- Implementación de un Centro de Operaciones de Seguridad (SOC).
- Segmentación de redes críticas y capacitación intensiva.

Este caso impulsó reformas regulatorias en Chile, destacando la Norma de Carácter General N° 461 de la Comisión para el Mercado Financiero (CMF), orientada a la gestión de continuidad operativa y resiliencia cibernética (CMF, 2020).

Caso de Referencia Banco Santander España

Banco Santander ha adoptado la norma ISO/IEC 27001 como base para un modelo sistemático de gestión de seguridad de la información, certificado en múltiples filiales. Este marco permite gestionar riesgos, estandarizar controles y alinear las prácticas con marcos como ISO/IEC 27002 y el RGPD (Santander, 2022).

Entre sus prácticas destacan:

- Políticas robustas de acceso y control.
- Auditorías internas y externas.
- Ciclo de mejora continua.
- Concienciación obligatoria en ciberseguridad.
- Visión integrada del riesgo operacional.

Esta implementación ha mejorado significativamente la madurez digital y la resiliencia operativa del banco.

Caso de Referencia JPMorgan Chase (EE.UU.)

JPMorgan Chase ha basado su estrategia en el NIST Cybersecurity Framework, aplicando las cinco funciones clave: *Identificar, Proteger, Detectar, Responder y Recuperar* (NIST, 2020).

Este enfoque ha sido reforzado por una inversión anual superior a 12 mil millones de dólares en ciberseguridad y tecnología (JPMorgan Chase, 2023).

Sus acciones clave incluyen:

- Operación avanzada de un SOC global.
- Pruebas de cibercrisis periódicas.
- Alianzas con entidades gubernamentales de inteligencia.
- Formación constante del personal.
- Medición y mejora continua con métricas clave.

Su modelo destaca por su enfoque preventivo y reactivo altamente integrado, convirtiéndolo en un referente global de resiliencia financiera digital.

El análisis del contexto externo evidencia que el sistema financiero mexicano enfrenta un entorno caracterizado por altas interdependencias digitales, exigencias regulatorias en evolución y una creciente exposición a riesgos cibernéticos globales.

La experiencia internacional muestra que los países que han fortalecido su gobernanza de TI y adoptados marcos normativos de referencia han logrado avanzar significativamente en su capacidad de resiliencia frente a ciberataques.

Casos como la adopción de ISO/IEC 27001 en Santander España, el modelo de ciberresiliencia basado en NIST en JPMorgan Chase, y la respuesta estructural del Banco de Chile tras el ataque SWIFT en 2018, confirman la importancia de integrar metodologías internacionales y aprendizajes derivados de incidentes críticos.

En este sentido, para el país resulta prioritario fortalecer su alineación con estándares internacionales, promover la cooperación entre instituciones y reguladores, e impulsar la madurez digital del sector como un factor de competitividad y estabilidad sistémica.

El contexto externo, por tanto, no solo constituye un referente comparativo, sino también un marco de aprendizaje que justifica la necesidad de propuestas innovadoras como el modelo híbrido planteado en este trabajo.

5. Contexto interno

Las instituciones financieras al tener ciberataques se pueden ver en afectaciones como:

- Afectaciones reputacionales: pérdida de clientes, impacto en imagen pública
- Afectaciones económicas: pérdidas millonarias, multas CNBV.
- Afectaciones operativas: interrupciones en servicios, planificaciones y desarrollo.

Afectaciones reputacionales

La información de las entidades afectadas por ciberataques puede ser divulgada por medios electrónicos, radio, televisión, generando un impacto negativo en su reputación y en la percepción de los servicios que proporcionan estas instituciones.

Este tipo de afectación afecta directamente a su desarrollo y crecimiento y es cuantitativa en función de la cantidad de usuarios que se ven afectados, y otras actividades de la institución como pueden ser: generación de nuevos productos, reducción de usuarios que se buscaban integrar al universo de clientes de las instituciones.

Afectaciones económicas

Generar calificaciones que se reflejan en penalizaciones económicas que son directamente relacionados a los tiempos en los cuales el servicio se vio afectado y estos son validados y medidos por la CNBV, la cual se encarga de realizar estas regulaciones y establecer la multa correspondiente a la afectación que se ha generado hacia los servicios financieros, para los clientes y usuarios del servicio.

Afectaciones operativas

Estas afectaciones también afectan las planificaciones y desarrollo de la entidad ya que las instituciones financieras tienen diferentes planes de desarrollo, transformación, actualización, reingeniería que son ejecutados de manera continua dentro de un roadmap.

Cuando se genera una afectación a la entrega del servicio, una incidencia ocasiona que los recursos que se encargan de desarrollar todos estos proyectos se vean volcados a atender las incidencias y reparación del servicio lo más pronto posible, de tal manera que la remediación a una incidencia tiene impacto directo en todas las planificaciones del propio banco o institución financiera.

El análisis del contexto interno requiere una comprensión detallada de las situaciones, capacidades, recursos y estructuras de la entidad financiera donde se pretende aplicar la propuesta. Este examen es fundamental para determinar el grado de madurez de la organización en materia de gobernanza de TI y ciberseguridad, así como para identificar áreas de oportunidad que puedan ser atendidas con el modelo híbrido.

En este sentido, el análisis debe dar respuesta a preguntas clave como:

¿Existen ya sistemas de gestión implementados? En la mayoría de las instituciones financieras se han adoptado procesos relacionados con la seguridad de la información, la continuidad operativa o la gestión de riesgos, aunque con distintos niveles de formalización y eficacia.

¿Qué tan efectivos son estos sistemas? La efectividad varía dependiendo de los recursos asignados, la capacidad de monitoreo y la integración de los sistemas con la estrategia institucional. En algunos casos, los marcos aplicados se limitan a cumplir con la regulación, sin alcanzar una gestión integral de riesgos tecnológicos.

¿Cómo se alinean o no con un marco de Gobierno de TI superior? Muchos de los sistemas actuales se desarrollan de forma fragmentada y sin una alineación plena con marcos de referencia superiores como COBIT o ISO/IEC 38500, lo que limita la capacidad de gobernanza estratégica.

¿La propuesta de gobierno busca mejorar o estructurar estos sistemas de gestión? El modelo híbrido planteado tiene como objetivo fortalecer y estructurar los sistemas existentes, promoviendo la integración de procesos, la estandarización de prácticas y la mejora continua, para evolucionar hacia un esquema de gobernanza más sólido y resiliente.

De esta manera, el contexto interno no solo diagnostica las condiciones actuales, sino que también delimita el punto de partida realista sobre el cual la propuesta metodológica puede generar mayor valor.

5.1 Factores organizacionales y culturales

Los factores organizacionales desempeñan un papel crucial en la vulnerabilidad de las instituciones financieras mexicanas frente a ciberataques como:

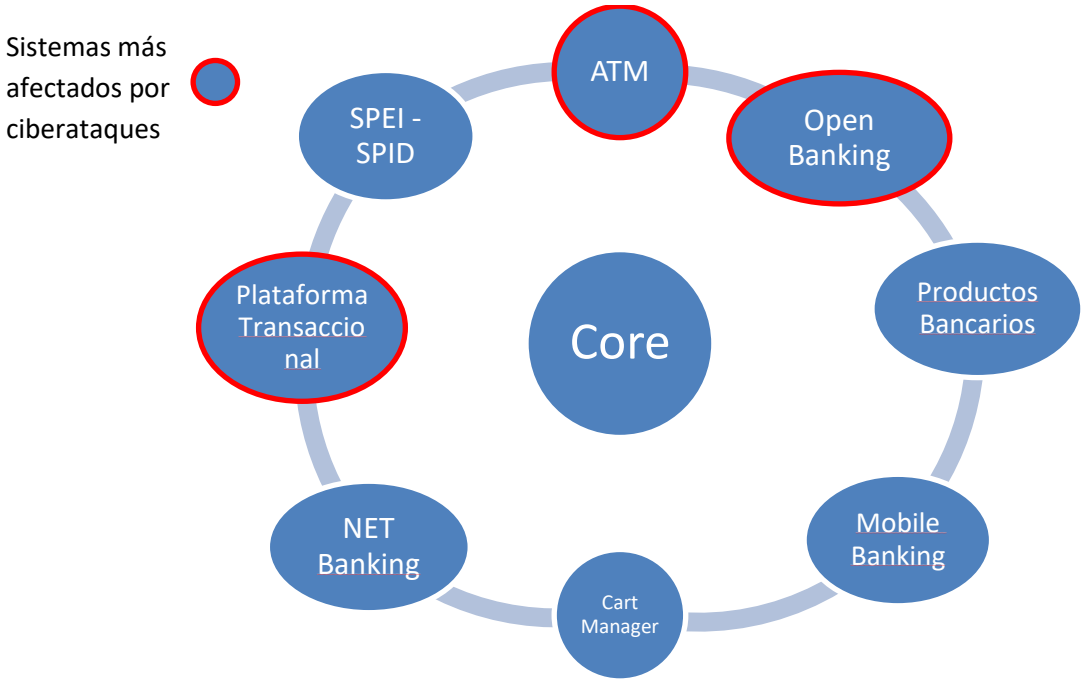
- **Falta de priorización de la ciberseguridad en instituciones**. La ciberseguridad no se percibe como una prioridad estratégica, lo que resulta en una asignación insuficiente de recursos y atención.

- **Estructuras jerárquicas rígidas**. Las organizaciones con estructuras jerárquicas inflexibles pueden dificultar la toma de decisiones rápidas y efectivas ante incidentes cibernéticos.
- **Procesos internos deficientes**. La falta de procesos claros y bien definidos para la gestión de riesgos y la respuesta a incidentes puede aumentar la exposición a amenazas.
- **Dependencia de sistemas heredados**. Muchas instituciones aún operan con tecnología obsoleta, lo que dificulta la implementación de medidas modernas de ciberseguridad.
- **Falta de monitoreo continuo**. La ausencia de sistemas de monitoreo en tiempo real limita la capacidad de detectar y responder a amenazas de manera oportuna.
- **La resistencia a adoptar nuevas tecnologías o prácticas**. Esta resistencia puede dejar a las instituciones expuestas a riesgos.
- **Falta de conciencia**. Tanto a nivel organizacional como entre los empleados, la falta de una cultura sólida de ciberseguridad aumenta la probabilidad de errores humanos, como clics en enlaces maliciosos o contraseñas débiles.
- **Subestimación de los riesgos**. Existe una percepción errónea de que los ciberataques son problemas aislados o improbables, lo que lleva a una preparación insuficiente.
- **La falta de comunicación efectiva entre departamentos** puede dificultar la implementación de estrategias de ciberseguridad integrales.
- **Enfoque reactivo en lugar de preventivo.** Muchas instituciones adoptan un enfoque reactivo, respondiendo a incidentes después de que ocurren, en lugar de invertir en medidas preventivas.

Todos los factores mencionados deben ser considerados, pero también deben de ser medidos para contar con una trazabilidad del avance y su efectividad para incidir ante los ciberataques.

6. Ubicación del problema

Para identificar dónde podemos encontrar el problema es importante conocer la arquitectura de TI de una institución financiera. Se mostrará esta arquitectura a muy alto nivel en la siguiente figura:



Pantoja, A. *Figura conceptual de la arquitectura TI: Modelo ilustrativo de sistemas financieros* [Imagen que representa los sistemas financieros e identifica los más afectados por ciberataques]. **Reporte de incidentes cibernéticos ocurridos en 2020-2024 en el sistema financiero nacional que han sido reportados al Banco de México.**

La figura nos muestra que la arquitectura de una institución financiera se conforma por soluciones satélites que se encuentran en torno a un sistema central que se denomina CORE el cual resguarda la información sensible de la institución y ésta es consumida, consultada y modificada por los distintos sistemas satélites.

En base a la información del Banco de México en **"Reporte de incidentes cibernéticos ocurridos en 2020- 2024 en el sistema financiero nacional que han sido reportados al Banco de México"** se identifica que, en los sistemas de la plataforma transaccional, ATM y Open banking, son más vulnerables por la recurrencia de los ciberataques y su alto volumen de operación.

Sin embargo, todos los sistemas financieros pueden ser afectados con impacto a los usuarios de la institución financiera. Podemos hablar de cientos de miles, incluso de millones de usuarios afectados por una falla en algún sistema. Esto dependerá del tamaño de la institución financiera, en cualquiera de los casos las afectaciones siempre son directamente a los usuarios y a la institución.

Todos los sistemas satélites y CORE pueden ser afectados por los ciberataques, por lo que el problema se puede ubicar en todos los sistemas y sub-sistemas que afectan a una entidad financiera.

7. Marco teórico

La gestión de los recursos tecnológicos de una organización se alinea y apoya el cumplimiento de los objetivos de las organizaciones.

Uno de los objetivos importantes es la implementación de la estrategia de ciberseguridad, protección, disponibilidad y confiabilidad de los datos, por lo que es necesario contar con una estrategia específica en el gobierno de tecnología.

Para el desarrollo e implementación de una estrategia de ciberseguridad y gobierno de TI es importante tomar los alineamientos de las estrategias de ciberseguridad que nos otorgan las entidades reguladoras como el Banco de México en su “Estrategia de ciberseguridad del banco de México 2024 -2027”.

