Informe Modelamiento de Amenazas del Sistema de Gestión de Transacciones Electrónicas (SGTE) de la Empresa FinSecure S.A.

MY. Carlos Augusto Uribe Vergara

CC. Danny Leomar Sánchez Ropero

CC. José Johan Martínez Rojas

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Curso de Estado Mayor - CEM 2025

Gestión de Riesgos Cibernéticos

Mag. Jaider Ospina Navas

19 de febrero de 2025

Sistema de Gestión de Transacciones Electrónicas (SGTE) en FINSECURE S.A.

FinSecure SA es una empresa dedicada a ofrecer servicios de seguridad cibernética, orientada específicamente al sector financiero; clasificada como de mediano tamaño de acuerdo a sus activos y pasivos, cuenta con un capital humano de 130 personas, y opera únicamente en Colombia, con sede principal en Bucaramanga Santander.

Entró en operación el 07 de enero de 2025 y rápidamente ha ido ganado espacio y reconocimiento en el sector, como una entidad confiable y profesional. Desde sus inicios, la alta dirección de la entidad ha establecido como activos críticos de especial protección los datos financieros y datos personales. Se ha identificado dentro de los principales riesgos la posibilidad de ocurrencia de ataques cibernéticos y filtración de datos importantes de la empresa; por lo tanto, el enfoque principal se centra en la protección de datos sensibles.

Descripción del escenario

La organización debe determinar los problemas externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados esperados de su sistema de gestión de seguridad de la información (ISO/IEC 27001:2022). Por lo descrito, es decisión de la Gerencia General de FinSecure SA realizar un análisis de riesgos periódico, considerando el cambiante entorno y desarrollo digital en la actualidad, así mismo, para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. De tal manera que se selecciona, dentro de las múltiples áreas donde se puede desarrollar un análisis orientado al tema, enfocar esfuerzos hacia el Sistema de Gestión de Transacciones Electrónicas (SGTE).

Un SGTE es una plataforma tecnológica utilizada por empresas financieras, fintechs y bancos para procesar, registrar y verificar transacciones monetarias en tiempo real. Este

sistema es clave para la ejecución de pagos, transferencias de fondos, compras en línea y otras operaciones financieras.

A continuacion, se muestra una arquitectura de red del SGTE (Figura 1).

Figura 1. Arquitectura de red SGTE de FinSecure SA

Fuente: Elaboración propia mediante Visio.

Es así que, el SGTE puede describirse como el núcleo del negocio, ya que a través de este se gestionan pagos, transferencias y otras transacciones financieras en tiempo real. Su integridad y disponibilidad son esenciales para la confianza de los clientes y la continuidad operativa. Un fallo o ataque exitoso al SGTE podría paralizar las operaciones de FinSecure S.A., generando pérdidas económicas y afectando la reputación de la empresa (Schneier, 2020).

Dentro de las funciones de un SGTE, se pueden mencionar, la autenticación y autorización (Verifica la identidad del usuario y autoriza la transacción), procesamiento de pagos (Gestión de pagos con tarjetas de crédito/débito, transferencias interbancarias y pagos digitales), integración con pasarelas de pago (Conexión con redes bancarias y sistemas de pago internacionales), registro y auditoría (Almacena transacciones con trazabilidad para auditorías y seguridad), monitoreo de fraude (Usa inteligencia artificial y análisis de patrones para detectar transacciones sospechosas), entre otras.

Análisis de riesgos

Para realizar el análisis de riesgos se propone inicialmente usar el modelamiento STRIDE, a través del cual se busca dar soporte (Microsoft, 2022), abarcando categorías de factores de amenazas, y para darle amplitud y robustes en la calificación del análisis se cita a la junta directiva en pleno.

