Gestión del Riesgo Cibernético

MY. Julián Andrés Quintero
MY. Luís Naranjo Suarez
MY. Cristiam Cáceres Camacho
CC. Andres Otero

SR. Jaider Ospina

Implementación del modelo STRIDE

Bogotá
2025

Introducción

Informe de vulnerabilidades

Este informe presenta las posibles vulnerabilidades en el modelo de gestión de base de datos y sistema de información de una empresa nacional de bienes y servicios, utilizando el modelo STRIDE. El propósito es mitigar las amenazas y gestionar el riesgo de manera eficiente y proactiva.

Es importante entender que este estudio se enfoca en cómo la empresa gestiona la información y recopila datos de sus clientes a través del Sistema de Gestión de Membresía (SMG), donde por su importancia, para este caso vamos considerar este sistema como un ***activo crítico*** debido a la clase de información que maneja que en cierta manera conduce para alcanzar los objetivos generales de nuestra empresa, entendiendo según (*ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online*, s. f.), "es esencial para que la empresa funcione correctamente y alcance los objetivos que se ha propuesto la alta dirección". Esto se debe a que el SMG maneja información personal y financiera de los clientes, lo que lo convierte en un blanco atractivo para posibles ataques cibernéticos.

Si llegara a ocurrir un ataque, podríamos enfrentar serios problemas en la integridad, disponibilidad y confidencialidad de la información. El impacto dependería de cuánto tiempo estuviera expuesta la información y de cuán bien la empresa pudiera recuperarse. Un ataque podría afectar no solo a los servidores, sino también a los clientes, creando un efecto cascada que podría resultar en pérdidas económicas, dañar la reputación de la empresa e incluso llevar a una crisis financiera o sanciones legales. Por eso, es crucial que implementemos medidas de

ciberseguridad efectivas para proteger este sistema y asegurar el buen funcionamiento de la organización.

Descripción del sistema de información, componentes de red y posibles amenazas.

Según (Implika, s. f.) **"**Una red de información es un conjunto de dispositivos que se encuentran interconectados entre si a través de un medio" estos intercambian información, gestionan, procesan y brindan los canales necesarios óptimos de comunicación entre varios actores que participan en una red con un propósito determinado en búsqueda de un beneficio particular. En nuestro caso vamos a describir los componentes más esenciales del sistema de información y red, basado en la base de datos proporcionado por los usuarios mediante el sistema de membresía de los aplicativos o plataformas de nuestra empresa de bienes y servicios.

El sistema cuenta con un servidor central de recolección de información que se alimenta de la información brindada a nivel regional e interactúan para la disponibilidad de la misma entre usuario y la organización, basado en una plataforma digital que le permite a los clientes acceder a varias funciones esenciales como el registro, gestión del aplicativo de la propia cuenta, realizar pagos de validación o renovación de la membresía mediante un sistema de pagos electrónicos, acceder a beneficios según el plan que tenga el cliente (bronce, plata y oro), recibir notificaciones y promociones al correo electrónico o al aplicativo, que se recolecta en una base de datos centralizada.

Una vez realizado un análisis general de los medios de información y los sistemas involucrados en nuestras operaciones, es fundamental identificar y evaluar las amenazas potenciales que podrían comprometer la integridad, disponibilidad y confidencialidad de nuestros datos. Este proceso implica la identificación de amenazas, reconociendo vulnerabilidades en el sistema; al

evaluar su impacto potencial podemos identificar las repercusiones a corto, mediano y largo plazo; establecer una probabilidad donde se analice las métricas y los diferentes sistemas de información comunes que nos ayuden a obtener información de la probabilidad de la ocurrencia de la amenaza y así lograr contextualizar debilidades en los propias sistema y la red de información; por ultimo vamos a sumar estos factores y los vamos a representar para establecer las medidas de mitigación bajo el sistema STRIDE de la siguiente, forma:

A AMENAZA	P PROBABILIDAD	I IMPACTO	M MEDIDAS DE MITIGACIÓN
• **SPOOFING (Robo de credenciales).**	• ALTO	• ALTO	• Detección de accesos inusuales, y políticas de bloqueo por intentos fallidos.
• **TAMPERING (Modificación de membresías)**	• MEDIA	• ALTO	• Uso de registros inmutables, auditorías periódicas y cifrado de bases de datos.
• **Repudiation (Negación de transacciones)**	• MEDIA	• MEDIA	• Registro de logs detallados y validación de transacciones con firma digital.
• **Information Disclosure (Filtración de datos)**	• ALTO	• ALTO	• Cifrado de datos en tránsito y en reposo, segmentación de bases de datos y controles de acceso estrictos.
• **Denial of Service (Ataque DDoS)**	• ALTO	• ALTO	• Implementar un WAF (Firewall de Aplicaciones Web), balanceo de carga y sistemas de mitigación de DDoS.
• **Elevation of Privilege (Acceso administrativo indebido),**	• MEDIA	• ALTO	• Aplicar el principio de privilegio mínimo, segmentación de accesos y monitoreo de logs de actividad.

