Modelamiento de Amenazas Banco “X”

MY. Mario Gómez Ortega

MY. Daniel Torres Jaramillo

MY. Luis Millán Ríos

MY. Yeferson Obando Vera

Gestión de Riesgos Cibernéticos

Docente: Jaider Ospina Navas

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Curso de Estado Mayor - CEM

2025

Modelamiento de Amenazas Banco “X”

1. Introducción

En el contexto financiero digital, la ciberseguridad desempeña un papel fundamental en la defensa de la operatividad y la confianza de los clientes. El Banco "X", una empresa emergente dentro del sector financiero busca afianzar su presencia en el mercado mediante la creación de un sistema de transacciones innovador. Sin embargo, el proceso acelerado de digitalización ha incrementado su exposición a diversas amenazas informáticas que pueden arriesgar la confidencialidad, integridad y disponibilidad de sus operaciones (Nieto, & Solís 2023 p. 547).

En consecuencia, la junta directiva del Banco "X" ha decidido pedir a un grupo de expertos la realización de un análisis que busque examinar los riesgos de seguridad cibernética del banco, quienes a través del modelo STRIDE, realizaron la presente identificación, clasificación y priorización de amenazas en seis categorías principales: suplantación de identidad, manipulación de datos, repudio, divulgación de información, denegación de servicio y escalamiento de privilegios, para posterior definir estrategias de prevención diseñadas para fortalecer (*hardening*) la seguridad de la infraestructura tecnológica y asegurar la estabilidad operativa de la entidad (Garg & Kohnfelder, 2006, p. 115), basados en controles de seguridad organizacionales, físicos y tecnológicos del Anexo A de la norma ISO/CEI 27001 tercera edición (2022) -10 “Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos”.

Por lo anterior, el desarrollo del presente análisis se desarrollará en las siguientes cuatro fases: descripción del contexto del Banco "X", la identificación de activos críticos, el análisis de riesgos basado en una matriz de impacto y probabilidad, y la propuesta de implementación de controles de seguridad según el enfoque de Defensa en Profundidad y la norma ISO/CEI 27001.

Al final y como parte de las conclusiones, se presentan recomendaciones estratégicas para minimizar vulnerabilidades, fortalecer la postura de seguridad cibernética del banco (Peltier, 2016, p. 98) y exponer la importancia de la gestión del riesgo en ciberseguridad

2. Descripción del Escenario

El Banco "X" al ser un banco emergente, busca en primera instancia su consolidación dentro del sector financiero colombiano y posteriormente a nivel internacional; por tal razón, se encuentra en el proceso de ofrecer servicios innovadores a los clientes que ya conocen parte de su esquema financiero, así como a aquellos nuevos clientes a los que les pueda parecer atractivo su modelo de negocio y servicios financieros.

De esta manera, el Banco “X” como parte de su estrategia de crecimiento, ha implementado un Sistema de Transacciones Digitales, desde el cual se permite realizar la gestión de cuentas, pagos y transferencias en tiempo real, por intermedio de su plataforma web y de su aplicación móvil.

Sin embargo, debido a la creciente demanda de sus servicios, el proceso de digitalización del banco se ha tenido que llevar a cabo de una manera rápida, razón por la cual se pueden haber obviado diferentes capas de seguridad. Así mismo, debido al alto nivel de digitalización requerido y el aumento exponencial en el manejo de datos financieros sensibles, el banco actualmente enfrenta la posible materialización e impacto de amenazas cibernéticas que pueden generar algún tipo de disrupción parcial o total sobre sus operaciones, así como generar una afectación reputacional a su imagen, lo que significaría una pérdida de clientes antiguos, potenciales y con ello la posible salida abrupta del banco del sector financiero antes de finalizar su primer año de operación.

Teniendo en cuenta lo mencionado, algunas de las principales amenazas cibernéticas a las cuales puede verse enfrentado el banco son el fraude financiero, los ataques a su infraestructura tecnológica, el robo de identidad y las vulneraciones de datos. Además, es importante destacar que el sector bancario es considerado como uno de los objetivos más atractivos para los ciberdelincuentes, quienes buscan vulnerabilidades en los sistemas y servicios bancarios, para posteriormente explotarlas y obtener un beneficio económico.

Ante este contexto, es imperativo que el Banco "X" conozca de manera clara las amenazas a las cuales se enfrenta, especialmente en su Sistema de Transacciones Digitales, considerado como la columna vertebral o servicio principal de su operación, motivo por el cual debe propender por el desarrollo de una gestión de riesgos eficiente, eficaz y efectiva, que le permita garantizar la seguridad de sus operaciones; en razón a los motivos expuestos, el Banco "X" ha decidido implementar el modelado de amenazas STRIDE, una metodología ampliamente utilizada para la identificación y clasificación de amenazas bajo seis (6) factores, con la finalidad de comprender las vulnerabilidades de los componentes del sistema previamente mencionado, detectar las posibles amenazas que las puedan explotar y priorizar las acciones de mitigación que permitan prevenir su materialización.

