MAXIMIZACIÓN DE LA SEGURIDAD EN SISTEMAS TRANSACCIONALES: REVISIÓN SISTEMÁTICA Y ENFOQUE INTEGRAL PARA MITIGACIÓN DE RIESGOS DE CIBERATAQUES

ADRIANO GUTIÉRREZ POCHE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA PLATA HUILA
2024

MAXIMIZACIÓN DE LA SEGURIDAD EN SISTEMAS TRANSACCIONALES: REVISIÓN SISTEMÁTICA Y ENFOQUE INTEGRAL PARA MITIGACIÓN DE RIESGOS DE CIBERATAQUES

ADRIANO GUTIÉRREZ POCHE

Monografía presentada para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. Joel Carroll Vargas
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
LA PLATA HUILA
2024

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

La Plata Huila, 12 de diciembre de 2024

DEDICATORIA

Con amor dedico este trabajo a Dios todo poderoso que me ha permitido avanzar y vencer las dificultades presentadas durante el proceso; con mucho amor a mi familia, mi esposa Francy Muñoz y mis hijos quienes creyeron en mí y con toda la paciencia y comprensión me han acompañado en cada etapa vivida de esta ardua experiencia académica, colaborándome de manera indirecta, minimizando mis preocupaciones. y brindándome el apoyo necesario para culminar este ciclo de aprendizaje.

AGRADECIMIENTOS

Agradezco a los directivos, líderes de programa y administrativos de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo y la implementación de políticas que permiten el acceso a la educación nos brindan la oportunidad de estudiar y laborar, por otro lado, agradezco a cada uno de los tutores y asesores y orientadores el acompañamiento desinteresado en el proceso formativo, les debo reconocer su trabajo y dedicación, porque sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

INTRODUCCIÓN 16
1 DEFINICIÓN DEL PROBLEMA 18
1.1 ANTECEDENTES DEL PROBLEMA 18
1.2 FORMULACIÓN DEL PROBLEMA 21
2 JUSTIFICACIÓN 22
3 OBJETIVOS 24
3.1 OBJETIVOS GENERAL 24
3.2 OBJETIVOS ESPECÍFICOS 24
4 MARCO REFERENCIAL 25
4.1 MARCO TEÓRICO 25
4.1.1 La teoría del riesgo. 25
4.1.2 Teoría del ataque distribuido. 26
4.1.3 Teoría del ataque de puerta trasera. 27
4.1.4 Teoría de la ingeniería social. 28
4.1.5 Teoría del mal funcionamiento humano. 29
4.2 MARCO CONCEPTUAL 29
4.2.1 Sistema transaccional. 30
4.2.2 Ciberseguridad. 30
4.2.3 Vector de ataque. 31
4.2.4 Hacker. 32
4.2.5 Malware. 32
4.2.6 Phishing. 33
4.2.7 Ingeniería social. 33
4.2.8 Firewall. 34
4.2.9 Autenticación. 35
4.2.10 Autorización. 36
4.2.11 Encriptación. 37
4.2.12 Seguridad en la red. 38
4.2.13 Protección de datos. 39

4.2.14 Monitoreo de redes. 39
4.2.15 Análisis de vulnerabilidades. 40
4.3 MARCO HISTÓRICO 41
4.4 ANTECEDENTES O ESTADO ACTUAL 44
4.5 MARCO CIENTÍFICO O TECNOLÓGICO 48
4.5.1 Sistemas de gestión de bases de datos. 48
4.5.2 Herramientas de análisis de vulnerabilidades. 48
4.5.3 Herramientas de análisis de tráfico de red. 48
4.5.4 Sistemas de detección de intrusiones. 48
4.5.5 Herramientas de análisis de código. 48
4.5.6 Plataformas de pruebas de penetración. 49
4.6 MARCO LEGAL 49
5 DISEÑO METODOLÓGICO 54
5.1 METODOLOGÍA. 54
5.1.1 Revisión bibliográfica. 54
5.1.2 Selección de fuentes. 54
5.1.3 Entrevistas a expertos. 54
5.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN 54
5.2.1 Revisión bibliográfica. 54
5.2.2 Análisis de incidentes. 55
5.2.3 Revisión de entrevistas. 55
6 FASE 1: IDENTIFICACION Y CONCEPTUALIZACION DE LOS TIPOS DE VECTORES DE ATAQUE 57
6.1 ESTADO DEL ARTE DE LOS VECTORES DE ATAQUE PREVALENTES EMPLEADOS POR LOS CIBERDELINCUENTES 57
6.1.1 El correo electrónico y la mensajería instantánea. 58
6.1.2 Los EndPoins, 59
6.1.3 el *software* de redes y sistemas mal configurados. desactualizado o no parcheado. 60
6.2 GENERALIDADES DE LOS SISTEMAS TRANSACCIONALES 62
6.2.1 Componentes de un sistema transaccional. 63

6.3 SISTEMAS TRANSACCIONALES VULNERADOS POR VECTORES DE ATAQUE. 64

7 FASE 2: EVALUACION DE LAS VULNERABILIDADES EN LOS SISTEMAS TRANSACCIONALES....72

7.1 CARACTERISTICAS DE LOS VECTORES DE ATAQUE EMPLEADOS POR LOS CIBERDELINCUENTES 72

7.1.1 Características generales del phishing. 73

7.1.2 Características generales del ataque distribuido de denegación de servicios (DDOS). 74

7.2 ELEMENTOS DE UN SISTEMA TRANSACCIONAL SUCEPTIBLE DE SER ATACADO....75

7.2.1 Base de datos.....75

7.2.2 Transacciones. 75

7.2.3 Concurrencia. 76

7.2.4 Control de concurrencia.....76

7.2.5 Recuperación. 76

7.2.6 Seguridad. 76

7.3 VULNERABILIDADES DE LOS SISTEMAS TRANSACCIONALES: DESAFIOS Y SOLUCIONES....80

7.3.1 Soluciones y Mitigaciones. 81

7.4 ANALISIS DE LOS DIFERENTES ATAQUES DESDE LA METODOLOGIA DE CICLO DE EVALUACION DE VULNERABILIDADES 81

7.4.1 Ataques SQL a Sistemas Transaccionales.....81

7.4.2 Ataques Cross-Site Scripting (XSS) en Sistemas Transaccionales.....82

7.4.3 Ataques a la Autenticación y Sesiones en Sistemas Transaccionales. ...83

7.4.4 Ataques a la Validación de Datos de Entrada en Sistemas Transaccionales.....84

7.4.5 Escalada de Privilegios en Ataques a Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidad. 85

7.4.6 Ataques de Ingeniería Social en Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidad. 85

7.5 FACTORES DE SEGURIDAD EN LOS SISTEMAS TRANSACCIONALES 86

7.6 ESTRATEGIAS DE MITIGACIÓN PARA PREVENIR ATAQUES A LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES 89

7.7 PANORAMA ACTUAL ACERCA DE LA MATERIALIZACION DE VECTORES DE ATAQUE EN EL ENTORNO EMPRESARIAL 94
7.7.1 Informe Sobre Motivos Específicos De Ataques Cibernéticos En El Entorno Empresarial 94
7.8 SISTEMAS TRANSACCIONALES ATACADOS EN COLOMBIA, ANÁLISIS DE CASOS 96
7.9 ANALISIS DEL CASO DE CIBERATAQUE A LA PLATAFORMA UBER ... 97
8 FASE 3: ELABORACION DE RECOMENDACIONES GENERALES APLICABLES A SISTEMAS TRANSACCIONALES 101
8.1 RECOMENDACIONES PARA EVITAR CIBERATAQUES EN LOS SISTEMAS TRANSACCIONALES..... 101
8.1.1 Auditoría de Seguridad Regular. 101
8.1.2 Gestión de Vulnerabilidades. 101
8.1.3 Políticas de Contraseñas Fuertes. 101
8.1.4 Control de Acceso. 101
8.1.5 Educación y Concienciación de los Empleados. 101
8.1.6 Protección contra *Malware*. 102
8.1.7 Respuesta a Incidentes. 102
8.1.8 Monitorización Continua. 102
8.1.9 Encriptación de Datos. 102
8.1.10 Actualización de Políticas y Procedimientos. 102
CONCLUSIONES 103
RECOMENDACIONES 105
BIBLIOGRAFÍA 106
ANEXOS 121
ANEXO A: 121

LISTA DE ILUSTRACIONES

pág.

Ilustración 1 Etapas de un ataque a un sistema transaccional 72
Ilustración 2 Empresas atacadas en Colombia durante el 2022 97
Ilustración 3 Esquema de red de la plataforma UBER.....98
Ilustración 4 Ruta del ataque realizado a la plataforma UBER 99

GLOSARIO

SEGURIDAD INFORMÁTICA.

ANTIVIRUS**:** es un *software* que se utiliza para detectar y eliminar virus y *malware* en los dispositivos.

AUTENTICACIÓN**:** es el proceso de verificar la identidad de un usuario o dispositivo para permitir el acceso a una red o sistema.

CIFRADO**:** es un proceso de codificación de información para protegerla de posibles accesos no autorizados.

*FIREWALL***:** es un *software* o *hardware* que se utiliza para proteger una red de posibles ataques externos.

VPN**:** siglas de *Virtual Private Network*. es una red privada que se utiliza para proteger la conexión a internet y garantizar la privacidad y seguridad de la información transmitida.

SISTEMAS TRANSACCIONALES.

CRM**:** siglas de *Customer Relationship Management*. es un sistema que se utiliza para gestionar la relación con los clientes y mejorar la satisfacción del cliente.

ERP**:** siglas de *Enterprise Resource Planning*. es un sistema que integra todos los procesos empresariales, como finanzas, recursos humanos, ventas y logística, en una sola plataforma.

OLAP**:** siglas de *Online Analytical Processing*. es un tipo de sistema que se utiliza para analizar grandes conjuntos de datos y proporcionar información valiosa para la toma de decisiones empresariales.
OLTP**:** siglas de *Online Transaction Processing*. es un tipo de sistema transaccional que procesa transacciones en tiempo real, como las compras en línea.

TPS**:** siglas de *Transaction Processing System*. es un sistema que procesa transacciones comerciales, como compras en línea o transferencias bancarias.

VECTORES DE ATAQUE.

BACKDOOR: es una puerta trasera o acceso secreto a un sistema o red que permite a los atacantes ingresar sin ser detectados.

DDOS**:** Siglas de Denegación de Servicio Distribuido. Es un ataque en el que se utiliza una red de dispositivos infectados para enviar tráfico a un servidor o sitio web, lo que provoca la caída del servicio.

*MALWARE**:*** es un *software* malicioso que se utiliza para infectar dispositivos y robar información, dañar archivos o tomar el control del dispositivo.

*MAN-IN-THE-MIDDLE***:** es un ataque en el que un atacante intercepta la comunicación entre dos partes y se hace pasar por ambas para obtener información confidencial.

*PHISHING**:*** es una técnica de ingeniería social que utiliza correos electrónicos o sitios web falsos para engañar a los usuarios y hacer que proporcionen información confidencial, como contraseñas o información financiera.

*RANSOMWARE***:** es un tipo de *malware* que cifra los archivos del dispositivo y exige un rescate para desbloquearlos.

*ZERO-DAY***:** es un *exploit* o vulnerabilidad de seguridad que aún no ha sido descubierto o solucionado por el desarrollador del *software*.

RESUMEN

La seguridad de los sistemas transaccionales es vital en el mundo empresarial, ya que los ciberataques causan pérdidas financieras y robo de información; los vectores son empleados para explotar vulnerabilidades y acceder a información confidencial; aunque existen medidas de seguridad los ataques son frecuentes y sofisticados, por lo que es necesario analizar los vectores de ataque más comunes para mitigar los riesgos.

Para ello, se realizará una revisión de literatura científica y técnica para identificar los tipos de ataques y vulnerabilidades que afectan a los sistemas y las técnicas de seguridad utilizadas para prevenir y mitigar estos riesgos; la revisión se enfocará en los vectores de ataque más comunes, como la fuerza bruta, inyección de código, denegación de servicio, *phishing, malware* y otros, también se analizarán las medidas de seguridad que se pueden implementar, como la autenticación multifactor, la encriptación de datos y la monitorización de la actividad de los usuarios.

También se abordará el rol de los usuarios en la seguridad y las medidas prácticas que pueden tomar para proteger sus datos personales y financieros, esto incluirá el uso de contraseñas seguras, la verificación de la autenticidad de los sitios web y la actualización regular del *software* de seguridad.

Como resultado de la compilación de información que busca maximizar la seguridad en los sistemas transaccionales se formulas las conclusiones del ejercicio de la revisión bibliográfica existente y se proponen las recomendaciones para los usuarios de este tipo de sistemas y para los lectores del documento; como conclusiones preliminares se establece que los sistemas transaccionales presentan diferentes niveles de vulnerabilidad frente a la presencia de los vectores

de ataque, si bien es cierto que los equipos de ciberseguridad implementan planes de prevención, contención y mitigación en las empresas, los ciberdelincuentes implementan ataques más sofisticados logrando vulnerar los sistemas. De igual forma se plantean recomendaciones preliminares enfocadas hacia el reconocimiento de las debilidades de los sistemas y de la presencia de vectores que pueden materializar un ataque a la seguridad informática de los sistemas transaccionales

Sistema transaccional, sistema informático, vector de ataque, vulnerabilidades, amenazas, *hacker*, DDOS, *phishing*, factor humano.

ABSTRACT

The security of transactional systems is vital in the business world, as cyber-attacks cause financial losses and information theft. Attack vectors are employed to exploit vulnerabilities and access confidential information. Although security measures exist, attacks remain frequent and sophisticated, making it necessary to analyze the most common attack vectors to mitigate risks.

To this end, a review of scientific and technical literature will be conducted to identify the types of attacks and vulnerabilities that affect systems and the security techniques used to prevent and mitigate these risks. The review will focus on the most common attack vectors, such as brute force, code injection, denial of service, phishing, malware, and others. Additionally, security measures like multifactor authentication, data encryption, and user activity monitoring will be analyzed.

The role of users in security and practical measures they can take to protect their personal and financial data will also be addressed. This will include the use of secure passwords, verification of website authenticity, and regular updates of security software.

As a result of the compilation of information aimed at maximizing the security of transactional systems, conclusions will be drawn from the review of existing literature, and recommendations will be proposed for users of such systems and the readers of this document. Preliminary conclusions establish that transactional systems present different levels of vulnerability to attack vectors. While cybersecurity teams implement prevention, containment, and mitigation plans in companies, cybercriminals carry out more sophisticated attacks that manage to breach these systems. Similarly, preliminary recommendations will be made, focusing on recognizing the weaknesses of systems and the presence of vectors that could materialize an attack on the cybersecurity of transactional systems.

INTRODUCCIÓN

La monografía maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques, se enfoca en la revisión sistemática, el análisis de documentos especializados y la literatura existente que abordan el tema de las amenazas o vulnerabilidades, que afectan a los sistemas informáticos, para este caso a los sistemas transaccionales.

Para abordar el tema de estudio, se contextualiza y se define la pregunta problema que será resuelta al final de la construcción del documento; de igual forma se realiza la formulación de los objetivos los cuales generan la ruta de desarrollo de la propuesta.

Cuando se habla de maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques, es necesario incorporar y aprehender las teorías existentes sobre el caso de estudio, que sirven de soporte para entender todas las afectaciones que sufren este tipo de sistemas. Como lo afirma Malik y Tosh[1] es importante la implementación de acciones que permitan evaluar y mitigar los efectos negativos de los ciberataques al interior de las organizaciones para reducir los resultados negativos en los activos de las empresas.

También es importante aclarar conceptos y definiciones de tópicos y términos fundamentales para el desarrollo de la monografía, esto se evidencia en la construcción del marco conceptual; otro aspecto relacionado con el desarrollo del trabajo es la revisión de casos históricos donde se evidencia que los sistemas transaccionales han sido vulnerados mediante la implementación de algún tipo de ataque, así como también se debe comparar con el estado actual en donde los ataques y vulneración de este tipo de sistemas es permanente bajo las mismas técnicas de penetración pero con un valor agregado que es la sofisticación de cada técnica y el uso avanzado de *software* y herramientas digitales.

Para el análisis de la problemática propuesta se construye un marco metodológico en donde se elige un tipo de investigación de carácter exploratoria descriptiva cualitativa con un enfoque cualitativo, en donde se implementa una metodología basada en la revisión documental y el análisis de la información recopilada con el fin de generar al finalizar el proceso propuestas para mitigar los efectos en caso de un posible incidente.

[1] A. A. Malik and D. K. Tosh, "Towards Developing a Scalable Cyber Risk Assessment and Mitigation Framework," *2024 IEEE International Systems Conference (SysCon)*, Montreal, QC, Canada, 2024, pp. 1-8, doi: 10.1109/SysCon61195.2024.10553535.

También, es necesario esbozar la problemática y temas a desarrollar en la presente monografía, de este modo se define como problema de estudio la necesidad de maximizar factores de seguridad para proteger los sistemas transaccionales de posibles ciberataques o en su defecto de implementar técnicas y herramientas para reducir y mitigar el impacto al interior de los sistemas transaccionales.

Teniendo en cuenta la temática sugerida en el desarrollo del documento, se destaca el estudio de los vectores de ataque típicos en los sistemas transaccionales teniendo en cuenta lo expresado en Byte TI[2], se debe reconocer que el uso del correo electrónico es uno de los principales vectores por medio del cual se materializa un ciberataque.

De igual manera, se aborda diferentes tipos de vectores que afectan los sistemas actuales, se trata de explicar cómo el *malware* es empleado para vulnerar los sistemas, así mismo, se identifica el *Phising* como el vector principal para materializar un ataque a un sistema, también se relaciona el estudio de los sistemas transaccionales, sus características y componentes y se describe la forma como se han vulnerado algunos sistemas en Colombia.

[2] TI, Redacción Byte. 2021. «Correo electrónico: principal vector de entrada de malware». 8 de febrero de 2021. https://revistabyte.es/ciberseguridad/el-correo-electronico-malware/.

1 DEFINICIÓN DEL PROBLEMA

En la actualidad la economía al igual que la tecnología está en constante evolución, la implementación de herramientas y sistemas tecnológicos ha sido una necesidad en el campo económico con el fin de convertir el sistema empresarial en un sistema competitivo, confiable y de fácil acceso, de este modo cobra relevancia los denominados sistemas transaccionales que automatizan los procesos para beneficiar a empresarios y clientes.

La economía y las finanzas digitales, según lo expresado por (ASOBANCARIA, 2022)[3] incluyen el uso de monedas y activos digitales para la comercialización y prestación de servicios, en este sentido el intercambio de un producto se efectúa mediante el uso de una aplicación o plataforma informática con el fin de facilitar el acceso al usuario; en esta era digital cobra relevancia el concepto de ciberseguridad debido a que los procesos que se involucran deben garantizar la seguridad tanto para el propietario de la empresa como para el usuario, citando a (YOUNIS & ALWAN, 2021)[4] quienes afirman que los avances tecnológicos han cambiado la forma de proveer y ofertar un producto o servicio, esta nueva forma incluye las transacciones electrónicas a través de la implementación de un sistema transaccional que garantice confiabilidad y seguridad en los procesos; pero los mismos autores relacionan en su artículo que dichos sistemas han sido vulnerables al robo de información y activos digitales, el correo electrónico y las transacciones electrónicas son vulnerables a ciberataques, por tanto es necesario maximizar los factores de seguridad en los sistemas transaccionales que permitan mitigar los riesgos de ciberataques

1.1 ANTECEDENTES DEL PROBLEMA

Las actividades humanas y en especial las económicas y comerciales han evolucionado buscando el mejoramiento continuo para alcanzar factores de eficiencia; en el campo empresarial, es importante que las organizaciones también implementen políticas y acciones tendientes a optimizar los procesos mediante la gestión de los procesos de negocios, de esta manera las empresas incorporan

[3] ASOBANCARIA. (2022). *La reinvencion financiera en la era digital 2022* (primera edición ed.). Recuperado el 28 de julio de 2024, de https://asobancaria.com/wp-content/uploads/La_reinvencion_financiera_en_la_era_digital-2022.pdf

[4] YOUNIS, M., & ALWAN, A. (2021). Design and Implementation of an IoT-based TransactionalSystem forQuality Management. *Iraqi Journal of Science*. doi:0.24996/ijs.2021.62.2.30

sistemas que le permiten automatizar procesos en beneficio de sus clientes, trabajadores y propietarios. (JIMÉNEZ, 2020)[5]

El sector financiero y comercial en su afán de innovar y enfrentar los desafíos de una evolución constante han incursionado en la constitución de sistemas transaccionales, Según Alegsa (2023), en su portal web define que ***"Un sistema transaccional es un tipo de sistema de información diseñado para recolectar, almacenar, modificar y recuperar todo tipo de información que es generada por las transacciones en una organización",*** (Diccionario de Informática y Tecnología, 2012)[6], retomando el texto citado, se puede intuir que los sistemas transaccionales almacenan y manipulan información que incluyen dentro de su estructura de hardware y *software*." En la parte lógica, se puede inferir la presencia de un sistema de almacenamiento, procesamiento y de entrada y salida de datos; otros autores como Coppola (2019)[7], retoman el concepto como un sistema que integra el *frontend* que permite la interacción de los usuarios y el *backend* que incorpora sistemas de procesamiento y la base de datos, que permite el almacenamiento de los datos.

Los sistemas transaccionales se han implementado en las empresas para optimizar procesos, como ejemplos se mencionan: un sitio web que permita realizar pagos a los usuarios, un sitio web de comercio electrónico o un simple cajero automático, son ejemplos de este tipo de sistemas.