7.1 Organizaciones de normalización del gobierno de TI

Existen diferentes organizaciones que se encargan de establecer y mantener normas y directrices de gobierno de TI como:

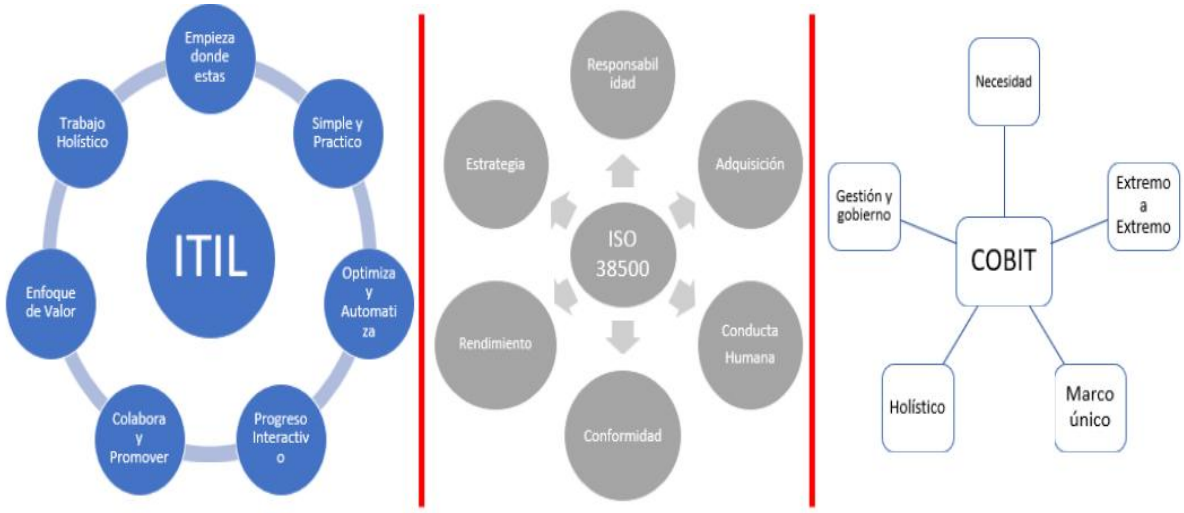
- **ISACA:** Information Systems Audit and Control Association, es una organización que proporciona credenciales a los profesionales de TI en áreas clave de auditoría, ciberseguridad.
- **Organización Internacional de Normalización:** esta organización no gubernamental elabora normas para todas las unidades empresariales, incluidas las operaciones de TI, con el fin de facilitar el comercio y la cooperación. Ha publicado varias normas, entre ellas la ISO/IEC 38500 sobre gobierno de TI, publicada en 2008, y la ISO 27001 sobre gestión de la seguridad de la información.
- **Axelos:** Originalmente una empresa conjunta entre el gobierno del Reino Unido y la empresa Capita, PeopleCert adquirió la organización en julio de 2021. Es responsable de varias certificaciones, incluida la biblioteca de infraestructuras de TI (ITIL).
- **COBIT** (Control Objectives for Information and Related Technologies): Este marco ayuda a las organizaciones a alinear sus objetivos de TI con los objetivos empresariales, minimizando riesgos y mejorando el gobierno.
- **NIST** Cybersecurity Framework: Este marco, desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., se centra en identificar, proteger, detectar, responder y recuperarse de ciber amenazas.

- **Gestión de servicios de TI (ITSM):** este marco implica planificar, implantar, gestionar para satisfacer las necesidades de los usuarios y ayudar a las organizaciones a alcanzar sus objetivos empresariales. ITSM consiste en proporcionar la implementación, el funcionamiento y la gestión óptimos de todos los recursos de TI para todos los usuarios de una empresa. Los usuarios pueden ser clientes, empleados o socios comerciales.

Los marcos de gobierno de TI tienen como alcance:

- **Alineación estratégica**
- **Ciberseguridad**
- **Gestión de recursos**
- **Recuperación ante desastres**
- **Conformidad normativa**

Tomaremos los marcos de referencia como elementos para el desarrollo de un nuevo modelo para la implementación que permita incidir en las afectaciones derivadas de los ciberataques a las organizaciones del sistema financiero de México.



Pantoja, A. *Marco teórico: Modelo ilustrativo* [Imagen que representa las metodologías que de utilizan para el modelo de propuesta].

La sola implementación de estos marcos de referencia es el principio de la solución y el nivel de madurez en gobierno de TI de las instituciones financieras mexicanas es otro paso ante la incidencia para enfrentar las afectaciones generadas por los ciberataques.

Existen otros factores que forman parte de las actividades para incidir en las afectaciones derivadas de los ciberataques, como es fomentar la capacitación especializada, invertir en infraestructura moderna y realizar evaluaciones regulares de madurez.

La implementación de las acciones de la **"Estrategia de ciberseguridad del banco de México 2024 -2027"** requiere contar con un gobierno de TI, por lo que éstas se encuentran directamente relacionadas para cumplir con los lineamientos y requerimientos de las entidades reguladoras de instituciones financieras.

Existen otros factores que deben ser considerados para la implementación de una estrategia de ciberseguridad y estos pueden ser factores organizacionales, culturales que juegan un papel importante para incidir en las afectaciones derivadas por los ciberataques.

7.2 Medir la efectividad

Medir la efectividad de las estrategias implementadas es importante para garantizar la resiliencia ante estos ciberataques, para medirla se requiere acotar la disponibilidad de los sistemas para lo cual podemos utilizar diferentes KPI´s como los siguientes:

- Tiempo de recuperación (RTO). Evalúa cuánto tiempo toma restablecer los servicios críticos después de un incidente.
- Punto de recuperación (RPO.) Mide la cantidad de datos que pueden perderse sin afectar significativamente las operaciones.
- Porcentaje de pruebas exitosas. Indica la efectividad de los simulacros y ejercicios de continuidad.
- Realizar simulacros de interrupciones para evaluar la capacidad de respuesta y la adherencia a los planes establecidos.
- Medir el tiempo de respuesta y la coordinación entre equipos durante los ejercicios.
- Contratar evaluaciones independientes para verificar la alineación con estándares internacionales como ISO 22301.
- Identificar áreas de mejora en los procesos y estrategias implementadas.
- Implementar herramientas de monitoreo para rastrear la disponibilidad de sistemas y detectar posibles fallas antes de que ocurran.
- Pruebas de Penetración.

Para ejecutar las actividades y medirlas es importante contar con el apoyo de la alta dirección la cual juega un papel muy importante en la prevención y gestión de incidentes de ciberseguridad dentro del sector financiero mexicano y en cualquier organización.

La alta dirección apoya con las siguientes actividades como:

- Definición de prioridades estratégicas
- Alineación de políticas y gobierno
- Liderazgo en la cultura organizacional
- Supervisión y monitoreo

- Toma de decisiones frente a incidentes
- Colaboración interinstitucional
- Evaluación y mejora continua
- Promoción de talento especializado

7.3 Barreras para implementar soluciones de ciberseguridad

El identificar las barreras que impidan la implementación de las acciones que incidan en los ciberataques nos permite gestionarlas con antelación y considerar la opción que se puede tomar ante su presentación, para entender cuáles pueden ser estas barreras vamos a enunciar algunas:

- **Falta de presupuesto.** No asignan suficientes recursos económicos para implementar tecnologías avanzadas de ciberseguridad, lo que limita su capacidad para protegerse contra amenazas sofisticadas.
- **Escasez de talento especializado.** La carencia de profesionales capacitados en ciberseguridad en México puede ser una barrera para la implementación y gestión de soluciones efectivas.
- **Resistencia al cambio organizacional.** Podemos encontrar resistencia a adoptar nuevas tecnologías o procesos debido a la falta de comprensión de los riesgos cibernéticos o al temor de interrumpir las operaciones existentes.
- **Complejidad regulatoria.** Existen regulaciones emitidas por la CNBV y el Banco de México y su cumplimiento puede ser complicado.
- **Interconexión de sistema.** La alta interconexión entre instituciones financieras aumenta la superficie de ataque.
- **Tecnología obsoleta.** Pueden existir tecnologías no compatibles con las soluciones modernas de ciberseguridad, lo que las hace más vulnerables.
- **Falta de colaboración interinstitucional.** La ausencia de una cooperación efectiva entre los involucrados puede limitar la capacidad de compartir información sobre amenazas y responder de manera coordinada a los incidentes.
- **Conciencia limitada sobre ciberseguridad.** Tanto a nivel organizacional como de usuarios finales pueden estar expuestos ante la falta de una cultura sólida de ciberseguridad.
- **Los proveedores externos y las tecnologías emergentes** pueden tener un impacto en la exposición a riesgos de ciberataques.

- **Los ciberdelincuentes**. Atacan a proveedores más vulnerables para infiltrarse en instituciones financieras más grandes. Esto se conoce como ataques de "cadena de suministro".
- **La supervisión insuficiente de las actividades** de las distintas áreas puede permitir comportamientos sospechosos o brechas de seguridad.

Las tecnologías emergentes es otro de los componentes que se deben de tomar en consideración para incidir en las afectaciones de los ciberataques, entre estas tecnologías encontramos el Cloud, el Internet de las cosas y las APIs por lo que describiremos algunos aspectos de estas tecnologías:

- Cloud ofrece escalabilidad y eficiencia, la nube puede ser vulnerable a accesos no autorizados si no se implementan controles adecuados como cifrado y autenticación multifactorial.
- El internet de las cosas (IoT) en los dispositivos amplía la superficie de ataque, ya que muchos de ellos pueden tener configuraciones de seguridad débiles. Esto puede ser explotado para acceder a redes financieras.
- Interface de programación de aplicaciones (APIs) facilitan la interconexión entre sistemas, pero si no están protegidas adecuadamente, pueden ser utilizadas para ataques como el robo de datos o la manipulación de transacciones.

Para estas tecnologías emergentes se tienen recomendaciones que pueden ayudar a mitigar y/o minimizar los riesgos de ciberataques e incidir en sus afectaciones como:

- Evaluación de proveedores: Realizar auditorías periódicas para garantizar que los proveedores cumplan con estándares de seguridad.
- Seguridad en la nube: Implementar políticas de acceso restringido y cifrado de datos.
- Protección de IoT: Asegurar que los dispositivos IoT estén configurados con contraseñas fuertes y actualizaciones regulares.
- Seguridad de APIs: Utilizar autenticación robusta y monitoreo continuo para detectar actividades sospechosas.

Existen otros factores de afectación a un sistema y estos otros factores suman a las afectaciones de los ciberataques por lo que es importante conocerlos.

7.4 Otros factores de falla

Algunas de las afectaciones con mayor impacto a un sistema es la indisponibilidad, la cual se determina por la falta de servicio por parte de los sistemas. Para entender mejor estos factores vamos a enunciar algunos y a continuación daremos detalle de ellos:

- Errores humanos
- Falla en componente clave
- Falla por desbordamiento o falta de capacidad
- Desbordamiento de la capacidad instalada de los sistemas
- Falta de coordinación y utilización de procesos
- Falla sistémica

Errores humanos

Es uno de los factores más comunes que se presenta dentro de la gestión de los sistemas, temas de procesos, implementación, comunicación, ejecución y planificación. Podemos encontrar desde un error de dedo, hasta todo un problema de comunicación, procesos de capacitación y madurez de estos.

Fallas en componentes clave

Todos los sistemas que son relevantes para el funcionamiento de una organización pueden contar con la alta disponibilidad. Pareciera muy sencillo entender que siempre se debe de contar con un backup o un entorno de contingencia o un sistema alterno o con algún mecanismo que nos permita continuar operando, a pesar de que tuviéramos una falla, sin embargo, este concepto de alta disponibilidad básicamente se refiere a contar con algún componente que continue operando en lugar del componente principal sin afectar el servicio.

Identificar dentro de la arquitectura de infraestructura todos los componentes necesarios para el funcionamiento y colocarlos en alta disponibilidad, podría ser muy costoso, es por eso por lo que siempre existirá un punto único de falla. Este punto único de falla hace referencia a precisamente la vulnerabilidad que tenemos dentro de los propios componentes de hardware y software que se integran en un sistema.

Falla por desbordamiento o falta de capacidad

Para atender todos los requerimientos y solicitudes que se ejecutan en el sistema del sector financiero, se requiere de una alta capacidad de procesamiento y este puede verse afectado por fluctuaciones importantes en las operaciones, si bien es cierto siempre tomamos en consideración una línea base que está constituida de la cantidad de usuarios que utilizan el sistema, los medios por los cuales pueden hacer diferentes operaciones y la cantidad de operaciones que se tienen registradas, estadísticas, métricas , estimaciones y análisis de

capacidad referentes, la utilización de los sistemas pueden sufrir modificaciones repentinas en función de los diferentes estímulos que están fuera del control del área de tecnología, llevando al desbordamiento de un sistema, los factores externos que responden a diferentes estímulos que son generados pueden ser efectos financieros, sociales y económicos.

Falla sistémica

Es una falla derivada por el comportamiento de un sistema a través de ciertas condiciones que pueden intervenir elementos físicos y mecánicos del propio del sistema, para poder entender mejor una falla comentaremos algunos ejemplos:

Ejemplo1.- Los equipos de cómputo se encuentran en un lugar específico que podemos determinar cómo SITE o centro de procesamiento o centro de cómputo, nos referimos a un lugar que tiene ciertas características físicas de humedad, temperatura y espacio adecuados para poder alojar computadoras, que se encargan de qué los sistemas funcionan y este hardware que está dentro de estas instalaciones requiere de ciertas condiciones específicas para su buen funcionamiento. Una falla por un tema físico podríamos identificar muy claramente que, si tuviéramos una falla eléctrica, una elevación de temperatura o un exceso de humedad en el entorno donde se encuentran estos servidores o computadoras de procesamiento, podrían llegar a generar una falla sistémica que podría paralizar un sistema

Ejemplo2.- Las fallas sistémicas que se presentan es que el propio sistema genera operaciones que a través de la propia recurrencia de la utilización de los recursos de las computadoras que ejecutan estas operaciones pueden generar recurrencia en la utilización de los propios recursos generando así un colapso, hablamos de que las propias computadoras al tener una gran utilización podrían llegar a no tener la capacidad de ir liberando sus propios recursos para ir atendiendo las nuevas peticiones y requerimientos.

Falta de coordinación y utilización de procesos

Este tipo de fallas se puede presentar ante las diferentes actividades que se desarrollan dentro de las instituciones financieras ya sea en el día a día o dentro de la ejecución de los procesos de proyectos en los cuales están participando, si bien es cierto que todas las actividades que se desarrollan forman parte de alguno de estos dos grandes rubros (ongoing o proyectos) que se ejecutan y que si tienes claridad al respecto del alcance de cada una de estas actividades podemos reconocer a qué tipo de marco metodológico o proceso pertenecen y sobre el cual deberíamos de buscar que se ejecute, sin embargo, esta identificación no siempre significa que se tenga un proceso perfectamente maduro o una precisa categorización de las actividades que se desarrollan.

El análisis de los factores de falla evidencia que, más allá de la dimensión técnica, la **falta de gestión integral y gobierno efectivo** representa una de las principales causas que amplifican la indisponibilidad de los sistemas financieros ante ciberataques. Aspectos como la insuficiencia de recursos, la resistencia al cambio organizacional, la ausencia de una cultura de ciberseguridad y la escasa coordinación interinstitucional no solo constituyen debilidades operativas, sino que también revelan vacíos en la toma de decisiones estratégicas y en la supervisión de la alta dirección.

En este sentido, la aplicación de un enfoque de **gestión y gobierno de TI** resulta indispensable para mitigar dichos factores de falla. A través de mecanismos de gobernanza claros, la definición de responsabilidades, la implementación de marcos normativos y la evaluación continua del desempeño, es posible transformar estos elementos en palancas de resiliencia. Así, la propuesta híbrida planteada en este trabajo se justifica como una alternativa sólida, capaz de estructurar y fortalecer la capacidad del sector financiero mexicano para anticipar, responder y recuperarse de incidentes críticos, asegurando tanto la **confianza pública** como la **continuidad operativa**.