3. Análisis de Riesgos

El Banco "X" determinó mediante un análisis de matriz DOFA realizado por expertos, que su sistema más crítico para su operación es el "*sistema de transacciones digitales*", ya que por intermedio de este se llevan a cabo actividades bancarias por parte de los clientes como la gestión de sus cuentas, la realización de pagos y transferencias en tiempo real. Igualmente, se realizó una identificación de los "*componentes tecnológicos críticos"* que lo componen, con la finalidad de

conocer de una manera más detallada las amenazas que puedan generar una posible afectación a su sistema y operación.

Dentro de los componentes tecnológicos críticos identificados se les aplicó una primera fase (Tabla 1) del modelo STRIDE se encuentran: la infraestructura de servidores y bases de datos, el API de integración con Fintech y otros bancos, la aplicación web y móvil para clientes, los mecanismos de autenticación y seguridad (MFA, biometría) y la red de comunicaciones y cifrado de datos.

3.1 Primera fase: Aplicación inicial del Modelo STRIDE

Tabla 1. Aplicación inicial del modelo STRIDE

SISTEMA	COMPONENTE TECNOLÓGICO	SPOOFING	TAMPERING	REPUDIATION	INFORMATION DISCLOSURE	DENIAL OF SERVICE	ELEVATION OF PRIVILEGE
SISTEMA DE TRANSACCIONES DIGITALES DEL BANCO EMERGENTE "X"	INFRAESTRUCTURA DE SERVIDORES Y BASES DE DATOS	Suplantación de credenciales de administrador para acceder a bases de datos.	Modificación maliciosa de registros financieros.	Eliminación de registros para ocultar actividades fraudulentas.	Robo de datos sensibles almacenados (credenciales, datos financieros).	Ataques DDoS para dejar inoperativos los servidores.	Vulnerabilidades explotadas para obtener acceso root en servidores.
	API DE INTEGRACIÓN CON FINTECH Y OTROS BANCOS	Suplantación de API Key o credenciales para realizar transacciones falsas.	Inyección de código malicioso en peticiones API.	Alteración de registros de transacciones sin trazabilidad clara.	Intercepción de datos en tránsito por mala configuración de seguridad.	Sobrecarga de peticiones maliciosas para degradar servicios.	Explotación de errores en API para elevar privilegios en la infraestructura.
	APLICACIÓN WEB Y MÓVIL PARA CLIENTES	Phishing para robar credenciales de clientes.	Modificación de parámetros en peticiones web (man-in-the-browser).	Rechazo de operaciones legítimas por usuarios fraudulentos.	Exposición de datos personales por mala configuración de seguridad.	Saturación de la aplicación con bots o tráfico malicioso.	Escalada de privilegios mediante vulnerabilidades en autenticación.
	MECANISMOS DE AUTENTICACIÓN Y SEGURIDAD (MFA, BIOMETRÍA)	Robo de tokens de autenticación o códigos MFA.	Manipulación de datos biométricos en el proceso de autenticación.	Usuarios niegan haber realizado transacciones mediante autenticación débil.	Filtración de datos biométricos almacenados.	Bloqueo masivo de cuentas a través de ataques automatizados.	Bypass de autenticación multifactor para obtener acceso total.
	RED DE COMUNICACIONES Y CIFRADO DE DATOS	Suplantación de servidores DNS para redirigir tráfico a sitios maliciosos.	Alteración de tráfico en tránsito (ataques MITM).	Intercepción de logs de comunicación sin trazabilidad confiable.	Exposición de datos cifrados si se usan algoritmos débiles.	Ataques DDoS contra firewalls o servidores de red.	Compromiso de equipos de red para escalar privilegios y acceder a sistemas internos.

Fuente: Diseño propio de los autores.

Con base a lo anterior, se logró identificar que en los cinco (5) componentes tecnológicos principales del sistema de transacciones digitales del Banco “X”, existen amenazas desde el modelo STRIDE que tienen el potencial de generar una afectación en la confidencialidad , integridad y disponibilidad de los servicios financieros del banco y con ello afectar su operación de manera parcial o total. Dentro de las principales consecuencias generales que se pueden producir de acuerdo a la materialización de estas amenazas, se tiene la pérdida de confianza de los clientes, enfrentar por parte del banco posibles sanciones legales, la generación de pérdidas económicas irremediables y de alto impacto para la operación del banco, enfrentar posibles procesos de demanda por parte de los clientes teniendo en cuenta la afectación de los mismos por la exfiltración de información sensible y con ello la posible materialización de fraudes.

En continuidad al proceso iniciado, el banco en procura de proteger sus activos críticos, continuar su fucionamiento operativo y garantizar la seguridad de las transacciones digitales a través de sus portales, realizó una segunda fase de este proceso en el cual se estableció un estándar y criterios orientadores, para poder establecer el nivel de riesgo en los componentes tecnológicos que componen el sistema objeto de análisis, permitiendo con esto determinar el impacto, la probabilidad y el nivel de riesgo para cada activo y sus amenazas identificadas.