Ahora bien, para garantizar que los sistemas cumplan los objetivos para lo cual fueron creados es necesario implementar factores de seguridad; en este caso la seguridad de los sistemas transaccionales es un tema crucial en el entorno empresarial actual para evitar pérdidas financieras, fugas de información y fraudes en los procesos de compra y venta, debido a que estos sistemas son fundamentales para la realización de transacciones financieras y comerciales en

---

[5] JIMÉNEZ FARFÁN, Junior A. "La Implementación de un sistema automatizado reduce los tiempos de atención en los procesos aplicables a la ventanilla única de turismo en la Municipalidad Provincial del Callao"**. Revista de Investigación Industrial Data {En línea}**. Vol. 23, No. 2. 2020. Universidad Nacional Mayor de San Marcos. {8 Mayo de 2023}. Disponible en: (https://revistasinvestigacion.unmsm.edu.pe/index.php/idata/article/view/15566) , (https://www.redalyc.org/journal/816/81665362003/html/) , (https://www.researchgate.net/publication/348320714_La_implementacion_de_un_sistema_automatizado_reduce_los_tiempos_de_atencion_en_los_procesos_aplicables_a_la_ventanilla_unica_de_turismo_en_la_Municipalidad_Provincial_del_Callao)

[6] ALEGSA, Leandro. "Definición de sistema transaccional (sistema de procesamiento de transacciones)". **{En línea}**. {9 Mayo de 2023}. Disponible en: https://www.alegsa.com.ar/Dic/sistema_transaccional.php#gsc.tab=0.

[7] COPPOLA, María. "Frontend y backend: qué son, en qué se diferencian y ejemplos". **{En línea}**. {9 Mayo de 2023}. Disponible en:(https://blog.hubspot.es/website/frontend-y-backend)

línea y por consiguiente se deben identificar los vectores de ataque que los afectan. Sabiendo que los vectores de ataque, como se menciona en el portal web *CloudFlare*[8]*,* son métodos utilizados por los ciberdelincuentes para explotar vulnerabilidades en este tipo de sistemas y obtener acceso no autorizado.

A pesar de que existen medidas de seguridad implementadas en los sistemas transaccionales, los ataques son frecuentes y más sofisticados; buscan explotar debilidades para acceder a información confidencial o realizar actividades maliciosas. Por ello, surge la necesidad de revisar la literatura existente para identificar los vectores de ataque más comunes y cómo se pueden mitigar estos riesgos.

A pesar de las medidas de seguridad que se implementan en los sistemas transaccionales, todavía existen riesgos y vulnerabilidades que pueden ser explotadas por los ciberatacantes. Por lo tanto, se debe identificar los ciberataques típicos, pero lo más relevante es realizar un análisis de los vectores de ataque más comunes que enfrentan estos sistemas y evaluar las medidas de seguridad que se pueden tomar para mitigar riesgos y proteger los datos confidenciales de la organización y de los usuarios.

Para lograr lo planteado, se utilizará una metodología de investigación basada en la revisión de literatura científica y técnica relevante en el campo de la seguridad de los sistemas transaccionales y los vectores de ataque; se recopilarán y analizarán estudios y artículos de investigación que aborden los diferentes tipos de ataques y vulnerabilidades que afectan a los sistemas transaccionales, así como las técnicas y medidas de seguridad utilizadas para prevenir y mitigar estos riesgos.

Se incluirá una revisión detallada de los vectores de ataque más comunes en los sistemas transaccionales, que incluyen ataques de fuerza bruta, inyección de código, ataques de denegación de servicio, *phishing*, *malware* y otros. La monografía también analizará cómo estos vectores pueden ser utilizados para comprometer la seguridad de los sistemas transaccionales y las consecuencias que pueden tener para las empresas y los usuarios.

Además, se enfocará en las medidas de seguridad que se pueden implementar para mitigar los riesgos de la materialización de un vector de ataque en este tipo de sistemas. Para ello se incluirá la revisión de técnicas y mejores prácticas para el diseño y la implementación, como la autenticación multifactor, la encriptación de datos y la monitorización de la actividad de los usuarios.

[8] ¿Qué es un vector de ataque? | *Cloudflare*. **{En línea}**. {9 Mayo de 2023}. Disponible en: (https://www.cloudflare.com/es-es/learning/security/glossary/attack-vector/)

Finalmente, se abordará el papel de los usuarios en la seguridad y cómo pueden protegerse contra los vectores de ataque, se analizarán medidas prácticas que los usuarios pueden tomar para proteger sus datos personales y financieros, como el uso de contraseñas seguras, la verificación de la autenticidad de los sitios web y la actualización regular del *software* de seguridad.

1.2 FORMULACIÓN DEL PROBLEMA

A raíz de los antecedentes y planteamiento general del problema es pertinente plantearse el siguiente interrogante que guía el proceso de revisión bibliográfica

¿Cómo maximizar los factores de seguridad en los sistemas transaccionales que permitan mitigar los riesgos de ciberataques a través de la revisión de masas documentales y la implementación de un enfoque integral de análisis, evaluación de vulnerabilidades y recomendaciones para organizaciones y usuarios?

2 JUSTIFICACIÓN

La seguridad de la información, según lo afirma (OSPINA Y SANABRIA,2023)[9] es un tema crítico en la era digital, las personas y organizaciones dependen cada vez más de las tecnologías de la información para realizar sus actividades, razón por la cual es necesario garantizar la seguridad de la información. Sin embargo, las brechas de seguridad en las infraestructuras de tecnologías de la información generadas por la ejecución exitosa de vectores de ataque, continúan siendo un problema recurrente.

A manera de justificación del problema acerca de los vectores de ataque en los sistemas transaccionales es necesario tener claro que estos buscan explotar vulnerabilidades en la seguridad de la información para obtener acceso no autorizado a los datos confidenciales del usuario, como información personal, financiera o de identificación. En este orden de ideas se hace necesario visibilizar los factores que generan el problema.

Por ello los vectores de ataque pueden incluir la Ingeniería social, donde los atacantes pueden utilizar técnicas para engañar a los usuarios y obtener acceso a sus credenciales de inicio de sesión o información personal; los ataques de fuerza bruta, donde los atacantes pueden intentar adivinar contraseñas mediante la utilización de herramientas automatizadas que prueban diferentes combinaciones de contraseñas hasta que encuentran la correcta, de igual forma, los ataques de inyección SQL donde los atacantes utilizan código malicioso para obtener acceso a la base de datos del sistema transaccional mediante la introducción de comandos SQL maliciosos en formularios *web* o enlaces.

Así como se justifica el trabajo realizando una identificación de los vectores de ataque de igual modo es necesario exponer las alternativas para mitigar estos riesgos, de allí que es importante implementar medidas de seguridad sólidas en el sistema transaccional como la educación del usuario, donde pueda identificar los riesgos de la ingeniería social y la importancia de utilizar contraseñas seguras y únicas para cada cuenta; la implementación de medidas de seguridad en el lado del servidor que se constituye como medidas de seguridad adicionales, como *firewalls* y detección de intrusos, para proteger la base de datos del sistema transaccional; la utilización de encriptación de datos que permite agregar niveles de seguridad a los datos para proteger la información confidencial del usuario durante el almacenamiento y la transmisión; la actualización regular del *software*,

[9] OSPINA, M y SANABRIA, P. “Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia”. **{En línea}**. {9 Mayo de 2023}. Disponible en: (http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S1794-31082020000200199&lng=en&nrm=iso&tlng=es)

ayuda a corregir vulnerabilidades conocidas y asegurar que el sistema esté protegido contra amenazas recientes. El uso de herramientas de seguridad automatizadas, como antivirus, detección de intrusiones, constituyen otra capa de seguridad para monitorear y detectar posibles amenazas en tiempo real.

En resumen, la justificación para el problema de la maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques radica en el riesgo que representan para la seguridad de la información del usuario y los datos confidenciales. Para mitigar estos riesgos, es necesario implementar medidas de seguridad sólidas, como la educación del usuario, la encriptación de datos, la actualización regular del *software* y el uso de herramientas de seguridad automatizadas.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Maximizar los factores de seguridad en los sistemas transaccionales y mitigar los riesgos de ciberataques a través de la revisión sistemática de literatura y la implementación de un enfoque integral de análisis, evaluación de vulnerabilidades y recomendaciones para organizaciones y usuarios

3.2 OBJETIVOS ESPECÍFICOS

- Desarrollar un estado del arte de los vectores de ataque prevalentes que comprometen la seguridad de los sistemas transaccionales por medio del análisis de casos documentados de sistemas vulnerados estableciendo características y nivel de impacto.

- Evaluar las vulnerabilidades en los sistemas transaccionales mediante la aplicación de la metodología del ciclo de Evaluación de Vulnerabilidades y la puntuación de los CVSS para que organizaciones y usuarios implementen medidas de seguridad para minimizar los riesgos.

- Elaborar recomendaciones para las empresas que emplean sistemas transaccionales con el fin de que implementen factores de seguridad que permitan prevenir los ciberataques mediante la materialización de los vectores.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Para abordar la temática referente a la maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques se hace necesario revisar diferentes teorías o postulados existentes en acerca de los vectores de ataque, teniendo en cuenta diferentes fuentes bibliográficas se pueden mencionar la teoría del riesgo, teoría del ataque distribuido, teoría de la puerta trasera, teoría de la ingeniería social y teoría del mal funcionamiento humano.

En el ámbito específico de los vectores de ataque que asociados con los sistemas transaccionales se determinan teorías generales como la teoría del ataque por fuerza bruta, teoría del ataque de *phishing*, del ataque de inyección de código SQL, la teoría de la denegación de servicios

A continuación, se describe cada una de las teorías relacionadas con la afectación que han tenido los sistemas transaccionales.

4.1.1 La teoría del riesgo. Es una rama de la matemática aplicada que se dedica a estudiar la toma de decisiones en situaciones donde existe incertidumbre y se enfrentan consecuencias potencialmente desfavorables. Según Kourouxous & Bauer (2019)10, quienes afirman que la teoría del riesgo surgió en la segunda mitad del siglo XX, y ha sido aplicada en campos como la economía y las finanzas para ayudar a los inversores a tomar decisiones informadas.

Uno de los fundamentos de la teoría del riesgo es el concepto de esperanza matemática, que indica el valor medio de los posibles resultados de una acción. Según Kahneman y Tversky (2000)[11], la toma de decisiones en situaciones de riesgo está influenciada por dos factores: el nivel de riesgo y la forma en que se presentan las opciones. En su artículo, los autores proponen el modelo de perspectiva, que explica cómo las personas toman decisiones al evaluar los resultados en relación con un punto de referencia y cómo la presentación de las opciones influye en sus elecciones.

---

[10] KOUROUXOUS, Thomas y BAUER, Thomas. “Violations of dominance in decision-making”**. Business Research {En línea}**. Vol. 12, No. 1, p. 209–239. 2019. DOI 10.1007/s40685-019-0093-7. {9 Mayo de 2023}. Disponible en: (https://doi.org/10.1007/s40685-019-0093-7)

[11] KAHNEMAN, Daniel y TVERSKY, Amos. “Choices, values, and frames”. Cambridge University Press: New York, NY, US, 2000. Choices, values, and frames. ISBN 978-0-521-62172-4.

Otro elemento importante de la teoría del riesgo es la utilización de medidas de riesgo, como la desviación estándar y el coeficiente de variación, para cuantificar la variabilidad de los resultados posibles. Según Markowitz[12] la diversificación de la cartera de inversiones es una estrategia efectiva para reducir el riesgo y maximizar el rendimiento potencial. El autor señala que, al combinar activos con diferentes riesgos, los inversores pueden crear una cartera que tenga un nivel de riesgo adecuado para sus objetivos y tolerancia al riesgo.

4.1.2 Teoría del ataque distribuido. Es una estrategia en la que un gran número de sistemas independientes atacan simultáneamente un objetivo en particular. Esta técnica se utiliza a menudo en los ataques cibernéticos para sobrecargar y comprometer un sistema específico. Según Andreasen y Yenkinson (2021), quienes afirman textualmente que "un ataque distribuido es una técnica de ataque en la que se coordinan varios puntos de ataque para desplegar una serie de compromisos de dispositivos remotos, buscando así dañar o controlar los recursos del objetivo"13; según el texto citado, para la ejecución de este tipo ataque se requiere de la intervención de varias máquinas desde diferentes puntos de acceso dirigido hacia un mismo objetivo con el fin de sobrecargar el sistema atacado.

Los ataques distribuidos pueden ser difíciles de detectar y pueden tener consecuencias graves en el objetivo, como la pérdida de datos críticos, la interrupción de servicios en línea y la exposición a violaciones de seguridad. Según Mishra y Gupta (2016), ***"la complejidad de estos ataques puede ser muy alta debido a las características de su estructura distribuida, lo que dificulta la detección y la defensa"***[14].

Finalizando se afirma que, la teoría del ataque distribuido es una técnica de ataque común utilizada en el mundo cibernético para causar daño y comprometer los sistemas de un objetivo. Es importante que las empresas y los individuos implementen medidas de seguridad, sólidas y efectivas para prevenir y defenderse de este tipo de ataques.

[12] MARKOWITZ, Harry M. Portfolio Selection: Efficient Diversification of Investments, 2nd Edition.

[13] ANDREASEN, J. y YENKINSON, C. “Understanding Denial-of-Service Attacks | CISA.” **{En línea}**. 2021. {8 Mayo de 2023}. Disponible en: (https://www.cisa.gov/news-events/news/understanding-denial-service-attacks)

[14] MISHRA, R. & GUPTA, N. K. (2016). “Literature Review: Detection of Distributed Denial of Service Attack”. **International Journal of Computer Science and Mobile Computing**. p. 5(6), 38-43.

4.1.3 Teoría del ataque de puerta trasera. Es una preocupación constante en el mundo de la seguridad informática. Según la definición de Poddebniak y Zalewski (1999), se trata de ***"una puerta de entrada secreta, por lo general creada por el autor del software original, para permitir el acceso al sistema sin la necesidad de una autenticación convencional"***[15]. La presencia de una puerta trasera significa que un atacante podría acceder al sistema sin ser detectado, lo que lo convierte en un objetivo potencial para los ciberdelincuentes.

En su trabajo sobre la seguridad en la era de la información, Stallings (2014), señala que ***"la creación de puertas traseras en dispositivos electrónicos o software es una práctica arriesgada que puede ser explotada por atacantes malintencionados"***[16]. De acuerdo con la expresión citada es necesario que en términos de programación se implementen las "buenas prácticas" con el fin de garantizar la seguridad; y en términos de producción de dispositivos finales es necesario la aplicación de normas que garanticen la seguridad evitando la presencia de puertas traseras o dispositivos que atenten contra la privacidad de los usuarios finales.

Otro ejemplo de la importancia de la teoría del ataque de puerta trasera, es el caso de la empresa de seguridad informática RSA, que en 2011 fue objeto de un ataque por parte del grupo de *hackers* conocido como *"Shadow Brokers*". Según información de la propia RSA, los *hackers* utilizaron una "vulnerabilidad en una versión antigua de *Adobe Flash*" para infiltrarse en el sistema e instalar una puerta trasera. (RSA, 2017)[17]. Este ataque se llevó a cabo con el objetivo de obtener información confidencial, lo que puso de manifiesto la necesidad de tener medidas de seguridad y prevención de este tipo de vulnerabilidades.

Por último, la teoría del ataque de puerta trasera es una preocupación de vital importancia para garantizar la seguridad en el mundo de la informática y tecnología, es importante que los fabricantes y desarrolladores de *software* tomen medidas de seguridad adecuadas para evitar la creación de puertas traseras que puedan ser explotadas por los ciberdelincuentes.

---

[15] PODDEBNIAK, D. y ZALEWSKI, M. "Back doors vs. front doors: Attacks and defenses in modern operating systems". (1999). Recuperado de: (http://phrack.org/issues.html?issue=54&id=8)

[16] STALLINGS, W. Seguridad en la era de la información. México: Pearson, 2014.

[17] RSA. "How the RSA breach happened". **{En línea}**. 2017. Recuperado de https://www.rsa.com/en-us/company/newsroom/company-news/how-the-rsa-breach-happened

4.1.4 Teoría de la ingeniería social. En esta teoría se propone y se ejecuta la estrategia de cómo influir en el comportamiento humano con el objetivo de obtener algún beneficio. Según Lazar, Feng y Hochheiser (2015), "la ingeniería social implica usar la persuasión y la manipulación para cambiar o influir en el comportamiento, actitudes o percepciones de las personas"18. Esta teoría se utiliza muchas veces en contextos de seguridad informática para engañar a los usuarios para que proporcionen información privada o hagan clic en enlaces maliciosos.

Algunos de los principales exponentes de esta teoría son Kevin Mitnick y William Simon, quienes afirman en su libro "*The Art of Deception*" que ***"la ingeniería social es la técnica más efectiva para la penetración de redes y sistemas"***. En este libro, Mitnick y Simon (2002),[19] explican varias técnicas que utilizan para obtener información de sus objetivos, como el uso de pretextos o la suplantación de identidad.

Otro autor que ha contribuido al desarrollo de esta teoría es Christopher Hadnagy, quien escribió el libro "*Social Engineering*: *The Art of Human Hacking*". Hadnagy (2018), define la ingeniería social como ***"el arte y la ciencia de manipular a las personas para que tomen acciones específicas que pueden no ser en su interés"***[20].

También proporciona varios ejemplos de cómo los ingenieros sociales han utilizado técnicas de persuasión para obtener información valiosa de las empresas; es necesario tener en claro que, la teoría de la ingeniería social propone utilizar técnicas de persuasión y manipulación para influir en el comportamiento humano y obtener algún beneficio. Los autores Kevin Mitnick y Christopher Hadnagy han sido importantes exponentes de esta teoría, ofreciendo técnicas y ejemplos para su implementación.

[18] LAZAR, J., FENG, J. H., y HOCHHEISER, H. Research methods in human-computer interaction. Elsevier. 2015

[19] MITNICK, K. D., y SIMON, W. L. The Art of Deception: Controlling the Human Element of Security. Wiley. 2002.

[20] HADNAGY, C. Social Engineering: The Art of Human Hacking. Wiley. 2018.

4.1.5 Teoría del mal funcionamiento humano. Esta teoría presenta una perspectiva que considera que la conducta desviada es una respuesta adaptativa del individuo que enfrenta dificultades en su entorno. (Greene, Oliver y Brodie, 2008).[21] También, sostiene que los comportamientos criminales son producto de una disfunción social, emocional o psicológica, en lugar de ser resultado de una elección racional (Walsh y Ellis, 2007)[22].

En el ámbito de la criminología, ha sido un enfoque ampliamente estudiado durante décadas. Puede ser encontrado en numerosas investigaciones de delitos violentos, donde se ha demostrado que la disfunción social, la adicción y otros trastornos psicológicos son comunes en individuos que han cometido crímenes violentos (Babcock, Green y Robie, 2004)[23].

La teoría también se ha aplicado al análisis de los comportamientos éticos y morales en el entorno empresarial, al identificar los factores que influyen en la ética laboral, varios estudios han demostrado que la disfunción psicológica, el abuso de sustancias y la pobreza pueden afectar negativamente el discernimiento para la toma de decisiones éticas en el lugar de trabajo (Aguinis y Glavas, 2020).[24]

Por último, la teoría del mal funcionamiento humano señala la importancia de considerar los factores sociales y psicológicos en la evaluación de la conducta y la toma de decisiones. Al entender que los comportamientos disfuncionales son una respuesta adaptativa a circunstancias adversas, se pueden desarrollar estrategias para abordar los factores subyacentes a través de la intervención temprana y la terapia.

4.2 MARCO CONCEPTUAL

Para abordar el problema planteado referente a la maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques se definen términos y expresiones claves que permiten comprender el propósito de la monografía

---

[21] GREENE, J., OLIVER, J. E., & BRODIE, N. “The opinion-policy nexus in a representative democracy”. **Journal of Politics**, 2008. p. 70(3), 717-736.

[22] WALSH, A., & ELLIS, L. “Criminology: An interdisciplinary approach”. Thousand Oaks, CA: **SAGE Publications**. 2007.

[23] BABCOCK, J. C., GREEN, C. E., & ROBIE, C. “Does batterers' treatment work? A meta-analytic review of domestic violence treatment”. **Clinical Psychology Review**, 2004. P. 23(8), 1023-1053.

[24] AGUINIS, H., & GLAVAS, A. “What We Know and Don't Know About Corporate Social Responsibility”. **Journal of Management**, 2020. P. 46(4), 1454-1488.

4.2.1 Sistema transaccional. Un sistema transaccional es un conjunto de procesos y herramientas que permiten la gestión electrónica de transacciones comerciales, financieras y administrativas entre dos o más entidades.

Estos sistemas no solo realizan la transacción en sí, sino también todas las actividades complementarias necesarias para su correcto registro contable, seguimiento y control. Según Liu (2017),[25] los sistemas transaccionales son esenciales en la actualidad para asegurar la eficiencia y eficacia en cualquier proceso transaccional. Debido a la creciente demanda de transacciones en línea y la necesidad de procesos más automatizados y seguros, estos sistemas se han convertido en una herramienta fundamental para las empresas y organizaciones. Así mismo, el sistema transaccional proporciona ventajas como la reducción de costos y tiempos de transacción, la automatización de procesos, la minimización de errores y la mejora en la calidad de la información. Todo esto, a su vez, contribuye a la mejora de los procesos de negocio de las organizaciones y al aumento de la competitividad.

Por último, los sistemas transaccionales son una herramienta imprescindible en la gestión electrónica de transacciones comerciales, financieras y administrativas. Su uso adecuado permite a las organizaciones mejorar la eficiencia, eficacia y competitividad en los procesos de negocio

4.2.2 Ciberseguridad. Se define como un conjunto de medidas, procedimientos y técnicas que tienen como objetivo proteger la información y los sistemas informáticos de posibles ataques malintencionados, fraudes electrónicos, robo de datos y otras amenazas cibernéticas. Según el INSTITUTO NACIONAL DE CIBERSEGURIDAD la ciberseguridad se define como ***"el conjunto de procesos, tecnologías y prácticas diseñadas para proteger redes, dispositivos, programas y datos de ataques, daños y accesos no autorizados"***[26]. En este sentido la ciberseguridad se ha convertido en un tema cada vez más importante en la era digital en la que vivimos, En la actualidad, millones de personas utilizan diariamente internet para realizar diversas tareas, tales como realizar compras en línea, enviar correos electrónicos, utilizar aplicaciones móviles, entre otras actividades que implican la transmisión y el almacenamiento de información personal y confidencial, Es por ello que, es necesario contar con medidas de seguridad adecuadas para proteger los datos personales de las personas, así como los sistemas informáticos que los albergan.