7.5 Casos de comparación

Para el desarrollo de la propuesta de solución es importante conocer los casos que se tienen de referencia mencionados en el apartado 4 y se enlistan a continuación:

Elemento clave	Banco de Chile	Santander España	JPMorgan Chase	Propuesta híbrida
Marco de referencia principal	Respuesta estructural post-ataque (mejores prácticas + normativas locales)	ISO/IEC 27001	NIST Cybersecurity Framework	COBIT (gestión), ITIL (servicios), ISO/IEC 38500 (gobierno estratégico)
Enfoque	Recuperación post-ataque / contención de incidentes	Seguridad de la información / cumplimiento normativo	Ciberresiliencia / monitoreo y prevención	Gobierno integral / disponibilidad operativa / prevención de ciberataques

Elemento clave	Banco de Chile	Santander España	JPMorgan Chase	Propuesta híbrida
Ámbito de implementación	Nacional (Chile)	Multisede internacional	Global (EE.UU. y operaciones internacionales)	Sector financiero mexicano
Controles principales	Segmentación de red, autenticación SWIFT, monitoreo SOC	Gestión de riesgos, controles técnicos, SGSI	Simulacros, inteligencia de amenazas, SOC	Procesos de madurez, auditorías, indicadores de disponibilidad
Herramientas clave	Malware forensics, remediación estructural	Auditorías ISO, ciclo PDCA, formación	Análisis de riesgos, NIST 800-53, SOC	Evaluaciones de madurez, RTO, MTTR, matriz de hallazgos
Fortalezas	Lecciones posts-incidentes, reforma normativa	Estandarización, cumplimiento, confianza del usuario	Alta inversión, simulación avanzada, colaboración institucional	Flexibilidad metodológica, adecuación regulatoria, escalabilidad progresiva
Limitaciones	Modelo reactivo (después del ataque)	Requiere mantenimiento constante de certificación	Costos elevados, alta dependencia de infraestructura tecnológica	Requiere madurez institucional, cambio cultural sostenido

Alberto Pantoja (2025). *Comparación de modelos de ciberseguridad en el sector financiero: Banco de Chile, Santander, JPMorgan y propuesta híbrida* [Tabla 1]. Elaboración propia con base en fuentes institucionales.

7.6 Enfoque desde la gestión y gobierno de TI

El abordaje de la indisponibilidad operativa provocada por ciberataques en el sistema financiero mexicano no solo debe entenderse como un desafío técnico o regulatorio, sino como una oportunidad para impulsar procesos de innovación tecnológica dentro de las instituciones financieras. En este sentido, la propuesta híbrida desarrollada en este trabajo se concibe como una intervención organizacional basada en principios de gestión del cambio, adopción tecnológica, madurez digital e innovación organizacional.

Gestión del cambio

La implementación de marcos como COBIT, ITIL e ISO/IEC 38500 requiere transformaciones culturales, estructurales y operativas al interior de las instituciones. Esto implica gestionar de forma planificada la resistencia al cambio, identificar agentes de cambio internos, promover liderazgos transformacionales y asegurar la comunicación efectiva entre áreas de TI, seguridad, negocio y alta dirección. La resistencia al cambio organizacional puede ser una barrera crítica, por lo que la gestión del cambio se convierte en un eje transversal del proceso de implementación.

Adopción tecnológica

El modelo híbrido propuesto considera la incorporación gradual de tecnologías y prácticas alineadas con los marcos de gobierno de TI, incluyendo herramientas de automatización, monitoreo continuo, respuesta a incidentes y evaluación de riesgos. La adopción tecnológica no debe limitarse a la adquisición de herramientas, sino contemplar la capacitación del personal, el rediseño de procesos y la alineación con los objetivos estratégicos de cada institución.

Madurez digital

La propuesta reconoce que no todas las instituciones financieras mexicanas tienen el mismo nivel de madurez digital, por lo que su enfoque es escalable y adaptable. Se parte de un diagnóstico de madurez en gobierno de TI que permite dimensionar el grado de preparación tecnológica, organizacional y cultural. Este diagnóstico es clave para definir ritmos de implementación, fases de despliegue y métricas de mejora. El uso de modelos de madurez facilita la identificación de brechas críticas y la planificación de inversiones en infraestructura, talento y procesos.

Innovación organizacional

El modelo híbrido no solo busca resolver un problema técnico, sino transformar la forma en que las instituciones abordan la ciberseguridad, la disponibilidad y la resiliencia operativa. Se plantea como un proceso de innovación organizacional que reconfigura roles, responsabilidades, cultura de seguridad y mecanismos de coordinación interinstitucional. Esta innovación tiene un enfoque holístico, integrando tecnologías emergentes, prácticas colaborativas y marcos normativos en una visión sistémica de mejora continua.

La propuesta metodológica planteada no es un producto estático, sino un proceso dinámico de transformación institucional, en el que la gestión de la innovación tecnológica constituye el eje articulador entre estrategia, tecnología, cultura y resiliencia. Este enfoque garantiza que las acciones para mitigar la indisponibilidad de TI por ciberataques trasciendan lo técnico y se conviertan en una palanca de evolución organizacional sostenida.

7.7 Modelos Teóricos

La propuesta metodológica híbrida planteada en este trabajo se fundamenta en tres modelos teóricos ampliamente reconocidos en el gobierno de tecnologías de la información: COBIT, ITIL e ISO/IEC 38500. Cada uno de estos marcos aporta un conjunto de principios, procesos y prácticas que permiten abordar el problema de la indisponibilidad operativa por ciberataques desde distintas dimensiones complementarias: estratégica, operativa y de cumplimiento.

COBIT es una metodología que aporta al problema la gestión riesgos tecnológicos y operativos, establecer una estructura de gobierno sólida y asegurar que la ciberseguridad se integre estratégicamente en la alta dirección. En el sector financiero mexicano, caracterizado por una alta regulación, interdependencia digital y necesidad de trazabilidad, COBIT permite establecer políticas claras, responsabilidades definidas y controles sistemáticos que reducen la exposición a incidentes y mejoran la capacidad de respuesta.

ITIL contribuye a garantizar la continuidad operativa, reducir los tiempos de indisponibilidad (MTTR) y responder eficientemente a incidentes críticos como ciberataques. Sus prácticas permiten organizar procesos de atención y recuperación, definir niveles de servicio (SLA) y establecer mecanismos de mejora continua. Para instituciones financieras mexicanas con alta demanda transaccional (por ejemplo, SPEI, banca móvil o cajeros automáticos), ITIL es esencial para mantener niveles aceptables de disponibilidad y servicio.

ISO/IEC 38500 refuerza la dimensión ética, estratégica y de rendición de cuentas en el uso de tecnologías, promoviendo un gobierno que no solo prevenga incidentes, sino que garantice el cumplimiento normativo de la CNBV y Banco de México. Para el sector financiero, esta norma impulsa una visión integral donde la ciberseguridad se incorpora como una responsabilidad de la alta dirección y no solo de las áreas técnicas.

8. Propuestas de solución

Existen varias mejores prácticas internacionales en gobierno de TI de las cuales partiremos para la propuesta que se plantea en este trabajo y consideraremos la **"Estrategia de ciberseguridad del Banco de México 2024 – 2027"** la cual citaremos sus objetivos:

"Objetivos hacia el Sistema Financiero que son:

SF-1 Fortalecer las disposiciones en materia de ciberseguridad. Emitir y actualizar las disposiciones del Banco de México, para que incorporen las mejores prácticas de ciberseguridad y ciber resiliencia, con base en estándares y principios internacionales.

SF-2 Reforzar el cumplimiento de las disposiciones en materia de ciberseguridad. Supervisar el cumplimiento de las disposiciones en materia de ciberseguridad por parte de las instituciones financieras reguladas y sancionar los incumplimientos detectados.

SF-3 Fomentar la colaboración y cooperación con las autoridades. Fomentar desde el ámbito de atribuciones del Banco de México, la coordinación entre autoridades del sistema financiero y de seguridad nacional, para la prevención y atención de incidentes, así como para la persecución de delitos.

SF-4 Fortalecer la ciber resiliencia en el sector financiero Banco de México. Realizar ejercicios periódicos para medir las capacidades de ciberseguridad y ciber resiliencia de las instituciones que conforman el sistema financiero, en coordinación con otras autoridades y organizaciones.

SF-5 Gestionar incidentes en el sector financiero. Fortalecer la colaboración entre instituciones y autoridades, para responder oportunamente a incidentes de ciberseguridad que se presenten en el sistema financiero."

La propuesta de solución considera un modelo de gobierno de TI para las instituciones financieras con las características específicas del sector, como la alta interconexión digital, la dependencia de infraestructura crítica y los desafíos regulatorios.

Para el desarrollo de la propuesta tomar los siguientes marcos de referencia:

COBIT (Control Objectives for Information and Related Technologies). Es un marco ideal para México debido a su enfoque en la alineación estratégica entre TI y los objetivos empresariales. COBIT permite gestionar riesgos, cumplir con regulaciones y optimizar recursos tecnológicos, lo cual es crucial para el sector financiero mexicano.

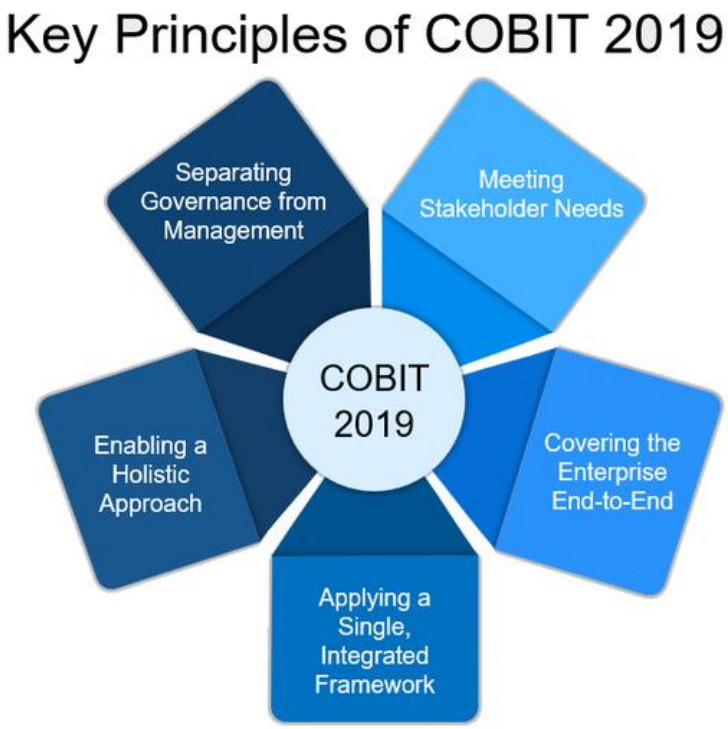
ITIL es útil para mejorar la gestión de servicios de TI, asegurando la continuidad operativa y la rápida recuperación ante incidentes. Su enfoque en la calidad del servicio y la satisfacción del cliente lo hace especialmente relevante para instituciones financieras.

ISO/IEC 38500 Este estándar internacional proporciona principios claros para el gobierno de TI, ayudando a las instituciones mexicanas a tomar decisiones responsables y alineadas con las mejores prácticas globales.

Antes de definir la solución híbrida presentada en este trabajo, se analizaron diversas alternativas metodológicas basadas en marcos de referencia reconocidos internacionalmente en materia de gobierno, gestión y dirección estratégica de tecnologías de la información. A continuación, se presentan tres propuestas alternativas, cada una sustentada en el uso exclusivo de un modelo: COBIT, ITIL o ISO/IEC 38500.

Propuesta 1.- COBIT

Esta alternativa se enfoca exclusivamente en el marco COBIT 2019, desarrollado por ISACA, el cual permite diseñar, implementar y mejorar la gobierno y gestión de TI en las organizaciones.



ITSM Docs. [*What is COBIT 2019*]. Recuperado 1 de Septiembre del 2023, de https://www.itsm-docs.com/blogs/cobit/what-is-cobit-2019

Bajo esta opción, se aplicarían los componentes de diseño de sistema de gobierno, dominios de gestión, procesos, metas de desempeño, y evaluaciones de madurez en la que se identifican las siguientes ventajas y limitaciones:

Ventajas:

- Permite una alineación estratégica entre TI y negocio.
- Facilita el control y gestión de riesgos de TI.
- Ofrece herramientas de evaluación de madurez y métricas.
- Está alineado con normas como ISO/IEC 27001, COSO, entre otras.

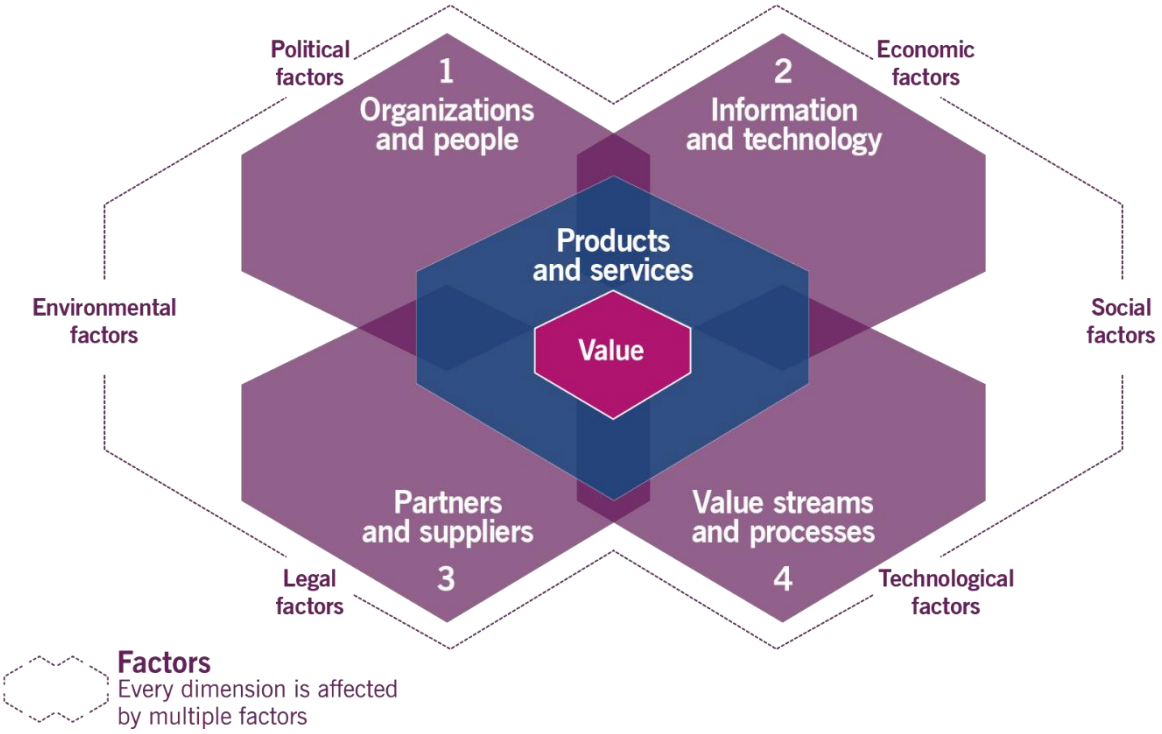
Limitaciones:

- Tiene menor enfoque operativo, por lo que no aborda directamente la continuidad de servicios.
- Requiere alto nivel de madurez organizacional para su implementación efectiva.
- No ofrece prácticas detalladas para gestión de incidentes o servicio al cliente.