3.2 Segunda fase: Determinación de la matriz de riesgos

Siguiendo la fórmula para el cálculo del nivel de riesgo de las amenazas identificadas se determinó que éste es el resultado del la sumatoria del impacto más la probabilidad (Figura 1).

Figura 1. Fórmula de Nivel de Riesgo

Fuente: Diseño propio de los autores.

- **Probabilidad**: La probabilidad de que una amenaza se materialice, con los siguientes criterios:
  - **Poco probable:** Amenaza con baja posibilidad de ocurrir, generalmente menos de un 10% de probabilidad.
  - **Probable:** Amenaza con una posibilidad moderada de ocurrir, típicamente entre el 11% y el 50% de probabilidad.
  - **Muy probable:** Amenaza con alta posibilidad de ocurrir, generalmente del 51% de probabilidad en adelante.
- **Impacto**: La magnitud de las consecuencias que tendría la materialización de la amenaza, también evaluada como baja, media o alta, con los siguientes criterios:
  - **Bajo:** La amenaza causa daños menores o limitados, sin afectar significativamente las operaciones ni la reputación.
  - **Medio:** La amenaza causa daños notables, afectando de manera moderada las operaciones o la reputación.
  - **Crítico:** La amenaza causa daños severos, impactando significativamente las operaciones, la seguridad, y/o la reputación de la empresa.

- **Nivel de Riesgo**: Una combinación de la probabilidad y el impacto, que puede clasificarse como bajo, medio o alto, con los siguientes criterios:
  - **Bajo:** Riesgo manejable sin necesidad de medidas especiales.
  - **Medio:** Riesgo significativo, puede requerir mitigación o control.
  - **Alto:** Riesgo alto, necesita atención urgente y medidas de mitigación.

De acuerdo con los criterios mencionados se estableció una matriz de riesgos (Figura 2) para determinar su corelación:

Figura 2. Matriz de Riesgos.

MATRIZ DE RIESGOS				
PROBABILIDAD	MUY PROBABLE	MEDIO	ALTO	ALTO
	PROBABLE	BAJO	MEDIO	ALTO
	POCO PROBABLE	BAJO	BAJO	MEDIO
		BAJO	MEDIO	CRÍTICO
		IMPACTO		

Fuente: Diseño propio de los autores.

3.3. Identificación de Amenazas Específicas y Priorización de acuerdo con su Nivel de Riesgo

En la misma segunda fase y teniendo en cuenta la matriz de riesgos establecidas por el personal del Banco “X” encargado de dar continuidad al presente proceso, se tomó de manera inicial el componente “Infraestructura de servidores y bases de datos”, al cual se le realizó un proceso de categorización de los activos que lo integran, como lo son el hardware, su infraestructura y la información; seguido de esto, se llevó a cabo el establecimiento del inventario de activos correspondiente a cada una de estas categorías, sirviendo de base para el

desarrollo de esta segunda fase de aplicación del modelo STRIDE, en la cual se identificaron las amenazas específicas (Tabla 2) de cada uno de estos activos bajo el modelo en mención.

Tabla 2. Identificación de amenazas específicas.

SISTEMA	COMPONENTE TECNOLÓGICO	CATEGORÍAS DE ACTIVOS	INVENTARIO DE ACTIVOS
Sistema de Transacciones Digitales del Banco Emergente "X"	Infraestructura de Servidores y Bases de Datos	Hardware	Servidores Físicos
		Infraestructura	Data Center
		Información	Datos Financieros y Transaccionales
			Registros de Clientes
			Logs de Auditoría

Fuente: Diseño propio de los autores.

Finalmente, mediante el empleo de la metodología DELPHI (*Juicio de expertos*), se llevó a cabo el proceso de evaluación y priorización de los riesgos según los factores de probabilidad, impacto y nivel de riesgo de cada una de las amenazas identificadas (Tabla 3), con el objetivo de determinar los riesgos que requieren una atención inmediata y los que pueden ser tratados a mediano y largo plazo, conforme a los criterios de evaluación establecidos previamente en la matriz de riesgos (Figura 2).