---

[25] LIU, Zhiyong. Proximal Operator Splitting for Multi-Constraint Dictionary Learning**. International Journal of Hybrid Information Technology {online}**. Vol. 10, No. 2, 2017. p. 107–116. DOI 10.14257/ijhit.2017.10.2.11. {9 Mayo de 2023}. Disponible en: (http://gvpress.com/journals/IJHIT/vol10_no2/11.pdf)

[26] Glosario de términos de ciberseguridad, una guía de aproximación para el empresario**.**

Según Warkentin, Herath y Rao (2020),[27] la ciberseguridad es una preocupación común tanto para las empresas como para los ciudadanos. Por lo que es fundamental la implementación de políticas y regulaciones que fomenten la protección de la información y la privacidad de las personas. También es importante tener en cuenta que la ciberseguridad es un tema en constante cambio, pues cada día surgen nuevas amenazas y es necesario actualizar constantemente las medidas de seguridad para resguardar la información.

Consolidando el concepto se define la ciberseguridad como el conjunto de medidas y prácticas que tienen como objetivo proteger la información y los sistemas informáticos de posibles amenazas cibernéticas. Es fundamental contar con medidas de seguridad adecuadas para garantizar la privacidad y protección de los datos personales de las personas y los sistemas informáticos. Por lo que, se recomienda la constante actualización y la implementación de políticas y regulaciones adecuadas para fomentar la protección cibernética.

4.2.3 Vector de ataque. Se refiere a la forma en que un atacante busca y explota las vulnerabilidades de un sistema informático con el fin de comprometerlo y obtener acceso no autorizado a información confidencial o realizar acciones maliciosas. Según Shacklett (2021),[28] un vector de ataque puede ser una técnica específica, como un correo electrónico de *phishing* o un *exploit* de *software*, el vector de ataque puede ser utilizado por un atacante para identificar y explotar una cadena de vulnerabilidades interconectadas en un sistema, como lo describe Shabtai et al. (2014) en su estudio sobre ataques de cadena en sistemas de control industrial.

Es importante prestar atención a los vectores de ataque utilizados por los atacantes, ya que pueden proporcionar información valiosa que ayuda a los defensores a mejorar su postura de seguridad. Como menciona SANS INSTITUTE (2021), "la identificación y la comprensión de los vectores de ataque ayudan a los analistas de seguridad a desarrollar estrategias de mitigación más efectivas".[29]

Concluyendo la definición, el vector de ataque es una técnica específica que está ligada directamente a las acciones que debe seguir un atacante para lograr explotar una vulnerabilidad con el fin de comprometer un sistema informático. Al comprender el funcionamiento y comportamiento de los vectores de ataque, se

---

[27] WARKENTIN, M., HERATH, T., y RAO, H.R. Business Data Ethics and Cybersecurity. 2020. Springer

[28]SHACKLETT, E. M. “Attack vector”. **TechTarget**. 2021. Recuperado de: (https://searchsecurity.techtarget.com/definition/attack-vector)

[29] Security Awareness Report | SANS Security Awareness. {online}. 2021 {9 Mayo de 2023}. Disponible en: (https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/)

pueden desarrollar estrategias de mitigación efectivas para protegerse contra los mismos.

4.2.4 Hacker. El término hacker es un concepto que ha sido objeto de diversas interpretaciones. Según Raymond los hackers son "aquellos que gozan explorando los detalles de los sistemas programáticos y extender sus habilidades técnicas más allá de lo que podrían hacer en un entorno impuesto"[30]. Esta definición se enfoca en la curiosidad y el deseo de alcanzar un mayor conocimiento técnico.

Por otro lado, Levy (2010), define a los *hackers* como "guerreros de la información que luchan por la libertad del flujo de información y contra aquellos que buscan controlarla"[31]. Esta definición se enfoca en el lado social y político de la cultura hacker.

Sintetizando, el término hacker se refiere a una persona con habilidades técnicas avanzadas y una fuerte curiosidad por explorar y extender sus límites en el mundo de la tecnología y la información. Además, hay una gran importancia en la libertad y el flujo de información en la cultura hacker.

4.2.5 Malware. Es un término acuñado para referirse a cualquier tipo de *software* malicioso diseñado para infiltrarse en sistemas informáticos con el propósito de dañarlos o robar información. Según la Asociación para la Tecnología de la Información de América (ITAA por sus siglas en inglés), el *malware* es "cualquier programa de *software* desarrollado con intención maliciosa para dañar, alterar o tomar control de un sistema de información" (ITAA, 2004).

Existen varios tipos de *malware*, entre ellos los virus, gusanos, troyanos, *spyware* y *adware*. Estos programas maliciosos pueden causar daños que van desde la destrucción de archivos hasta el robo de información confidencial. Según el informe "*The State of Malware* 2020" de *Malwarebytes Labs*, el *malware* sigue siendo una amenaza importante para los usuarios de computadoras, especialmente debido a la creciente sofisticación de las técnicas utilizadas por los ciberdelincuentes (*Malwarebytes Labs*, 2020).

La protección contra el *malware* es una prioridad para los usuarios de la tecnología. La instalación de programas antivirus, la actualización del *software* y el

[30] RAYMOND, Eric S. “Cómo ser un hacker”. {En línea}. {9 Mayo de 2023}. Disponible en: (https://www.smaldone.com.ar/documentos/docs/comoserhacker.shtml)

[31] LEVY, Steven. *Hackers*: Heroes of the Computer Revolution - 25th Anniversary Edition. **O’Reilly Media**, Inc., 2010. ISBN 978-1-4493-9374-8.

uso sensible de contraseñas son formas efectivas de prevenir el ataque del *malware* en un sistema.

4.2.6 Phishing. Se reconoce como una técnica de fraude que consiste en la obtención de información personal y confidencial de los usuarios a través de la suplantación de identidad. Según la Asociación de Internautas (2018)32, el Phishing es un intento fraudulento de obtener información confidencial como contraseñas, números de tarjeta de crédito y otros datos sensibles, utilizando técnicas como el engaño mediante correos electrónicos, sitios web falsos, mensajes de texto y llamadas telefónicas.

Esta técnica de fraude se ha convertido en una amenaza cada vez más sofisticada y peligrosa en el mundo digital. Según Kaspersky Lab (2019)[33], una compañía de seguridad informática, el *Phishing* es una de las principales amenazas en línea, y ha experimentado un gran aumento en los últimos años.

Para prevenir este tipo de fraude, es importante que los usuarios estén alertas y conozcan cómo detectar intentos de *Phishing*. Según la *Office of the Australian Information Commissioner*[34], algunos de los signos comunes de un mensaje de *Phishing* incluyen la solicitud de información personal, un enlace sospechoso o una dirección de correo electrónico desconocida.

Teniendo en cuenta los párrafos anteriores el *Phishing* es una técnica de fraude digital que busca obtener información confidencial de los usuarios a través de la suplantación de identidad. Como usuarios, es importante estar alerta y conocer las señales de advertencia para prevenir ser víctimas de este tipo de fraude.

4.2.7 Ingeniería social. La Ingeniería Social se define como una técnica utilizada para obtener información, acceso o beneficios a través del engaño y la manipulación psicológica de personas, ya sea de manera presencial, telefónica o virtual. Según Mitnick y Simon (2002), ***"La ingeniería social se ha convertido en la herramienta preferida de los criminales informáticos en el siglo XXI"***[35]. Lo mencionado antes toma sentido cuando se evidencia que el elemento de un sistema con mayor debilidad es el factor humano

---

[32] Asociación de Internautas. (2018). Guía Práctica de Seguridad en Internet. Recuperado de: (https://www.internautas.org/pdf/2018/guia-practica-de-seguridad-en-internet.pdf)

[33] Kaspersky Lab. (2019). *Phishing*: Qué es, cómo funciona y cómo prevenirlo. Recuperado de: https://latam.kaspersky.com/resource-center/threats/*phishing*

[34] Office of the Australian Information Commissioner. 2019. *Phishing*. Recuperado de https://www.oaic.gov.au/privacy/guidance-and-advice/*phishing*/

[35] MITNICK, K. D., & SIMON, W. L. (2002). La arte de la infiltración en la ingeniería social. En Secure Networks (pp. 1-9).

Los ingenieros sociales pueden utilizar diversas técnicas para lograr sus objetivos, tales como la persuasión, el engaño, la intimidación o la suplantación de identidad. Según Todorov y Jordanov (2016), ***"Las técnicas de la ingeniería social pueden ser muy sencillas, como la simple manipulación de la conversación o muy avanzadas, como la creación de sitios web falsos, correos electrónicos phishing o pretextos detallados"***[36].

La Ingeniería Social es una práctica común en el ámbito de la seguridad informática, y se considera una amenaza importante para empresas, organizaciones y usuarios individuales. De acuerdo con Hadnagy (2011), ***"La ingeniería social es una amenaza muy peligrosa y cada vez más sofisticada, que puede poner en riesgo la seguridad de la información y la privacidad de las personas o empresas que sean objeto del engaño"***[37].

4.2.8 Firewall. Es un "sistema o grupo de sistemas que decide qué paquetes de red deben ser permitidos a través del *firewall*"[38] (Bosworth, Kabay y Whyne, 2009, p. 178). El propósito de un *firewall* es proteger a una organización contra amenazas externas, como *hackers o malware*. El *firewall* actúa como una barrera entre la red privada de la organización y el mundo exterior. Según Chapple (2018), un *firewall* puede basarse en reglas de filtrado de paquetes que establecen qué tipo de tráfico se permite o se bloquea en función de la dirección IP, el puerto o el protocolo. También puede usar inspección de estado, que *"examina el contenido de los paquetes y las conexiones para determinar si deben ser permitidos o rechazados"*[39].

Para tener en cuenta, un *firewall* es "un componente crucial de la seguridad de la red que puede ayudar a mitigar muchos de los riesgos de seguridad asociados con las redes de computadoras"[40]

---

[36] TODOROV, D., & JORDANOV, K. Ingeniería social: aspectos conceptual y técnico. 2016. En Revista técnica de seguridad informática (pp. 1-10).

[37] HADNAGY, C. Ingeniería social: la amenaza más peligrosa de hoy en día. 2011. En Revista de seguridad de la información (pp. 1-12).

[38] BOSWORTH, S., KABAY, M. E., & WHYNE, E. Computer security handbook (6th ed.). 2009. John Wiley & Sons.

[39] CHAPPLE, M. *Firewall*. En M. Chapple (Ed.), The CISSP prep guide: Mastering the ten domains of computer security. 2018. (3rd ed., pp. 745-746). John Wiley & Sons.

[40] BOSWORTH, S., KABAY, M. E., & WHYNE, E. Op. Cit., p. 178).

4.2.9 Autenticación. Cuando se habla de autenticación se hace referencia a la verificación de la identidad de un usuario y es uno de los aspectos más importantes en el ámbito de la seguridad cibernética. De acuerdo con Cao, Chen y Yan (2022), la autenticación ***"permite el ingreso al sistema de sólo los usuarios verdaderamente autorizados y que estos accedan a los recursos de la red"***[41].

La autenticación se basa en la idea de que cada usuario tiene un conjunto único de credenciales de acceso, que pueden incluir una combinación de nombre de usuario y contraseña, un *token* de seguridad o incluso un escaneo biométrico. Según Sharma y Dahiya (2020), ***"la autenticación se convierte en un medio eficaz para identificar a los usuarios y concederles acceso sólo a los recursos a los que tienen derecho"***[42]; en este sentido, es de resaltar que la autenticación no puede garantizar completamente al 100%, la seguridad en línea; en la misma dirección, Han y Han (2020), indican que ***"la autenticación es un mecanismo importante; pero no es realmente cierto que sea totalmente suficiente para proteger completamente los recursos de una red"***[43]. Por lo tanto, es necesario complementar la autenticación con otros mecanismos de seguridad, como la autorización y la implementación de técnicas de cifrado.

Para destacar, la autenticación es esencial en la ciberseguridad y en la protección de los sistemas transaccionales porque permite verificar la identidad de los usuarios y restringir el acceso no autorizado a los recursos. Pero, es importante utilizar otros mecanismos de seguridad para garantizar la protección completa de los datos sensitivos en línea.

[41] CAO, J., CHEN, X. & YAN, Y. "A Survey on Authentication Mechanisms in Cybersecurity". **Journal of Information Security**, 2022. P. 11(2), 81-96. Doi: 10.4236/jis.2020.112007

[42] SHARMA, N., & DAHIYA, R. "A Comprehensive Review of Authentication Mechanisms in Network Security". **International Journal of Computer Sciences and Engineering**, 2020. P. 8(3), 7-13. Doi: 10.1109/IEMTRONICS48171.2020.9123550

[43] HAN, Y. & HAN, K. "A Review of Authentication Techniques for Cloud Computing". **International Journal of Network Security**, 2020. P. 21(3), 468-478.

4.2.10 Autorización. La autorización en ciberseguridad es un proceso que se utiliza para permitir o denegar el acceso a recursos y servicios en línea a individuos o sistemas en función de criterios previamente definidos. Según la información proporcionada por la NSA (2014),[44] la autorización es una de las cuatro funciones principales de la gestión de identidades y accesos en sistemas transaccionales y ciberseguridad.

Para que la autorización sea efectiva, es necesario que se establezcan distintos niveles de permisos o privilegios, los cuales deben otorgarse en función del rol y responsabilidades asignadas a cada usuario. Como señala la Guía NIST SP 800-53 (2013),[45] para la gestión de la seguridad de la información, la autorización debe estar basada en la mínima necesidad de acceso, es decir, que cada usuario solo debe tener acceso a los recursos y servicios necesarios para realizar sus tareas y responsabilidades; en términos prácticos, la autorización implica la definición de permisos de acceso para distintos tipos de usuarios a recursos y servicios en línea, tales como bases de datos, sistemas de correo electrónico, servidores y aplicaciones web. Según la Guía ISO/IEC 27001 (2013),[46] para la gestión de la seguridad de la información, la autorización debe estar respaldada por políticas y procedimientos bien documentados, los cuales deben ser aplicados de manera rigurosa y consistente.

Por último, se puede afirmar que la autorización es un elemento clave en la gestión de la seguridad de la información en línea, ya que permite controlar y limitar el acceso a recursos y servicios en función de criterios de necesidad y minimización de riesgos. Su implementación efectiva requiere la definición de políticas y procedimientos claros, los cuales deben ser aplicados de manera constante en toda la organización.

[44] National Security Agency. (2014). Identity and Access Management. Recuperado de: (https://www.nsa.gov/Portals/70/documents/resources/cybersecurity-technical-best-practices-23july2014.pdf)

[45] National Institute of Standards and Technology. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. Recuperado de: (https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final)

[46] International Organization for Standardization. (2013). Information Technology - Security Techniques - Information Security Management Systems - Requirements. Recuperado de: (https://www.iso.org/standard/54534.html)

4.2.11 Encriptación. En la actualidad las organizaciones y sistemas que implementan transacciones en línea, tiene la necesidad de proteger los datos que se envían a través de una red; citando a (Carvajal, 2019), la encriptación "***para las empresas es prioritaria para poder adoptar una cultura de encriptación de datos, que si bien es cierto que no es la solución total a la problemática de delitos informáticos, si representa una gran resistencia o barrera para las amenazas cibernéticas y de ciberseguridad que enfrenta"***[47].

Para ampliar el concepto de encriptación la consulta se extiende a fuentes en idioma inglés, en este caso se relaciona el siguiente texto:

> *The encryption is a crucial aspect of cybersecurity, as it involves the conversion of data into a code that is unreadable without a key. The primary goal of encryption is to protect sensitive information from being accessed and used by unauthorized parties. As noted by John Kindervag (2018), Vice President and Principal Analyst at Forrester Research, "Encryption is a fundamental enabler of secure communications and information sharing in a world where cyberthreats are pervasive and attacks are constant"*[48]
>
> *There are various forms of encryption, including symmetric-key encryption and public-key encryption. Symmetric-key encryption uses the same key to encrypt and decrypt data, while public-key encryption uses a pair of keys - a public key and a private key - to encrypt and decrypt data. This approach was first introduced by Whitfield Diffie and Martin Hellman in their 1976 paper "New Directions in Cryptography,"*[49] *which suggested using a public key for encryption and a private key for decryption. (*Diffie y Hellman, 1976).
>
> *Encryption has become increasingly important in the age of digital communication, where sensitive data can be easily intercepted and stolen by cybercriminals. As noted by the National Institute of Standards and Technology (NIST), "Encryption is one of the most powerful tools available for protecting sensitive information from unauthorized disclosure"*[50]
> *.*

---

[47] CARVAJAL, Carlos. "La encriptación de datos empresariales: ventajas y desventajas. **{En línea}**. 2019. Universidad Agraria del Ecuador. Doi: https://doi.org/10.26820/recimundo/3.(2).abril.2019.980-997 {9 Mayo de 2023}. Disponible en: (https://recimundo.com/index.php/es/article/view/487)

[48] KINDERVAG, J. (2018). The future of encryption. Forrester Research.

[49] DIFFIE, W., & HELLMAN, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory. P. 22(6), 644-654.

[50] National Institute of Standards and Technology. (2016). NIST Special Publication 800-131A rev. 2: Transitioning the use of cryptographic algorithms and key lengths. U.S. Department of Commerce.

> *In conclusion, encryption is a critical component of cybersecurity, as it helps to ensure the confidentiality, integrity, and authenticity of sensitive information. As noted by security expert Bruce Schneier, "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on"*[51] (Schneier, 2013)*.*

Teniendo en cuenta el texto citado, Kindervag se enfoca en la necesidad de encriptar los datos, proteger la información implementando técnicas de cifrado eficientes que impidan el acceso no autorizado de los ciberdelincuentes.

4.2.12 Seguridad en la red. La seguridad en la red es un concepto crucial en la era digital actual, especialmente cuando se trata de sistemas transaccionales y financieros, la ciberseguridad se ha convertido en una preocupación clave debido al aumento en la cantidad de amenazas y ataques cibernéticos en línea. En este campo se puede relacionar la seguridad en la red y la ciberseguridad en sistemas transaccionales.

La seguridad en la red se refiere a la capacidad de proteger los datos que se transmiten a través de redes de comunicación, esto se alcanza mediante la implementación de medidas de seguridad y tecnologías que protegen los sistemas, redes y dispositivos de los ataques y del acceso no autorizado, la seguridad en la red es esencial en el contexto de sistemas transaccionales, ya que se trata de sistemas que procesan información financiera sensible, como transacciones bancarias, compras en línea y transferencias de fondos.

Ahora bien, la ciberseguridad en sistemas transaccionales es un aspecto particular de la seguridad en la red que se centra en la protección de los datos financieros y transaccionales en línea, según un informe de la Comisión Europea (2018)[52], los sistemas financieros son uno de los principales objetivos de los ciberataques debido a la gran cantidad de datos financieros y personales que se manejan. El informe también indica que los ciberataques pueden resultar en pérdidas económicas significativas, lo que enfatiza la importancia de la seguridad en la red en sistemas transaccionales.

Para fortalecer la ciberseguridad en este tipo de sistemas se pueden utilizar diversas tecnologías y técnicas para asegurar la seguridad en la red, el cifrado de datos es una medida fundamental para garantizar la confidencialidad de los datos transmitidos a través de la red. Los cortafuegos y los sistemas de detección de

---

[51] SCHNEIER, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 2013

[52] COMISIÓN EUROPEA. La estrategia de ciberseguridad de la UE: hacia un enfoque de seguridad cibernética más fuerte y resiliente. 2018. Luxembourg: Publications Office of the European Union. Recuperado de (https://ec.europa.eu/digital-single-market/en/news/strategia-de-ciberseguridad-de-la-ue-hacia-un-enfoque-de-seguridad-cibernetica-mas-fuerte-y-resiliente)

intrusos ayudan a defender los sistemas y las redes de los ataques malintencionados. Asimismo, la implementación de medidas de autenticación y autorización ayuda a garantizar que solo los usuarios autorizados accedan a los datos financieros.

4.2.13 Protección de datos. La protección de datos en sistemas transaccionales se refiere a la seguridad que se debe mantener en los procesos de transacciones electrónicas, como compras y transferencias de dinero a través de internet. Según la Organización Internacional de Normalización (ISO), la protección de datos en sistemas transaccionales se define como "las medidas técnico-administrativas que se toman para asegurar la necesaria integridad, confidencialidad y disponibilidad de los datos en transacciones"[53] (ISO/IEC, 2023).

Es importante destacar que, en la actualidad, la mayoría de las transacciones financieras se realizan en línea, lo que ha generado un aumento en los ataques cibernéticos y los delitos informáticos. Por ello, la seguridad y la protección de los datos son fundamentales para garantizar la confianza y la credibilidad en los procesos de transacciones electrónicas; según un informe elaborado por la empresa de seguridad informática *McAfee (2018),*[54] los ciberdelitos relacionados con las transacciones financieras, han aumentado en un 75% en los últimos años. Por esta razón, las empresas y los usuarios deben tomar medidas de protección para evitar posibles ataques informáticos y fraudes electrónicos.

Entre las medidas de protección recomendadas se encuentran la utilización de *software* de seguridad, la actualización regular del *software* y la realización de copias de seguridad de los datos. También es importante informarse sobre las políticas de seguridad de las empresas y sitios web donde se realicen transacciones financieras.

4.2.14 Monitoreo de redes. Cuando se aborda el concepto de monitoreo de redes, referido a la ciberseguridad en sistemas transaccionales, se afirma que es un proceso integral que busca proteger los datos y las transacciones realizadas a través de internet, este proceso implica el monitoreo constante de los sistemas y redes que están involucrados en las transacciones, con el fin de detectar posibles vulnerabilidades y amenazas que puedan afectar la seguridad de los datos y la integridad de las transacciones.

[53] ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization. 2013

[54] McAfee. (2018). Crimen financiero en línea. Recuperado de: (https://www.mcafee.com/es/resources/reports/rp-economic-cybercrime-on-the-rise.pdf)

Teniendo en cuenta lo expuesto por Anderson y Moore (2009)[55], la seguridad de los sistemas y redes transaccionales está en riesgo debido a los ciberdelincuentes que buscan explotar posibles vulnerabilidades y brechas en la seguridad para obtener información confidencial de los usuarios, por esta razón, es importante implementar medidas de protección como el monitoreo de redes por las cuales se transportan los datos de los sistemas transaccionales.