En esta opción se identifica con una gran aplicabilidad en el contexto de las instituciones del sector financiero mexicano con estructura de gobierno clara, alta formalización, y capacidad para estructurar y controlar procesos complejos.

Propuesta 2.- ITIL

Esta alternativa propone utilizar solamente el marco ITIL 4, centrado en la gestión de servicios de TI.



QRP [*What is ITIL*]. Recuperado 14 de Abril del 2024, de https://www.qrpinternational.be/blog/it-governance-and-service-management/what-is-itil/

Se emplearían las prácticas de gestión de incidentes, continuidad del servicio, gestión de problemas, niveles de servicio y mejora continua, con enfoque en la operación y soporte en la cual podemos encontrar las siguientes ventajas y limitaciones.

Ventajas:

- Mejora la disponibilidad y calidad de los servicios tecnológicos.
- Reduce los tiempos de respuesta ante incidentes (MTTR).
- Favorece una cultura de mejora continua basada en KPIs.
- Es más fácil de adoptar operativamente, especialmente por áreas técnicas.

Limitaciones:

- Tiene poca orientación estratégica o de gobierno corporativo.
- No cubre temas como riesgo, auditoría o toma de decisiones en la alta dirección.
- Puede generar dependencia en el área operativa sin integrarse al negocio.

La utilización en el contexto de las instituciones del sistema financiero mexicano podría ser recomendable para operaciones altamente digitalizadas, que buscan optimizar su disponibilidad operativa sin reestructurar su gobierno.

Propuesta 3.- ISO/IEC 38500

Esta alternativa se basa en el uso exclusivo de la norma ISO/IEC 38500, que establece principios y lineamientos para el gobierno corporativo de TI y se enfoca en el papel de la alta dirección en el uso responsable, estratégico y ético de la tecnología la cual apoya a una implementación dirigida en la cual podemos encontrar las siguientes ventajas y limitantes.

Ventajas:

- Fomenta la toma de decisiones informadas y responsables en TI.
- Asegura la alineación de TI con las metas corporativas.
- Promueve el cumplimiento regulatorio y la transparencia.

Limitaciones:

- Es un marco normativo y general, sin detalle técnico u operativo.
- No incluye metodologías para gestión de incidentes ni operación de servicios.
- Requiere compromiso del más alto nivel directivo.

El aplicar esta propuesta en el contexto del sector financiero mexicano podemos encontrar que esta propuesta puede ser adecuada para instituciones en proceso de transformación digital, con foco en el cumplimiento normativo, ética corporativa y gobierno de TI, como casas de bolsa o fintechs.

Propuesta 4.- Solución hibrida

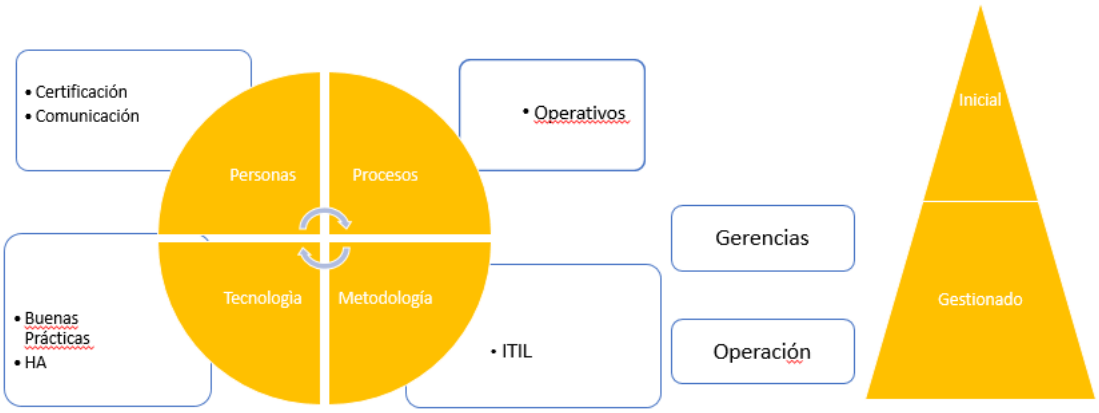
En la propuesta híbrida en la que se integran las tres propuestas anteriores ya que cada marco tiene fortalezas claras en su dominio de aplicación, ninguno de ellos, por separado, aborda de forma integral los tres niveles del problema: estratégico, táctico y operativo.

La propuesta híbrida seleccionada como propuesta de solución a la problemática identificada integra COBIT (gobierno y control), ITIL (operación y disponibilidad) e ISO/IEC 38500 (dirección y responsabilidad organizacional), permitiendo una respuesta más robusta y escalable ante la indisponibilidad de TI provocada por ciberataques en el sistema financiero mexicano.

En esta propuesta se obtendrían las ventajas de cada una de las propuestas antes mencionadas y se busca mitigar las limitantes de cada una de ellas para formar un esquema holístico para la atención de la problemática.

De forma conceptual la propuesta híbrida permite complementar el gobierno de Ti con madurez , mejora continua y complementar lo existente sin el riesgo de la transición disruptiva esta evolución en la implementación de la solución y su evolución se muestra en las siguientes imágenes:

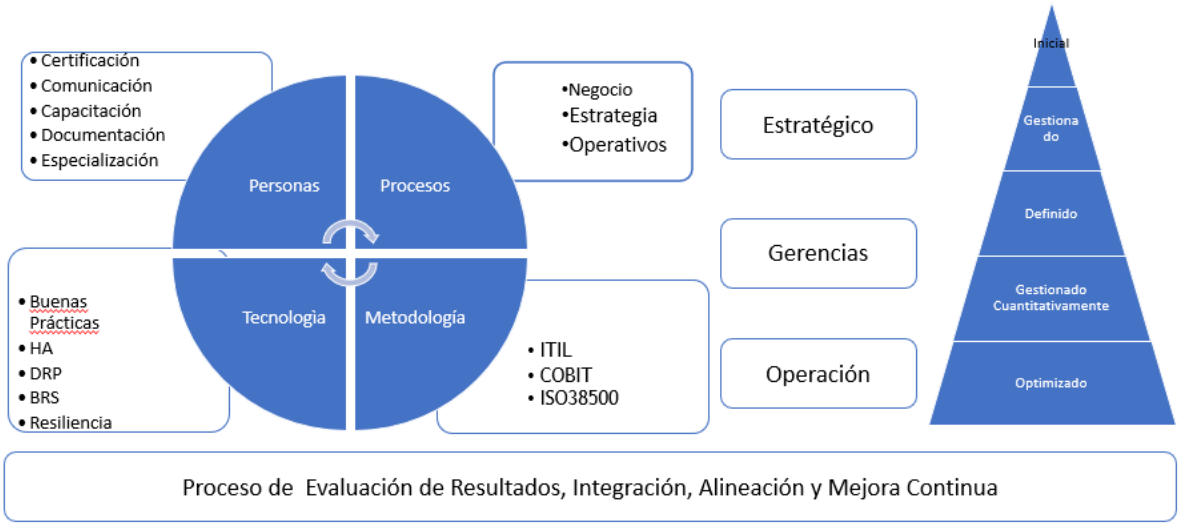
Actual:



Pantoja, A. . *Gobierno de TI Inicial* [Imagen de la situación inicial].

En la Imagen de la situación inicial en la que se identifican elementos de gobierno, metodologías, grado de madurez y participación de niveles de operativos y gerenciales donde se concentra la toma de decisiones que permiten mantener las operaciones con las diferentes complicaciones que se buscar

Propuesto:



Pantoja, A. . *Propuesta de modelo propuesto de gobierno de TI* [Imagen que ilustra los pasos de implementación gradual, monitoreo y auditorías de la solución propuesta].

En la imagen se busca mostrar el desarrollo de la solución propuesta y cómo se da la interacción de su implementación utilizando las diferentes recursos y marcos de referencia existentes tomando diferentes metodologías y procesos que se vuelven un ciclo continuo de mejora, así como un análisis de crecimiento en la madurez de los procesos que se buscan implementar.

Todos estos procesos son evaluados, medidos, integrados, auditados y por supuesto alineados a la estrategia de desarrollo de crecimiento de la institución financiera.

La propuesta identifica que con la implementación busca incidir en las afectaciones y mantener la tendencia de reducción en las afectaciones para el año 2025 de forma integral para la institución financiera en la que se implemente de manera holística con las áreas de tecnología, seguridad y negocio.

Describiremos los elementos de la propuesta de solución:

- Criterios de selección
- Proceso metodológico de la solución
- Componentes de la solución
- Aplicación de la solución
- Pasos para implementar la solución
- Implementación e incidencia en el problema
- Evaluación de impacto y mejora continua
- Adaptación cultural y organizacional

- Colaboración inter-institucional
- Metodologías cualitativas y cuantitativas
- Proceso de validación y aplicación de propuesta
- Validación con Expertos
- Requisitos y Consideraciones
- Metodología de trabajo

9 Criterios de selección

Para seleccionar la propuesta híbrida fue necesario considerar los siguientes elementos: enfoques principales, nivel de aplicación, fortaleza, limitaciones, adecuación al contexto mexicano, capacidad para mitigar indisponibilidad por ciberataques tal como se muestran en la siguiente tabla:

Elemento / Propuesta	Propuesta 1: COBIT	Propuesta 2: ITIL	Propuesta 3: ISO/IEC 38500	(Propuesta 4: Híbrida COBIT + ITIL + ISO/IEC 38500)
Enfoque principal	Gobierno y gestión de TI	Gestión de servicios de TI	Gobierno corporativo de TI	Gobierno integral: estrategia, operación y dirección
Nivel de aplicación	Estratégico y táctico	Táctico y operativo	Estratégico	Estratégico, táctico y operativo
Fortalezas	Evaluación de madurez	Mejora la disponibilidad, reducción de incidentes	Alineación con negocio	Cobertura integral, escalabilidad, sinergia entre niveles organizacionales
Limitaciones	Requiere alta madurez organizacional	Limitada visión estratégica, dependencia operativa	Generalidad, poco detalle técnico-operativo	Mayor complejidad de implementación, requiere gestión del cambio

Elemento / Propuesta	Propuesta 1: COBIT	Propuesta 2: ITIL	Propuesta 3: ISO/IEC 38500	(Propuesta 4: Híbrida COBIT + ITIL + ISO/IEC 38500)
Adecuación al contexto mexicano	Bancos con estructura madura y procesos controlados	Instituciones con alta operación digital	Entidades con foco en cumplimiento y ética	Sector financiero con alta interdependencia digital y necesidades de resiliencia
Capacidad para mitigar indisponibilidad por ciberataques	Parcial: enfoque en riesgos y control	Alta: respuesta operativa inmediata	Baja: depende del compromiso directivo	Alta: fortalece prevención, operación y gobierno
Requerimientos de implementación	Marco formal, recursos de planificación	Procesos técnicos, KPIs, cultura de servicio	Alta dirección involucrada, alineación con misión	Integración organizacional, gestión del cambio, evaluación de madurez

Alberto Pantoja (2025). *Comparación de cuatro propuestas metodológicas [Tabla 2]. Elaboración propia con base en fuentes institucionales.*

En la tabla podemos visualizar que el enfoque de sumar las ventajas de cada una de las soluciones basadas en una metodología especifica aportan de manera conjunta a una solución integral

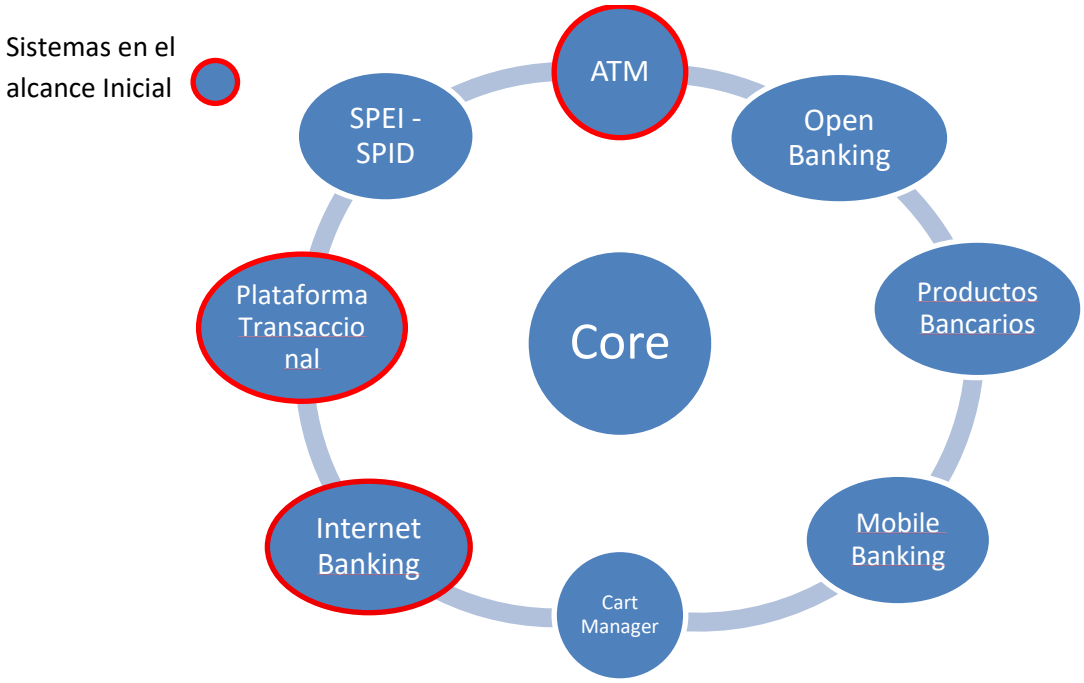
10 Proceso metodológico de la solución

El proceso metodológico cita la solución considera los elementos de alcance, proceso y validación como se muestra en la siguiente figura:

Pantoja, A. (2025). *Criterios de selección de la solución* [Imagen que ilustra del proceso metodológico de la solución propuesta].