Tabla 3. Proceso de evaluación y priorización de los riesgos

CATEGORÍA DE ACTIVOS	INVENTARIO DE ACTIVOS	STRIDE	PRINCIPALES AMENAZAS X ACTIVO	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
Hardware	Servidores Físicos	Spoofing	Acceso no autorizado a través de credenciales robadas	Probable	Critico	Alto
		Tampering	Alteración de configuraciones del sistema o BIOS	Poco Probable	Medio	Bajo
		Repudiation	Borrado o modificación de logs del sistema	Probable	Medio	Medio
		Information Disclosure	Exposición de datos sensibles almacenados en servidores	Muy Probable	Critico	Alto
		Denial Of Service	Ataques DDoS o sobrecarga que dejan inoperativos los servidores	Muy Probable	Critico	Alto
		Elevation Of Privilege	Explotación de vulnerabilidades para obtener acceso administrativo	Probable	Critico	Alto
Infraestructura	Data Center	Spoofing	Uso de credenciales falsas para acceder al Data Center	Probable	Critico	Alto
		Tampering	Modificación de configuraciones en servidores críticos	Poco Probable	Critico	Medio
		Repudiation	Eliminación de registros de acceso físico o digital al Data Center	Probable	Medio	Medio
		Information Disclosure	Filtración de datos sensibles por intrusión física o ataques cibernéticos	Muy Probable	Critico	Alto
		Denial Of Service	Ataque físico o eléctrico que interrumpe la operatividad del Data Center	Muy Probable	Critico	Alto

		Elevation Of Privilege	Uso de vulnerabilidades para obtener acceso administrativo en servidores	**Probable**	**Critico**	**Alto**
Información	Datos Financieros y Transaccionales	Spoofing	Uso de credenciales robadas para realizar transacciones fraudulentas	**Probable**	**Critico**	**Alto**
		Tampering	Alteración de registros de transacciones para modificar montos o cuentas	**Probable**	**Critico**	**Alto**
		Repudiation	Usuarios malintencionados niegan haber realizado transacciones fraudulentas	**Probable**	**Medio**	**Medio**
		Information Disclosure	Robo de datos financieros por ataque a bases de datos o API	**Muy Probable**	**Critico**	**Alto**
		Denial Of Service	Ataques DDoS contra plataformas de transacciones bloqueando operaciones	**Probable**	**Critico**	**Alto**
		Elevation Of Privilege	Explotación de vulnerabilidades en el sistema para acceder a datos financieros confidenciales	**Probable**	**Critico**	**Alto**
	Registros de Clientes	Spoofing	Robo de identidad mediante credenciales comprometidas	**Muy Probable**	**Critico**	**Alto**
		Tampering	Modificación no autorizada de registros de clientes	**Probable**	**Critico**	**Alto**
		Repudiation	Negación de actividad fraudulenta por parte de usuarios o atacantes	**Muy Probable**	**Medio**	**Alto**
		Information Disclosure	Fuga de datos personales de clientes debido a accesos no autorizados	**Muy Probable**	**Critico**	**Alto**
		Denial Of Service	Ataques que bloquean el acceso a registros de clientes	**Probable**	**Critico**	**Alto**
		Elevation Of Privilege	Acceso administrativo no autorizado para modificar datos de clientes	**Probable**	**Critico**	**Alto**
	Logs de Auditoría	Spoofing	Uso de credenciales robadas para alterar o eliminar registros de auditoría	**Probable**	**Critico**	**Alto**
		Tampering	Modificación no autorizada de logs para ocultar actividades maliciosas	**Probable**	**Critico**	**Alto**
		Repudiation	Eliminación o alteración de registros para evitar la trazabilidad de acciones fraudulentas	**Muy Probable**	**Critico**	**Alto**
		Information Disclosure	Exposición de registros de auditoría con información sensible sobre sistemas y usuarios	**Probable**	**Critico**	**Alto**
		Denial Of Service	Saturación del sistema de loging que impida registrar eventos críticos	**Poco Probable**	**Medio**	**Bajo**
		Elevation Of Privilege	Acceso no autorizado a sistemas de auditoría para modificar o eliminar registros	**Probable**	**Critico**	**Alto**

Fuente: Diseño propio de los autores.

De acuerdo con el análisis realizado por el grupo de expertos, este arrojó como resultado la identificación de veinticuatro (24) riesgos de nivel crítico, cuatro (4) riesgos de nivel medio y dos (2) riesgos de nivel bajo en el componente de infraestructura de servidores y bases de datos. En consecuencia a los resultados obtenidos, se procede a realizar la gestión de los riesgos de una manera efectiva para mitigar su impacto en la organización y así mismo para reducir su probabilidad de ocurrencia.

3.4 Tratamiento del Riesgo

Continuando con el análisis, se procede a definir el respectivo tratamiento del riesgo (Tabla 4) con el propósito de tener una claridad en la estrategia a implementar para su respectiva

gestión, según los criterios del grupo de expertos, definiendo así el tratamiento más adecuado según su nivel de criticidad, con los siguientes parámetros de decisión:

- Reducir: Implementar controles para minimizar la probabilidad o impacto del riesgo.
- Transferir: Delegar el riesgo a un tercero.
- Aceptar: Asumir el riesgo si el costo de mitigación es mayor que el impacto.
- Eliminar/Rechazar: Si es posible, eliminar el riesgo eliminando la vulnerabilidad.

