



ESCUELA SUPERIOR  
DE GUERRA

"General Rafael Reyes Prieto"

Colombia

# MODELO DE AMENAZAS BANCO EMERGENTE "X"

MY. DANIEL TORRES - MY. MARIO GÓMEZ

MY. YEFERSON OBANDO - MY. LUIS MILLÁN



# 1. INTEGRANTES



• MY. YEFERSON  
OBANDO



• MY. LUIS C.  
MILLAN



• MY. MARIO  
GÓMEZ



• MY. DANIEL  
TORRES

GRUPO “MOGT”

# AGENDA

- 1 DESCRIPCIÓN DEL ESCENARIO
- 2 ANÁLISIS DE RIESGOS Y APLICACIÓN MODELO “STRIDE”
- 3 DETERMINACIÓN NIVEL DE RIESGO PARA CADA ACTIVO Y SUS AMENAZAS IDENTIFICADAS
- 4 MATRÍZ DE RIESGOS
- 5 METODOLOGIA “DELPHI”
- 6 TRATAMIENTO DEL RIESGO
- 7 CONCLUSIONES
- 8 BIBLIOGRAFÍA

# AGENDA



# 1. DESCRIPCIÓN DEL ESCENARIO

## BANCO EMERGENTE “X”

### Propósito

#### Sistema de Transacciones Digitales

01 Consolidación financiera a nivel regional e internacional

02 Mediante:

- Modelos innovadores,
- Prácticos y de última tecnología.

03 Sistema de Transacciones digitales:

- Gestión de cuentas,
- Pagos y Transferencias en tiempo real,
- Plataforma web y
- Aplicación Móvil.



### Creciente Demanda de Servicios

- Proceso de digitalización del banco rápida, omitido capas de seguridad.
- Aumento exponencial de datos financieros sensibles.
- Disrupción parcial o total en sus operaciones.
- Afectación reputacional.



### Amenazas Ciberneticas

- Fraude Financiero.
- Ataque a infraestructura tecnológica.
- Robo de Identidad.
- Vulneración de Datos.

### Desarrollo Gestión de Riesgos

- Eficiente-Eficaz-Efectivo.
- Garantizar Seguridad en las Operaciones.
- Implementación Modelo STRIDE.
- Identificación y clasificación de amenazas bajo 6 Factores.

## 2. ANÁLISIS DE RIESGOS Y APLICACIÓN MODELO “STRIDE”

SISTEMA	COMPONENTE TECNOLÓGICO	SPOOFING	TAMPERING	REPUDIATION	INFORMATION DISCLOSURE	DENIAL OF SERVICE	ELEVATION OF PRIVILEGE
SISTEMA DE TRANSACCIONES DIGITALES DEL BANCO "X"	INFRAESTRUCTURA DE SERVIDORES Y BASES DE DATOS	Suplantación de credenciales 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 -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	Modificación de parámetros en peticiones web (man-in-the-browser).	Rechazo de operaciones legítimas por usuarios fraudulentos.	Exposición de datos personales- 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 (MFA) 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.

### 3. DETERMINACIÓN NIVEL DE RIESGO PARA CADA ACTIVO Y SUS AMENAZAS IDENTIFICADAS



**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.

**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.

**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.

# 4. MATRÍZ DE RIESGOS

## MAPA DE RIESGOS

PROBABILIDAD	MUY PROBABLE	MEDIO	ALTO	ALTO
	PROBABLE	BAJO	MEDIO	ALTO
	POCO PROBABLE	BAJO	BAJO	MEDIO
		BAJO	MEDIO	CRÍTICO
IMPACTO				

## CATEGORIZACIÓN DE ACTIVOS

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

# 5. METODOLOGÍA “DELPHI”

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 logging 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

# 6. TRATAMIENTO DEL RIESGO - ANÁLISIS



- 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.

# 6. TRATAMIENTO DEL RIESGO - ANÁLISIS



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
	Logs De Auditoría	Elevation Of Privilege	Acceso administrativo no autorizado para modificar datos de clientes	ALTO	Reducir
		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.

# ■ 6. PLAN DE TRATAMIENTO DE RIESGOS

INVENTARIO DE ACTIVOS	PRINCIPALES AMENAZAS X ACTIVO	NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO	PLAN DE TRATAMIENTO DE RIESGOS				
				OBJETIVO	CONTROL	ACCIONES	RECURSOS	RESPONSABLES
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.
	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.
	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.
	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.
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.
	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.
	Ataque físico o eléctrico que interrumpe la operatividad del Data Center	ALTO	Reducir	Asegurar la continuidad operativa del Data Center.	Implementar redundancia eléctrica y respaldo UPS.	Instalar generadores y verificar protocolos de recuperación.	Generadores eléctricos, UPS redundantes.	Director de Infraestructura, Jefe de Mantenimiento.
	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.
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.
	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.
	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.
	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.
	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.