10.1 Alcance de la propuesta de solución

Partiendo en los sistemas en los cuales se ha detectado la mayor incidencia de ciberataques que son **Internet Bancking, Plataforma Transaccional y ATM** en una institución financiera en México como un programa piloto que posteriormente se pueda implementar en los otros sistemas de TI como se muestra en la siguiente figura:



Pantoja, A. (2025). *Figura conceptual de la arquitectura TI: Modelo ilustrativo de sistemas financieros* [Imagen que identifica el alcance inicial de la propuesta].

10.2 Proceso de la propuesta de solución

De manera secuencial se integra un proceso en el cual se muestra en la siguiente figura:

Pantoja, A. (2025). *Criterios de selección de la solución* [Imagen que ilustra del proceso de la solución propuesta].

Diagnóstico

En este primer punto del proceso se desarrollan entrevistas con los responsables de la operación y se desarrollan cuestionarios y/o requerimientos de información para para hacer una diligencia que permita recabar la información y evaluación de madurez utilizando las

herramientas como check list, matriz de evaluación de madurez necesaria para para desarrollo de los documentos que se trabajan en el siguiente paso.

La identificación de hallazgos

En este paso del proceso iniciamos con el desarrollo de dos entregables que se complementan, el primero es una matriz de hallazgos en los cuales se integra el ID de hallazgos, recomendaciones para mitigar el hallazgo, prerrequisitos para la implementación de la recomendación y/o solución, Criticidad con la que se atenderá la acción correctiva , observaciones al respecto del hallazgo identificado, afectaciones identificadas a los sistemas de negocio y un plazo estimado en el cual se puede implementar la solución.

El segundo entregable es un documento donde se detalla y documentan las evidencias al respecto de los hallazgos, se integra el detalle de la solución con el soporte de las buenas practicas de los fabricantes de tecnologías, apego a las normas internacionales y políticas del Banco de México, así como el listado de los componentes afectados y necesarios para la implementación de la solución.

Diseño de modelos

Tomando los entregables del paso anterior podemos desarrollar una propuesta de modelo a implementar para atender los hallazgos en base a su prioridad y presupuesto disponible para para la implementación de las remediaciones en las distintas áreas donde se identificaron áreas de oportunidad, necesidad de herramientas, capacitación y procesos.

Despliegue de la solución

El despliegue de las distintas soluciones es planificado, probado, desplegado, monitoreado, medido para contar con registros de su incidencia en los impactos provocados por su remediación ante los ciberataques, mejora en la disponibilidad, madurez en el gobierno de TI y capacitación.

Evaluación y mejora continua

Ya con los registros generados post-implementación de la solución se recaban esos registros para construir una tendencia, evaluación y predicción de necesidades que se requieren los sistemas para su operación y funcionamiento, así como una integración a un proceso de mejora continua que permita identificar los ajustes necesarios para su optimización.

10.3 Validación de la propuesta de solución

Para el proceso de validación se requieren contar con las respectivas mediciones post-implementación de las soluciones y estas son integradas en informes periódicos que pueden ser diarios, semanales, mensuales, trimestrales, semestrales en los cuales se plasman los datos del comportamiento de las soluciones implementadas y son utilizados para crear métricas, gráficas, estadísticas, tendencias, predicciones y estimaciones.

10.4 Recomendaciones para la replicabilidad de la solución híbrida

La solución híbrida propuesta, busca responder ante las afectaciones ocasionadas por los ciberataques en instituciones del sector financiero mexicano. Sin embargo, su valor estratégico puede extenderse a otros entornos institucionales, siempre que se realicen adaptaciones contextuales que consideren el tamaño, recursos, madurez digital y entorno regulatorio de cada organización.

Replicar la solución depende de la capacidad de adaptación, la flexibilidad del modelo propuesto y el liderazgo, el aplicar estos lineamientos prácticos, las organizaciones podrán ajustar la solución híbrida a sus propias necesidades y reducir la exposición a riesgos cibernéticos.

A continuación, se proponen algunas recomendaciones concretas para su replicabilidad y adaptación según el nivel de madurez digital, utilización de procesos y tamaño de la organización y algunos factores de éxito:

Bajo nivel de madurez (nivel 1–2 COBIT):

- Comenzar por aplicar solo los componentes más operativos del modelo, priorizando ITIL para mejorar disponibilidad básica y gestión de incidentes.
- Implementar un diagnóstico inicial de madurez y una hoja de ruta simplificada.
- Limitar el enfoque a los sistemas más críticos (por ejemplo, plataformas de pagos, acceso remoto o canales digitales).

Organizaciones con madurez media o alta (nivel 3–5):

- Aplicar el modelo completo, incluyendo componentes estratégicos de COBIT e ISO/IEC 38500.
- Integrar la solución en su plan de gobierno de TI, con roles formales, auditorías regulares y métricas de desempeño.

Implementación en instituciones pequeñas y medianas puede implementarse una versión simplificada del modelo, priorizando la gestión operativa y controles básicos como:

- Implementar mediante una solución modular y progresiva, iniciando con manuales, checklists y buenas prácticas de ITIL.
- Considerar servicios de seguridad tercerizados para optimizar costos.
- Aplicar el enfoque híbrido de forma estructurada y por áreas, iniciando por aquellas con alta exposición digital.
- Establecer oficinas de gobierno de TI como una PMO.
- Considerar la certificación en ISO 27001.

Escalabilidad progresiva en la cual se implemente por fases que permita:

- Iniciar en un área piloto o proceso.
- Evaluar resultados, documentar aprendizajes y escalar gradualmente a otras áreas.
- Utilizar herramientas como matrices de madurez, KPIs y checklist de cumplimiento para validar avances.
- Integrar un ciclo de mejora continua con retroalimentación periódica.

Adaptación al entorno normativo el cual este alineado a normas regulatorias nacionales como:

- Disposiciones y normas de la CNBV sobre ciberseguridad
- Requisitos de continuidad del Banco de México
- Normas de la ISO/IEC 27001
- Contar con un programa de auditorías Internas

Factores de éxito pueden se replicados para otras instituciones son:

- Compromiso de la alta dirección para la ejecución del proyecto.
- Asignación de un responsable de gobierno de TI y ciberseguridad.
- Acceso a recursos y sensibilización de la importancia del proyecto en la organizacional de forma continua.
- Posibilidad de establecer alianzas estratégicas con proveedores especializados en materia de gobierno y ciberseguridad.
-

10.5 Caso simulado

Sabadell es una institución financiera mediana con presencia nacional, que opera servicios digitales como SPEI, banca móvil y Productos Financieros. En un periodo de 12 meses ha registrado cuatro eventos de indisponibilidad operativa vinculados a incidentes

cibernéticos, uno de los cuales impactó directamente el servicio de pagos en línea, ante estos eventos, la dirección general solicitó un servicio de assessment del cual se derivó a todo un trabajo conjunto que apoyo a la reducción de la exposición a ciberataques y se estructuro un modelo de gobernó y operación que permitió incrementar la disponibilidad de sus servicios.

En este caso se aplicaron los pasos de la solución sin que esta fuera planificada desde un inicio, en el caso las actividades se fueron ejecutando en base a los resultados obtenidos de cada una de ellas y con esto se obtuvo la confianza del banco para continuar con el proceso de implementación de una solución integral en la que podemos describir que se ejecuto con los siguientes pasos:

Diagnóstico institucional (Assessment)

Se solicita y secaba información para validar la madurez basada en COBIT para evaluar los niveles actuales de gobierno de TI, gestión de riesgos, continuidad operativa y hallazgos.

Resultado fue que Sabadell presenta un nivel de madurez 2/5.

Se detecta ausencia de procesos formales para gestión de incidentes y nula participación de la alta dirección en temas de ciberseguridad.

Se presentaron los resultados alineando objetivos y se identifica el estado actual de gobernó, capacidades operativas y brechas críticas.

Diseño del modelo adaptado

Se personaliza el modelo para el entorno de Sabadell en el cual se define:

- Necesidad de la estructura de gobierno y evaluación de procesos.
- Define los procedimientos de gestión de incidentes, continuidad y recuperación.
- Se emplea para definir roles y responsabilidades directivas.

Como resultado se establece una oficina de gobierno, se formalizan procesos críticos y se aprueba un comité de ciberseguridad liderado por un director adjunto.

Se presento una solución metodológica adaptada a la organización que mitigue la indisponibilidad operativa.

Validación con simulacro

El escenario simulado fue un ataque de denegación de servicio saturación del canal de banca móvil y bloquea el portal transaccional.

Respuesta según modelo en el cual el equipo de soporte activa el plan de continuidad, redirige a un entorno alterno y se ejecuta el protocolo de recuperación.

Se mide el tiempo medio de recuperación RTO, RPO, MTTR y el nivel de cumplimiento de controles establecidos.

- El resultado fue la reducción del MTTR de 6 a 2.5 horas.
- La evaluación posterior identificó 3 desviaciones menores que fueron corregidas.

Con esta prueba se validó la eficacia operativa y organizacional de la propuesta ante escenarios reales.

Implementación progresiva

Banco Sabadell al ser en un banco de empresas se inició con los procesos prioritarios SPEI, Internet Banking.

Se utilizaron herramientas como Checklist de controles, matriz de roles y responsabilidades, KPIs de disponibilidad, informes mensuales y sesiones de revisión periódicas.

Se desarrollaron programas de capacitación a más de 50 colaboradores reciben formación en gestión de incidentes y gobierno de TI.

Se logró en los primeros 3 meses, no se registran nuevas caídas, se logran niveles de disponibilidad >99.9% y se integra la evaluación al comité de riesgos institucional.

El trabajo conjunto de las áreas logró disminuir las afectaciones operativas provocadas por ciberataques.

Evaluación y mejora continua

Se revisan indicadores de desempeño y se recogen percepciones internas a través de sesiones de seguimiento, entrevistas y encuestas de satisfacción.

El 86% del personal considera que el modelo ha mejorado la respuesta a incidentes. Se identifican oportunidades para automatizar alertas y expandir el modelo a áreas no críticas.

Se establece un ciclo de mejora continua basado en evidencia y retroalimentación.

La siguiente tabla muestra el antes y después de la implementación de una solución integral:

Dimensión evaluada	Antes de la implementación	Después de la implementación
Nivel de madurez COBIT	2/5	3.5 / 5
Disponibilidad de SPEI	98.7%	99.98%
Tiempo promedio de recuperación (MTTR)	6 horas	2.5 horas
Cumplimiento de controles	61%	89%
Participación directiva	Ocasional	Institucionalizada

Alberto Pantoja (2025). *Comparación de resultados cuantitativos [Tabla 3]. Elaboración propia con base en fuentes institucionales.*

En el caso Sabadell permite demostrar la viabilidad, aplicabilidad y adaptabilidad de la solución híbrida propuesta en este trabajo en un entorno financiero realista. La implementación por fases, la combinación de marcos complementarios y el uso de herramientas de diagnóstico y mejora continua, permitieron elevar significativamente la disponibilidad operativa, reducir los riesgos y fomentar una cultura de gobierno proactiva. Este caso respalda la tesis de que el enfoque híbrido es una alternativa robusta y escalable frente a los desafíos actuales de ciberseguridad en el sistema financiero mexicano.

11 Componentes de la solución

Una solución híbrida que combina elementos de COBIT, ITIL e ISO/IEC 38500 puede ser una solución efectiva para abordar las necesidades específicas del sector financiero mexicano.

El enfoque híbrido permite aprovechar las fortalezas de cada marco y adaptarlas a las regulaciones locales como las que se mencionan a continuación:

- Alineación con regulaciones nacionales e internacionales: Cumple con normativas locales (CNBV, Banco de México) y se adapta a estándares globales, fortaleciendo la confianza de los stakeholders.
- Resiliencia tecnológica: Reduce la vulnerabilidad a ciberataques al integrar medidas preventivas y correctivas en un único modelo de gobierno.
- Optimización de recursos: Permite priorizar inversiones en tecnología e infraestructura de acuerdo con análisis de riesgos y necesidades críticas.

- Mejora continua: Promueve la evaluación periódica y la mejora continua mediante auditorías internas y externas, asegurando la vigencia del marco híbrido.
- Fomento de la colaboración: Integra una perspectiva de colaboración entre instituciones financieras, reguladores y autoridades, fortaleciendo la respuesta conjunta ante incidentes.

12 Aplicación de la solución

Ante cualquier amenaza o ataque de ciberseguridad existen opciones de gestión que nos permiten aislar, minimizar, mitigar, anticipar o evadir los riegos que conllevan. Mencionaremos algunas de las recomendaciones para llevar a cabo la implementación de las acciones para incidir en las afectaciones de los ciberataques como pueden ser:

- Invertir en soluciones de automatización puede reducir la dependencia de personal y mejorar la eficiencia de las operaciones de ciberseguridad.
- Establecer colaboraciones con universidades, empresas tecnológicas y centros de formación para fomentar el desarrollo de talento local en ciberseguridad.
- Implementar programas internos de capacitación para mejorar las habilidades del personal existente y mantenerlo actualizado frente a las amenazas emergentes.
- Alinear sus estrategias de TI y ciberseguridad con los objetivos generales del negocio, lo que resulta en una protección insuficiente frente a amenazas emergentes.
- Implementación de estándares internacionales, aunque existen marcos como COBIT, ITIL e ISO 27001, su adopción no es uniforme. Esto deja brechas en la gestión de riesgos y en la implementación de controles efectivos.
- Supervisión y monitoreo insuficientes, la falta de monitoreo continuo y auditorías regulares dificulta la detección temprana de vulnerabilidades y actividades sospechosas.
- Contar con profesionales capacitados en ciberseguridad y gobierno de TI.
- Eliminar de la operación la infraestructura tecnológica obsoleta.
- Fortalecer una cultura organizacional en ciberseguridad.
- Cumplir de forma rigurosa las recomendaciones emitidas por la CNBV y el Banco de México.
- Fomentar el intercambio de información y colaboración entre instituciones financieras y autoridades para facilitar la respuesta coordinada ante ciberataques.
- Fomentar una cultura de ciberseguridad e implementar programas de capacitación y concienciación para todos los niveles de la organización.

- Modernizar la infraestructura tecnológica y sustituir sistemas heredados por tecnologías más seguras y actualizadas.
- Establecer procesos claros, definidos y documentar procedimientos para la gestión de riesgos y la respuesta a incidentes.
- Promover la colaboración interna facilitar la comunicación entre departamentos para una estrategia de ciberseguridad más cohesionada.

13 Pasos para implementar la solución

El proceso de acción para la implementación es el siguiente:

- Diagnóstico inicial
- Identificación de hallazgos
- Gestión de riesgos y cumplimiento normativo
- Integración gradual de marcos
- Alineación estratégica
- Desarrollo de capacidades

Diagnóstico inicial: Podemos evaluar la madurez actual del gobierno de TI y los riesgos específicos del entorno, aplicar modelos como COBIT o la evaluación de madurez de ITIL para medir el estado actual de los procesos de TI, comparar el nivel de implementación con estándares internacionales como ISO/IEC 38500.