El proceso de monitoreo de redes enfocado hacia la ciberseguridad en sistemas transaccionales implica la identificación y mapeo de las redes involucradas en las transacciones, así como la detección de posibles amenazas a través del análisis de *logs*, la identificación de patrones de tráfico e incluso la monitorización de las direcciones IP, entre otros. Según la *National Institute of Standards and Technology* (NIST) (2018),[56] el monitoreo de redes enfocado hacia la ciberseguridad en sistemas transaccionales debe contemplar la implementación de herramientas de análisis de *logs*, la detección y prevención de intrusiones, el monitoreo de los accesos, el análisis de vulnerabilidades y la implementación de políticas de seguridad.

El monitoreo de redes enfocado hacia la ciberseguridad en sistemas transaccionales representa una medida muy importante para proteger los datos y las transacciones de los usuarios, su efectividad dependerá en gran medida de la implementación adecuada de medidas de seguridad y de la capacitación constante del personal encargado del monitoreo.

4.2.15 Análisis de vulnerabilidades. Se considera que es uno de los “procesos donde se evalúa los activos en búsqueda de debilidades o fallos del sistema que puedan ser aprovechadas los atacantes” (KOSINSKI & FORREST, 2023).
En éste, se evalúa una determinada infraestructura de sistemas transaccionales en busca de puntos débiles que puedan ser explotados por agentes malintencionados en contra de la ciberseguridad. Por ende, este análisis se trata de una práctica muy importante para garantizar la protección de los datos y transacciones de los usuarios.

De forma específica, la ciberseguridad en sistemas transaccionales requiere de una atención rigurosa para mitigar los riesgos y amenazas que se presentan. Las vulnerabilidades más comunes en este tipo de sistemas incluyen acceso no autorizado, inyección de código malicioso, interceptación de comunicaciones,

[55] ANDERSON, R., & MOORE, T. The economics of information security. Science. 2009. Pág. 314(5799), 610-613.

[56] National Institute of Standards and Technology (NIST). (2018). Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information systems and Organizations. Washington, DC: National Institute of Standards and Technology.

vulnerabilidades de los componentes web, entre otros. Para llevar a cabo un adecuado análisis de vulnerabilidades en sistemas transaccionales, es necesario adoptar un enfoque proactivo e integral, lo que significa que se debe hacer una revisión exhaustiva de los protocolos de seguridad, infraestructuras de red, sistemas operativos, aplicaciones, entre otros componentes claves del sistema; en este sentido, existen diferentes herramientas de análisis de vulnerabilidades en el mercado que son capaces de identificar las debilidades del sistema, este tipo de herramientas se basan en diferentes métodos, tales como análisis de código fuente, pruebas de intrusión, escaneo de puertos, entre otros.

Finalmente, el análisis de vulnerabilidades es una práctica fundamental en la ciberseguridad de sistemas transaccionales. Es una tarea constante que debe ser llevada a cabo por expertos en la materia para proteger los datos y transacciones de los usuarios. La implementación de metodologías y herramientas adecuadas para el análisis de vulnerabilidades puede marcar la diferencia en la seguridad de un sistema transaccional.

4.3 MARCO HISTÓRICO

Los sistemas transaccionales han sido una parte integral del mundo empresarial durante décadas, y con el advenimiento de la era digital, se han vuelto cada vez más avanzados y sofisticados. Sin embargo, junto con la evolución de estos sistemas, también han evolucionado los vectores de ataque que los amenazan.

Durante la década de 1970, los sistemas transaccionales se convirtieron en una herramienta cada vez más común en el mundo empresarial, lo que los convirtió en un objetivo principal para los *hackers* y otros atacantes cibernéticos. En aquellos días, la seguridad de los sistemas informáticos no era una preocupación prioritaria, y los vectores de ataque podían ser simples y efectivos.

Según el libro "*Computer Security: Art and Science*" de Matt Bishop (2002), uno de los primeros vectores de ataque utilizados en los sistemas transaccionales de la década de 1970 fue la "suplantación de identidad"[57]. Los atacantes obtenían información de los usuarios legítimos del sistema, como contraseñas o nombres de usuario, y luego se hacían pasar por ellos para acceder a la información privilegiada. Bishop destaca que este tipo de ataque aún es común hoy en día, aunque las medidas de seguridad son mucho más rigurosas.

Otro vector de ataque utilizado en los sistemas transaccionales de los años 70 fue el *"sniffing"* o espionaje de datos en tránsito. Según el libro "*Hacker's Delight*" de Henry S. Warren (2003),[58] los atacantes podían utilizar herramientas

[57] BISHOP, M. Computer security: Art and science. Addison-Wesley. 2002
[58] WARREN, H. S. Hacker's delight. Addison-Wesley. 2003

especializadas para interceptar los datos que viajaban entre el usuario y el sistema, lo que les permitía acceder a información confidencial, como contraseñas y números de cuenta bancaria.

Por último, el libro *"Computer Crime: A Crimefighter's Handbook"* de David Icove, Karl Seger y William VonStorch (1995), señala que los atacantes también podían utilizar técnicas de "manipulación de datos"[59] para realizar transacciones fraudulentas en los sistemas transaccionales. Por ejemplo, podían modificar los montos de las transacciones o transferir fondos a cuentas ficticias.

Finalmente, durante la década de 1970, los sistemas transaccionales eran vulnerables a una serie de vectores de ataque comunes. La suplantación de identidad, el espionaje de datos en tránsito y la manipulación de datos eran algunos de los métodos utilizados por los atacantes. Aunque las medidas de seguridad han mejorado significativamente desde entonces, estas técnicas de ataque aún son utilizadas hoy en día en formas más sofisticadas.

Durante la década de 1980, los sistemas transaccionales continuaron siendo un objetivo principal para los atacantes cibernéticos debido a su valor comercial y financiero. Los avances tecnológicos de la época también permitieron la creación de nuevas técnicas de ataque que aumentaron la vulnerabilidad de estos sistemas.

Según el artículo *Security Issues in Database Systems* de R. T. Snodgrass y A. Ahuja (1986), uno de los principales vectores de ataque a los sistemas transaccionales en la década de 1980 fue la "inyección de código"[60]. Los atacantes podían insertar código malicioso en los comandos de entrada del sistema, lo que les permitía manipular o acceder a la información de manera no autorizada. Esta técnica sigue siendo una preocupación actual, ya que los sistemas actuales aún pueden ser vulnerables a la inyección de código.

Otro vector de ataque común en la década de 1980 fue la "denegación de servicio"[61] (DoS). Según el artículo *Denial of Service in Computer Networks* de Dorothy E. *Denning* (1987), los atacantes podían utilizar herramientas de *software* para inundar el sistema con tráfico de red falso o solicitudes de servicio, lo que causaba la interrupción del servicio y el acceso no autorizado a los datos. Este tipo de ataque DoS sigue siendo una amenaza para los sistemas actuales, aunque las medidas de seguridad han mejorado.

---

[59] ICOVE, D., SEGER, K. & VONSTORCH, W. Computer crime: A crimefighter's handbook. 1995 O'Reilly.
[60] SNODGRASS, R. T. & AHUJA, A. Security issues in database systems. ACM Press. 1986
[61] DENNING, D. E. Denial of service in computer networks. 1987. ACM Press.

En la década de 2000, los sistemas transaccionales son víctima de los atacantes cibernéticos quienes emplean los avances tecnológicos de la época para crear nuevas técnicas de ataque las cuales logran aumentar la vulnerabilidad de estos sistemas.

Según el artículo SQL *Injection Attacks and Defense* de Justin Clarke-Salt (2004), la inyección de código SQL se convirtió en un vector de ataque cada vez más común en los sistemas transaccionales durante la década de 2000. Clarke-Salt afirma que "la inyección SQL es un tipo de ataque de seguridad de aplicaciones web en el que el atacante introduce código SQL malicioso en los campos de entrada de una aplicación web, lo que le permite tomar el control de la base de datos subyacente".[62] Esta técnica sigue siendo una amenaza actual para los sistemas informáticos, especialmente en las aplicaciones web.

Otro vector de ataque común en la década de 2000 fue el *"phishing"*. Según el informe de la Comisión Federal de Comercio de Estados Unidos sobre el fraude en línea (2004), el *phishing* era "un tipo de estafa de correo electrónico que busca engañar a los destinatarios para que revelen información financiera o personal, como contraseñas y números de tarjetas de crédito."[63] Los atacantes utilizaban técnicas de ingeniería social para convencer a los usuarios de que proporcionaran esta información confidencial.

Por último, en esta década, el libro "*Hacking Exposed 5th Edition*" de Stuart McClure, Joel Scambray y George Kurtz (2005), destacan que la "suplantación de identidad"[64] se convirtió en un vector de ataque común durante la década de 2000. Los atacantes podían utilizar técnicas de *phishing* o de ingeniería social para obtener credenciales de inicio de sesión legítimas y luego utilizarlas para acceder a información confidencial o realizar transacciones fraudulentas en nombre de los usuarios legítimos.

En resumen, durante la década de 2000, los sistemas transaccionales fueron vulnerables a varios vectores de ataque, como la inyección de código SQL, el *phishing* y la suplantación de identidad. Estos vectores de ataque siguen siendo una amenaza actual para los sistemas informáticos, y se han desarrollado nuevas técnicas de ataque para explotar vulnerabilidades en los sistemas transaccionales.

Durante la década de 2020, los sistemas transaccionales siguieron siendo uno de los objetivos principales para los ciberdelincuentes. Uno de los vectores de ataque más comunes durante este período fue el *ransomware*. Según un informe de la

[62] CLARKE-SALT, J. SQL injection attacks and defense. 2004. SANS Institute.

[63]Comisión Federal de Comercio de Estados Unidos. (2004). Fraude en línea: cómo evitar convertirse en una víctima. FTC.

[64]MCCLURE, S., SCAMBRAY, J. & KURTZ, G. Hacking exposed 5th edition. 2005. McGraw-Hill.

empresa de ciberseguridad *SonicWall* (2021), "los ataques de *ransomware* alcanzaron un máximo histórico en 2020, con un aumento del 62% respecto al año anterior"[65]. Los atacantes utilizan el *ransomware* para cifrar los datos de los sistemas transaccionales y exigir un rescate para su recuperación.

Otro vector de ataque común en la década de 2020 fue el ataque de denegación de servicio distribuido (DDoS). Según un informe de la empresa de ciberseguridad *Cloudflare (*2021), "los ataques DDoS se convirtieron en una amenaza mucho más grave durante la pandemia COVID-19, con un aumento del 40% en la cantidad de ataques DDoS por día en comparación con el año anterior"[66]. También en esta década los atacantes utilizan técnicas de *botnet* para inundar los sistemas transaccionales con tráfico malintencionado, lo que provoca la interrupción de los servicios.

finalmente, durante la década de 2020, los sistemas transaccionales continuaron siendo vulnerables a los ataques cibernéticos, que conjugan todos los vectores de ataque de la historia, estos vectores de ataque se han convertido en amenazas cada vez más sofisticadas y persistentes para la seguridad de los sistemas transaccionales.

4.4 ANTECEDENTES O ESTADO ACTUAL

Para verificar la existencia de autores que han abordado el tema de la maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques fue necesario revisar minuciosamente diferentes fuentes bibliográficas y emplear herramientas o motores de búsqueda especializados; producto de esta búsqueda se relacionan los siguientes antecedentes.

La seguridad de los sistemas transaccionales es una preocupación constante en la actualidad debido al aumento de las amenazas cibernéticas. En este contexto, **la monografía "Análisis de vectores de ataque en sistemas transaccionales: un enfoque basado en el análisis de amenazas"** de *Carlos García y José González (2017),* presenta un análisis detallado de los vectores de ataque en estos sistemas, así como un enfoque para su detección y prevención basado en el análisis de amenazas.

Los autores *García y González (2017),* comienzan por definir los sistemas transaccionales como aquellos que procesan transacciones comerciales,

[65]SONICWALL. SonicWall cyber threat report. 2021. Recuperado de: (https://www.sonicwall.com/techdocs/pdf/SonicWall-2021-Cyber-Threat-Report.pdf)

[66]CLOUDFLARE. Cloudflare's DDoS trends report: Q1 2021. Recuperado de: (https://www.cloudflare.com/zh-tw/learning/ddos/ddos-trends-report-q1-2021/)

financieras o de otro tipo, y que involucran el intercambio de información entre varias partes. A continuación, identifican los principales vectores de ataque en estos sistemas, que incluyen la suplantación de identidad, el robo de credenciales, la explotación de vulnerabilidades y la ingeniería social.

Para abordar estas amenazas, los autores proponen un enfoque basado en el análisis de amenazas, que implica la identificación de las posibles vulnerabilidades y amenazas en el sistema, la evaluación de su impacto potencial y la implementación de medidas de seguridad adecuadas. Como señalan los autores *Carlos García y José González (2017)*, ***"el analizar de las amenazas es un proceso que ayuda a la caracterización y valoración de todo tipo de riesgo asociado a una amenaza potencial y proporciona los fundamentos sólidos para tomar decisiones informadas en cuanto a la ejecución de medidas de seguridad"*** (*García y González, 2017)*[67] .

En este sentido, los autores proponen un modelo de análisis de amenazas específico para los sistemas transaccionales, que incluye la identificación de las amenazas, la evaluación del impacto y la probabilidad de ocurrencia de cada amenaza, y la implementación de medidas de seguridad adecuadas para mitigar los riesgos. Como indican los autores *Carlos García y José González (2017)*, ***"el modelo de análisis de amenazas propuesto, proporciona una metodología efectiva y sistemática para la caracterización y mitigación de los vectores de ataque en sistemas transaccionales"*** (*García y González, 2017).*[68]

Por último, la monografía revisada presenta un análisis detallado de los vectores de ataque en sistemas transaccionales y propone un enfoque basado en el análisis de amenazas para su detección y prevención. Este enfoque proporciona una metodología efectiva y sistemática para identificar y mitigar los vectores de ataque en estos sistemas críticos.

La monografía *"Seguridad en sistemas transaccionales: análisis de vectores de ataque y propuestas de mitigación"* de *Ana Torres (2018)*, presenta un análisis detallado de los vectores de ataque en sistemas transaccionales, así como propuestas para su mitigación.

En primer lugar, Torres (2018), identifica los sistemas transaccionales como aquellos que ***"facilitan la gestión de las transacciones comerciales, financieras o*** **de cualquier otra índole entre diferentes entidades"**[69] A

[67] GARCÍA, C. y GONZÁLEZ, J. Análisis de vectores de ataque en sistemas transaccionales: un enfoque basado en el análisis de amenazas. 2017. Monografía de grado. Universidad Nacional de Colombia.
[68] Ibid., p. 9
[69] Torres, A. Seguridad en sistemas transaccionales: análisis de vectores de ataque y propuestas de mitigación. 2018. Trabajo de Grado. Universidad de Salamanca.

continuación, la autora explica que estos sistemas son vulnerables a una serie de vectores de ataque, tales como el robo de credenciales, la suplantación de identidad, el uso de *malware* y la explotación de vulnerabilidades.

Para hacer frente a estas amenazas, Torres (2018), propone una serie de medidas de mitigación que incluyen la implementación de controles de acceso, el uso de autenticación multifactor y la aplicación de parches de seguridad. En palabras de la autora, ***"la implementación de las medidas de mitigación ayudará a garantizar la seguridad de los sistemas transaccionales y a reducir el riesgo de ataques"*** (Torres, 2018).[70]

Cabe destacar que la autora hace hincapié en la importancia de la concientización del personal en materia de seguridad, señalando que ***"los empleados son el eslabón más débil en la cadena de seguridad de los sistemas transaccionales"*** (Torres, 2018).[71] En este sentido, la autora propone la realización de programas de formación y sensibilización sobre seguridad para el personal que trabaja en estos sistemas.

Otro documento consultado fue la monografía *"Estudio de los vectores de ataque en sistemas transaccionales en línea"* de Laura Pérez y Rafael Rodríguez (2019), donde se presenta un análisis exhaustivo de los vectores de ataque en los sistemas transaccionales en línea, enfocado en las amenazas que enfrentan los usuarios y las empresas que utilizan estos sistemas.

En primer lugar, Pérez y Rodríguez (2019), definen los sistemas transaccionales en línea como ***"aquellos que permiten realizar transacciones comerciales, financieras o de cualquier otra naturaleza a través de Internet"***[72]. Los autores señalan que estos sistemas son vulnerables a una amplia variedad de vectores de ataque, como el *phishing*, el *malware* y la ingeniería social.

Los autores también destacan la importancia de la autenticación y la identificación segura en los sistemas transaccionales en línea, señalando que ***"la autenticación débil y la falta de protección de la identidad del usuario son factores clave en la mayoría de los ataques a sistemas transaccionales en línea"***[73]. En este sentido, Pérez y Rodríguez (2019), proponen medidas para mejorar la

---

[70] Ibid., p. 13

[71] Ibid., p. 10

[72] PÉREZ, L. y RODRÍGUEZ, R. Estudio de los vectores de ataque en sistemas transaccionales. **{En línea}**. 2019. Revista Científica de Tecnología e Innovación, p. 5(1), 1-12.

[73] PÉREZ, L. y RODRÍGUEZ, R. Op. Cit., p. 7

autenticación y la identificación, como el uso de autenticación multifactorial y la implementación de medidas de protección de la identidad.

Además, los autores señalan lo relevante de la educar y concientizar a los usuarios y empresas, sobre las amenazas en los sistemas transaccionales en línea. En palabras de los autores, "la educación y la concientización son elementos significativos para usuarios y empresas implementen y ejecuten medidas de seguridad adecuadas" (Pérez y Rodríguez, 2019).[74]

En conclusión, esta monografía ofrece un análisis detallado de las amenazas a los sistemas transaccionales en línea y propone medidas para mejorar la seguridad de estos sistemas. Los autores destacan la importancia de la autenticación y la identificación segura; así como la educación y la concientización de usuarios y empresas.

En la monografía "Análisis de vectores de ataque en sistemas transaccionales basados en *blockchain*" de David Gómez (2020), se presenta un análisis detallado de los vectores de ataque en sistemas transaccionales basados en *blockchain*, una tecnología que ha ganado gran popularidad en los últimos años por su capacidad para garantizar la seguridad y transparencia de las transacciones. En este texto, se analizarán los principales puntos tratados por el autor, haciendo uso de citas textuales y referencias bibliográficas consultadas.

En primer lugar, Gómez (2020), define los sistemas transaccionales basados en *blockchain* como ***"un tipo de sistema transaccional en línea que utiliza la tecnología blockchain para registrar y validar las transacciones"***[75]. El autor señala que, aunque los sistemas basados en *blockchain* ofrecen una mayor seguridad que los sistemas tradicionales, también son vulnerables a una serie de vectores de ataque.

Entre los vectores de ataque en sistemas transaccionales basados en *blockchain*, Gómez (2020), destaca el ataque del 51%, el ataque de hombre en el medio (MITM) y el ataque *Sybil.* El autor señala que estos ataques pueden comprometer la integridad de la cadena de bloques y la seguridad de las transacciones.

Para mitigar estos riesgos, Gómez (2020), propone una serie de medidas de seguridad, como la implementación de contratos inteligentes, la autenticación multifactorial y el uso de protocolos de consenso seguros. En palabras del autor, ***"la seguridad en los sistemas transaccionales basados en tecnología***

[74] PÉREZ, L. y RODRÍGUEZ, R. Op. Cit., p. 10

[75] GÓMEZ, D. Análisis de vectores de ataque en sistemas transaccionales basados en blockchain. 2020. Revista de Tecnología, Información y Comunicación en Educación, p. 10(1), 1-10.

blockchain requieren una dirección integral que incluya medidas técnicas, legales y organizacionales" (*Gómez, 2020).*[76]

En conclusión, esta monografía realiza un análisis detallado de los vectores de ataque en sistemas transaccionales basados en *blockchain* y propone medidas para mejorar su seguridad. El autor destaca la importancia de un enfoque integral que abarque medidas técnicas, legales y organizacionales.

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

Cuando se analizan los vectores de ataque que tienen incidencia en los sistemas transaccionales se debe realizar un estudio de las herramientas tecnológicas y científicas que ayudan a gestionar los procesos de auditoría y por ende permiten entender el funcionamiento de los vectores de ataque en especial los que afectan los sistemas transaccionales; algunas herramientas que podrían resultar útiles son:

4.5.1 Sistemas de gestión de bases de datos. Para analizar las vulnerabilidades en los sistemas transaccionales, es importante contar con conocimientos de bases de datos y sistemas de gestión de bases de datos. Algunos ejemplos de sistemas de gestión de bases de datos populares son MySQL, Oracle, SQL Server y *PostgreSQL*.

4.5.2 Herramientas de análisis de vulnerabilidades. Existen muchas herramientas disponibles para analizar y evaluar la seguridad de los sistemas transaccionales. Algunas herramientas populares son *Nessus, Metasploit, Nmap y OpenVAS*.

4.5.3 Herramientas de análisis de tráfico de red. Para entender cómo los vectores de ataque se propagan a través de una red, es importante tener herramientas para analizar el tráfico de red. Algunas herramientas útiles son *Wireshark, tcpdump* y *ngrep*.

4.5.4 Sistemas de detección de intrusiones. Para detectar y prevenir los vectores de ataque, es importante contar con sistemas de detección de intrusiones. Algunos ejemplos de sistemas populares son *Snort, Suricata* y *OSSEC*.

4.5.5 Herramientas de análisis de código. Para entender cómo los vectores de ataque se explotan en el código fuente de los sistemas transaccionales, es importante tener herramientas para analizar el código. Algunas herramientas útiles son *SonarQube*, *Checkmarx y Veracode*.

[76] GOMEZ, op. Cit., p. 9

4.5.6 Plataformas de pruebas de penetración. Las plataformas de pruebas de penetración son entornos seguros diseñados para simular ataques en sistemas transaccionales. Algunas plataformas populares son *Kali Linux, Parrot Security OS* y *BackBox.*

Al utilizar estas herramientas en conjunto, se puede tener un enfoque integral para investigar y analizar los vectores de ataque a sistemas transaccionales, lo que puede ayudar a identificar y prevenir vulnerabilidades en estos sistemas críticos.

4.6 MARCO LEGAL

Es de anotar que toda investigación o documentación debe estar regida por los parámetros legales; para abordar el tema referente a los vectores de ataque a sistemas transaccionales, este debe realizarse dentro de un marco legal y ético apropiado.