Mencionado ente administrativo está organizado en seis áreas (para efectos académicos se denominarán: Área 1, Área 2, Área 3, Área 4, Área 5, Área 6), de acuerdo con el mapa de procesos de la entidad. A los respectivos jefes de área se les entrega una guía completa para ambientarlos sobre múltiples amenazas cibernéticas actuales, consecuencias, impactos, e inclusive algunas lecciones aprendidas en el mercado actual, con el objetivo de impulsar el pensamiento crítico y propender que el conocimiento que cada quien tiene de sus actividades y responsabilidades, las proyecte a un entorno con posibles amenazas, especificándoles la necesidad de pensar, identificar y valorar, la probabilidad de ocurrencia y el posible impacto que se causaría a la empresa.

Para entrar en contexto, a través del modelamiento STRIDE se representan seis tipos de amenazas a la seguridad, lo que facilita la clasificación y organización del listado de amenazas identificadas. Para efectos académicos se registra una amenaza por cada tipo, y se le asigna un código de identificación para efectos prácticos (Tabla 1).

Tabla 1. Relación de Amenazas con Base en la Metodología STRIDE

MODELO STRIDE	AMENAZA	COD.
Spoofing (Suplantación de identidad)	Un atacante suplanta a un usuario legítimo para acceder al sistema.	A1
Tampering (Manipulación de datos)	Modificación no autorizada de datos financieros o transaccionales.	A2

Repudiation (Repudio de transacciones)	Un usuario niega haber realizado una transacción legítima.	A3
Information Disclosure (Divulgación de información)	Exposición de datos sensibles por fallos en la seguridad.	A4
Denial of Service (Denegación de servicio)	Ataques que inhabilitan el sistema, impidiendo transacciones.	A5
Elevation of privilege (Elevación de privilegios)	Un atacante obtiene permisos más altos de los que debería tener.	A6

Fuente: Elaboración propia.

Se da inicio a la Junta Directiva con una exposición de casos, y una completa explicación sobre la metodología. Así mismo se le presenta el listado de amenazas identificadas, requiriéndole a cada jefe de áreas que califique en probabilidad (Porcentaje) e impacto (Nota de 1 a 10) de cada una de las amenazas (Tabla 2).

Tabla 2. Consolidado de calificaciones de la Junta Directiva

COD.	PROBABILIDAD						IMPACTO					
	Área 1	Área 2	Área 3	Área 4	Área 5	Área 6	Área 1	Área 2	Área 3	Área 4	Área 5	Área 6
A1	98%	90%	94%	90%	70%	99%	9	10	7	9	8	9
A2	10%	5%	30%	30%	10%	20%	5	6	3	4	5	4
A3	60%	50%	55%	41%	61%	37%	6	8	7	6	5	8
A4	85%	70%	60%	50%	30%	60%	9	10	8	7	9	9
A5	49%	80%	77%	100%	37%	88%	3	4	1	2	4	3
A6	40%	51%	64%	50%	30%	80%	10	9	9	10	10	9

Fuente: Elaboración propia.

Una vez consolidada y analizada la información, las calificaciones de las diferentes áreas son ponderadas, y así se genera una matriz de riesgos, por probabilidad (P) e impacto (I) (Tabla 3).

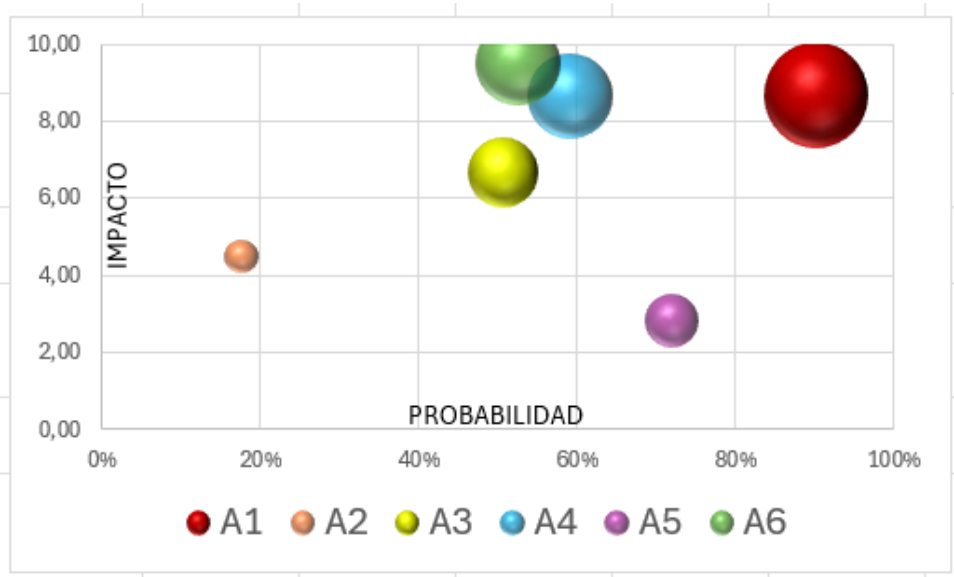
Tabla 3. Matriz de riesgos de FinSecure SA usando STRIDE