Identificación de hallazgo: Identificamos áreas de oportunidad, riesgos, amenazas a la disponibilidad del sistema, observaciones o recomendaciones del cumplimiento normativo y vulnerabilidades en la resiliencia ante ciberataques, detectar deficiencias en procesos de respuesta a incidentes y recuperación ante desastres, se identifican necesidades de resguardo y protección de datos.

Una vez identificados los hallazgos, se debe diseñar un modelo de gobierno que se ajusten a la remediación de cada uno.

Gestión de riesgos y cumplimiento normativo: Se define la implementación de un marco de gobierno que garantice el cumplimiento de regulaciones locales, así como Integrar procesos de auditoría y monitoreo para reducir riesgos.

Integración gradual de marcos: Se incorporan los elementos más relevantes de cada marco, priorizando áreas críticas como ciberseguridad y recuperación ante desastres, optimización de servicios de TI y resiliencia, se aplican prácticas con el caso de ITIL para mejorar la gestión de incidentes y continuidad del servicio, fortalecer la utilización de procesos definidos.

Alineación estratégica: Se busca garantizar que los objetivos de TI estén alineados con la estrategia de negocio del banco y evaluar el impacto de la TI en la rentabilidad y operaciones de la institución.

Desarrollo de capacidades: Se implementa capacitación continua del personal para mejorar la gestión de procesos de toma de decisiones basados en el gobierno de TI, se invierte en formación para el personal y fomentar una cultura sólida.

14 Implementación e incidencia en el problema

Para integrar el modelo de solución sin afectar las operaciones, se recomienda una implementación gradual en fases de la solución híbrida en la cual se identifica la incidencia a la problemática planteada.

Fase de diagnóstico, diseño y validación

En esta fase se tiene el objetivo de identificar brechas en gobierno, operación y control en la cual se identifica la incidencia directa en el problema en los siguientes puntos:

- Se aplica una matriz de madurez para evaluar la capacidad de respuesta actual ante incidentes que afectan plataformas críticas como Internet Banking, Open Banking, ATM y Plataforma Transaccional.
- Se detectan vulnerabilidades organizacionales y técnicas que contribuyen a la indisponibilidad, como falta de protocolos de recuperación, duplicación de procesos o ausencia de roles definidos.
- Definir políticas de gobierno de TI del marco híbrido a todos los sistemas CORE y satélites.
- Asignar responsables para cada área clave (riesgos, cumplimiento, operaciones).

Fase de Implementación

En esta fase se tiene el objetivo de personalizar el modelo híbrido según el nivel de madurez y características de la institución en la cual Incidimos de forma directa en el problema:

- Se prioriza la integración de controles en sistemas de alto riesgo: SPEI, canal móvil y ATM, definiendo roles, flujos y políticas con base en COBIT e ISO 38500.
- Se diseñan procesos operativos específicos bajo ITIL para la gestión de incidentes, continuidad y recuperación ante las contingencias en el sistema de TI definidos en el BIA (Análisis de Impacto Empresarial) de la Institución financiera.

- Adoptar mejores prácticas de COBIT para la gestión de riesgos tecnológicos en sistema de TI.
- Implementar procesos de ITIL para mejorar la gestión de servicios financieros digitales en los sistemas Satélites.
- Alinear los principios de ISO 38500 con las decisiones estratégicas de los sistemas de Producto Bancario.

Fase de evaluación y mejora continua

En esta fase se tiene el objetivo medir resultados, corregir desviaciones y garantizar sostenibilidad de validar funcionalidad del modelo con expertos y pruebas piloto la cual Incide de forma directa en el problema:

- Se realizan simulacros de ataques a ATM, Net Bancking, Open Bancking y Plataforma Transaccional, evaluando el tiempo de recuperación (MTTR), la efectividad de las respuestas, y la coordinación entre áreas de los tres niveles de la organización.
- Se ajusta el modelo según hallazgos obtenidos en los puntos críticos, corrigiendo debilidades y reforzando mecanismos de respuesta de todas las implementaciones en cada uno de los sistemas.
- Establecer métricas clave para medir la efectividad del modelo híbrido en cada uno de los sistemas.
- Realizar pruebas de ciberseguridad y auditorías de cumplimiento de los sistemas expuestos en la res desmilitarizada.
- Ajustar la estrategia según los resultados obtenidos.
- Monitoreo y Auditoría Supervisar continuamente el desempeño de los sistemas y realizar auditorías regulares para identificar brechas.
- Monitoreo de indicadores clave como: frecuencia de fallas, cumplimiento de SLAs, tiempos de indisponibilidad y eficacia de la respuesta ante incidentes.
- Se consolida un ciclo de mejora continua, que permite anticiparse a nuevas amenazas cibernéticas y reforzar de forma sistemática la disponibilidad de servicios.

Este despliegue por fases asegura que la solución híbrida responda directamente a los síntomas concretos del problema identificado, evitando propuestas genéricas y centrando los esfuerzos en los puntos neurálgicos donde la indisponibilidad genera mayor impacto, tanto económico como reputacional, se busca elevar la resiliencia digital de las instituciones financieras mexicanas mediante una estrategia estructurada, adaptable y medibles como se muestra en la siguiente tabla:

Fase	Puntos críticos	Indicadores de mejora
Diagnóstico	Se toman los sistemas de alcance inicial	Grado de madurez, identificación de hallazgos
Diseño	Procesos de continuidad, ciberseguridad, procesos y capacitación	Modelos ajustados a necesidades ante riesgos de ciberataques
Validación	Respuesta ante ciberataques simulados	MTTR, KPI´s, RTO , RPO
Implementación	Los sistemas de alcance inicial	Disponibilidad > 99.9%, cumplimiento normativo
Evaluación/mejora continua	Toda la infraestructura crítica y su operación	KPIs actualizados, auditorías cumplidas, resiliencia, reducción de afectaciones y No de ciberataques

Alberto Pantoja (2025). *Relación entre fases, puntos críticos e indicadores [Tabla 4]. Elaboración propia.*

15 Evaluación de impacto y mejora continua

Esta etapa permite medir los resultados reales de la intervención, identificar áreas de oportunidad, y garantizar que la solución no solo funcione en el corto plazo, sino que se ajuste y evolucione frente a nuevos desafíos y cambios en el entorno.

Una vez desplegado el enfoque híbrido, es esencial medir su efectividad y realizar mejoras definiendo Indicadores de desempeño como:

- Reducción de incidentes de ciberseguridad (medido por número de ataques y tiempos de respuesta).
- Mejora en disponibilidad de sistemas financieros (reducción del tiempo de inactividad – MTTR Mean Time to Repair).
- Nivel de cumplimiento normativo (cumplimiento con regulaciones de la CNBV y Banco de México).
- Satisfacción del usuario (evaluada por encuestas y métricas de servicio).

El ciclo de mejora continua se adopta con un enfoque basado en el ciclo PDCA (Plan – Do – Check – Act), ampliamente utilizado en marcos como ITIL e ISO/IEC 27001. Este ciclo permite una gestión iterativa que fortalece la resiliencia operativa:

- Plan (Planificar): Establecer objetivos, métricas y planes de implementación.
- Do (Hacer): Ejecutar la solución híbrida por fases.
- Check (Verificar): Medir resultados, identificar desviaciones y realizar auditorías.
- Act (Actuar): Ajustar el modelo, rediseñar procesos y escalar buenas prácticas.

Este enfoque promueve una postura dinámica frente a riesgos, en lugar de un modelo rígido.

16 Adaptación cultural y organizacional

Es fundamental que el modelo incluya estrategias para fomentar una cultura de ciberseguridad y capacitar al personal. Esto ayudará a superar barreras como la resistencia al cambio y la falta de talento especializado.

Uno de los principales desafíos en la implementación de modelos de gobierno de TI, como el propuesto en esta investigación, no reside únicamente en la tecnología, sino en la capacidad de las organizaciones para adaptarse cultural y estructuralmente a nuevas formas de trabajo, control, colaboración y toma de decisiones. La solución híbrida basada en COBIT, ITIL e ISO/IEC 38500 exige cambios no solo en procesos, sino también en valores, comportamientos y dinámicas organizacionales.

La cultura organizacional influye directamente en la adopción, resistencia o éxito de iniciativas de transformación digital y de ciberseguridad.

Para que la propuesta híbrida funcione correctamente, es necesario que las organizaciones promuevan una cultura:

- Orientada a la mejora continua
- Basada en el aprendizaje organizacional
- Comprometida con la gestión de riesgos
- Que valore la colaboración interfuncional
- Con alto nivel de concientización sobre ciberseguridad

La adaptación cultural y organizacional es un requisito y pilar para la solución híbrida propuesta. Se requiere de una base cultural sólida, la propuesta no se limita a definir procesos, sino que propone una transformación institucional que alinee personas, procesos

y tecnología hacia una visión compartida de resiliencia, continuidad y responsabilidad digital.

17 Colaboración inter-institucional

Promover la cooperación entre instituciones financieras, reguladores y autoridades nacionales e internacionales es clave para fortalecer la resiliencia del sistema financiero mexicano.

Para identificar y mitigar vulnerabilidades críticas en los sistemas de TI financieros, se pueden utilizar metodologías de evaluación de riesgos tanto cualitativas como cuantitativas.

Uno de los factores críticos para enfrentar eficazmente los riesgos de indisponibilidad operativa por ciberataques en el sistema financiero mexicano es la colaboración interinstitucional.

Debido al carácter altamente interconectado, regulado y dependiente de infraestructura compartida del sistema financiero, ninguna institución puede afrontar estos riesgos de manera aislada. Esto puede verse en una interrupción en plataformas como SPEI, SPID o CoDi que puede afectar a múltiples bancos y usuarios de forma simultánea. Esto convierte los ciberataques en riesgos transversales y no solo en amenazas aisladas.

Infraestructura crítica compartida entre las Instituciones financieras dependen de servicios, como el centro de datos del Banco de México, redes SWIFT o proveedores tecnológicos tercerizados como es la Nube y/o el SOC lo que hace necesaria la gestión colaborativa de riesgos comunes.

Necesidad de respuesta coordinada en ataque masivos como ataques dirigidos al sector, la respuesta efectiva requiere cooperación entre instituciones afectadas, autoridades regulatorias y entidades de apoyo como proveedores especializados.

Se consideran mecanismos de comunicación interinstitucionales como son:

- Circulares y lineamientos del Banco de México y CNBV
- Espacios de colaboración entre instituciones, impulsados por asociaciones como iniciativas del Banco de México.
- Establecer protocolos de alertar a otras instituciones y evitar propagación de ataques.

18 Metodologías cualitativas y cuantitativas

Estas metodologías se centran en la evaluación subjetiva de los riesgos, utilizando escalas descriptivas y análisis experto. Son útiles cuando no se dispone de datos precisos o cuando se requiere una evaluación rápida.

El presente trabajo adopta un enfoque metodológico mixto, combinando métodos cuantitativos y cualitativos, así como técnicas e instrumentos de análisis validados en el campo del gobierno de TI y la ciberseguridad. Esta integración permite abordar la problemática de la indisponibilidad operativa causada por ciberataques desde múltiples dimensiones: estratégica, táctica y operativa.

Cuantitativos

Se utilizaron para medir de manera objetiva variables como:

- Tiempos promedio de recuperación (MTTR)
- Frecuencia de incidentes de disponibilidad
- Porcentaje de cumplimiento de niveles de servicio (SLA)

Estos datos permiten cuantificar el impacto de la solución híbrida y generar comparativos antes y después de su aplicación.

Cualitativos

Permitieron comprender fenómenos organizacionales no observables directamente, tales como:

- Percepciones sobre cultura de ciberseguridad
- Barreras para la adopción tecnológica
- Nivel de compromiso de la alta dirección

Las entrevistas, análisis de contenido y observación participativa se emplearon para enriquecer la comprensión contextual del problema.

Mixtos

Se integró también una estrategia comparativa mediante con el fin de:

- Contrastar la propuesta con prácticas aplicadas en los casos de Banco de Chile, Santander y JPMorgan
- Identificar buenas prácticas adaptables al contexto mexicano

Análisis de Impacto y Probabilidad:

- Clasifica los riesgos en función de su impacto y probabilidad de ocurrencia

- Se utiliza en combinación con matrices de riesgo para priorizar amenazas

Evaluación basada en escenarios:

- Simula posibles ataques y analiza cómo afectarían a la organización
- Nivel de cumplimiento normativo (cumplimiento con regulaciones de la CNBV y Banco de México)
- Desarrollar encuestas de satisfacción

En el desarrollo de la propuesta híbrida se requiere de la utilización de:

- Técnicas
- Instrumentos

18.1 Técnicas utilizadas

En la propuesta híbrida se plantea la utilización de técnicas como las que se enuncian en la siguiente tabla donde se describen las técnicas y se desarrolla su justificación para ser utilizadas en la propuesta:

Técnica	Descripción	Aplicación
Análisis de impacto y probabilidad	Evaluación de amenazas y vulnerabilidades con enfoque en impacto y probabilidad.	Priorización en los procesos definidos en el BIA
Entrevistas	Aplicación de guías semiestructuradas a expertos de TI, seguridad, reguladores y usuarios clave.	Validación cualitativa y viabilidad del modelo propuesto.
Pruebas de DRP y penetración (Pentest)	Pruebas controladas de incidentes y ciberataques	Validación técnica de la capacidad de respuesta y recuperación.

Alberto Pantoja (2025). *Relación de Técnicas , Descripción y aplicación [Tabla 5]. Elaboración propia.*

18.2 Herramientas Utilizadas

Para la propuesta de solución se requieren de herramientas para el desempeño de funciones específicas de la solución y de las cuales se desarrolla su justificación para ser utilizadas en la propuesta:

Instrumento	Función	Justificación
Encuestas	Medir la percepción sobre prácticas de gobierno.	Permite cuantificar la adopción del modelo propuesto.
Matriz de evaluación de madurez	Evalúa el nivel de madurez del gobierno de TI.	Es el diagnóstico y da pauta de las acciones para implementación.
Checklists	Permite validar la entrega de requerimientos de información.	Asegura trazabilidad y cumplimiento de requerimientos.
Matriz de hallazgos	Información obtenida durante entrevistas y evidencias.	Permite identificar y catalogar áreas de oportunidad a trabajar en la propuesta.

Alberto Pantoja (2025). *Relación de instrumentos, función y justificación [Tabla 6]. Elaboración propia*

18.3 Justificación del enfoque metodológico

El uso combinado de métodos, técnicas e instrumentos de la solución híbrida son:

- Medir de forma objetiva del impacto de la solución híbrida.
- Validar su aplicabilidad y aceptación organizacional en instituciones financieras.
- Asegurar que el modelo responda tanto a necesidades técnicas como estratégicas, promoviendo una transformación organizacional.