Tabla 4. Análisis para el tratamiento del riesgo

CATEGORÍA DE ACTIVOS	INVENTARIO DE ACTIVOS	STRIDE	PRINCIPALES AMENAZAS X ACTIVO	NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO
Hardware	Servidores Físicos	Spoofing	Acceso no autorizado a través de credenciales robadas	ALTO	Reducir
		Information Disclosure	Exposición de datos sensibles almacenados en servidores	ALTO	Reducir
		Denial Of Service	Ataques DDoS o sobrecarga que dejan inoperativos los servidores	ALTO	Reducir
		Elevation Of Privilege	Explotación de vulnerabilidades para obtener acceso administrativo	ALTO	Reducir
Infraestructura	Data Center	Spoofing	Uso de credenciales falsas para acceder al Data Center	ALTO	Reducir
		Information Disclosure	Filtración de datos sensibles por intrusión física o ataques cibernéticos	ALTO	Reducir
		Denial Of Service	Ataque físico o eléctrico que interrumpe la operatividad del Data Center	ALTO	Reducir
		Elevation Of Privilege	Uso de vulnerabilidades para obtener acceso administrativo en servidores	ALTO	Reducir
Información	Datos Financieros Y Transaccionales	Spoofing	Uso de credenciales robadas para realizar transacciones fraudulentas	ALTO	Reducir
		Tampering	Alteración de registros de transacciones para modificar montos o cuentas	ALTO	Reducir
		Information Disclosure	Robo de datos financieros por ataque a bases de datos o API	ALTO	Reducir
		Denial Of Service	Ataques DDoS contra plataformas de transacciones bloqueando operaciones	ALTO	Reducir
		Elevation Of Privilege	Explotación de vulnerabilidades en el sistema para acceder a datos financieros confidenciales	ALTO	Reducir
	Registros De Clientes	Spoofing	Robo de identidad mediante credenciales comprometidas	ALTO	Reducir
		Tampering	Modificación no autorizada de registros de clientes	ALTO	Reducir
		Repudiation	Negación de actividad fraudulenta por parte de usuarios o atacantes	ALTO	Reducir
		Information Disclosure	Fuga de datos personales de clientes debido a accesos no autorizados	ALTO	Reducir
		Denial Of Service	Ataques que bloquean el acceso a registros de clientes	ALTO	Reducir
		Elevation Of Privilege	Acceso administrativo no autorizado para modificar datos de clientes	ALTO	Reducir
	Logs De Auditoría	Spoofing	Uso de credenciales robadas para alterar o eliminar registros de auditoría	ALTO	Reducir
		Tampering	Modificación no autorizada de logs para ocultar actividades maliciosas	ALTO	Reducir
		Repudiation	Eliminación o alteración de registros para evitar la trazabilidad de acciones fraudulentas	ALTO	Reducir
		Information Disclosure	Exposición de registros de auditoría con información sensible sobre sistemas y usuarios	ALTO	Reducir
		Elevation Of Privilege	Acceso no autorizado a sistemas de auditoría para modificar o eliminar registros	ALTO	Reducir

Fuente: Diseño propio de los autores.

3.5 Plan de Tratamiento de Riesgos

Por último, el equipo de expertos encargado de la gestión de riesgos del Banco "X", tomó la decisión de tratar los riesgos críticos bajo el factor de tratamiento del riesgo "reducir", buscando establecer para cada uno de los riesgos identificados una serie de controles de seguridad tecnológicos basados en la norma ISO/CEI 27, así como también acciones para su remediación o robustecimiento de la seguridad, el empleo de recursos para su desarrollo, el establecimiento de responsables para cada una de esas acciones y por último con el propósito de poder medir su avance en la implementación, establecer un plazo para su cumplimiento y de esta manera tener claramente definido su "Plan de Tratamiento de Riesgos" (Tabla 5).