Si analizamos el impacto de la amenaza después de categorizarlo entre (Bajo, medio y alto) es necesario comprender en cada caso el sistema STRIDE; y en primera medida con el robo de credenciales se presentaría acceso no autorizado a datos personales y financieros, que perjudicarían directamente al cliente, lo que notablemente dañaría la reputación de la organización a nivel general sino se logra gestionar de forma oportuna y adecuada; es importante

aclarar que no se vería comprometidos los sistemas de información de base de datos de la organización, si el atacante no tiene la capacidad de escalar privilegios.

En el segundo evento se analizan las pérdidas económicas resultantes de la penetración o manipulación de datos, incluyendo las membresías de los clientes y la modificación de los registros de pago. Esto afecta directamente a las bases de datos del servidor central, generando efectos en cada nivel regional y produciendo pérdidas económicas.

En el repudio transaccional, se verá afectado la parte financiera y la forma como los clientes realizasen los pagos, alegando pagos no autorizados, esto quiere decir que si el sistema no tiene una forma de autenticación de pagos eficiente el cliente, al final no pagaría por los servicios adquiridos, en adición la organización podría verse involucrada en conflictos legales.

La filtración de datos tiene un efecto demasiado catastrófico en todo el sistema y la red a nivel global. Por medio de las membresías se tiene acceso al 100% de la información del cliente, donde las consecuencias van desde el robo de la identidad, suplantación, perdida de la información financiera, acciones legales en contra de la organización por mal manejo de las políticas de privacidad y el daño reputacional de la entidad, generando pérdidas económicas y de clientes hasta la desaparición de la organización sino es gestionado a tiempo el ataque con un plan de respuestas y contingencias oportuno.

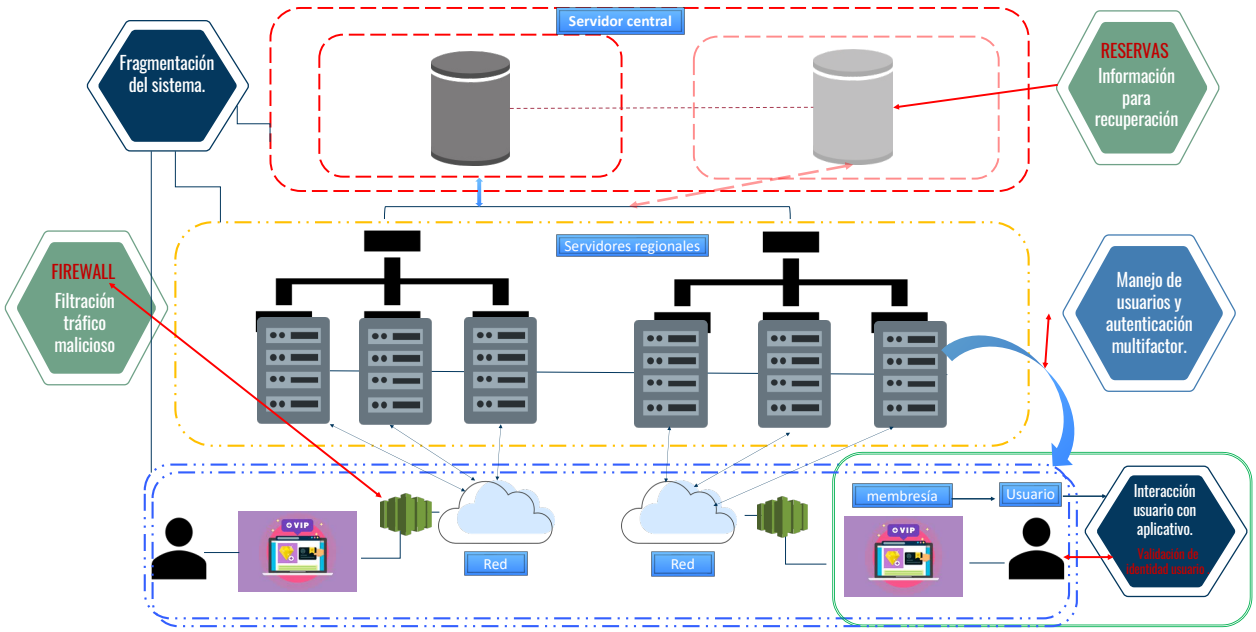
Por el lado de la denegación de servicio se impedirá el acceso a las plataformas y la interrupción de esta, afectando la interfaz entre usuario y plataforma, no permitiendo actualizaciones de base de datos antiguos y nuevos clientes, el ingreso de usuario y acceso a pagos, es muy problema que esta situación en particular produzca pérdidas económicas significativas, dependiendo de los tiempos de exposición, capacidad de reacción y restablecimiento del servicio.