COD.	MD	AMENAZA	PROBABILIDAD		IMPACTO		PxI
A1	S	Un atacante suplanta a un usuario legítimo para acceder al sistema.	90%	ALTA	8,67	ALTA	7,81
A2	T	Modificación no autorizada de datos financieros o transaccionales.	18%	BAJA	4,50	MEDIA	0,79
A3	R	Un usuario niega haber realizado una transacción legítima.	51%	MEDIA	6,67	MEDIA	3,38
A4	I	Exposición de datos sensibles por fallos en la seguridad.	59%	MEDIA	8,67	ALTA	5,13
A5	D	Ataques que inhabilitan el sistema, impidiendo transacciones.	72%	ALTA	2,83	BAJA	2,04
A6	E	Un atacante obtiene permisos más altos de los que debería tener.	53%	MEDIA	9,50	ALTA	4,99

Fuente: Elaboración propia.

Esta información también es presentada en gráfico de burbuja (Figura 2), a través del cual se observa gráficamente el resultado obtenido, y, por ende, el enfoque del esfuerzo propuesto.

Figura 2. Diagrama de burbujas, análisis de riesgos de FinSecure SA



Fuente: Elaboración propia.

Sin embargo, el grupo analista de riesgos cibernéticos considera prudente e importante aplicar una metodología complementaria, para validar o desvirtuar la cuantificación realizada por la junta directiva, y así evitar caer en posibles errores causados por prejuicios o facilismos; el uso del modelamiento DREAD, que consiste en cuantificar las categorías de Daño, Reproducibilidad, Explotabilidad, Usuarios Afectados y Descubrimiento, con los parámetros de calificación según Threat-Modeling.com (2025).

Tabla 4. Análisis de riesgos de FinSecure SA, combinando STRIDE y DREAD

COD.	**AMENAZA**	D	R	E	A	D	**CALIF. FINAL**	
A1	Un atacante suplanta a un usuario legítimo para acceder al sistema.	10	8	10	3	9	40	CRITICO
A2	Modificación no autorizada de datos financieros o transaccionales.	5	5	1	2	3	16	MEDIO

A3	Un usuario niega haber realizado una transacción legítima.	1	5	10	2	3	21	MEDIO

COD.	AMENAZA	D	R	E	A	D	CALIF. FINAL	
A4	Exposición de datos sensibles por fallos en la seguridad.	8	5	2,3	9	6	30,3	ALTO
A5	Ataques que inhabilitan el sistema, impidiendo transacciones.	4	1	2	6	0	13	MEDIO
A6	Un atacante obtiene permisos más altos de los que debería tener.	8	0	1	6	9	24	MEDIO

Fuente: Elaboración propia.

El producto de la combinación de modelamientos STRIDE y DREAD (Tabla 4), se compara con el resultado mostrado anteriormente, y de esta manera se valida el excelente ejercicio realizado por la junta directiva, solo con una consideración de mediana relevancia con respecto a la amenaza A2 que fue clasificada como “baja”, sin embargo, a través del modelamiento DREAD, se clasifica como “media”, y en consecuencia así será considerada para el diseño de los controles de seguridad propuestos.