Dentro del ámbito legal se considera necesario realizar una revisión bibliográfica de las leyes que rigen las actuales organizaciones o países considerados como potencias económicas y potencias desarrolladas a nivel científico y tecnológico a nivel global; lo antes mencionado se sustenta teniendo en cuenta que muchas de las normas que rigen en el país tiene sus orígenes en la legislación de los países desarrollados o simplemente las regulaciones locales dependen de convenios establecidos entre los países miembros de ciertas organizaciones haciendo caso a los mandatos promulgados por entidades como la organización de naciones unidas, la unión europea, comunidad de estados latinoamericanos y caribeños, la organización de estados americanos; quienes ostentan gran influencia en países como Colombia; atendiendo al párrafo anterior se presentan algunas leyes y regulaciones que se aplican en diferentes países y de las cuales Colombia toma algunos principios y consideraciones generales, asumiendo que el campo de estudio de la ciberseguridad y en específico de la presente monografía “el delito informático se considera un delito transnacional”[77]

En Estados Unidos, existen diversas leyes y regulaciones que podrían ser relevantes, pero en este caso se menciona la ley de Privacidad de la Información y la Seguridad de la Información de 1998 (Gramm-Leach-Bliley Act)

Esta ley constituye un acta que fue promulgada por el Congreso de los Estados Unidos para proteger la información personal de los ciudadanos estadounidenses. Esta ley establece que las empresas y el gobierno deben recopilar, procesar y

[77] LISA Institute. “Ciberseguridad ante el Crimen transnacional y la Ciberdelincuencia [Parte 1/4]”. **{En línea}**. {10 Mayo de 2023}. Disponible en: (https://www.lisainstitute.com/blogs/blog/ciberseguridad-crimen-transnacional-ciberdelincuencia)

almacenar la información personal de los ciudadanos de manera responsable, y deben tomar medidas para proteger esa información de cualquier uso inapropiado o ilegal.

La Ley de Privacidad de la Información y la Seguridad de la Información de 1998 también establece que los ciudadanos tienen el derecho de acceder a su propia información y de conocer cómo se está utilizando y protegiendo su información personal. Además, la Ley exige que las empresas y organizaciones notifiquen a los ciudadanos en caso de que se produzca una violación de seguridad de los datos y de que su información personal sea comprometida.

De igual forma, establece penalización para aquellos que violen la privacidad y seguridad de la información. Las sanciones pueden incluir multas que pueden llegar hasta los $10,000 dólares por cada violación y prisión de hasta 5 años.

Finalmente, la Ley de Privacidad de la Información y la Seguridad de la Información, es una importante ley para proteger la privacidad y la seguridad de la información personal de los ciudadanos estadounidenses, esta ley establece estándares y medidas específicas para asegurar que la recopilación, procesamiento y almacenamiento de información personal se realice de manera responsable y segura, la aplicación de la ley también establece medidas de penalización para aquellos que violen la privacidad y la seguridad de la información personal.

También se puede mencionar la Ley de Fraude y Abuso en los Cuidados de Salud de 1977 (FCA), la Ley de Protección de Datos de 2002 (Data Protection Act), la Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996 (HIPAA), la Ley de Modernización de la Seguridad Social de 2014 (SSMA)

Por otro lado, en Europa se implementa el Reglamento General de Protección de Datos (RGPD) es una regulación que establece los derechos de los ciudadanos europeos en cuanto a la protección de sus datos personales. También existen otras regulaciones que varían según el país.

Además, cualquier investigación relacionada con la seguridad informática debe seguir los principios éticos establecidos por la comunidad científica, como el respeto por los derechos y la privacidad de los sujetos de investigación, la minimización del riesgo y la maximización del beneficio, y la transparencia y la divulgación de los resultados.

La Organización de los Estados Americanos (OEA) viene trabajando en la implementación de medidas normativas relacionadas con la seguridad de la información y los delitos informáticos, a fin de garantizar la protección de los ciudadanos ante el avance constante de la tecnología.

En este sentido, la OEA ha establecido diversos acuerdos y convenios para promover la ciberseguridad, como el Tratado de Budapest sobre Ciberdelincuencia, ratificado por 24 estados miembros de la organización; este tratado establece normas internacionales para la lucha contra el delito cibernético y busca prevenir y perseguir delitos como el acceso no autorizado a sistemas informáticos, la alteración de datos informáticos y la distribución de virus informáticos, entre otros.

Además, en 2016, la OEA adoptó la Estrategia Interamericana de Ciberseguridad, que tiene como objetivo mejorar la capacidad de los estados miembros para proteger a sus ciudadanos de las amenazas cibernéticas y fomentar la cooperación interamericana en la lucha contra el cibercrimen, esta estrategia establece principios como la protección de la privacidad y la libertad de expresión en internet, así como la necesidad de fomentar una cultura de seguridad en línea.

En cuanto a las políticas internas de la OEA, esta organización cuenta con un equipo dedicado a la seguridad de la información y la tecnología de la información (TI), que realiza un monitoreo constante de los sistemas informáticos y trabaja en la implementación de medidas de protección contra el cibercrimen; además, la OEA ha adoptado políticas de acceso a la información y protección de los datos personales de sus empleados y beneficiarios.

Resumiendo, la OEA ha establecido una serie de medidas normativas y políticas internas en materia de seguridad de la información y cibercrimen, con el objetivo de garantizar la protección de los ciudadanos ante las amenazas cibernéticas constantes. Estas normativas están en línea con los convenios internacionales y establecen principios fundamentales como la protección de la privacidad y la libertad de expresión en línea; es importante que los estados miembros de la OEA sigan trabajando juntos para implementar medidas de protección y prevención contra el cibercrimen, a fin de garantizar un ambiente seguro y confiable en línea.

Ahora bien, en Colombia existe un marco legal establecido por la Constitución Política de Colombia y las leyes que regulan el uso de las tecnologías de la información y la protección de los datos personales; la Constitución Política de Colombia reconoce el derecho a la privacidad de los ciudadanos y establece que la protección de los datos personales es un derecho fundamental. Además, el Código Penal colombiano tipifica los delitos informáticos, como el acceso abusivo a un sistema informático, la interceptación de datos informáticos y la falsedad informática, entre otros.

también, la Ley 1581 de 2012 regula el tratamiento de los datos personales en Colombia y establece las obligaciones que deben cumplir los responsables y encargados del tratamiento de los datos personales. Asimismo, la Superintendencia de Industria y Comercio (SIC) es la entidad encargada de vigilar y controlar el cumplimiento de esta ley. Otras leyes y normativas que podrían ser

relevantes para la investigación sobre vectores de ataque a sistemas transaccionales en Colombia; se puede mencionar la Ley 1273 de 2009, que tipifica los delitos informáticos en Colombia, y la Resolución 2400 de 1979, que establece las normas de seguridad industrial en Colombia.

Es importante mencionar que cualquier investigación relacionada con la seguridad informática debe seguir los principios éticos establecidos por la comunidad científica, como el respeto por los derechos y la privacidad de los sujetos de investigación, la minimización del riesgo y la maximización del beneficio, y la transparencia y la divulgación de los resultados.

Con el fin de profundizar el estudio en el ámbito legal colombiano se relatan las siguientes normas que inciden de forma directa en el tema central de la monografía, entre ellas se mencionan:

Ley 1273 de 2009: Esta ley establece los delitos informáticos y establece las penas y sanciones correspondientes. También se refiere a la responsabilidad penal de los proveedores de servicios de internet y de los usuarios que cometan delitos a través de las redes informáticas. La Ley Colombiana 1273 de 2009 es una norma fundamental en el país, debido a que busca proteger los derechos fundamentales de las personas en el uso de las tecnologías de la información y la comunicación; esta ley se enfoca en la prevención del delito informático y establece medidas para garantizar la seguridad de la información en línea.

Una de las disposiciones más importantes que contiene la Ley 1273 es la tipificación de los delitos informáticos. En Colombia, estos delitos se clasifican en seis categorías que van desde la interceptación ilegal de datos e información, hasta el acceso abusivo a sistemas informáticos; cada uno de estos delitos es sancionado de acuerdo con su gravedad y, en muchos casos, puede ser castigado con prisión.

Otra de las medidas importantes que establece la Ley 1273 es la obligación de las empresas de implementar medidas de seguridad adecuadas para proteger la información de sus clientes y usuarios, esto significa que las empresas deben adoptar medidas técnicas, físicas y organizativas para evitar la pérdida, alteración o divulgación no autorizada de información sensible.
Sin embargo, a pesar de que la Ley 1273 es una herramienta importante para luchar contra los delitos informáticos, aún existen desafíos importantes que enfrentar. Uno de los problemas más graves es la falta de conciencia de las personas sobre los riesgos y amenazas que existen en línea; muchos usuarios de Internet no son conscientes de los riesgos de compartir información personal y financiera en línea o incluso no toman medidas básicas de seguridad, como utilizar contraseñas seguras y actualizar regularmente sus sistemas operativos.

Finalmente se concluye que la Ley Colombiana 1273 de 2009 es una herramienta fundamental para proteger a las personas y empresas en línea, es importante que todas las personas tomen conciencia de los riesgos existentes en la internet y tomen medidas para protegerse, pero también es fundamental que las empresas respeten la privacidad y seguridad de la información de sus clientes; para lograr esto, es necesario una cooperación mutua entre el gobierno, los ciudadanos y las empresas para garantizar un uso seguro y responsable de la tecnología.

Igualmente, las siguientes normas complementan la jurisprudencia en relación con los delitos informáticos y la protección de datos, en este orden de ideas se menciona la ley 1581 de 2012 que establece el régimen de protección de datos personales en Colombia y establece las obligaciones de las empresas y organizaciones públicas que manejan información personal de sus usuarios.

El decreto 1078 de 2015 que regula el uso de la firma electrónica en Colombia y establece los requisitos y procedimientos para su utilización; el decreto 364 de 2013 que establece el régimen de seguridad de la información en Colombia y establece las medidas de protección que deben adoptar las entidades públicas y privadas para garantizar la integridad, confidencialidad y disponibilidad de la información.

Ley 1801 de 2016 establece las medidas que deben adoptar las autoridades policiales y judiciales para combatir el cibercrimen y establece las penas y sanciones correspondientes, la ley 1978 de 2019: que establece las medidas de protección que deben adoptar las empresas que ofrecen servicios de tecnología de la información y las comunicaciones y establece las obligaciones en materia de seguridad para garantizar la privacidad de sus usuarios.

Finalmente se afirma que Colombia es una nación de leyes, a nivel legislativo existen las garantías y procedimientos para actuar en contra de la delincuencia, pero es importante resaltar que los ciberdelincuentes cada día optimizan sus técnicas de ataque y muchas veces ponen en jaque a las autoridades quienes se ven impedidos para aplicar la normativa existente.

5 DISEÑO METODOLÓGICO

Teniendo en cuenta que una monografía es totalmente diferente a un proyecto de investigación, por ende, no aplica el diseño metodológico, pero en este caso los párrafos siguientes buscan explicar y describir de forma general como se pretende desarrollar el estudio o revisión documental acerca de los vectores de ataque en los sistemas transaccionales; de ahí que se observa la necesidad de plantear los siguientes criterios que guiarán el proceso de revisión bibliográfica.

5.1 METODOLOGÍA.

La metodología que se utilizará para el estudio de los vectores de ataque a sistemas transaccionales se compone de las siguientes fases:

5.1.1 Revisión bibliográfica. Se realizará una búsqueda exhaustiva de fuentes bibliográficas en bases de datos especializadas en seguridad informática y tecnologías de la información, tales como IEEE *Xplore*, ACM *Digital Library*, *ScienceDirect,* entre otras. La búsqueda se realizará utilizando términos clave como vectores de ataque, sistemas transaccionales, seguridad, ciberseguridad, ataques.

5.1.2 Selección de fuentes. Se seleccionarán las fuentes bibliográficas más relevantes y actualizadas que permitan responder a los objetivos específicos del estudio.

5.1.3 Entrevistas a expertos. Se evaluarán entrevistas a expertos en seguridad informática existentes en la web, donde se aborde la temática acerca de los vectores de ataque a sistemas transaccionales y las técnicas utilizadas por los atacantes.

5.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN.

Las técnicas de recolección de información que se utilizarán para el estudio de los vectores de ataque a sistemas transaccionales serán las siguientes:

5.2.1 Revisión bibliográfica. Se utilizará la búsqueda de fuentes bibliográficas en bases de datos especializadas en seguridad informática y tecnologías de la información.

5.2.2 Análisis de incidentes. Estudiar casos de incidentes de seguridad en sistemas transaccionales para identificar los vectores de ataque más utilizados.

5.2.3 Revisión de entrevistas. Con el fin de recabar más información, es necesario analizar las entrevistas realizadas a expertos en seguridad informática que hayan trabajado en el diseño, implementación o gestión de sistemas transaccionales.

Además de los aspectos generales mencionados en el texto anterior, es conveniente afirmar que para el análisis de las vulnerabilidades se implementará el ciclo de evaluación de vulnerabilidades. Es necesario aclarar que el presente documento además de realizar un análisis a los vectores de ataque, también se enfoca en la elaboración de recomendaciones para identificar enfrentar y mitigar posibles ataques y se propone implementar la metodología de ciclo de evaluación de vulnerabilidades, la cual pretende dar orientaciones para atender las vulnerabilidades de los sistemas y se describe a continuación:

La seguridad de la información es una preocupación crítica para organizaciones de todo tipo; los sistemas de información transaccional y en general cualquier sistema está expuesto a una variedad de amenazas, desde ataques cibernéticos hasta vulnerabilidades de configuración; para mitigar estos riesgos, se utiliza el Ciclo de Evaluación de Vulnerabilidades; es una metodología que permite identificar, evaluar y gestionar las debilidades en un sistema de manera sistemática y efectiva. Como se expone detalladamente en párrafos siguientes.

El Ciclo de Evaluación de Vulnerabilidades se puede definir como un proceso continuo y estructurado que se utiliza para evaluar la seguridad de un sistema de información, esta metodología implica varios pasos interconectados que abordan la identificación, evaluación y mitigación de vulnerabilidades. Los pasos clave en esta metodología incluyen:

Identificación de activos: En esta etapa, se enumeran y se identifican todos los activos críticos dentro de una organización, como servidores, aplicaciones, bases de datos, dispositivos de red, etc. Esto proporciona una visión completa de lo que se necesita proteger.

Recopilación de información: Se reúne información técnica detallada sobre los activos identificados, incluyendo versiones de software, configuraciones y arquitectura de red.

Descubrimiento de vulnerabilidades: Se utilizan herramientas de escaneo y evaluación de vulnerabilidades para buscar debilidades en los activos, incluyendo vulnerabilidades conocidas, debilidades de configuración y fallos de seguridad.

Clasificación de vulnerabilidades: Las vulnerabilidades se clasifican en función de su gravedad y se priorizan según criterios específicos, como el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS).

Evaluación de riesgos: Se evalúan los riesgos asociados con cada vulnerabilidad, considerando la gravedad de la vulnerabilidad, la probabilidad de explotación y las posibles consecuencias para la organización.

Remediación o mitigación: Se toman medidas para remediar o mitigar las vulnerabilidades identificadas. Esto puede incluir la aplicación de parches, cambios en la configuración o la implementación de medidas de seguridad adicionales.

Verificación y validación: Después de realizar las correcciones, se realizan pruebas para asegurarse de que las vulnerabilidades se han solucionado de manera efectiva.

Informe y documentación: Se documentan todas las etapas del ciclo de evaluación de vulnerabilidades, incluyendo los activos, las vulnerabilidades identificadas, las acciones tomadas y los resultados de la verificación.

Monitoreo continuo: La seguridad de la información es un proceso en constante evolución. Por lo tanto, se debe monitorear regularmente el entorno de TI en busca de nuevas vulnerabilidades y amenazas. Esto implica repetir el ciclo de evaluación de vulnerabilidades de manera periódica.

Como conclusión se puede afirmar que la metodología denominada el Ciclo de Evaluación de Vulnerabilidades es una metodología fundamental en la gestión de la seguridad de la información. Ayuda a las organizaciones a identificar y abordar las debilidades en sus sistemas de manera estructurada y eficiente, la seguridad de la información es un campo en constante evolución, y esta metodología permite a las organizaciones adaptarse a las amenazas cambiantes y proteger sus activos críticos.

6 FASE 1: IDENTIFICACION Y CONCEPTUALIZACION DE LOS TIPOS DE VECTORES DE ATAQUE

6.1 ESTADO DEL ARTE DE LOS VECTORES DE ATAQUE PREVALENTES EMPLEADOS POR LOS CIBERDELINCUENTES

Con el fin de desarrollar la temática propuesta en la presente monografía visualiza el estado del arte de los vectores de ataque típicos que afectan los sistemas transaccionales, ahora, se propone redefinir a partir de la teoría y bibliografías encontradas los conceptos de este tipo de vectores. Vector de ataque. Un método utilizado por los atacantes para explotar una vulnerabilidad en un sistema informático o en una red. Según Nelson y Phillips, los vectores de ataque son "las formas en que los atacantes aprovechan las debilidades de un sistema para lograr sus objetivos malintencionados"[78]. Los vectores de ataque pueden variar, desde técnicas simples, como el *phishing*, hasta métodos más complejos, como la explotación de vulnerabilidades en el *software*. De acuerdo con el NIST (Instituto Nacional de Estándares y Tecnología), los vectores de ataque se refieren a la "forma específica en que un ataque se lleva a cabo"[79]. Estos pueden incluir la explotación de una debilidad en un sistema o red, o la manipulación del comportamiento del usuario para lograr acceso no autorizado. Concluyendo la definición, los vectores de ataque son técnicas utilizadas por los atacantes para explotar debilidades en los sistemas y redes con el fin de lograr acceso no autorizado o causar daño. Estos vectores pueden variar en complejidad y sofisticación, y es importante que los usuarios y administradores de sistemas estén al tanto de los diferentes tipos de vectores de ataque para poder tomar medidas preventivas y mitigar los riesgos de seguridad.

[78] Vectores de ataque habituales | BCSC. **{En línea}**. {12 Mayo de 2023}. Disponible en: (https://www.ciberseguridad.eus/ciberpedia/vulnerabilidades/vectores-de-ataque-habituales)

[79] OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf. **{En línea}**. {12 Mayo de 2023}. Disponible en: (https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf)

6.1.1 El correo electrónico y la mensajería instantánea. Se han convertido en vectores de ataque comunes en el mundo digital de hoy. Según un informe de Verizon (2020),[80] el correo electrónico sigue siendo la principal fuente de ataques de *phishing*, y el 96% de los ataques de correo electrónico en 2020 se clasificaron como *phishing*. Los atacantes utilizan el correo electrónico para enviar mensajes de *phishing* que parecen legítimos, con el objetivo de engañar a los usuarios para que compartan información confidencial o hagan clic en enlaces maliciosos. La mensajería instantánea también puede ser utilizada para lanzar ataques. Los atacantes pueden enviar mensajes maliciosos a través de aplicaciones de mensajería instantánea, que contienen enlaces maliciosos o archivos adjuntos infectados. Cuando los usuarios hacen clic en estos enlaces o descargan estos archivos, su dispositivo puede verse comprometido. Para protegerse contra estos vectores de ataque, es importante tener precaución al interactuar con correos electrónicos y mensajes de mensajería instantánea. Verificar la dirección de correo electrónico del remitente y analizar cuidadosamente los enlaces y archivos adjuntos antes de interactuar con ellos puede ayudar a evitar posibles ataques. Además, es importante mantener las aplicaciones de correo electrónico y mensajería instantánea actualizadas y utilizar herramientas de seguridad, como antivirus y *software* de prevención de *phishing*. En resumen, el correo electrónico y la mensajería instantánea son vectores de ataque comunes en la actualidad digital. Los usuarios deben ser conscientes de los posibles riesgos y tomar medidas de precaución para protegerse contra los ataques. La navegación web. Es un vector de ataque común y una de las principales formas en que los ciberdelincuentes pueden comprometer la seguridad en línea de un usuario. Según un informe de Symantec (2020), los sitios web maliciosos aumentaron en un 56% en 2020 en comparación con el año anterior. Además, el informe destaca que "los ataques de inyección de código malicioso (MCI) en sitios web han aumentado en más del 20%".[81]

Las aplicaciones web, Portales corporativos, intranets y redes sociales. Son vectores de ataque que utilizan los ciberdelincuentes y pueden comprometer la seguridad de una organización. Según un informe de Positive Technologies (2020), "las aplicaciones web y las redes sociales son los vectores de ataque más comunes para las empresas".[82] Los sitios web maliciosos pueden tomar formas diferentes. Pueden ser falsos y diseñados para parecerse a sitios web legítimos, o sitios web legítimos que han sido comprometidos por los atacantes. Los atacantes también pueden insertar código malicioso en los sitios web, como scripts o *malware,* que pueden infectar automáticamente los dispositivos de los usuarios

[80] SENTINELONE. Informe de Verizon sobre investigaciones de fugas de datos 2020 – Guía rápida para los CISO. **SentinelOne ES {Blog En línea}**. 2020. {12 Mayo de 2023}. Disponible en: (https://es.sentinelone.com/blog/the-cisos-quick-guide-to-verizons-2020-data-breach-investigations-report/)

[81] (Symantec, 2020)

[82] **(Positive Technologies, 2020).**

que visitan el sitio web. Una forma de protegerse contra los sitios web maliciosos es utilizar herramientas de seguridad en línea. Por ejemplo, un navegador con una función de detección de *phishing* puede alertar al usuario si están navegando en un sitio web sospechoso. Además, los usuarios pueden utilizar *software* de seguridad, como un antivirus o una solución de seguridad en línea, que pueden bloquear sitios web maliciosos y proteger contra ataques de inyección de código malicioso.

6.1.2 Los EndPoins, Reconocidos como dispositivos finales, se convierten en un vector de ataque común utilizado por los ciberdelincuentes para comprometer la seguridad de una organización. Según un informe de CrowdStrike (2021), "los dispositivos finales representan uno de los vectores de ataque críticos que los adversarios utilizan para llevar a cabo ataques".83 Estos pueden incluir una variedad de dispositivos, como computadoras de escritorio, portátiles, teléfonos móviles y tabletas. Los atacantes pueden utilizar diferentes técnicas para comprometer la seguridad, entre éstas se mencionan: la explotación de vulnerabilidades de software, el uso de ataques de phishing para engañar a los usuarios para que descarguen y ejecuten malware en sus dispositivos. Una forma de protegerse contra los ataques de EndPoins es utilizar software de seguridad, como un antivirus o una solución de seguridad en línea. Además, las organizaciones pueden implementar políticas de seguridad y realizar entrenamientos regulares para educar a los usuarios sobre las mejores prácticas de seguridad y cómo evitar ataques. Por último, los EndPoins son un vector de ataque común y crítico utilizado por los ciberdelincuentes. Es importante que las organizaciones y los usuarios individuales estén conscientes de los posibles riesgos y tomen medidas de precaución para protegerse contra los ataques.