Tabla 5. Análisis para el tratamiento del riesgo

INVENTARIO DE ACTIVOS	PRINCIPALES AMENAZAS X ACTIVO	NIVEL DE RIESGO	TTO DEL RIESGO	PLAN DE TRATAMIENTO DE RIESGOS					
				OBJETIVO	CONTROL	ACCIONES	RECURSOS	RESPONSABLES	PLAZO
Servidores Físicos	Acceso no autorizado a través de credenciales robadas	ALTO	Reducir	Implementar autenticación robusta para evitar accesos no autorizados.	Autenticación multifactor (MFA) para administradores.	Configurar y habilitar MFA en accesos a servidores.	Software MFA, Servidor de autenticación.	Jefe de Seguridad, Administrador de Sistemas.	1 mes
	Exposición de datos sensibles almacenados en servidores	ALTO	Reducir	Proteger la confidencialidad de los datos almacenados en servidores.	Implementar cifrado AES-256 en datos en reposo.	Configurar cifrado en bases de datos y discos de almacenamiento.	Software de cifrado, Claves criptográficas.	CISO, Administrador de Bases de Datos.	2 meses
	Ataques DDoS o sobrecarga que dejan inoperativos los servidores	ALTO	Reducir	Garantizar la disponibilidad de los servidores ante ataques DDoS.	Implementar firewalls y soluciones anti-DDoS en la infraestructura.	Configurar firewall con reglas de mitigación de tráfico malicioso.	Firewall de nueva generación, Plataforma anti-DDoS.	Administrador de Redes, CISO.	1 mes
	Explotación de vulnerabilidades para obtener acceso administrativo	ALTO	Reducir	Minimizar el riesgo de escalada de privilegios en servidores.	Aplicar gestión de parches y monitoreo de accesos.	Implementar actualizaciones de seguridad periódicas y monitoreo SIEM.	Plataforma SIEM, Herramienta de gestión de parches.	Administrador de Seguridad, Auditor de TI.	3 meses
Data Center	Uso de credenciales falsas para acceder al Data Center	ALTO	Reducir	Restringir accesos físicos no autorizados.	Implementar controles biométricos en accesos.	Instalar sistema de autenticación biométrica.	Control de acceso biométrico, Tarjetas RFID.	Jefe de Seguridad Física, Administrador de Infraestructura.	2 meses
	Filtración de datos sensibles por intrusión física o ataques cibernéticos	ALTO	Reducir	Proteger la integridad de los datos almacenados.	Implementar monitoreo 24/7 con detección de anomalías.	Instalar SIEM y configurar alertas de seguridad.	SIEM, Sensores de detección de intrusión.	CISO, Responsable de Seguridad TI.	3 meses
	Ataque físico o eléctrico que interrumpe la	ALTO	Reducir	Asegurar la continuidad	Implementar redundancia	Instalar generadores y verificar	Generadores eléctricos,	Director de Infraestructura, Jefe de Mantenimiento.	4 meses

	operatividad del Data Center			operativa del Data Center.	eléctrica y respaldo UPS.	protocolos de recuperación.	UPS redundantes.		
	Uso de vulnerabilidades para obtener acceso administrativo en servidores	ALTO	Reducir	Minimizar la explotación de vulnerabilidades en el Data Center.	Aplicar segmentación de red y gestión de accesos.	Configurar VLANs y reforzar permisos administrativos.	Switches VLAN, Herramienta IAM.	Administrador de Seguridad, Responsable de Redes.	3 meses
Datos Financieros Y Transaccionales	Uso de credenciales robadas para realizar transacciones fraudulentas	ALTO	Reducir	Prevenir el uso indebido de credenciales robadas.	Implementación de autenticación multifactor (MFA).	Configurar MFA en accesos y transacciones sensibles.	Software MFA, Servidor de autenticación.	Jefe de Seguridad, Administrador de Aplicaciones.	1 mes
	Alteración de registros de transacciones para modificar montos o cuentas	ALTO	Reducir	Garantizar la integridad de los registros financieros.	Implementar control de integridad con hashing o blockchain.	Configurar auditoría de cambios en bases de datos.	Software de auditoría, Algoritmos de hashing.	Administrador de Bases de Datos, Auditor de Seguridad.	2 meses
	Robo de datos financieros por ataque a bases de datos o API	ALTO	Reducir	Evitar la exposición de datos financieros sensibles.	Cifrado de datos en tránsito y en reposo (AES-256, TLS 1.3).	Configurar cifrado en bases de datos y redes.	Software de cifrado, Certificados TLS.	CISO, Administrador de Seguridad TI.	2 meses
	Ataques DDoS contra plataformas de transacciones bloqueando operaciones	ALTO	Reducir	Garantizar la disponibilidad de las plataformas transaccionales.	Implementación de firewall avanzado y mitigación DDoS.	Configurar reglas anti-DDoS en firewall y balanceo de carga.	Firewall NG, Plataforma de mitigación DDoS.	Administrador de Redes, Responsable de Infraestructura.	1 mes
	Explotación de vulnerabilidades en el sistema para acceder a datos financieros confidenciales	ALTO	Reducir	Evitar accesos no autorizados con privilegios elevados.	Aplicación de gestión de accesos y privilegios (PAM).	Implementar segregación de funciones y monitoreo de accesos.	Herramienta PAM, Plataforma SIEM.	Administrador de Seguridad, Responsable de Cumplimiento.	3 meses
Registros De Clientes	Robo de identidad mediante credenciales comprometidas	ALTO	Reducir	Proteger las cuentas de clientes contra accesos no autorizados.	Implementación de autenticación multifactor (MFA).	Habilitar MFA en accesos a cuentas de clientes.	Software MFA, Tokens de autenticación.	Jefe de Seguridad, Administrador de Aplicaciones.	1 mes
	Modificación no autorizada de registros de clientes	ALTO	Reducir	Asegurar la integridad de los datos de clientes.	Control de auditoría y logs de modificaciones.	Configurar monitoreo de cambios en registros de clientes.	SIEM, Software de auditoría.	Administrador de Bases de Datos, Auditor de Seguridad.	2 meses
	Negación de actividad fraudulenta por parte de usuarios o atacantes	ALTO	Reducir	Asegurar la trazabilidad de transacciones y accesos.	Implementación de registros de auditoría inmutables.	Configurar blockchain o logs con firma digital.	Plataforma de auditoría, Algoritmos de firma digital.	Responsable de Cumplimiento, Auditor de TI.	3 meses
	Fuga de datos personales de clientes debido a accesos no autorizados	ALTO	Reducir	Evitar la exposición de datos personales de clientes.	Cifrado de datos en tránsito y en reposo.	Configurar cifrado AES-256 en bases de datos y TLS en redes.	Software de cifrado, Certificados TLS.	CISO, Administrador de Seguridad TI.	2 meses
	Ataques que bloquean el acceso a registros de clientes	ALTO	Reducir	Garantizar la disponibilidad de los registros de clientes.	Implementación de mitigación de DDoS en bases de datos y servidores.	Configurar firewall con reglas de protección contra DDoS.	Firewall NG, Plataforma anti-DDoS.	Administrador de Redes, Responsable de Infraestructura.	1 mes
	Acceso administrativo no autorizado para modificar datos de clientes	ALTO	Reducir	Prevenir accesos no autorizados con privilegios elevados.	Implementación de gestión de privilegios y roles (PAM).	Configurar restricciones de acceso basadas en roles (RBAC).	Herramienta PAM, Plataforma SIEM.	Administrador de Seguridad, Responsable de Cumplimiento.	3 meses
Logs De Auditoría	Uso de credenciales robadas para alterar o eliminar	ALTO	Reducir	Evitar el acceso no autorizado a los registros de auditoría.	Implementación de autenticación multifactor	Configurar MFA en accesos administrativos y segmentar	Software MFA, Sistema de gestión de accesos.	Jefe de Seguridad, Administrador de SIEM.	1 mes