Diseño de controles de seguridad

Se propone iniciar fortaleciendo las políticas de seguridad de la información en la entidad, incluyendo:

- Se realizará una evaluación de impacto para tres meses, con el propósito de realizar una mejora continua.
- Autenticación y Control de Acceso: Implementar MFA en clientes y empleados.

- Cifrado Obligatorio: TLS 1.3 para comunicación, AES-256 en bases de datos.
- Monitoreo Continuo: Detección de intrusos con SIEM y análisis de tráfico.
- Resiliencia ante DDoS: CDN con protección DDoS, equilibrio de carga inteligente.
- Gestión de Identidades y Privilegios: Aplicar el principio de mínimo privilegio (Cisco, 2022).

En forma seguida, para el diseño y propuesta de control de seguridad, el grupo de desarrollo se basa inicialmente en MITRE ATT&CK, que es una base de conocimientos de acceso global sobre tácticas y técnicas de adversarios basadas en observaciones del mundo real. La base de conocimientos ATT&CK se utiliza como base para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad (MITRE, s.f.).

Es de esta manera que se ambienta a la alta dirección con una relación de amenazas, impactos y medidas de mitigación (Tabla 5), sin embargo, también se entrega un planteamiento de sistema de defensa en profundidad, como una estructura robusta y organizada.

Tabla 5. Relación de medidas de mitigación SGTE de FinSecure SA

COD.	MD	AMENAZA	IMPACTO	MITIGACIÓN
A1	S	Un atacante suplanta a un usuario legítimo para acceder al sistema.	Robo de credenciales, fraude financiero, acceso no autorizado a cuentas.	Autenticación Multifactor (MFA), biometría, tokens dinámicos.
A2	T	Modificación no autorizada de datos	Alteración de registros de pago, fraude, pérdida de integridad de datos.	Cifrado de extremo a extremo (TLS 1.3), firma digital en transacciones.

		financieros o transaccionales.		
A3	R	Un usuario niega haber realizado una transacción legítima.	Disputas financieras, fraude, pérdida de confianza en el sistema.	Registros de auditoría inmutables, blockchain para trazabilidad.
A4	I	Exposición de datos sensibles por fallos en la seguridad.	Filtración de datos personales y financieros, incumplimiento normativo.	Cifrado AES-256 en bases de datos, control de acceso basado en roles (RBAC).
A5	D	Ataques que inhabilitan el sistema, impidiendo transacciones.	Interrupción de pagos y servicios, impacto económico y reputacional.	Protección DDoS con balanceo de carga y firewalls inteligentes.
A6	E	Un atacante obtiene permisos más altos de los que debería tener.	Control total del sistema, manipulación de registros financieros.	Principio de mínimo privilegio, monitoreo de accesos y logs de seguridad.

Fuente: Elaboración propia.

Es clave implementar estrategias de seguridad multicapa, incluyendo cifrado de extremo a extremo, autenticación multifactor (MFA), monitoreo en tiempo real y auditorías continuas. Un SGTE se diseña bajo una arquitectura distribuida y segura para garantizar confidencialidad, integridad y disponibilidad (Figura 3).

Figura 3. Propuesta diagrama multicapa para SGTE de FinSecure SA

Nota. El contenido relacionado es elaborado con bases y soporte según OpenAI (2025).

Fuente: Elaboración propia.

Responsabilidades

Para lograr una futura evaluación y planteamiento de posibles mejoras, se considera necesario la asignación de responsables dentro de la entidad, de tal manera se propone el uso de la matriz RACI, que es una forma de identificar los roles y responsabilidades de los

equipos de tu proyecto para cualquier tarea, logro o entrega del proyecto. Al seguir la matriz RACI, puedes aclarar cómo está distribuida la responsabilidad y reducir la confusión (Martins, 2025).

En este ejemplo se han definido los siguientes roles:

- CISO: Jefe de Seguridad de la Información (quien aprueba y se hace responsable a nivel estratégico).
- Ingeniero de Seguridad: Encargado de la implementación técnica y ejecución de las tareas (responsable directo).
- Administrador de Sistemas: Soporte técnico y experto en infraestructura (consultado para aspectos de integración y configuración).
- Auditor de Seguridad: Encargado de verificar el cumplimiento de normativas y mejores prácticas (consultado para validar la seguridad).
- CTO: Director de Tecnología (informado sobre el avance y resultados).