Este enfoque metodológico busca no solo probar la viabilidad del modelo híbrido, sino también generar aprendizajes transferibles y recomendaciones prácticas para su replicabilidad, alineando tecnología, procesos y personas en la mejora continua de la resiliencia operativa.

19 Proceso de validación y aplicación de propuesta

El proceso de validación establece criterios claros que permitan medir el éxito de la alternativa. Algunos criterios relevantes para este caso podrían ser:

Alineación estratégica: La alternativa debe integrarse con los objetivos de negocio y regulaciones locales (CNBV y Banco de México).

Efectividad: Capacidad para reducir los tiempos de indisponibilidad de los sistemas y la frecuencia de los ciberataques.

Viabilidad técnica: Compatibilidad con la infraestructura y recursos tecnológicos actuales.

Sostenibilidad: Factibilidad de mantener la solución a largo plazo sin incurrir en costos excesivos.

Impacto medible: Capacidad para demostrar mejoras en métricas clave como MTTR, disponibilidad y cumplimiento normativo.

Medición del desempeño como son:

- Tasa de disponibilidad del sistema.
- Reducción del MTTR
- Número de ciber incidentes durante el período
- Porcentaje de cumplimiento con estándares y regulaciones
- Feedback del personal especializado (TI, seguridad, operaciones)
- Realiza encuestas para medir la percepción de los usuarios sobre la disponibilidad y confiabilidad de los servicios.

Evaluación de riesgos e identificar nuevas vulnerabilidades: Durante la validación prestar atención a posibles brechas de seguridad o desafíos imprevistos que surjan al implementar la solución.

Realiza un análisis comparativo de los resultados obtenidos tras la implementación de la alternativa piloto con la situación inicial.

Auditorías externas: Contrata evaluadores independientes para validar que la alternativa cumple con los estándares internacionales y locales.

20 Validación con Expertos

La propuesta de solución se valida con los siguientes perfiles de las áreas de infraestructura, operaciones y ciberseguridad de una institución financiera.

A continuación, se presentan los perfiles de los responsables con los que se validó la solución:

Puesto	Gerente Infraestructura	Gerente Operaciones	Especialista Ciberseguridad
Perfil	Ing. Sistemas Certificado PMP , ITIL Más de 10 años de experiencia en puestos de gestión de infraestructura en el sector financiero. Responsable de gestión de infraestructura de servidores , base de datos y telecomunicaciones. Experiencia en proyectos de upgrade, refresh, migraciones, DRP y BCP.	Lic. Tecnologías de la información Certificación ITIL Sólidos conocimientos de PMP . Más de 10 años de experiencia en operaciones del sector financiero. Amplia experiencia en desarrollo de reglas de negocio y cumplimiento normativo .	Ing. Sistemas Certificado en seguridad de nube de Google y AWS. Más de 5 años em desarrollo de arquitectura de seguridad y desarrollo de políticas de seguridad. Sólidos conocimientos en hacking ético. Más de 10 años de experiencia en áreas de ciberseguridad en instituciones del sector financiero.

Alberto Pantoja (2025). *Descripción de perfiles de expertos [Tabla 7]. Elaboración propia*

Se comentaron los diferentes elementos que constituyen la solución planteada como es el alcance, la viabilidad, el planteamiento, la planificación y las expectativas de los resultados que se estarían presentando para que esta propuesta se materialice dentro de la institución financiera.

Se obtuvieron comentarios que sugieren desarrollar un primer ejercicio o prueba piloto que permita tomar los primeros Inputs para el desarrollo de una primera matriz de hallazgos, desarrollo de una matriz alineada, catalogada, priorizar y estimar tiempos que permitan completar una propuesta de proyecto, documentando las actividades que se desarrollen para la implementación de la solución propuesta.

Como parte de la validación de la propuesta se desarrolló una agenda con la que se trabajó en reuniones para obtener sus comentarios.

Esta agenda fue la siguiente:

- El alcance de la propuesta se encuentra alineados a los objetivos organizaciones
- Cuáles son las fases para la implementación de la solución
- Cuáles son los pasos a seguir para la implementación de la solución
- Como medir la efectividad de la implementación

En base a estas mesas de trabajo de justaron aspectos de la propuesta de solución.

Puntos relevantes que se obtuvieron de estas sesiones de trabajo son:

- Las metodologías planteadas por sí solas no cuentan con los alcances para incidir por completo en las afectaciones derivadas por ciberataques por lo que la utilización de la solución híbrida es la más completa para el objetivo planteado.
- Las propuestas utilizando de manera separada cada una de las propuestas de metodología tiene distintos enfoques para cada uno de los niveles de la organización
- La utilización de metodologías sin una medición holística se puede ver sesgadas de los objetivos estratégicos de la organización.
- La medición e interacción entre las tres metodologías planteadas para el desarrollo de la propuesta híbrida integra elementos y asume las limitantes de las anteriores.
- La solución híbrida representa una inversión en la cual los elementos cuantitativos tienen la expectativa de que puede producir un financiamiento tangible al no tener afectaciones económicas, impactando directamente al negocio lo cual la convierte en una solución rentable.
- Se identifica la necesidad de una interacción activa entre las distintas áreas involucradas, generando un entorno de trabajo que obliga a la coordinación estrecha y romper con barreras de comunicación dan apertura a la comunicación y coordinación ágil.
- La solución que se plantea debe ser dotada de un liderazgo y capacidad de comunicación en los distintos niveles de la organización lo cual se debe definir una implantación en fases.
- La priorización de los sistemas sobre los cuales se busca trabajar es definida por la alta dirección.
- La propuesta debe ser evaluada por la alta dirección para su implementación.
- El periodo de evaluación de la propuesta y asignación de recurso podría no estar disponible para el actual año por lo que podría estar proyectado para el año 2026.

Ante la retroalimentación se determinó que el proyecto se evaluará y se podría implementar para el año 2026 en caso de que sea aprobado el presupuesto para su ejecución y desarrollo.

En la propuesta se desarrolló el siguiente cronograma para contar con una duración estimada y poder tener una referencia de los recursos humanos para el proyecto en el cual se definen indicadores de avance por cada una de las fases del proyecto.

Fase	Actividad clave	Duración en semanas	Responsables	Indicadores de avance
Diagnóstico	Aplicar encuesta de madurez, entrevistas, y matriz de hallazgos	1–3	TI, Auditoría, Seguridad, Consultores	Porcentaje de áreas evaluadas Nivel de madurez base (1–5) Informe de hallazgos
Diseño	Adaptar el modelo híbrido a la institución Definir roles y procesos clave	4–6	Oficina de Proyectos, TI, RH	Porcentaje de procesos definidos No roles establecidos Modelos validados
Validación	Mesas con expertos, simulacro de incidentes controlados	7–8	Seguridad, Dirección TI, SOC	Simulacro realizado Tiempo de respuesta (MTTR) Porcentaje de hallazgos corregidos
Implementación inicial	Despliegue piloto en SPEI, banca móvil, ATM, capacitación al personal	9–12	TI Operaciones, RH	Porcentaje de sistemas intervenidos Porcentaje de personal capacitado No. controles operativos activos
Evaluación y ajustes	Revisión de checklist, matriz de hallazgos, retroalimentación interna	13–15	Auditoría, Riesgos, Seguridad	Porcentaje de hallazgos mitigados No. de desviaciones corregidas Nivel o porcentaje de cumplimiento del checklist
Consolidación	Análisis de resultados (KPIs pre/post), propuesta de escalamiento	16	Alta dirección, Cumplimiento, TI	Porcentaje de variación en la disponibilidad Porcentaje de reducción de incidentes Plan de continuidad y DRP aprobado

Alberto Pantoja (2025). *Cronograma de implementación de la solución [Tabla 8]. Elaboración propia*

El cronograma presentado es el resultado del análisis de los expertos que emitieron sus recomendaciones al respecto de los tiempos y los indicadores de avance que se pueden medir y permiten la gestión del proyecto.

El desarrollo del cronograma y el análisis de los expertos permitió acortar el proyecto a 16 semanas agregando una última fase de consolidación.

21 Requisitos y Consideraciones

Para que la solución híbrida sea efectiva en mitigar la indisponibilidad operativa causada por ciberataques en el sector financiero, es indispensable que la institución en la que se implemente reúna una serie de condiciones mínimas organizacionales, técnicas y de gobierno. Estas condiciones permiten garantizar la viabilidad, sostenibilidad y escalabilidad del modelo propuesto.

21.1 Nivel de madurez tecnológica

La solución híbrida requiere que la organización cuente con un nivel de madurez digital y de TI mínimo de nivel 2 a 3, según el modelo de madurez de COBIT. Esto implica que:

- Existan procesos básicos definidos y documentados en áreas clave como gestión de TI, seguridad y continuidad operativa.
- Haya infraestructura tecnológica funcional y auditada, incluyendo respaldo de datos, monitoreo básico y conectividad segura.
- Se cuente con un inventario actualizado de activos críticos, especialmente aquellos relacionados con SPEI, banca móvil, cajeros automáticos y plataformas de pagos.

Sin este nivel básico de madurez, la solución requerirá primero una etapa previa de fortalecimiento institucional y técnico.

21.2 Compromiso de la alta dirección

La participación activa de la alta dirección (consejo, dirección general, directores de TI, riesgos y cumplimiento) es una condición esencial, ya que:

- ISO/IEC 38500 establece que el gobierno de TI es una responsabilidad directiva, no exclusivamente técnica.
- COBIT requiere que la toma de decisiones esté alineada con la estrategia de negocio y que se asignen roles claros de gobierno y gestión.
- La adopción del modelo implica cambios organizacionales, reasignación de recursos, gestión del cambio y priorización presupuestaria, lo cual no es posible sin liderazgo desde el más alto nivel.

Además, la alta dirección debe patrocinar públicamente la implementación, promover la cultura de ciberseguridad y supervisar los avances por medio de indicadores claros.

21.3 Capacidad presupuestal

Aunque la propuesta es escalable y adaptable, se requiere una inversión mínima inicial para asegurar su despliegue básico, que puede cubrir:

- Capacitación del personal en COBIT, ITIL y buenas prácticas de ciberseguridad.
- Consultoría o acompañamiento externo durante el diagnóstico, diseño y validación.
- Herramientas para auditoría, monitoreo, gestión de incidentes y evaluación de madurez.
- Implementación de controles de seguridad (por ejemplo, autenticación multifactor, respaldo de datos, segmentación de red).

El presupuesto puede modularse según el tamaño de la institución, pero sin recursos básicos se comprometería la efectividad del modelo y su continuidad.

21.4 Cultura organizacional orientada a la mejora continua

La solución propuesta se basa en la mejora continua (ciclo PDCA) y en la adopción de prácticas sostenibles. Para ello, se requiere:

- Disposición al cambio por parte del personal técnico, operativo y administrativo.
- Colaboración interdepartamental, especialmente entre áreas de TI, seguridad, cumplimiento y negocio.
- Un entorno que incentive la evaluación de procesos, el aprendizaje organizacional y la revisión constante de indicadores.

Si no existe esta cultura, es recomendable iniciar con actividades de sensibilización, capacitación básica y construcción de una visión compartida.

21.5 Infraestructura de ciberseguridad y continuidad

Finalmente, la institución debe contar con una infraestructura mínima de ciberseguridad y continuidad operativa, que incluya:

- Mecanismos de respaldo y recuperación ante fallos.

- Controles de acceso y monitoreo de actividades críticas.
- Manuales operativos y de contingencia actualizados.
- Capacidad de realizar simulacros y auditorías internas.

Estas condiciones garantizan que el modelo híbrido no solo se implemente, sino que funcione de manera efectiva y genere resultados medibles.

22 Metodología de trabajo

La metodología de trabajo utilizaremos el diseño transversal, entendido como aquel que recolecta y analiza datos en un solo momento en el tiempo, permitiendo identificar patrones, correlaciones y comportamientos actuales en relación con el fenómeno estudiado.

La muestra de datos analizados se acotó a un periodo de los últimos cinco años (2020–2024), con el objetivo de considerar únicamente eventos recientes, marcos normativos vigentes y tendencias actuales en ciberseguridad.

Este diseño permite captar una fotografía actual del contexto operativo y normativo del sistema financiero mexicano en materia de ciberataques, así como del nivel de madurez digital y organizacional frente a estos riesgos.

La investigación aplicada que busca resolver un problema práctico mediante una intervención concreta con la propuesta de solución de un modelo híbrido.

El enfoque cuantitativo que se plantea buscará medir las diferentes variables como son: capacitación, y afectaciones generadas por los ciberataques, KPIs, encuestas, análisis de indicadores

En la población se define a una institución financiera.

Se plantea utilizar las técnicas de investigación por medio de entrevistas, estadísticos utilizando herramientas como entrevistas y cuestionarios para obtener información de especialistas en las distintas áreas involucradas de seguridad, TI y Operaciones.

Utilizando los siguientes instrumentos:

Instrumento	Propósito
Matriz de madurez	Evaluar el nivel de madurez
Checklist de controles	Verificar cumplimiento de requerimientos.

Matriz de hallazgos	Permite identificar y catalogar áreas de oportunidad a trabajar en la propuesta.
KPIs operativos	Medir de forma cuantitativa los eventos de la operación.

Alberto Pantoja (2025). *Relación de Instrumentos y su propósito [Tabla 9]. Elaboración propia*

Con la información obtenida se realizarán análisis de datos (estadísticos descriptivos) con los cuales se generarán gráficos, métricas, estadísticas y diagramas utilizando herramientas de office para su desarrollo y colaboración con las distintas áreas involucradas, que permitirán para la validación de la efectividad de la solución y obtener una hipótesis de plan de acción.

A continuación, se muestra un diagrama de la metodología planteada:

Pantoja, A. (2025). *Metodología de trabajo* [Imagen que ilustra la metodología de trabajado de la solución propuesta].

La propuesta fue validada a través de:

- Mesas técnicas con expertos en ciberseguridad, TI y operaciones.

22 Conclusión

Este enfoque híbrido permite integrar los beneficios de COBIT, ITIL e ISO 38500 en un modelo adaptable a las necesidades del sector financiero mexicano. Con una planificación adecuada, implementación estructurada y medición constante, las instituciones pueden fortalecer su postura de ciberseguridad y garantizar la disponibilidad de los sistemas financieros.

El proceso de validación asegura que la alternativa seleccionada no solo sea viable, sino también efectiva y sostenible. Este enfoque iterativo garantiza que cada fase aporte valor al objetivo final de mejorar la resiliencia en la institución del sistema financiero mexicano.