El escalamiento de privilegios con acceso indebidos de la información produce un impacto catastróficamente en los objetivos generales de la organización debido a que se pierde el control total de la infraestructura; cuando sucede esto, el factor decisivo dependerá del tiempo de exposición del atacante y las puertas traseras abiertas que se dejen en la línea de tiempo desde que inicio el ataque hasta la detección del mismo , esto permite a los atacantes robar información privilegiada y así mismo difundirla de forma irregular, esta clase de amenazas suelen ser silenciosas y difíciles de detectar, requieren un sistema de monitoreo constante que detecte cambios significativos y el accesos de plataformas de escaneo y de análisis de vulnerabilidades que detecten comportamientos inusuales en el sistema.

Por último las probabilidades de medición medias observadas dentro del análisis, no indica que no se pueda producir un ataque utilizando estos tipos técnicas de amenazas, sino que para este estudio este término intermedio se basa en factores externos de accesibilidad como la interconexión atacantes y atacados, el tiempo y el tipo de exposición, los medios de autenticación multifactor de los servidores, historial de incidentes de estas categorías y las habilidades técnicas o capacidades que tenga el atacante, en donde se requiere un estudio social de las víctimas y una preparación y rigorosa de los atacantes para poder llegar a estas vulnerabilidades.

Diagrama de arquitectura de seguridad.

El diagrama representa la estructura de seguridad cibernética para nuestro sistema de gestión de membresías de nuestra empresa de bienes y servicios, en donde se referencia como se conectan los sistemas e interactúan desde el usuario hasta la base de datos central conectando los componentes críticos de los sistemas.



Es importante analizar las medidas de seguridad pertinentes con el que cuenta el sistema iniciando desde la interacción del usuario con la plataforma o el aplicativo, donde existe una validación de datos, con autenticaciones multifactor para garantizar el uso legítimo por parte del usuario a través del filtro y barrido del sistema.

La información se transmite a través de la red, donde un firewall filtra el tráfico malicioso dirigido a los servidores. Estos servidores están organizados en dos categorías: regionales y central. Cada servidor regional es administrado localmente y está interconectado con los demás para facilitar el intercambio de información y la visualización de datos de clientes con privilegios limitados. Esta estructura permite transferir la información al servidor central, que se encarga de centralizar todas las operaciones.

El servidor central almacena, administra y procesa la información de las membresías de los clientes, tanto personal como financiera, y cuenta con un sistema de recuperación que se

encuentra fragmentado con un módulo de información Back-up en caso de incidentes o ataques al sistema.

En este modelo se intenta aplicar e implementar en el desarrollo de defensa en profundidad, (*¿Qué es la defensa en profundidad?*, s. f.) “es una estrategia que aprovecha múltiples medidas de seguridad para proteger los activos de una organización”. Tratando de proteger cada capa de segmentación con una estructura modular para mantener un alto nivel de seguridad.

Políticas de seguridad propuestas.

Las políticas de seguridad de la organización juegan un papel fundamental para la contención de amenazas e involucra todas las esferas de la organización, estas políticas crean unas normas, que deben de cambiar la cultura y la forma pensar. Según (Ortega, 2023) “ Son documentos que establecen las normas y los procedimientos que una organización debe seguir para proteger sus sistemas de información y sus datos. Las políticas de ciberseguridad se crean con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información crítica” como lo identificamos anteriormente nuestro Sistema de Gestión de Membresías por sus características lo catalogamos como infraestructura critica, es por ello de la claridad y rigurosidad que se debe tener en la observancia y toma de políticas claras y eficientes.

Para este caso vamos a dividir estas políticas en dos bloques, identificando en el primero unas que son generales que impactan a todos los miembros de la organización de forma interna en

cuanto a cultura o factores individuales y el segundo bloque trata de políticas específicas que impactan las vulnerabilidades observadas en el modelo STRIDE.