Tabla 6. Propuesta de matriz RACI de FinSecure SA

AREA	Responsable (R)	Aprobador (A)	Consultado (C)	Informado (I)
Autenticación Multifactor (MFA)	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO
Biometría	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO
Tokens dinámicos	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO
Cifrado de extremo a extremo (TLS 1.3)	Ingeniero de Seguridad	CISO	Administrador de Sistemas	CTO
Firma digital en transacciones	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO

Registros de auditoría inmutables	Ingeniero de Seguridad	CISO	Auditor de Seguridad, Administrador de Sistemas	CTO
Blockchain para trazabilidad	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO
Cifrado AES-256 en bases de datos	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO
Control de acceso basado en roles (RBAC)	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO
Protección DDoS con balanceo de carga y firewalls inteligentes	Ingeniero de Seguridad	CISO	Administrador de Sistemas	CTO
Principio de mínimo privilegio	Ingeniero de Seguridad	CISO	Administrador de Sistemas, Auditor de Seguridad	CTO
Monitoreo de accesos y logs de seguridad	Ingeniero de Seguridad	CISO	Auditor de Seguridad, Administrador de Sistemas	CTO

Nota. El contenido relacionado es elaborado con bases y soporte según OpenAI (2025).

Fuente: Elaboración propia.

Conclusiones y recomendaciones

- La implementación de un Sistema de Gestión de Transacciones Electrónicas (SGTE) en una empresa financiera requiere una atención prioritaria y un enfoque robusto en ciberseguridad para garantizar la protección de los datos sensibles.
- La combinación de los modelamientos STRIDE y la metodología DREAD sirven de complemento para la validación del análisis de riesgos en forma cuantificada del impacto y probabilidad de cada amenaza en la organización.
- La matriz RACI se integra como una excelente herramienta se asignación de responsabilidades, con las cuales se facilitará una evaluación e impactos.

- Adoptar una arquitectura de seguridad multicapa que incluya protección en cada nivel del SGTE, desde la capa de cliente hasta la integración con bancos y pasarelas de pago.
- Es necesario realizar auditorías de seguridad periódicas y pruebas de penetración para identificar y corregir vulnerabilidades en el sistema.
- Se debe capacitar continuamente al personal en buenas prácticas de seguridad informática para reducir el riesgo de ataques de ingeniería social.

Bibliografía

- Cisco. (2022). *Mejores prácticas de arquitectura de seguridad de red*. Documentos técnicos de seguridad de Cisco.
- ISO/IEC 27001:2022. *Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos*. Organización Internacional de Normalización.
- Martins, J. (2025, 6 de febrero). *Matriz raci: Qué es, cómo crearla con ejemplos y alternativas online*. Asana. https://asana.com/es/resources/raci-chart
- Microsoft. (2022). *Modelado de amenazas STRIDE: identificación y mitigación de amenazas de seguridad*. Blog de seguridad de Microsoft. Recuperado de https://www.microsoft.com/security/blog
- MITRE. (s.f.). *MITRE ATT&CK framework*. MITRE. https://attack.mitre.org/
- NIST. (2021). *Marco para mejorar la ciberseguridad de infraestructuras críticas (versión 1.1)*. Instituto Nacional de Estándares y Tecnología (NIST). Recuperado de https://www.nist.gov/cyberframework
- OpenAI. (2025, 18 de febrero). *Respuesta generada por ChatGPT* [Modelo de lenguaje de IA]. OpenAI. Disponible en https://chat.openai.com
- Schneier, B. (2020). *Criptografía aplicada: protocolos, algoritmos y código fuente en C*. John Wiley & Sons.
- Threat-Modeling.com. (2025). *DREAD Threat Modeling*. https://threat-modeling.com/dread-threat-modeling/