El trabajo destaca que la indisponibilidad de TI en el sector financiero es un problema multidimensional, con causas técnicas, organizacionales y regulatorias. La solución fortalece el gobierno de TI, mejorar la cultura de ciberseguridad, invertir en infraestructura moderna y promover la cooperación interinstitucional. El enfoque híbrido propuesto podría reducir la vulnerabilidad de las instituciones y garantizar la continuidad operativa, mejorando la confianza de los usuarios en el sistema financiero.

El presente trabajo abordó el problema de las afectaciones a los servicios financieros en México provocada por ciberataques, una amenaza creciente que compromete la estabilidad del sistema, la confianza del usuario y el cumplimiento regulatorio de las instituciones. A partir del análisis del contexto nacional e internacional, así como de casos documentados relevantes, se identificó la necesidad de adoptar una solución integral que permita fortalecer la resiliencia tecnológica del sector financiero.

Se propone una solución híbrida, basada en la integración de tres marcos de referencia complementarios: COBIT, que proporciona una estructura de gobierno alineada al negocio; ITIL, que permite gestionar la disponibilidad y continuidad de los servicios; e ISO/IEC 38500, que establece principios para la toma de decisiones responsables por parte de la alta dirección. Esta solución fue estructurada en fases y validada mediante un enfoque metodológico mixto, utilizando simulacros, entrevistas, benchmarking y matrices de evaluación.

Asimismo, se establecen indicadores clave de desempeño y un ciclo de mejora continua que permite ajustar el modelo conforme a los resultados obtenidos y a las necesidades específicas de cada organización.

Se concluye que la solución propuesta es viable, aplicable y escalable, especialmente en organizaciones con un nivel medio de madurez digital y su éxito depende de factores clave como la cultura organizacional, la gestión del cambio, la disponibilidad presupuestal y la existencia de mecanismos efectivos de coordinación interinstitucional.

Finalmente, este trabajo se encuentra en fase de solicitud de presupuesto para su implementación en una institución financiera y puede sentar las bases para la implementaciones y adaptaciones del modelo en otros sectores.

23 Bibliografía

Axelos. (2021). *ITIL Service Management*. https://www.axelos.com/certifications/itil-service-management/itil-4-foundation

Banco de Chile. (2018). *Informe sobre el incidente de ciberseguridad SWIFT – Comunicación oficial*. Santiago, Chile. https://www.infosecurity-magazine.com/news/bank-of-chile-suffers-10m-loss

Banco de México. (2024). *Estrategia de Ciberseguridad del Banco de México 2024 – 2027*. https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html

Banco de México. (2024). *Reporte de estabilidad financiera 2024*. Recuperado de https://www.banxico.org.mx

BBVA. (s.f.). *¿Qué es el valor en riesgo (VaR)?* Recuperado de https://www.bbva.com/es/economia-y-finanzas/que-es-el-valor-en-riesgo-var/

FAIR Institute. (2025). *Factor Analysis of Information Risk (FAIR) Standard v3.0*. Recuperado de https://www.fairinstitute.org/

FireEye. (2019). *Insights on Financial Sector Attacks in Latin America* [Whitepaper]. Mandiant. https://www.fireeye.com

IBM. (2024). *Ataques cibernéticos*. https://www.ibm.com/mx-es/topics/cyber-attack

Instituto Nacional de Estándares y Tecnología (NIST). (2020). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdfzz

JPMorgan Chase. (2023). *Annual Report 2023: Cybersecurity & Technology Investments*. https://www.jpmorganchase.com

Keith O'Brien & Amanda Downie. (2024, julio). *gobiernode TI*. https://www.ibm.com/es-es/think/topics/it-governance

Ministerio del Interior y Seguridad Pública. (2020). *Estrategia Nacional de Ciberseguridad 2020–2025*. Gobierno de Chile. https://www.interior.gob.cl

Santander. (2022). *Banco Santander renueva su certificación ISO 27001 en ciberseguridad*. https://www.santander.com/es/stories/ciberseguridad-certificacion-iso-27001

24 Introducción

El presente trabajo aborda el problema de las afectaciones generadas por los ciberataques a las instituciones del sistema financiero mexicano. Esta situación representa una amenaza crítica para la continuidad de servicios esenciales como ATM (cajeros automáticos), banca en línea y plataforma transaccional, generando afectaciones económicas, reputacionales y regulatorias tanto para las instituciones como para los usuarios del sistema financiero.

Para atender esta problemática, se adopta un enfoque híbrido de solución, basado en la integración de metodologías que enunciamos a continuación y su aportación para solucionar la problemática:

- COBIT que aporta estructura y control estratégico.
- ITIL orientado a la operación y disponibilidad de servicios.
- ISO/IEC 38500 que establece principios de gobiernoy responsabilidad desde la alta dirección.

Este enfoque se complementa con elementos de gestión de la innovación tecnológica, tales como la madurez digital, la gestión del cambio y la mejora continua.

El desarrollo del proyecto se estructura en las siguientes etapas principales:

1. Diagnóstico del problema y análisis de contexto
2. Revisión del marco teórico y normativo
3. Evaluación de alternativas metodológicas
4. Diseño y validación de la solución propuesta
5. Implementación piloto por fases
6. Evaluación de resultados con base en indicadores clave

A través de este proceso, se busca proponer una solución aplicable, escalable y alineada a las necesidades del sector financiero mexicano frente a los crecientes desafíos y amenazas de los grupos criminales que se encuentran en tendencia de crecimiento esto en base a los informes del Banco de México donde se detallan incidentes como ransomware, códigos maliciosos, amenazas persistentes avanzadas (APT), y troyanos y se estima una afectación económica que supera los $1,168.98 millones de pesos, aunque algunas pérdidas no están cuantificadas.

25 Anexos

25.1 Incidentes cibernéticos reportados al Banco de México

Estrategia de Ciberseguridad del Banco de México 2024 – 2027

Reporte de Incidentes cibernéticos ocurridos en 2024 en el sistema financiero nacional que han sido reportados al Banco de México

Reporte de Incidentes cibernéticos ocurridos en 2023 en el sistema financiero nacional que han sido reportados al Banco de México

Reporte de Incidentes cibernéticos ocurridos en 2022 en el sistema financiero nacional que han sido reportados al Banco de México

Reporte de Incidentes cibernéticos ocurridos en 2021 en el sistema financiero nacional que han sido reportados al Banco de México

Reporte de Incidentes cibernéticos ocurridos en 2020 en el sistema financiero nacional que han sido reportados al Banco de México

25.2 Ciberataques en los últimos 5 años reportados al Banco de México

Tabla de datos con los distintos ciberataques que se han presentado en los últimos 5 años en base a "**Reporte de Incidentes cibernéticos ocurridos en 2020-2024 en el sistema financiero nacional que han sido reportados al Banco de México**".

ID	AÑO	Mes	Descripción	Servicios Afectados	Afectación a la entidad (MDP)
1	2020	Abril	Ransomware	Banca Por Internet (Internet Bancking)	Sin Cuantificación
2	2020	Agosto	Ransomware	Ventanilla en Sucursales (Open Banking)	Sin Cuantificación
3	2020	Noviembre	Ransomware	Dispersión de Fondos (Plataforma Transaccional)	Sin Cuantificación
4	2020	Noviembre	Ransomware	Banca Por Internet (Internet Bancking)	Sin Cuantificación

ID	AÑO	Mes	Descripción	Servicios Afectados	Afectación a la entidad (MDP)
5	2021	Enero	Ataque a cajeros automáticos	Cajero Automático (ATM)	0.63
6	2021	Enero	Ataque a cajeros automáticos	Cajero Automático (ATM)	0.13
7	2021	Enero	Ransomware	Banca Por Internet (Internet Bancking)	Sin Cuantificación
8	2021	Febrero	Ataque a cajeros automáticos	Cajero Automático (ATM)	8.1
9	2021	Febrero	Ataque a cajeros automáticos	Cajero Automático (ATM)	0.8
10	2021	Marzo	Ataque a cajeros automáticos	Cajero Automático (ATM)	3.01
11	2021	Marzo	Ataque a transferencias	Transferencia en Sucursales (Open Banking)	474.4
12	2021	Abril	Ataque a cajeros automáticos	Cajero Automático (ATM)	4
13	2021	Abril	Ataque a cajeros automáticos	Cajero Automático (ATM)	0.73
14	2021	Junio	Ataque aplicativo	Cajero Automático (ATM)	79
15	2022	Junio	Amenaza persistente avanzada	Banca Por Internet (Internet Bancking)	25.25
16	2022	Diciembre	Difusión no autorizada de información, crediticia de clientes.	Base de datos crediticios (Infraestructura)	Sin Cuantificación
17	2023	Febrero	Ataque a cajeros automáticos	Cajero Automático (ATM)	11.83
18	2023	Marzo	Código malicioso	Transferencia en Sucursales (Open Banking)	55.71
19	2023	Mayo	Troyano	Transferencia en Sucursales (Open Banking)	0.07
20	2023	Julio	Ransomware	Transferencia en Sucursales (Open Banking), Cajero Automático (ATM),	21.47

ID	AÑO	Mes	Descripción	Servicios Afectados	Afectación a la entidad (MDP)
				Banca Por Internet (Internet Bancking)	
21	2024	Marzo	Vulneración informática	Dispersión de Fondos (Plataforma Transaccional)	101.36
22	2024	Abril	Ransomware	Transferencia en Sucursales (Open Banking)	16.38
23	2024	Noviembre	Vulneración informática	Dispersión de Fondos (Plataforma Transaccional)	161.99
24	2024	Diciembre	Vulneración informática	Dispersión de Fondos (Plataforma Transaccional)	204.12

26 Glosario de Términos

CORE: Sistema se encarga de la concentración de todos los elementos que conforman la información personal y sensible de cada uno de los usuarios de tal manera que es el sistema que lleva el registro de todos los movimientos que se hacen los usuarios y/o clientes siendo el sistema central de la institución financiera.

SPEI: Sistemas de Pagos Electrónicos Interbancarios. Este sistema como su acrónimo lo describe hoy es el sistema responsable de regular y controlar los diferentes pagos que se realizan entre las diferentes plataformas transaccionales de cada una de las entidades financieras.

SPED: Sistemas de Pagos Electrónicos Interbancarios en Dólares. Este sistema como su acrónimo lo describe hoy es el sistema responsable de regular y controlar los diferentes pagos que se realizan entre las diferentes plataformas transaccionales de cada una de las entidades financieras que se realizan en dólares americanos.

ATM: Siglas en inglés de Automated Taller Machines, estos cajeros ATM son dispositivos electrónicos diseñados para facilitar transacciones financieras sin la necesidad de la intervención de un empleado bancario.

Mobile banking: Sistema que se encarga de las operaciones que se ejecutan en una APP de un celular de la institución financiera y que se comunica con los sistemas CORE.

Net banking: Sistema que se encarga de las operaciones que son realizadas desde la página de la institución. Hoy es lo que comúnmente conocemos como una banca net o como un portal donde podamos hacer pagos transacciones transferencias desde una computadora.

Open banking: Sistema que se encarga de todas las operaciones que se ejecutan desde las diferentes sucursales, se encarga de hacer todas esas transacciones que son ejecutadas desde las terminales que son operadas en las diferentes sucursales o centros financieros según se conozcan estas localidades o locales donde se prestan servicios por parte de la institución.

Plataforma transaccional: Sistema encargado de hacer una interconexión entre los diferentes tipos de sistemas entradas y salidas de las diferentes transacciones con otras instituciones, por ejemplo: temas relacionados entre las diferentes relaciones de sistemas de entrega de información a entidades reguladoras como la CNBV.

Manejador de tarjetas: Sistema mejor conocido como CartManager, encargado de la gestión de todas las tarjetas o plásticos físicos con todos estos chips que contienen y que nos permiten tener la relación de los datos de los clientes de las tarjetas de crédito, tarjetas de débito, monederos electrónicos. Hablamos de todas aquellas tarjetas que son utilizadas dentro de la institución, es el sistema es el encargado de hacer la gestión de estos plásticos con la respectiva personalización o en su defecto sólo manejar la información relevante de la tarjeta.

Servicios y Productos Financieros: Sistemas encargados de hacer todo lo referente a los productos propios que hoy la institución financiera oferta como son; créditos de diferente naturaleza como autos, casas, créditos de nómina, toda esta cartera de diferentes servicios que el banco oferta como cuentas de nómina, cuentas de cheques, cuentas nacionales e internacionales, inversiones en casa de bolsa, inversiones a través de la misma institución financiera, controla el portafolio de servicios. Estos sistemas están directamente relacionados con todos estos productos financieros, son la base tecnológica que utiliza el banco para hacer su gestión.

Incidencia: Interrupción no planificada de un servicio, o reducción en la calidad de un servicio.

Disponibilidad: Capacidad de un servicio de TI u otro elemento de configuración para realizar su función acordada cuando sea necesario.

Ciberataque: Cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

MTTR Mean Time to Repair: Tiempo Medio de Reparación.

Card seller: Actores de amenaza cuya principal actividad consiste en robar información relativa a tarjetas bancarias de los clientes de las instituciones financieras, con el fin de vender dicha información en foros clandestinos de internet.

Ciber espionaje: Amenaza cuya finalidad es extraer información sensible de instituciones gubernamentales o de grandes corporaciones.

Grupo cibercriminal: Amenaza derivada de actividades delictivas dirigidas a aprovecharse de los sistemas informáticos que brindan servicios a los clientes de las instituciones, con la finalidad de obtener recursos económicos en cuentas bancarias controladas por los atacantes. En esta categoría se agrupan las amenazas generalizadas a que están expuestos los sistemas transaccionales de las instituciones y que no se pueden asociar a alguna de las otras categorías.

Malware: Amenaza diseñada para comprometer la confidencialidad, integridad o disponibilidad de la información de un sistema informático.

Ransomware: Tipo de software malicioso cuyo fin es secuestrar información sensible de un sistema informático, a fin de que la víctima pague por el rescate de esta o evite su publicación en foros clandestinos de Internet.

Access broker: Actor de amenaza que accede ilegalmente a redes informáticas de organizaciones y revende los accesos a través de foros clandestinos de Internet. APT: Amenaza Persistente Avanzada, por sus siglas en inglés, cuenta con altos niveles de especialidad en técnicas de hackeo y con los recursos y el tiempo que requiera para que, a través de la utilización de distintos vectores de ataque sofisticados.

Una amenaza persistente avanzada: También conocida por sus siglas en inglés, APT (por Advanced Persistent Threat), es un conjunto de procesos informáticos sigilosos orquestados por un tercero (organización, grupo delictivo, una empresa, un estado, etc.) con la intención y la capacidad de atacar de forma avanzada (a través de múltiples vectores de ataque) y continuada en el tiempo, un objetivo determinado (empresa competidora, estado, etc.).