[83] **(CrowdStrike, 2021)**

6.1.3 el *software* de redes y sistemas mal configurados. desactualizado o no parcheado. Puede ser utilizado para comprometer la seguridad de una organización. Según un informe de Verizon (2021), "la falta de parches y actualizaciones oportunas sigue siendo una de las principales causas de las violaciones de seguridad en las organizaciones".[84] Los atacantes pueden aprovecharse de las vulnerabilidades en el *software* de redes y sistemas para acceder a información confidencial o tomar el control de los sistemas. Las organizaciones deben asegurarse de tener políticas y procesos claros para mantener su *software* actualizado y parcheado, y garantizar que todos los sistemas de red y dispositivos estén configurados correctamente. Para protegerse contra los ataques a través de este vector, es importante que las organizaciones implementen medidas de seguridad, como el monitoreo constante de los sistemas de la red y la implementación de políticas de seguridad. Además, es importante que los empleados estén capacitados para reconocer y evitar los ataques a través de *software* mal configurado, desactualizado o no parcheado. Las credenciales de usuario comprometidas. Son un vector de ataque que permiten al ciberdelincuente acceder a los sistemas y datos de una organización. Según un informe de Microsoft (2020), "en la mayoría de los casos, los ataques a las organizaciones son el resultado de credenciales de usuario comprometidas".[85] Los atacantes pueden obtener las credenciales de usuario a través de métodos como *phishing*, ingeniería social o la explotación de vulnerabilidades en el *software* utilizado por la organización. Una vez que los atacantes tienen acceso a las credenciales de usuario, pueden acceder a los sistemas y datos de la organización, lo que puede resultar en la pérdida de información confidencial o daños financieros. Para protegerse contra los ataques a través de este vector, es importante que las organizaciones implementen medidas de seguridad, como la autenticación multifactorial y la implementación de políticas de contraseñas seguras. Además, es importante que los empleados estén capacitados para reconocer y evitar los ataques de *phishing* y la ingeniería social. Las contraseñas y credenciales predecibles o por defecto. Se consideran un vector de ataque utilizado por los ciberdelincuentes para acceder a los sistemas y datos de una organización. Según un informe de Verizon (2021), "el uso de contraseñas predecibles o débiles sigue siendo uno de los principales problemas de seguridad en las organizaciones".[86] Los atacantes pueden aprovecharse de las contraseñas y credenciales predecibles o por defecto para acceder a sistemas y datos confidenciales. Muchos dispositivos y sistemas vienen con contraseñas preestablecidas que son fáciles de adivinar o están ampliamente conocidas por los atacantes. Para protegerse contra los ataques a través de este vector, es importante que las organizaciones implementen políticas de contraseñas seguras y cambien regularmente las contraseñas predeterminadas en todos los dispositivos y sistemas. Además, es importante que los empleados estén capacitados para crear contraseñas seguras

[84] **(Verizon, 2021).**
[85] **(Microsoft, 2020)**
[86] **(Verizon, 2021).**

y evitar el uso de contraseñas predecibles o débiles. Los *insiders*. Son un vector de ataque interno que puede ser especialmente peligroso, ya que los atacantes ya tienen acceso a los sistemas y datos de la organización. Según un informe de IBM (2020), "el 60% de todos los ataques cibernéticos son perpetrados por actores internos".[87] Los *insiders* pueden incluir empleados descontentos, contratistas o incluso socios de negocios que tienen acceso a los sistemas de la organización. Estos atacantes pueden utilizar su acceso para robar información confidencial o causar daños a los sistemas de la organización. Para protegerse contra los ataques a través de este vector, es importante que las organizaciones implementen políticas de seguridad y supervisión adecuadas. Esto incluye la implementación de controles de acceso adecuados, el monitoreo de los registros de actividad del sistema y la capacitación regular de los empleados sobre los riesgos de la seguridad cibernética. El cifrado. El cifrado es una herramienta clave para proteger la confidencialidad y la privacidad de los datos en línea. Sin embargo, las carencias en el cifrado pueden dejar los datos expuestos a posibles ataques. Un ejemplo de esto es el ataque *"man-in-the-middle"*, donde un atacante intercepta la comunicación entre dos partes y puede leer o alterar la información. Según un informe de la firma de seguridad cibernética F5 *Networks (2020)*, "el 50% de las vulnerabilidades de cifrado detectadas son causadas por una configuración incorrecta o por el uso de versiones antiguas o inseguras de protocolos criptográficos".[88] Esto demuestra la importancia de tener una configuración adecuada y actualizada del cifrado para evitar posibles vulnerabilidades. Otro ejemplo de carencia en el cifrado es el uso de contraseñas débiles o predecibles para proteger los datos cifrados. Según un informe de Verizon (2020), "el 80% de la violación de datos involucra el uso de contraseñas débiles o robadas".[89] Esto demuestra la importancia de utilizar contraseñas seguras y cambiarlas regularmente para proteger los datos cifrados. La cadena de suministro. Las cadenas de suministro se refieren a todas las actividades involucradas en la producción y distribución de bienes y servicios. Sin embargo, las debilidades en la cadena de suministro pueden ser explotadas por los atacantes para comprometer la seguridad de una organización. Una de las debilidades comunes en la cadena de suministro es el uso de *software* o hardware de terceros que pueden contener vulnerabilidades o puertas traseras que permiten a los atacantes acceder a la red de la organización. Según un informe de Symantec (2019), "el 71% de las organizaciones encuestadas experimentaron una violación de seguridad como resultado de una cadena de suministro comprometida".[90] Además, los atacantes pueden comprometer a un proveedor o socio comercial de la organización para acceder a sus sistemas y datos. Un

[87] **(IBM, 2020).**
[88] **(F5 Networks, 2020)**
[89] **(**SENTINELONE. Informe de Verizon sobre investigaciones de fugas de datos 2020 – Guía rápida para los CISO. **SentinelOne ES {Blog En línea}**. 2020. {12 Mayo de 2023}. Disponible en: (https://es.sentinelone.com/blog/the-cisos-quick-guide-to-verizons-2020-data-breach-investigations-report/)
[90] **(Symantec, 2019)**

ejemplo de esto es el ataque a Target en 2013, donde los atacantes obtuvieron acceso a los sistemas de la compañía a través de un proveedor de servicios de calefacción y aire acondicionado. Para mitigar las debilidades en la cadena de suministro, es importante implementar medidas de seguridad como la verificación y validación de los proveedores, la auditoría de sus sistemas y el monitoreo constante de los posibles riesgos. También es esencial establecer un plan de respuesta a incidentes para actuar rápidamente en caso de una violación de seguridad.

6.2 GENERALIDADES DE LOS SISTEMAS TRANSACCIONALES

Un sistema transaccional concebido como la plataforma de *software* que fue diseñada para gestionar y procesar transacciones financieras, como compras, ventas, pagos y transferencias de fondos, este tipo de sistemas son ampliamente utilizados en la industria financiera, tanto en entornos empresariales como personales; De acuerdo con O'Brien y Marakas[91] (2011), un sistema transaccional tiene como propósito procesar y almacenar información de transacciones financieras, así como en garantizar la integridad y la precisión de los datos en tiempo real. Por otro lado, Laudon y Laudon (2016),[92] explican que un sistema transaccional es un componente clave de los sistemas de información empresarial, que ayuda a las organizaciones a administrar y controlar sus operaciones financieras, Además, un sistema transaccional puede integrarse con otros sistemas, como sistemas de contabilidad, sistemas de gestión de inventario y sistemas de gestión de recursos humanos, esta integración ayuda a las organizaciones a tener una visión completa de sus operaciones y a tomar decisiones informadas basadas en datos precisos y actualizados. Un sistema transaccional es una herramienta crucial para las organizaciones que necesitan procesar y gestionar transacciones financieras de manera eficiente y precisa, a través de su integración con otros sistemas empresariales, ayuda a las organizaciones a mejorar su productividad y su capacidad para tomar decisiones; Para diferenciar un sistema transaccional se establecen sus características generales de ahí que este tipo de sistemas corresponden a una aplicación que permite a los usuarios interactuar con una base de datos a través de operaciones de transacción, en que se definen una unidad lógica de trabajo que se realiza en la base de datos. Según Silberschatz, Korth y Sudarshan (2010), ***"una transacción es una secuencia de operaciones que se ejecutan como una sola unidad de trabajo, de tal manera que se garantiza la integridad de los datos".***[93] Entre las

[91] O'BRIEN, J. A., & MARAKAS, G. M. Management Information Systems. McGraw-Hill Education, 2011.

[92] LAUDON, K. C., & LAUDON, J. P. Management Information Systems: Managing the Digital Firm. Pearson Education. 2016.

[93] SILBERSCHATZ, A., KORTH, H. F. & SUDARSHAN, S. Database system concepts. McGraw-Hill Education, 2010.

características de un sistema transaccional, se pueden destacar la atomicidad, las transacciones se ejecutan como una unidad atómica, es decir, se realizan todas las operaciones de la transacción o ninguna. Como señalan Silberschatz et al. (2010), "El resultado de una transacción debe ser una base de datos consistente y válida"[94]. Otra característica es la consistencia, ésta permite que la base de datos debe permanecer en un estado consistente antes y después de la ejecución de una transacción; si una transacción no cumple con los requisitos de consistencia, se debe revertir a su estado anterior; De igual manera se caracteriza por el aislamiento, en este aspecto las transacciones deben ejecutarse de forma aislada, lo que significa que el resultado de una transacción no debe afectar a otras transacciones en ejecución; Por último, la durabilidad, permite que una vez que una transacción se ha completado correctamente, sus cambios deben ser permanentes y duraderos, incluso en caso de falla del sistema.

6.2.1 Componentes de un sistema transaccional. También reconocido como un sistema de base de datos que se utiliza para gestionar transacciones, el sistema transaccional consta de varios componentes que trabajan juntos para procesar y administrar transacciones; Algunos de los componentes del sistema transaccional incluyen elementos básicos como el gestor de transacciones, se considera el componente central de un sistema transaccional, es responsable de iniciar, procesar y completar transacciones. Según Elmasri y Navathe (2010), afirma que "el gestor de transacciones es el componente responsable de controlar el acceso a la base de datos y garantizar la integridad de las transacciones"[95]. El bloqueo de transacciones se reconoce como un mecanismo utilizado para controlar el acceso concurrente a la base de datos, los bloqueos se utilizan para garantizar que las transacciones no interfieran entre sí. Según Silberschatz, Korth y Sudarshan (2010), "los bloqueos se utilizan para controlar el acceso a la base de datos y garantizar que las transacciones no interfieran entre sí"[96]. Otro elemento constitutivo del sistema transaccional es el control de concurrencia, se compone de un conjunto de técnicas utilizadas para garantizar que las transacciones se ejecuten de manera aislada y segura. El control de concurrencia se basa en el bloqueo de transacciones y en otras técnicas de coordinación. Según Ramakrishnan y Gehrke (2003), ***"el control de concurrencia se utiliza para garantizar que las transacciones se ejecuten de manera segura y aislada."***[97]

---

[94] Silberschatz et al. 2010

[95] ELMASRI, R. & NAVATHE, S. B. Fundamentals of database systems. Pearson Education India. 2010.

[96] Silberschatz et al. 2010

[97] RAMAKRISHNAN, R., & GEHRKE, J. Database management systems. McGraw-Hill Education. 2003.

Por último, se encuentra el registro de transacciones el cual determina una técnica utilizada para garantizar la durabilidad de las transacciones. El registro de transacciones se utiliza para registrar todas las operaciones realizadas en la base de datos, de manera que, si ocurre una falla del sistema, se pueden recuperar los datos de la última transacción. Según Elmasri y Navathe (2010), ***"el registro de transacciones se utiliza para garantizar la durabilidad de las transacciones, de manera que, si ocurre una falla del sistema, los datos pueden recuperarse de la última transacción".***[98]

6.3 SISTEMAS TRANSACCIONALES VULNERADOS POR VECTORES DE ATAQUE.

Para realizar un análisis de los sistemas transaccionales atacados, es difícil debido a que las empresas no comparten este tipo de información, en este campo la información existente no es relevante, se presume que las empresas vulneradas no quieren "perder prestigio ante sus usuarios", se infiere que es una de las razones de mayor peso para no compartir o publicar dicha información. Pero de manera general se tienen noticias de las siguientes empresas u organizaciones que han sido vulnerados por acción de los vectores de ataque. En Colombia según (Infobae, 2023), se puede mencionar que "En total fueron 34 las empresas que sufrieron una situación así, o por lo menos el número de los que se conocieron, ya que la mayoría no cuenta o logran pasar desapercibidas debido a la mala reputación que trae el conocer que hubo un ataque cibernético de cualquier tipo" (Infobae, 2023).[99] De igual manera, afirma Infobae (2023), que al terminar el 2022 los ataques informáticos a empresas colombianas tuvo éxito en varios casos entre los que se pueden mencionar el de la empresa Keralty, que fue víctima de accesos no autorizados y pierde documentación importante de sus usuarios, entre estos documentos se destacan las historias clínicas, este caso el director ejecutivo de la empresa afirma que la "prioridad es restablecer nuestros servicios y cuidar a la gente" y que lamentan "profundamente las consecuencias que esto ha tenido para nuestros usuarios; cuentan con nuestro compromiso para el restablecimiento de nuestro sistema".[100] Se registra que la empresa EPM fue víctima de un grupo de piratas informáticos que afectaron servicios de pago en línea durante quince días; así mismo, se menciona que el canal caracol fue afectado por la delincuencia informática generando afectación en programas de grabación y diseño y sistemas operativos de la empresa, en 2013, la cadena de tiendas Target sufrió un ataque

[98] ELMASRI, R. & NAVATHE, S. B. Fundamentals of database systems. Pearson Education India. 2010

[99] Infobae. (2 de enero de 2023). infobae. Recuperado el 14 de abril de 2023, de: (https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/)

[100] Ibíd., p. s

en su sistema transaccional que afectó a más de 40 millones de tarjetas de crédito de sus clientes, en este evento los atacantes hurtan información personal y financiera de los clientes. En 2014, Sony Pictures fue víctima de un ataque cibernético que afectó a su sistema transaccional, los atacantes lograron acceder a información personal de los empleados, como números de seguridad social y direcciones, así como a información financiera; en 2017, Equifax, una de las tres principales agencias de informes crediticios de Estados Unidos, sufrió un ataque que afectó a más de 147 millones de clientes. Los atacantes robaron información personal y financiera, incluyendo números de seguridad social y números de tarjetas de crédito; en 2018, Marriott International anunció que había sufrido un ataque en su sistema transaccional que afectó a más de 500 millones de clientes. Los atacantes lograron acceder a información personal, como nombres, direcciones y fechas de nacimiento, así como a información financiera; en 2019, la empresa de tarjetas de crédito *Capital one* anunció que había sufrido un ataque que afectó a más de 100 millones de clientes. Los atacantes lograron acceder a información personal y financiera, incluyendo números de seguridad social y números de cuentas bancarias; en 2022, se conoce que la empresa prestadora de salud Sánitas fue víctima de un ataque informático que logró tumbar los servicios en línea de la empresa por más de 48 horas como se menciona en noticia de la revista semana[101] fueron muchos de los usuarios perjudicados debido a que no tenían acceso al sistema para agendar consultas, ni para mirar los resultados de algunos exámenes que comúnmente se entregan Online; en el año 2023 existe evidencia de ataques cibernéticos destacándose el ataque a los ayuntamientos de Bizkaia, según lo informado por la agencia eitb[102] no se trata de un ataque efectivo sino de un intento de ataque, pero en la realidad los servicios de informáticos de estos ayuntamientos fueros suspendidos, lo cual configura un ataque de denegación de servicios. Después de los casos mencionados anteriormente, se pretende realizar la revisión de los casos representativos de ciberataque tratando de establecer el vector de ataque empleado, la vulnerabilidad explotada, y los efectos que produjo dicho evento.

Caso 1. Ataque a Audifarma, el ataque cibernético a la infraestructura tecnológica de una entidad comercializadora de medicamentos, Según el comunicado emitido por la empresa, fueron víctimas de un ataque informático externo y activaron sus

[101]SEMANA. Gravísimo: EPS Sanitas confirmó que fue víctima de un potente ciberataque; mientras, pacientes inundan las redes de quejas y hay aglomeraciones en centros. **Semana.com Últimas Noticias de Colombia y el Mundo. {En línea}.** 2022. {12 Mayo de 2023}. Disponible en: (https://www.semana.com/salud/articulo/la-eps-sanitas-confirmo-que-fue-victima-de-un-ciberataque-los-pacientes-inundan-las-redes-de-quejas/202228/)

[102] EITB. El intento de ciberataque afecta a 107 de los 112 ayuntamientos de Bizkaia. **EITB {En línea}.** 2023. {12 Mayo de 2023}. Disponible en: (https://www.eitb.eus/es/noticias/sociedad/detalle/9093283/el-intento-de-ciberataque-afecta-a-107-de-112-ayuntamientos-de-bizkaia/)

protocolos de seguridad para contener la afectación y restablecer los sistemas, como resultado los servicios digitales y la aplicación móvil de Audifarma fueron temporalmente deshabilitados, aunque la entrega de medicamentos continuó sin interrupciones; expertos en ciberseguridad consultados, entre ellos “Hernando José Peña Hidalgo, ingeniero y analista del Centro de Respuesta a Incidentes de Seguridad Informática CSIRT Académico UNAD”[103] explicaron que el ataque posiblemente se realizó utilizando la técnica de denegación de servicios, que busca limitar el acceso a la información o explotar vulnerabilidades en el sistema, Aunque Audifarma no ha confirmado el robo o fuga de información de los usuarios, en este tipo de ataques los ciberdelincuentes suelen sustraer bases de datos, lo que representa un riesgo para los usuarios cuyos datos personales estén almacenados en las plataformas de la marca; se menciona que los *ciberdelincuentes* pueden utilizar la información robada para extorsionar a la entidad atacada exigiendo pagos para evitar la divulgación de los datos o vender la información en el mercado negro. Además, existe la posibilidad de que los datos terminen en manos de otros delincuentes que los utilicen para realizar estafas o acceder a las plataformas digitales de las víctimas; en el artículo de la revista semana también aborda las posibles razones detrás de los ciberataques, incluyendo brechas de seguridad en la infraestructura tecnológica de la organización y acciones negligentes del personal o falta de conocimiento en ciberseguridad por parte de los usuarios. Se resalta la importancia de fortalecer las capacidades de identificación, detección, contención, respuesta y recuperación ante incidentes informáticos, tanto por parte de las organizaciones como de los usuarios individuales; aunque no se ha confirmado la identidad del grupo responsable del ataque, expertos sugieren que podría estar relacionado con otros ataques cibernéticos en el sector salud, se destaca el aumento de los ataques de *ransomware* en Colombia y América Latina, y se enfatiza la necesidad de tomar medidas de ciberseguridad para proteger los datos personales y prevenir futuros ataques; Un aspecto importante que se debe aclarar en el análisis del caso 1, es determinar si Audifarma corresponde a una Infraestructura transaccional, y en este punto se deduce que es una entidad comercializadora de medicamentos, en el artículo no se detalla específicamente la infraestructura. Sin embargo, es posible inferir algunos aspectos generales sobre su infraestructura tecnológica considerando el contexto y las prácticas comunes en el sector; Como empresa que ofrece servicios digitales y una aplicación móvil, Audifarma probablemente cuenta con una infraestructura tecnológica que incluye servidores, sistemas de almacenamiento de datos y redes de comunicación, estos componentes permiten el funcionamiento de sus plataformas digitales y la gestión de la información relacionada con la comercialización de medicamentos; en cuanto a la arquitectura