	registros de auditoría				(MFA) y restricción de accesos.	accesos según roles.			
	Modificación no autorizada de logs para ocultar actividades maliciosas	ALTO	Reducir	Asegurar la integridad y no alteración de los registros de auditoría.	Implementación de logs inmutables con firma digital o blockchain.	Configurar registros de auditoría con firma digital para prevenir modificaciones.	Software de auditoría, Algoritmos de firma digital.	Responsable de Cumplimiento, Administrador de Seguridad.	2 meses
	Eliminación o alteración de registros para evitar la trazabilidad de acciones fraudulentas	ALTO	Reducir	Garantizar la trazabilidad y preservación de registros de auditoría.	Implementación de archivado seguro con retención obligatoria de logs.	Configurar políticas de retención de logs y copias de seguridad cifradas.	Almacenamiento seguro, Software de retención de logs.	Auditor de TI, Administrador de Seguridad.	3 meses
	Exposición de registros de auditoría con información sensible sobre sistemas y usuarios	ALTO	Reducir	Evitar la fuga de información confidencial contenida en logs.	Cifrado de logs en reposo y en tránsito (AES-256, TLS).	Configurar cifrado en registros de auditoría y acceso restringido a logs.	Software de cifrado, Certificados TLS.	CISO, Responsable de Cumplimiento.	2 meses
	Acceso no autorizado a sistemas de auditoría para modificar o eliminar registros	ALTO	Reducir	Evitar accesos no autorizados con privilegios elevados a los sistemas de auditoría.	Aplicación de gestión de privilegios (PAM) y segregación de funciones.	Configurar acceso basado en roles y monitoreo continuo de accesos.	Herramienta PAM, Plataforma SIEM.	Administrador de Seguridad, Responsable de Infraestructura.	3 meses

Fuente: Diseño propio de los autores.

De acuerdo con el plan de tratamiento de riesgos relacionado, se implementaron diferentes controles de seguridad tecnológicos, con el propósito de reducir las vulnerabilidades críticas evidenciadas en los activos, las cuales podrían ser explotadas por los atacantes y de esta manera materializar las amenazas de nivel alto identificadas. Sin embargo, también es importante que se considere por parte del Banco "X" la implementación de sistemas de monitoreo y detección de amenazas en tiempo real, con el fin de hacer un seguimiento a las amenazas identificadas, recibiendo alertas oportunas y de esta manera junto con el desarrollo e implementación de planes de respuesta y recuperación ante incidentes, tener protocolos de actuación adecuados que permitan gestionar los incidentes cibernéticos que busquen generar un impacto en la continuidad del negocio.