Políticas generales.

Estas políticas tienen como propósito generar una cultura organizacional interna y crear tácticas, técnicas y procedimientos estandarizados, es por ello que a nivel nacional se habla de integración de la parte pública y privada en las acciones necesarias que permitan la creación de hábitos de uso seguro y responsable de las TIC, como se especifica en el («CONPES 3995», 2020), ahora para alcanzar estos objetivos como organización, iniciamos con un punto de partida donde tocaremos el tema de la capacitación y preparación del personal.

Como primera medida es necesario crear una cultura y esta política va enfocada a evitar, controlar el mal uso de los sistemas de información que permiten penetraciones a los sistemas internos o base de datos, elevación de protocolos como un objetivo principal, con un alcance hacia los empleados con acceso a los sistemas de información y administradores con acceso a privilegios para la gestión de la plataforma. Estas temáticas de capacitación va dirigidas y deben ser enfocadas a diferentes audiencia, de acuerdo sus conocimientos, función y capacidad de acceso a la información, en donde se traten de temas básicos como conciencia y conocimiento básico de ciberseguridad, gestión y utilización de contraseñas, administración de correos electrónicos y restricción y uso de dispositivos externos; en una fase intermedia protección de datos personales, buenas prácticas en el uso de los sistemas y en una fase más avanzada se pueden tocar temas de administración de redes, simulacros de ataques, Etc. Estos planes de capacitación deben tener una frecuencia e intensidad y deben de tener un control, seguimiento y evaluación de estos, lo que crea una conciencia y cultura de ciberseguridad de cero confianzas.

En segundo lugar, es fundamental establecer planes de contención y mitigación ante un ataque, que incluyan funciones específicas y claras para todo el personal de la organización. Además de contar con estos planes, es necesario realizar simulacros periódicos para evaluar tiempos de reacción, resiliencia y recuperación. Estas actividades son cruciales, ya que refuerzan la cultura de ciberseguridad y permiten identificar posibles fallos y vulnerabilidades en los sistemas. Asimismo, se debe contar con una política clara de respuesta a incidentes que especifique los roles y responsabilidades del personal involucrado. Es vital que exista sinergia en momentos de crisis, tanto en la atención a usuarios externos como en la gestión interna por parte de los administradores del sistema. La gerencia, por su parte, debe comprender la importancia de proporcionar todos los recursos necesarios para gestionar el riesgo de manera ágil, minimizando así el impacto en los objetivos estratégicos de la organización.

Políticas Específicas.

Según el análisis del modelo STRIDE, se analiza las amenazas en una combinación de probabilidad Vs Impacto y en nuestro sistema de gestión de membresías, se lograron identificar 03 variables de generalidad alta, así:

A AMENAZA	P PROBABILIDAD	I IMPACTO	M MEDIDAS DE MITIGACIÓN
• **SPOOFING (Robo de credenciales).**	• ALTO	• ALTO	• Detección de accesos inusuales, y políticas de bloqueo por intentos fallidos.
• **Information Disclosure (Filtración de datos)**	• ALTO	• ALTO	• Cifrado de datos en tránsito y en reposo, segmentación de bases de datos y controles de acceso estrictos.
• **Denial of Service (Ataque DDoS)**	• ALTO	• ALTO	• Implementar un WAF (Firewall de Aplicaciones Web), balanceo de carga y sistemas de mitigación de DDoS.

Basado en estas amenazas de probabilidad e impacto alto vamos a determinar políticas técnicas de funcionamiento de la siguiente forma; iniciando con las políticas de seguridad de acceso, en donde se enfoca en reducir los ataque de fuerza bruta y robo de credenciales, y se inicia con normas de implementación de sistemas multifactor con un mínimo de tres factores de verificación para personal con acceso a información crítica, y en este sentido todos los integrantes de la organización desde los propios usuarios hasta los mismo funcionarios deben acogerse a esta política de seguridad y privacidad sin excepción algún. Así mismo se establecen otras políticas como el monitoreo de sesiones abiertas con tiempo máximo de actividad, como lo realizan las aplicaciones bancarias y bloqueo de contraseña tras tres intentos fallidos, esto conlleva a la necesidad de la creación de equipos de monitoreo para estas funciones específicas que detecten movimientos inusuales.