[103] SEMANA. Hackeo a Audifarma: además de largas filas y demoras en servicios, ¿qué otras afectaciones podrían enfrentar sus usuarios?,. **Semana.com Últimas Noticias de Colombia y el Mundo. {En línea}.** 2022. {12 Mayo de 2023}. Disponible en: (https://www.semana.com/tecnologia/articulo/hackeo-a-audifarma-ademas-de-largas-filas-y-demoras-en-servicios-que-otras-afectaciones-podrian-enfrentar-sus-usuarios/202302/)

tecnológica, es probable que Audifarma emplee un enfoque basado en la nube, lo que implica utilizar servicios y recursos de computación remotos a través de internet, esto le proporcionaría flexibilidad y escalabilidad en el manejo de sus operaciones y datos; es importante destacar que, para garantizar la seguridad de su infraestructura tecnológica, Audifarma debería contar con medidas de protección adecuadas como la de incluir sistemas de detección y prevención de intrusiones, *firewall*s, sistemas de cifrado para proteger los datos sensibles, políticas de acceso y autenticación robustas, así como protocolos de seguridad y continuidad del negocio; en términos de *software*, Audifarma podría utilizar aplicaciones personalizadas para gestionar sus operaciones comerciales, como el control de inventario, la gestión de pedidos y la administración de clientes, además, probablemente implemente sistemas de gestión de bases de datos para almacenar y organizar la información relevante para sus servicios y operaciones, es importante destacar que esta descripción de la infraestructura tecnológica de Audifarma es una suposición basada en el contexto general y las prácticas comunes en la industria farmacéutica y el comercio electrónico; asumiendo que existe la intervención de hardware y *software*, además se manifiesta la existencia de una aplicación móvil y permite el comercio electrónico, sin duda se configura un sistema transaccional. Teniendo en cuenta que en el caso 1 no se detalla información sobre el vector de ataque específico empleado contra Audifarma se menciona que generalmente este tipo de acciones se ejecutan mediante la implementación del vector de ataque de denegación de servicios, La denegación de servicios (DDoS, por sus siglas en inglés) es un tipo de ataque cibernético en el cual los perpetradores intentan sobrecargar los sistemas y recursos de una organización impidiendo que los usuarios legítimos accedan a los servicios y aplicaciones; si bien no se especifica cómo se llevó a cabo el ataque en el caso de Audifarma, es común que los ataques DDoS se realicen mediante el envío masivo de tráfico falso o solicitudes de conexión a los servidores de la organización, lo que provoca una saturación de los recursos y afecta el rendimiento y disponibilidad de los servicios en línea; Además del ataque DDoS, existen otros vectores de ataque comunes que podrían haber sido utilizados contra Audifarma, aunque no se mencionan directamente en el artículo, se presume que estos vectores de ataque podrían incluir la ingeniería social, en donde los ciberdelincuentes podrían haber utilizado técnicas de manipulación psicológica para engañar a los empleados de Audifarma y obtener acceso no autorizado a la infraestructura tecnológica o información confidencial; el *phishing* pudo ser utilizado por los *hackers* para enviar correos electrónicos falsos o mensajes de texto que parecen legítimos para engañar a los usuarios y obtener sus credenciales de acceso o información confidencial; las vulnerabilidades del *software* podrían ser un vector de ataque, si Audifarma utiliza *software* desactualizado o tiene sistemas con vulnerabilidades conocidas, los atacantes podrían haber aprovechado esas vulnerabilidades para infiltrarse en la infraestructura y comprometer la seguridad de la empresa; el uso de *malware* pudo ser utilizado por los ciberdelincuentes haciendo circular *malware* a través de correos electrónicos infectados, descargas maliciosas o sitios web comprometidos;

el *malware* podría haber sido diseñado para robar información, obtener acceso no autorizado o interrumpir el funcionamiento de los sistemas; es importante tener en cuenta que esta descripción de los posibles vectores de ataque se basa en suposiciones y en los métodos comúnmente utilizados por los *hackers*. La información precisa sobre el vector de ataque empleado contra Audifarma requeriría una investigación detallada y específica del incidente. En conclusión, el ataque a Audifarma, subraya la urgente necesidad de fortalecer las defensas cibernéticas en todas las organizaciones. La falta de información detallada sobre el vector de ataque específico enfatiza la complejidad de las amenazas actuales, lo que destaca la importancia de abordar los aspectos generales de la ciberseguridad, desde la protección de datos hasta la capacitación del personal. Solo mediante un enfoque integral y proactivo se podrán mitigar los riesgos y salvaguardar la integridad de las operaciones digitales en el mundo empresarial actual. El nivel de afectación de la implementación del vector de ataque de denegación de servicios en Audifarma tuvo un impacto significativo en la organización y sus usuarios, este incidente cibernético ha expuesto las vulnerabilidades en la infraestructura tecnológica de la empresa lo que ha generado múltiples afectaciones en diferentes aspectos; la interrupción de los servicios digitales de Audifarma ha causado inconvenientes y molestias para los usuarios, las plataformas en línea y la aplicación móvil han sido temporalmente deshabilitadas, lo que impide a los usuarios acceder a los servicios y realizar sus transacciones de manera eficiente, consecuencia de ello fue evidente las largas filas y demoras en la entrega de medicamentos, afectando la experiencia del cliente y su confianza en los servicios de la empresa; las molestias a corto plazo representadas en la preocupación legítima sobre la seguridad de los datos personales de los usuarios, aunque Audifarma no ha confirmado la fuga o robo de información la posibilidad de que los ciberdelincuentes hayan accedido a los datos de los usuarios es una amenaza latente, esto puede poner en riesgo la privacidad de los clientes y exponerlos a posibles fraudes, estafas o suplantación de identidad; la incertidumbre en torno a la acción de los *hackers* genera preocupación y desconfianza en la capacidad de Audifarma para proteger la información confidencial de sus usuarios; además, el impacto financiero también es una consecuencia importante de este ataque cibernético. Audifarma ha tenido que destinar recursos significativos para contener la afectación y restablecer los sistemas. Esto implica gastos adicionales en medidas de seguridad, investigación forense y posibles compensaciones a los usuarios afectados estos costos pueden tener un impacto negativo en las finanzas de la empresa y en su capacidad para invertir en otras áreas importantes, como la mejora de los servicios o la innovación tecnológica; otro aspecto para considerar es el daño a la reputación de Audifarma, la divulgación pública de este incidente puede socavar la confianza de los usuarios, los socios comerciales y la comunidad en general hacia la empresa, la percepción de una infraestructura tecnológica vulnerable y una respuesta inadecuada a la amenaza pueden tener consecuencias a largo plazo en la relación de la empresa con sus diferentes partes interesadas; para finalizar, la implementación del vector de ataque empleado contra Audifarma ha tenido un

nivel de afectación significativo en términos de interrupción de servicios, preocupaciones sobre la seguridad de los datos, impacto financiero y daño a la reputación. Este incidente destaca la importancia crítica de la ciberseguridad y la necesidad de que las organizaciones inviertan en medidas de protección robustas para salvaguardar la información y mantener la confianza de sus usuarios. Asimismo, resalta la importancia de una respuesta rápida y efectiva ante los incidentes cibernéticos para minimizar los impactos negativos en todos los aspectos de la organización.

Caso 2 ataque a *capital one*. Siendo uno de los principales bancos del mundo, sufrió un incidente de seguridad que comprometió los datos personales y financieros de más de 100 millones de usuarios en los Estados Unidos y Canadá, según los informes un hacker logró acceder a los servidores de la nube de Amazon donde *Capital one* almacenaba datos de sus clientes y copió información importante como nombres, direcciones, números de teléfono, direcciones de correo electrónico, fechas de nacimiento y números de seguridad social, el sospechoso, una ex ingeniera de *software* de Amazon identificada como Paige A. Thompson, fue detenida por las autoridades federales en julio de 2019 después de publicar información sobre el incidente en línea. Según el Departamento de Justicia de los Estados Unidos, Thompson se enfrenta a cargos de fraude electrónico y robo de datos informáticos; *Capital one* se disculpó públicamente por el incidente y se comprometió a trabajar para garantizar la seguridad de los datos de sus clientes. La empresa también ofreció servicios gratuitos de monitoreo de crédito y protección de identidad a las personas afectadas por el incidente; la situación de *Capital one* es un recordatorio para todas las empresas de la importancia de mantener una seguridad cibernética sólida y efectiva para proteger los datos de sus clientes. Las empresas deben tomar medidas para asegurar que sus sistemas y procesos sean resistentes a los ciberataques y estén preparadas para responder rápidamente en caso de una violación de seguridad. El vector de ataque en el caso del incidente de *Capital one* en 2019 fue una vulnerabilidad en el *firewall* de la nube que permitió a un pirata informático acceder a la información de más de 100 millones de clientes y solicitantes de la compañía. El atacante aprovechó una brecha en la configuración del *firewall* para acceder al servidor de almacenamiento de datos en la nube de *Amazon Web Services* (AWS), lo que le permitió acceder a información personal y financiera sensible, incluidas las solicitudes de tarjetas de crédito y los números de Seguridad Social; El incidente se produjo debido a una vulnerabilidad en el *firewall* de la nube de *Amazon Web Services* (AWS) de *Capital one*, un atacante pudo aprovechar esta vulnerabilidad para acceder a los datos personales de los clientes, incluyendo información de cuentas bancarias y números de seguridad social. Esto fue posible debido a un error en la configuración del *firewall*, que permitía al atacante saltarse los controles de acceso y obtener acceso a los datos sensibles. El atacante logró acceder a los datos de más de 100 millones de clientes de *Capital one*, lo que convierte a este incidente en uno de los mayores casos de ciberdelincuencia mediante la sustracción de datos en la historia informática moderna y actual de los Estados

Unidos. En el caso 2 se analiza que el vector de ataque corresponde a las configuraciones inadecuadas del *software*, la vulnerabilidad explotada en este caso fue un error en la configuración de un *firewall* de aplicación web (WAF, por sus siglas en inglés), que permitió a un atacante acceder y obtener acceso no autorizado a datos confidenciales de aproximadamente 100 millones de clientes; la vulnerabilidad en cuestión se originó en una configuración incorrecta del WAF, que es una medida de seguridad diseñada para proteger las aplicaciones web contra ataques comunes, en lugar de configurar el WAF para bloquear ciertos tipos de solicitudes o filtrar datos sensibles se estableció incorrectamente para permitir el acceso no autorizado a los datos almacenados en la nube; el atacante explotó esta configuración incorrecta enviando solicitudes especialmente diseñadas a través de una aplicación web vulnerable alojada en los servidores de *Capital one*, estas solicitudes permitieron al atacante acceder a información confidencial, como nombres, direcciones, números de seguridad social y números de cuentas bancarias, Además de la configuración incorrecta del WAF, se descubrió que también existían otras debilidades en los controles de seguridad que facilitaron el éxito del ataque, estas debilidades incluían una gestión inadecuada de los certificados de seguridad y una falta de monitoreo y detección temprana de actividades sospechosas; una vez que el atacante obtuvo acceso a los datos, utilizó técnicas de ocultación para evitar ser detectado y explotó la información robada para obtener beneficios personales, el incidente fue descubierto y reportado por un investigador de seguridad lo que llevó a la identificación y detención del atacante; el caso de *Capital one* destaca la importancia de una configuración adecuada de los sistemas de seguridad, así como la necesidad de implementar controles de seguridad sólidos y realizar auditorías y monitoreo continuo para detectar y responder a incidentes de seguridad de manera oportuna. En conclusión, el caso de Capital One destaca la necesidad crítica de una seguridad cibernética sólida y efectiva en un entorno digital en constante evolución, las empresas deben aprender de este incidente, fortaleciendo sus medidas de seguridad, implementando configuraciones adecuadas en sus sistemas y realizando auditorías periódicas, además, la colaboración entre el sector privado y las autoridades gubernamentales es esencial para abordar las amenazas cibernéticas de manera integral. Solo a través de estos esfuerzos conjuntos se podrá garantizar la protección de los datos sensibles y la seguridad de las operaciones en la era digital. El nivel de afectación de la implementación del vector de ataque configuración inadecuada de *software* dejó al descubierto la vulnerabilidad y los riesgos que enfrentan las instituciones financieras en la era digital, este incidente no solo puso en riesgo la información personal y financiera de aproximadamente 100 millones de clientes, sino que también expuso las deficiencias en la seguridad cibernética de una de las principales entidades financieras de Estados Unidos, el ataque fue significativo en el sentido que la confianza de los clientes en la institución se vio seriamente comprometida, la filtración de información personal sensible, como nombres, direcciones y números de seguridad social, generó una preocupación masiva sobre el potencial robo de identidad y el uso indebido de los datos, provocando que muchos clientes

perdieran la confianza en *Capital one*; además, el impacto financiero que tuvo que asumir debido a los costos asociados con el incidente, incluyendo investigaciones forenses, notificaciones a los clientes afectados y medidas de mitigación, estos gastos, sumados a las posibles demandas legales y las multas impuestas por las autoridades regulatorias, representaron un golpe significativo para la entidad financiera, la reputación de la compañía se vio dañada lo que podría afectar su capacidad para atraer nuevos clientes y mantener relaciones comerciales sólidas; el incidente de *Capital one* puso de manifiesto la importancia de la seguridad cibernética en el sector financiero y en todas las organizaciones que manejan datos sensibles, reveló deficiencias en los controles de seguridad, como una configuración errónea del *firewall* de aplicación web y una gestión inadecuada de los certificados de seguridad. Estas fallas demuestran la necesidad de inversiones continuas en seguridad cibernética, así como una mayor conciencia y capacitación de los empleados sobre las mejores prácticas de seguridad; concluyendo, el ataque cibernético afectó la confianza de los clientes, el impacto financiero y la reputación de la institución, el incidente destaca la importancia de la seguridad cibernética en la era digital y subraya la necesidad de una inversión continua en medidas de protección y una cultura de seguridad sólida en todas las organizaciones, solo a través de la adopción de prácticas de seguridad rigurosas y el fortalecimiento de las defensas cibernéticas se podrá mitigar el riesgo de futuros ataques y proteger los datos confidenciales de los clientes.

7 FASE 2: EVALUACION DE LAS VULNERABILIDADES EN LOS SISTEMAS TRANSACCIONALES

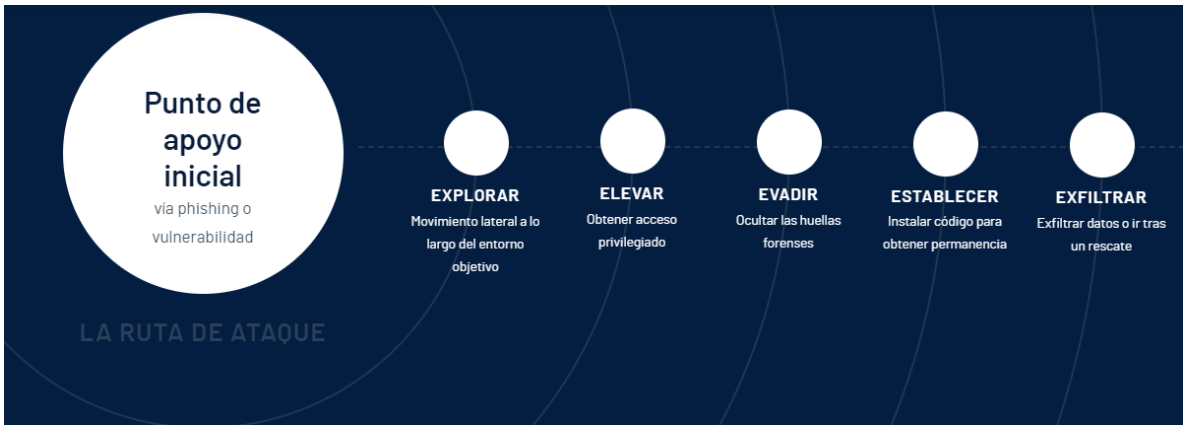
7.1 CARACTERISTICAS DE LOS VECTORES DE ATAQUE EMPLEADOS POR LOS CIBERDELINCUENTES

Como se menciona en el capítulo anterior es importante visibilizar y caracterizar los vectores de ataque implementados en el ataque a los sistemas transaccionales Audifarma y *capital one* donde los ciberdelincuentes lograron afectar significativamente estos sistemas.

De forma general se analiza las etapas de un ataque cibernético a cualquier sistema o red de servicios, en la ilustración se evidencia las etapas fundamentales de un ataque; donde el atacante recurriendo a la implementación de diferentes técnicas descubre un vector de ataque o evidencia una vulnerabilidad la cual explota mediante el uso de técnicas y metodologías de intrusión con el fin de escalar privilegios, acceder y comprometer el sistema y finalmente tomar el control y extraer información importante del sistema que en este caso se refiere a u sistema transaccional.

.

Ilustración 1 Etapas de un ataque a un sistema transaccional



Fuente 11. Tenable.ad. Tenable® [online]. [Consultado: 12 May 2023]. Disponible en: https://es-la.tenable.com/products/tenable-ad.

Si se hace referencia a un sistema transaccional la ilustración anterior sugiere la línea de acción para efectuar un ataque riguroso y exitoso.

7.1.1 Características generales del phishing. Es un vector de ataque que ha demostrado ser altamente efectivo en la actualidad. Según Doe (2019),[104] una de las características principales del *phishing* es el engaño y la suplantación de identidad, los atacantes se hacen pasar por entidades legítimas, utilizando logotipos y diseños similares para generar confianza en sus víctimas, esta táctica de engaño se basa en la psicología humana y busca aprovechar la credulidad de los usuarios.

En relación con esto, Smith (2018),[105] destaca la importancia de la ingeniería social en el *phishing*. Los atacantes utilizan estrategias psicológicas para manipular emocionalmente a las personas, generando un sentido de urgencia o amenazando con consecuencias negativas si no se toman medidas inmediatas. Esta forma de manipulación es clave para persuadir a los usuarios a revelar información confidencial.

Una de las formas más comunes de *phishing* es a través de correos electrónicos fraudulentos. Teniendo en cuenta a Johnson (2020),[106] los atacantes envían mensajes masivos no solicitados, conocidos como spam, a una amplia cantidad de destinatarios. Estos correos pueden contener enlaces maliciosos o archivos adjuntos infectados que, una vez abiertos, permiten a los atacantes acceder a los datos personales de los usuarios. Esta estrategia se basa en la falta de atención y el descuido de los usuarios al abrir correos electrónicos no deseados.

Además, el *phishing* se caracteriza por la creación de sitios web falsos que imitan la apariencia de sitios legítimos. Según Brown (2017),[107] los atacantes utilizan enlaces maliciosos para redirigir a los usuarios a estos sitios falsos, donde se les solicita ingresar información confidencial, como contraseñas o datos bancarios. Estos sitios son diseñados meticulosamente para ser visualmente similares a los originales, lo que dificulta su detección.

Es importante destacar que el *phishing* ha evolucionado con el tiempo. Referenciando a Green (2021),[108] los atacantes han desarrollado técnicas más sofisticadas, como el *spear phishing* y el *whaling*. El *spear phishing* se enfoca en objetivos específicos, como individuos o grupos, personalizando los mensajes para aumentar su efectividad. Por otro lado, el *whaling* se dirige a individuos de

---

[104] DOE, J. "El impacto del *phishing* en los sistemas transaccionales". **Revista de Seguridad Informática,** 2019. P. 15(2), 45-56.
[105] SMITH, A. La ingeniería social como táctica de *phishing*. 2018. En Congreso Internacional
[106] JOHNSON, M. "*Phishing* Attacks via Email: Techniques and Countermeasures". **International Journal of Information Security,** 2020. P. 15(2), 145-162.
[107] BROWN, R. "*Phishing*: Creating Fake Websites to Steal Personal Information". **Journal of Cybersecurity,** 2017. P. 10(3), 123-136.
[108] GREEN, A. "*Phishing* Evolution: From Simple Attacks to *Spear Phishing* and Whaling. **Journal of Computer Security,** 2021. P.12(4), 321-336.

alto nivel, como altos ejecutivos, quienes pueden tener acceso a información confidencial valiosa.

7.1.2 Características generales del ataque distribuido de denegación de servicios (DDOS). El ataque distribuido de denegación de servicios (DDoS, por sus siglas en inglés) es un vector de ataque que ha ganado notoriedad en el ámbito de la ciberseguridad. Según Smith (2018),109 este tipo de ataque se caracteriza por inundar un sistema o red con un flujo abrumador de tráfico, con el objetivo de sobrecargar sus recursos y dejarlo inaccesible para los usuarios legítimos. Los atacantes utilizan redes de bots, también conocidas como botnets, para coordinar y lanzar los ataques.

Los ataques DDoS han evolucionado en complejidad y magnitud en los últimos años. Atendiendo a lo expresado por Jones (2019),[110] los atacantes han empleado técnicas de amplificación, como el uso de servidores DNS abiertos o servidores de tiempo, para multiplicar la cantidad de tráfico dirigido hacia el objetivo. Estas técnicas permiten que los atacantes generen un tráfico mucho mayor al utilizar solicitudes legítimas de servicios públicos que responden con respuestas voluminosas.

Una característica clave del ataque DDoS es su capacidad para afectar tanto a las grandes organizaciones como a los sitios web individuales. Como menciona Thompson (2020),[111] los ataques DDoS pueden provocar interrupciones significativas en los servicios en línea, causando pérdidas económicas y daños a la reputación de las empresas. Además, los ataques DDoS pueden ser utilizados como una distracción para llevar a cabo otros ataques cibernéticos, como el robo de datos o el acceso no autorizado a sistemas.

Es importante destacar que la detección y mitigación de los ataques DDoS pueden resultar desafiantes. Según White (2017),[112] los atacantes pueden utilizar técnicas de enmascaramiento para ocultar el origen real del ataque, lo que dificulta la identificación de los responsables. Además, la magnitud y diversidad del tráfico generado por una *bot*net pueden hacer que la distinción entre tráfico legítimo y malicioso sea complicada.

---

[109] SMITH, J. "Understanding DDoS Attacks: Types, Vectors, and Mitigation Strategies". **International Journal of Information Security and Cybercrime,** 2018. P. 7(1), 15-22.

[110] JONES, A. "DDoS Attacks and Countermeasures: Trends, Challenges, and Opportunities". **Journal of Cybersecurity**, 2019. P.3(2), 123-136.

[111] THOMPSON, M. "Impacto y consecuencias de los ataques DDoS en las organizaciones". **Revista de Seguridad Informática**, 2020. P. 8(2), 45-56.

[112] WHITE, J. Mitigating Distributed Denial of Service Attacks. En S. J. Schmidt (Ed.), 2017. Advances in Digital Forensics XIII (pp. 129-142). Springer.

Para hacer frente a los ataques DDoS, las organizaciones deben implementar medidas de seguridad adecuadas. Según Black (2018),[113] es fundamental contar con sistemas de detección y mitigación de ataques DDoS que sean capaces de identificar patrones de tráfico malicioso y responder de manera rápida y eficiente. Además, es importante fortalecer la infraestructura de red y utilizar soluciones de balanceo de carga y redundancia para distribuir la carga de tráfico y mitigar los impactos de los ataques.

En conclusión, el ataque distribuido de denegación de servicios es un vector de ataque que busca sobrecargar los recursos de un sistema o red, dejándolo inaccesible para los usuarios legítimos. Los ataques DDoS han evolucionado en complejidad y magnitud, utilizando técnicas de amplificación y enmascaramiento para dificultar su detección y mitigación. Para contrarrestar estos ataques, es necesario implementar medidas de seguridad adecuadas y fortalecer la infraestructura de red. Solo de esta manera se podrá garantizar la disponibilidad y funcionalidad de los sistemas transaccionales.

7.2 ELEMENTOS DE UN SISTEMA TRANSACCIONAL SUCEPTIBLE DE SER ATACADO

Tomando como base que un sistema transaccional propone elementos fundamentales en muchas organizaciones y se utilizan para procesar y administrar transacciones comerciales, estos sistemas están diseñados para garantizar la integridad, confiabilidad y consistencia de las transacciones realizadas. Algunos de los elementos fundamentales de un sistema transaccional son los siguientes:

7.2.1 Base de datos. La base de datos es el componente central de un sistema transaccional. Almacena y gestiona la información relacionada con las transacciones, como registros de clientes, productos, ventas, pagos, etc. La base de datos debe ser segura, escalable y capaz de manejar un alto volumen de transacciones en tiempo real.

7.2.2 Transacciones. Las transacciones son unidades lógicas de trabajo que representan una serie de operaciones relacionadas. Estas operaciones pueden incluir inserciones, actualizaciones o eliminaciones de datos en la base de datos. Las transacciones deben ser atómicas, lo que significa que deben ser completas o no realizarse en absoluto. Esto garantiza la consistencia de los datos y evita situaciones en las que se realicen solo algunas operaciones y otras no.