# 6. PLAN DE TRATAMIENTO DE RIESGOS

INVENTARIO DE ACTIVOS	PRINCIPALES AMENAZAS X ACTIVO	NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO	PLAN DE TRATAMIENTO DE RIESGOS					
				DETALLE DE TRATAMIENTO	MEDIDAS DE SEGURIDAD	TIPO DE USUARIO	FECHA DE IMPLEMENTACIÓN	RESPONSABLE	NOTAS
Datos Financieros Y Transaccionales	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

# 6. PLAN DE TRATAMIENTO DE RIESGOS



INVENTARIO DE ACTIVOS	PRINCIPALES AMENAZAS X ACTIVO	NIVEL DE RIESGO	TRATAMIENTO DEL RIESGO	PLAN DE TRATAMIENTO DE RIESGOS					
				OBJETIVO	CONTROL	ACCIONES	RECURSOS	RESPONSABLES	PLAZO
Logs De Auditoría	Uso de credenciales robadas para alterar o eliminar registros de auditoría	ALTO	Reducir	Evitar el acceso no autorizado a los registros de auditoría.	Implementación de autenticación multifactor (MFA) y restricción de accesos.	Configurar MFA en accesos administrativos y segmentar accesos según roles.	Software MFA, Sistema de gestión de accesos.	Jefe de Seguridad, Administrador de SIEM.	1 mes
	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

# 6. CONTROLES ADICIONALES (ORG)

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	Verficar mensualmente

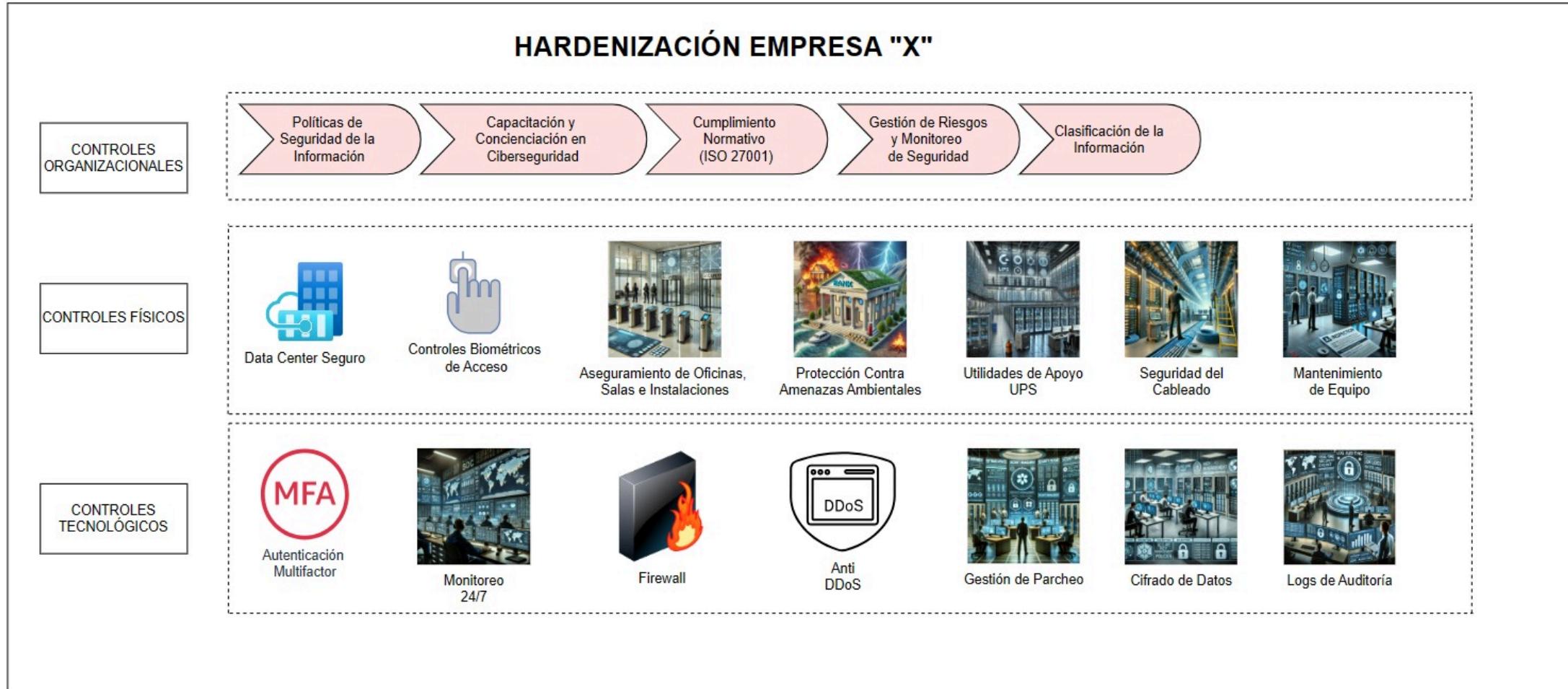


# 6. CONTROLES ADICIONALES (FÍSICOS)

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	Verificar mensualmente



# 6. DIAGRAMA DE ARQUITECTURA DE SEGURIDAD



# 7. CONCLUSIONES

Se 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.

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.

xt here.

## 8. 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 (2<sup>a</sup> ed.) (Auerbach Publications p. 98).



# Preguntas



@EsdegCol



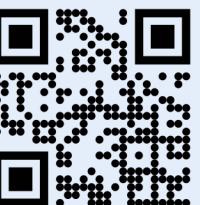
Escuela Superior  
de Guerra



Escuela Superior  
de Guerra



Escuela Superior  
de Guerra



[www.esdegue.edu.co](http://www.esdegue.edu.co)



ISO 9001:2015  
ISO 21001:2018  
**BUREAU VERITAS**  
Certification



La *Escuela Superior de Guerra "General Rafael Reyes Prieto"* está certificada  
bajo las normas internacionales **ISO 9001:2015 e ISO 21001:2018**.



# Gracias



@EsdegCol



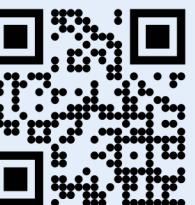
Escuela Superior  
de Guerra



Escuela Superior  
de Guerra



Escuela Superior  
de Guerra



[www.esdegue.edu.co](http://www.esdegue.edu.co)