Es importante destacar, que adicional a los controles tecnológicos debido a los riesgos identificados por amenazas/vulnerabilidades, el equipo de expertos también puso a

consideración el implementar (*hardening*) los dos tipos de controles de seguridad de la información adicionales organizacionales (Tabla 6) y físicos (Tabla 7) al Banco "X" conforme al Anexo A de la norma ISO/CEI 27001 tercera edición (2022) -10 "Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos", como se muestra a continuación:

Tabla 6. Controles organizacionales adicionales sugeridos

No.	Tipo de Control	Control	Responsable	Plazo
5.1	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.	Alta gerencia	Cada vigencia (1 año)
5.4	responsabilidades de gestión	La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.	Alta gerencia	Verificar trimestralmente
5.6	Contacto con grupos de interés especial	La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.	Oficina de Tecnologías de la información	Verificar trimestralmente
5.12	Clasificación de la información	La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.	Oficina de Tecnologías de la información	Verificar trimestralmente
6.3	Concientización, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.	Alta gerencia y oficina de personal	Verficiar mensualmente

Fuente: Norma ISO/CEI 27001 tercera edición (2022) -10.

Tabla 7. Controles físicos adicionales sugeridos

No.	Tipo de Control	Control	Responsable	Plazo
7.3	Asegurar oficinas, salas e instalaciones	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.	Oficina de Tecnologías de la información	Verificar mensualmente
7.5	Protección contra amenazas físicas y ambientales.	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.	Alta gerencia	Verificar anualmente
7.11	Utilidades de apoyo	Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.	Oficina de Tecnologías de la información	Verificar trimestralmente
7.12	seguridad del cableado	Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.	Oficina de Tecnologías de la información	Verificar trimestralmente
7.13	Mantenimiento de equipo	El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.	Oficina de Tecnologías de la información	Verficiar mensualmente

Fuente: Norma ISO/CEI 27001 tercera edición (2022) -10.

Por último, es imperativo destacar que se puede efectuar un análisis adicional en detalle con el modelo STRIDE y su respectiva matriz de riesgo a cada una de las amenazas que se pudiesen identificar en las capas de los controles organizacional y físico, con el fin de robustecer aún más los sistemas adicionales donde se presenten riesgos bajos.

4. Conclusiones y Recomendaciones

Como parte del ejericio de análisis; el grupo de expertos, recomienda que el Banco "X" adopte el modelo STRIDE para identificar y mitigar de forma proactiva las amenazas cibernéticas, con el fin garantizar la seguridad de sus operaciones, y proteger la confianza de sus clientes (buen nombre – *good will),* para consolidar su posición en el sector financiero. Además, la

implementación de controles de seguridad robustos *(hardening)* es fundamental para prevenir riesgos que podrían poner en peligro su supervivencia en el mercado.

Los resultados de la aplicación de los controles de seguridad propuestos por el grupo de expertos, permitirán minimizar vulnerabilidades, fortalecer la postura de seguridad cibernética del Banco "X" (Peltier, 2016, p. 98) y exponer la importancia de la gestión del riesgo en ciberseguridad, con el fin de evitar la materialización de amenazas, como la pérdida de confianza de los clientes e inversionistas, enfrentar posibles sanciones legales, generación de pérdidas económicas irremediables o enfrentar posibles procesos de demanda por parte de los clientes teniendo en cuenta la afectación de los mismos por la exfiltración de información sensible y con ello la posible materialización de fraudes.

En cuanto a los controles de tecnología, es importante que se considere la implementación de sistemas adicionales de monitoreo y detección de amenazas en tiempo real, junto con el desarrollo e implementación de planes de respuesta y recuperación ante incidentes, y tener protocolos de actuación adecuados que permitan gestionar los incidentes cibernéticos que busquen generar un impacto en la continuidad del negocio.

Finalmente, se concluye que el uso del modelo STRIDE, permite la clara identificación de activos críticos de cualquier organización que use tecnologías de la información, los cuales al ser analizados mediante una matriz de impacto y probabilidad permiten la gestión de los riesgos identificados mediante la propuesta de implementación de controles de seguridad (tecnológicos, organizacionales y físicos) según el enfoque de Defensa en Profundidad y la norma ISO/CEI 27001.

5. Referencias Bibliográficas

Microsoft. (2023). The STRIDE threat model. Recuperado de https://docs.microsoft.com/en-us/security/engineering/threat-modeling

ISO/IEC 27001. (2022). Information security management. International Organization for Standardization.

PwC. (2023). Global Economic Crime and Fraud Survey. Recuperado de https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

Shostack, A. (2014). Threat modeling: Designing for security. Wiley.

National Institute of Standards and Technology (NIST). (2021). Framework for improving critical infrastructure cybersecurity. Recuperado de https://www.nist.gov/cyberframework

Nieto, A., Meléndez, M., Herrera, A., & Solís, O. (2023). Estrategia de ciberseguridad para fortalecer el sector financiero. Revista Semilla Científica, 1(4), 540–549. https://doi.org/10.37594/sc.v1i4.1297).

Garg, P., & Kohnfelder, L. (2006). Threat modeling: Designing for security (Microsoft Press p. 115).

Peltier, T. R. (2016). Information security risk analysis (2ª ed.) (Auerbach Publications p. 98).