En cuanto a la prevención de ataques, donde incluimos la denegación del servicio y la filtración de datos, podemos implementar la WAT (Web Application Firewall) (*¿Qué es WAF firewall? | Cortafuegos de aplicaciones web | Cloudflare*, s. f.) “Un firewall de aplicaciones web (WAF) ayuda a proteger las aplicaciones web al filtrar y monitorizar el tráfico HTTP entre una aplicación web e Internet”, esto bloqueando el tráfico de datos sospechosos. En cuento a la

denegación del servicio se debe realizar monitoreo constante de los servidores analizando el tráfico sospechoso o voluminoso por parte de los equipos de prevención donde se puedan neutralizar y contener; pero si tenemos un servicio robusto que manejan demasiado información como el que planteamos en nuestro caso, es necesario invertir recursos en tecnología que nos ayuden a: 1. Monitorear nuestro servidores con plataformas que permitan identificar vulnerabilidades y generen alertas de conductas inusuales 2. Buscar la redundancia de nuestros servidores con una fragmentación, evitando sobrecargas al sistema y teniendo un respaldo de información que permita la resiliencia ante un ataque. Otros tipo de políticas que se podrían implementar van desde métodos de reducción de superficie de ataque, la dispersión de tráfico a múltiples servidores y limitaciones de velocidad del tráfico, como lo tífica (*¿Cómo evitar ataques DDoS?*, s. f.), pero como lo explicamos anteriormente para poder aplicar todos estos métodos se requiere una cultura organizacional, que entienda y comprenda que el mantenimiento de la seguridad requiere compromisos tanto económicos, como de seguimiento y control constante para garantizar la integridad, disponibilidad y confidencialidad de la información del sistema de gestión de membresías

Conclusiones y recomendaciones

Dentro del sistema de gestión de membresías de nuestra empresa de bienes y servicios, utilizando el modelo STRIDE, se logró identificarte impactos altos con probabilidades que suceda un evento critico que coloca en riesgo la seguridad de la organización y que deben ser atendidos con políticas empresariales de seguridad de acceso, protección de datos, prevención de ataques, auditorias y cumplimiento esto nos lleva a pensar que las medidas de detección y respuesta debe ser efectivos y consistentes para garantizar la disponibilidad, confidencialidad y la integridad de la información en todo momento ante un ataque ; adicional a lo anterior se debe

realizar un seguimiento y una verificación periódica de las amenazas de probabilidad media, como lo es el tampering, repudiación, elevación of privilege, esto en razón a que las amenazas mutan y las capacidades de los atacantes se transforma buscando tácticas y métodos que le permitan realizar ataques con mayor impacto y con una capacidad de explotación mayor.

Es fundamental recomendar que la implementación de políticas sea acompañada de seguimientos oportunos, garantizando así el cumplimiento de los objetivos establecidos. Además, es crucial fortalecer los controles de autenticación, disponibilidad e integridad del sistema. Para ello, se sugiere la utilización de servidores centrales tipo espejo, que no solo mejoran la resiliencia del sistema, sino que también facilitan la fragmentación de la información. Esto permitirá una respuesta más ágil ante posibles incidentes y asegurará la continuidad operativa. En resumen, la combinación de un seguimiento riguroso y el fortalecimiento de los controles técnicos contribuirá significativamente a la eficacia y seguridad del sistema, promoviendo un entorno más robusto y confiable.

Bibliografía

¿Cómo evitar ataques DDoS?| Métodos y herramientas. (s. f.). Recuperado 19 de febrero de 2025, de https://www.cloudflare.com/es-es/learning/ddos/how-to-prevent-ddos-attacks/

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL CONPES. (2020). *Departamento de Planeación*, 28.

Implika. (s. f.). *Qué son las redes informáticas y cómo funcionan*. Implika. Recuperado 17 de febrero de 2025, de https://www.implika.es/blog/que-son-redes-informaticas

ISO 27001—Certificado ISO 27001 punto por punto—Presupuesto Online. (s. f.). Norma ISO 27001. Recuperado 17 de febrero de 2025, de https://www.normaiso27001.es/

Ortega, K. (2023, noviembre 8). *¿Qué son las políticas de ciberseguridad?* [Saint Leo University]. Saint Leo University. https://worldcampus.saintleo.edu/blog/que-son-las-politicas-de-ciberseguridad-y-su-importancia

¿Qué es la defensa en profundidad? Definición y explicación. (s. f.). Fortinet. Recuperado 20 de febrero de 2025, de https://www.fortinet.com/lat/resources/cyberglossary/defense-in-depth.html

¿Qué es WAF firewall? | Cortafuegos de aplicaciones web | Cloudflare. (s. f.). Recuperado 18 de febrero de 2025, de https://www.cloudflare.com/es-es/learning/ddos/glossary/web-application-firewall-waf/