[113] BLACK, S. (2018). Mitigating DDoS Attacks. Communications of the ACM, P. 61(2), 70-78.

7.2.3 Concurrencia. Los sistemas transaccionales a menudo tienen múltiples usuarios o procesos que acceden a la base de datos simultáneamente. La concurrencia se refiere a la capacidad del sistema para administrar y coordinar el acceso simultáneo a los datos por parte de múltiples usuarios o procesos. Esto implica garantizar que las transacciones se ejecuten de manera aislada y que no haya conflictos o inconsistencias en los datos debido a accesos concurrentes.

7.2.4 Control de concurrencia. El control de concurrencia es el mecanismo utilizado para garantizar que las transacciones se ejecuten de manera coordinada y sin conflictos. Esto implica la implementación de técnicas como el bloqueo de datos, la serialización y la resolución de conflictos para garantizar la consistencia y la integridad de los datos.

7.2.5 Recuperación. La recuperación se refiere a la capacidad del sistema para recuperarse de posibles fallas o interrupciones. Esto implica la implementación de técnicas de respaldo y recuperación que aseguren que los datos estén protegidos y que sea posible restaurarlos en caso de un fallo del sistema.

7.2.6 Seguridad. Los sistemas transaccionales deben ser seguros para proteger la integridad y confidencialidad de los datos. Esto implica implementar mecanismos de autenticación y autorización para controlar el acceso a los datos, así como técnicas de encriptación para proteger la información sensible.

Según lo anterior, un sistema transaccional se compone de una base de datos central, transacciones atómicas, mecanismos de control de concurrencia, recuperación de fallos y medidas de seguridad. Estos elementos son fundamentales para garantizar la integridad, confiabilidad y consistencia de las transacciones comerciales en el sistema.

Después de reconocer las generalidades de los sistemas transaccionales pasamos a reconocer las características de los vectores de ataque que han intervenido en los casos antes mencionados.

En este caso se evidencia que el *phishing* se ha convertido en uno de los principales vectores de ataque que afectan los sistemas transaccionales en la actualidad. Este método de ingeniería social se basa en engañar a los usuarios para que revelen información confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios. Tanto *Capital one* como Audifarma han sido víctimas de ataques de *phishing*, lo que demuestra la efectividad y la gravedad de este tipo de amenaza.

En el caso de *Capital one*, uno de los mayores bancos de Estados Unidos, sufrió un ataque masivo de *phishing* en el año 2019. Un hacker logró acceder a los datos personales de más de 100 millones de clientes, incluyendo nombres, direcciones, números de seguro social y números de cuentas bancarias. Según el informe de la

investigación, el ataque se realizó mediante el envío de correos electrónicos fraudulentos que parecían provenir de la propia institución bancaria. Los usuarios, confiando en la apariencia legítima de los mensajes, proporcionaron sus datos personales, cayendo en la trampa del *phishing*.

De manera similar, Audifarma, una entidad comercializadora de medicamentos en Colombia, también sufrió un ataque de *phishing* a su infraestructura tecnológica. Aunque no se han revelado detalles específicos sobre el incidente, se especula que los *hackers* utilizaron falsos correos electrónicos o mensajes engañosos para obtener acceso a los sistemas y posiblemente a la información de los usuarios. Este tipo de ataque tiene como objetivo principal obtener información personal y financiera de los usuarios, lo cual puede tener consecuencias graves, como el robo de identidad o el fraude financiero.

El *phishing* se ha vuelto cada vez más sofisticado y difícil de detectar. Los atacantes utilizan técnicas de ingeniería social avanzadas, como la personalización de los correos electrónicos y la creación de sitios web falsos que imitan la apariencia de instituciones legítimas. Estos métodos engañosos hacen que los usuarios confíen y compartan su información sin sospechar que están siendo víctimas de un ataque.

Es importante destacar la responsabilidad tanto de las instituciones como de los usuarios en la prevención de ataques de *phishing*. Las organizaciones deben implementar medidas de seguridad sólidas, como filtros de correo electrónico y capacitación en concienciación sobre seguridad, para proteger a sus clientes de posibles ataques. Los usuarios, por su parte, deben estar alerta y aprender a reconocer las señales de un intento de *phishing*, como direcciones de correo electrónico sospechosas, errores gramaticales o solicitudes inusuales de información personal.

Por último, el *phishing* es un vector de ataque altamente efectivo que afecta a los sistemas transaccionales, tal como se evidenció en los casos de *Capital one* y Audifarma; estos ataques demuestran la importancia de implementar medidas de seguridad robustas y de educar a los usuarios sobre los riesgos del *phishing*. Solo a través de una combinación de esfuerzos por parte de las organizaciones y los usuarios se podrá mitigar esta amenaza y proteger la integridad de los sistemas transaccionales.

Ahora teniendo en cuenta el vector de ataque DDOS (ataque distribuido de denegación de servicio) se ha convertido en un vector de ataque que afecta significativamente los sistemas transaccionales en la actualidad. Esta técnica maliciosa busca saturar los recursos de un sistema, impidiendo que los usuarios legítimos accedan a los servicios o realicen transacciones. Tanto *Capital one* como Audifarma han experimentado ataques de denegación de servicios que

demuestran la gravedad de esta amenaza y la necesidad de abordar las vulnerabilidades y configuraciones deficientes en el *software*.

En el caso de *Capital one*, uno de los mayores bancos de Estados Unidos, sufrió un ataque de denegación de servicios en el año 2019. Este ataque afectó la disponibilidad de los servicios en línea del banco, lo que resultó en interrupciones significativas y afectó a millones de clientes. Según los informes, el ataque se realizó aprovechando una configuración deficiente en uno de los servidores de la institución, lo que permitió a los atacantes sobrecargar el sistema y causar una interrupción en los servicios.

De manera similar, Audifarma, una entidad comercializadora de medicamentos en Colombia, también fue víctima de un ataque de denegación de servicios en su infraestructura tecnológica. Aunque los detalles específicos no se han revelado, se cree que los atacantes aprovecharon vulnerabilidades en el *software* o la infraestructura de la empresa para sobrecargar los servidores y afectar la disponibilidad de los servicios en línea. Esto generó inconvenientes para los usuarios que intentaban acceder a los servicios de la compañía, lo cual afectó negativamente sus operaciones y la satisfacción de los clientes.

La denegación de servicios se ha vuelto una amenaza creciente debido a las numerosas vulnerabilidades presentes en los sistemas y las configuraciones deficientes en el *software*. Los atacantes utilizan diversas técnicas, como ataques de inundación de paquetes o ataques distribuidos de denegación de servicios (DDoS), para abrumar los servidores y agotar los recursos disponibles. Esto puede tener consecuencias devastadoras, ya que los sistemas transaccionales dependen de una infraestructura estable y confiable para operar de manera eficiente.

Es importante destacar que la prevención y mitigación de los ataques de denegación de servicios requieren un enfoque integral que aborde las vulnerabilidades del sistema y las configuraciones deficientes en el *software*. Las organizaciones deben implementar medidas de seguridad adecuadas, como *firewall*s, sistemas de detección de intrusiones y sistemas de mitigación de DDoS, para proteger sus sistemas y detectar posibles ataques. Además, es esencial llevar a cabo pruebas regulares de penetración y evaluaciones de vulnerabilidades para identificar y solucionar las debilidades existentes en la infraestructura.

Otro vector de ataque dentro de un sistema transaccional en donde se observa que la seguridad de los sistemas transaccionales es crucial para garantizar la confidencialidad, integridad y disponibilidad de la información sensible. Sin embargo, a menudo se pasa por alto y que es un factor clave en la cadena de seguridad es el elemento humano; el factor humano puede ser considerado como un vector de ataque en sí mismo, ya que es el último ejecutor de las instrucciones incorporadas dentro de un *software* malicioso. A través de engaños, errores o

negligencia, el elemento humano puede comprometer la seguridad de los sistemas transaccionales.

El factor humano se convierte en un vector de ataque potencial cuando los usuarios caen en la trampa de la ingeniería social. Los atacantes utilizan técnicas persuasivas para engañar a los usuarios y lograr que realicen acciones no deseadas, como abrir archivos adjuntos maliciosos o hacer clic en enlaces peligrosos. Un ejemplo común es el envío de correos electrónicos de *phishing*, que parecen legítimos y solicitan información confidencial, como contraseñas o datos bancarios. Si los usuarios no son lo suficientemente cautelosos y caen en el engaño, pueden abrir la puerta a amenazas cibernéticas.

El caso de *Capital one* evidencia cómo el elemento humano puede ser explotado como un vector de ataque. En el incidente ocurrido en 2019, el atacante utilizó la ingeniería social para obtener acceso a los datos personales de millones de clientes. Según los informes, el hacker aprovechó la vulnerabilidad del sistema y persuadió a un empleado de la compañía a ejecutar una serie de instrucciones maliciosas. Esto permitió que el atacante accediera a información confidencial y causara un daño significativo a la organización y sus clientes.

De manera similar, en el caso de Audifarma, se cree que los atacantes aprovecharon debilidades en la cadena de seguridad y lograron persuadir a algún empleado para que realice acciones que comprometieron la infraestructura tecnológica de la compañía. Si bien no se han revelado detalles específicos sobre el incidente, es importante reconocer cómo el factor humano puede ser aprovechado para comprometer la seguridad de los sistemas transaccionales.

Es esencial comprender que el factor humano no siempre actúa de manera intencionada. Los errores o la negligencia también pueden abrir la puerta a amenazas cibernéticas. Por ejemplo, la descarga de archivos adjuntos de fuentes no confiables o el uso de contraseñas débiles pueden exponer los sistemas a ataques. Además, la falta de conciencia sobre las mejores prácticas de seguridad, como la actualización regular del *software* y la capacitación en concienciación sobre seguridad, también puede aumentar el riesgo de comprometer los sistemas transaccionales.

Para abordar este vector de ataque, es fundamental implementar medidas de seguridad que incluyan la capacitación y concienciación del personal. La formación en ciberseguridad debe ser integral y continua, para garantizar que los empleados estén informados sobre las amenazas existentes y las mejores prácticas para prevenirlas. Además, es necesario establecer políticas y procedimientos claros que promuevan la seguridad y la responsabilidad de todos los usuarios.

sintetizando, el factor humano constituye un vector de ataque en los sistemas transaccionales que puede ser explotado a través de las sensaciones, sentimientos, es decir puede ser explotado a través del engaño.

7.3 VULNERABILIDADES DE LOS SISTEMAS TRANSACCIONALES: DESAFIOS Y SOLUCIONES

Para abordar las vulnerabilidades es necesario entender que, en la era digital actual, los sistemas transaccionales desempeñan un papel crucial en la operación de organizaciones, instituciones financieras y plataformas de comercio electrónico; estos sistemas facilitan la realización de transacciones comerciales, transferencias de fondos, procesos de ventas y compras, entre otros. Sin embargo, debido a su importancia, los sistemas transaccionales se han convertido en un objetivo atractivo para los ciberdelincuentes. Por tal motivo el propósito del presente documento es abordar las vulnerabilidades comunes que afectan los sistemas transaccionales y explorar soluciones que permitan mitigar los riesgos asociados.

Como ya se ha visto en páginas anteriores, como vulnerabilidades comunes de los Sistemas Transaccionales se cuentan las siguientes:

Ataques de Inyección SQL: Los ataques de inyección SQL son una amenaza constante para los sistemas transaccionales. Los ciberdelincuentes pueden manipular las consultas SQL para acceder, modificar o eliminar datos sensibles.

Ataques de Cross-Site Scripting (XSS): Los ataques XSS permiten a los atacantes ejecutar scripts maliciosos en el navegador de un usuario, lo que puede dar lugar al robo de credenciales o datos sensibles.

Vulnerabilidades en Autenticación y Sesiones: La falta de autenticación adecuada y la gestión inadecuada de sesiones pueden permitir a los atacantes acceder a cuentas de usuario legítimas o realizar transacciones en nombre de otros usuarios.

Falta de Validación de Datos de Entrada: La falta de validación adecuada de los datos de entrada puede permitir la introducción de datos maliciosos que afectan la integridad de las transacciones.

Escalada de Privilegios: Las vulnerabilidades que permiten a los atacantes aumentar sus privilegios dentro del sistema pueden resultar en accesos no autorizados y transacciones fraudulentas.

7.3.1 Soluciones y Mitigaciones. Seguridad en el Desarrollo: La implementación de prácticas de desarrollo seguro, como la validación de entrada, la autenticación sólida y la gestión adecuada de sesiones, es de suma importancia y base fundamental con el fin de evitar debilidades desde la concepción del diseño y desarrollo del proceso de software.

Firewalls de Aplicación Web (WAF): Los WAF pueden ayudar a detectar y bloquear ataques comunes, como inyecciones SQL y XSS, antes de que lleguen a la aplicación.

Monitoreo Continuo: Implementar sistemas de monitoreo de seguridad que puedan detectar actividad anómala y alertar sobre posibles ataques o violaciones de seguridad.

Auditorías de Seguridad: Realizar auditorías regulares de seguridad y pruebas de penetración para identificar y corregir vulnerabilidades en los sistemas transaccionales.

7.4 ANALISIS DE LOS DIFERENTES ATAQUES DESDE LA METODOLOGIA DE CICLO DE EVALUACION DE VULNERABILIDADES

7.4.1 Ataques SQL a Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidades. Teniendo en cuenta que un ataque SQL (Structured Query Language) a un sistema transaccional es una amenaza cibernética en la que un atacante intenta explotar vulnerabilidades en una aplicación o sistema que utiliza una base de datos; los ataques SQL se producen cuando un atacante manipula maliciosamente las consultas SQL enviadas a la base de datos con el fin de acceder, modificar o eliminar datos en la base de datos, o incluso tomar el control del sistema subyacente.

Fases del Ciclo de Evaluación de Vulnerabilidades en un Ataque SQL

La evaluación de vulnerabilidades en un ataque SQL se puede analizar siguiendo las fases del ciclo de evaluación de vulnerabilidades:

Reconocimiento: El atacante identifica el sistema transaccional y su estructura de base de datos. Busca información sobre las tablas, columnas y esquema de la base de datos.

Exploración: Se investigan las posibles vulnerabilidades, como la falta de validación de entrada en formularios web. Se determina si la aplicación es propensa a ataques SQL mediante pruebas de inyección.

Explotación: El atacante ejecuta consultas SQL maliciosas para aprovechar vulnerabilidades identificadas. Puede buscar datos sensibles o intentar modificar registros en la base de datos.

Elevación de Privilegios: Si el atacante tiene éxito, puede intentar aumentar sus privilegios para obtener un mayor control del sistema. Esto puede incluir la escalada de privilegios a cuentas administrativas.

Mantenimiento del Acceso: Una vez que se ha comprometido el sistema, el atacante puede tratar de mantener el acceso persistente para futuras acciones maliciosas.

Reporte y Mitigación: La organización afectada debe tomar medidas para mitigar el ataque, como corregir las vulnerabilidades, restablecer contraseñas comprometidas y revisar los registros de seguridad.

7.4.2 Ataques Cross-Site Scripting (XSS) en Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidad. Un ataque XSS es una vulnerabilidad que permite a un atacante inyectar scripts maliciosos en páginas web vistas por otros usuarios. En el contexto de sistemas transaccionales, esto puede tener consecuencias graves, ya que los atacantes pueden explotar esta vulnerabilidad para robar credenciales, datos sensibles o incluso realizar transacciones fraudulentas en nombre de un usuario legítimo. Los ataques XSS ocurren cuando los datos ingresados por un usuario no se validan o escapan adecuadamente antes de mostrarlos en una página web.

Fases del Ciclo de Evaluación de Vulnerabilidad en un Ataque XSS

La evaluación de vulnerabilidades en un ataque XSS se puede analizar siguiendo las fases del ciclo de evaluación de vulnerabilidades:

Reconocimiento: El atacante identifica la presencia de formularios web y áreas donde se puede ingresar información. Busca vulnerabilidades, como la falta de validación de entrada en formularios o la omisión de filtrado de salida en la presentación de datos.

Exploración: El atacante envía datos de entrada maliciosos, como scripts JavaScript, para evaluar si se pueden inyectar en la página. Intenta encontrar maneras de engañar a los mecanismos de seguridad, como los encabezados Content Security Policy (CSP).

Explotación: Una vez que se identifica una vulnerabilidad, el atacante inyecta scripts maliciosos. Estos scripts pueden ser utilizados para robar cookies de sesión, capturar datos del usuario o redirigir a páginas maliciosas.

Mantenimiento del Acceso: El atacante puede mantener el acceso persistente a través de scripts inyectados que se ejecutan en cada visita del usuario.

Reporte y Mitigación: La organización afectada debe tomar medidas para mitigar el ataque, como corregir las vulnerabilidades, implementar encabezados CSP y educar a su personal sobre las mejores prácticas de seguridad.

7.4.3 Ataques a la Autenticación y Sesiones en Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidad. Los ataques a la autenticación y sesiones en sistemas transaccionales son acciones maliciosas dirigidas a comprometer la identidad de un usuario legítimo o a secuestrar su sesión activa. Estos ataques pueden permitir a los intrusos acceder a cuentas de usuario, realizar transacciones fraudulentas o acceder a datos confidenciales. Los atacantes a menudo explotan debilidades en las prácticas de autenticación, como contraseñas débiles o técnicas de ingeniería social, así como problemas en la gestión de sesiones, como la falta de control de acceso adecuado.

Fases del Ciclo de Evaluación de Vulnerabilidad en Ataques a la Autenticación y Sesiones

La evaluación de vulnerabilidades en ataques a la autenticación y sesiones se puede analizar siguiendo las fases del ciclo de evaluación de vulnerabilidad:

Reconocimiento: El atacante busca identificar los sistemas transaccionales y las prácticas de autenticación utilizadas. Recopila información sobre usuarios, contraseñas y mecanismos de autenticación.

Exploración: El atacante busca debilidades en la autenticación, como la exposición de contraseñas en texto claro o la falta de bloqueo de cuentas después de varios intentos fallidos. Identifica vulnerabilidades en la gestión de sesiones, como la falta de expiración de sesiones inactivas.

Explotación: Si se encuentran vulnerabilidades, el atacante puede intentar eludir la autenticación o secuestrar la sesión de un usuario legítimo. Esto podría permitirle acceder a la cuenta de un usuario o realizar transacciones no autorizadas.

Mantenimiento del Acceso: Una vez que se ha comprometido una cuenta o sesión, el atacante puede intentar mantener el acceso persistente para futuros ataques.

Reporte y Mitigación: La organización afectada debe tomar medidas para mitigar el ataque, como fortalecer la autenticación, implementar políticas de bloqueo de cuentas y garantizar la expiración adecuada de sesiones inactivas.

7.4.4 Ataques a la Validación de Datos de Entrada en Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidad. Los ataques a la validación de datos de entrada se producen cuando un atacante aprovecha debilidades en la forma en que un sistema procesa y valida la información proporcionada por los usuarios. Estas debilidades pueden permitir que los atacantes introduzcan datos maliciosos o inapropiados en un sistema. Estos ataques pueden dar lugar a la ejecución de código malicioso, la exposición de datos sensibles o la manipulación de las transacciones.

Fases del Ciclo de Evaluación de Vulnerabilidad en Ataques a la Validación de Datos de Entrada

La evaluación de vulnerabilidades en ataques a la validación de datos de entrada se puede analizar siguiendo las fases del ciclo de evaluación de vulnerabilidad:

Reconocimiento: El atacante investiga la estructura y el funcionamiento del sistema transaccional. Identifica áreas donde se ingresa información por parte del usuario y busca debilidades en la validación de entrada.

Exploración: El atacante intenta introducir datos maliciosos, como secuencias de comandos o caracteres especiales, en las áreas de entrada. Observa la respuesta del sistema para determinar si los datos maliciosos son aceptados o si se producen errores.

Explotación: Si se descubren debilidades en la validación de datos de entrada, el atacante puede inyectar datos maliciosos para lograr sus objetivos. Esto podría incluir la ejecución de código malicioso o la manipulación de datos para realizar transacciones no autorizadas.

Mantenimiento del Acceso: Una vez que el atacante ha comprometido el sistema, puede intentar mantener el acceso persistente para futuros ataques.

Reporte y Mitigación: La organización afectada debe tomar medidas para mitigar el ataque, como fortalecer la validación de entrada, corregir vulnerabilidades y educar a su personal sobre las mejores prácticas.

7.4.5 Escalada de Privilegios en Ataques a Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidad. Los ataques a la validación de datos de entrada se producen cuando un atacante aprovecha debilidades en la forma en que un sistema procesa y valida la información proporcionada por los usuarios. Estas debilidades pueden permitir que los atacantes introduzcan datos maliciosos o inapropiados en un sistema. Estos ataques pueden dar lugar a la ejecución de código malicioso, la exposición de datos sensibles o la manipulación de las transacciones.

Fases del Ciclo de Evaluación de Vulnerabilidad en Ataques a la Validación de Datos de Entrada

La evaluación de vulnerabilidades en ataques a la validación de datos de entrada se puede analizar siguiendo las fases del ciclo de evaluación de vulnerabilidad:

Reconocimiento: El atacante investiga la estructura y el funcionamiento del sistema transaccional. Identifica áreas donde se ingresa información por parte del usuario y busca debilidades en la validación de entrada.

Exploración: El atacante intenta introducir datos maliciosos, como secuencias de comandos o caracteres especiales, en las áreas de entrada. Observa la respuesta del sistema para determinar si los datos maliciosos son aceptados o si se producen errores.

Explotación: Si se descubren debilidades en la validación de datos de entrada, el atacante puede inyectar datos maliciosos para lograr sus objetivos. Esto podría incluir la ejecución de código malicioso o la manipulación de datos para realizar transacciones no autorizadas.

Mantenimiento del Acceso: Una vez que el atacante ha comprometido el sistema, puede intentar mantener el acceso persistente para futuros ataques.

Reporte y Mitigación: La organización afectada debe tomar medidas para mitigar el ataque, como fortalecer la validación de entrada, corregir vulnerabilidades y educar a su personal sobre las mejores prácticas.

7.4.6 Ataques de Ingeniería Social en Sistemas Transaccionales. Evaluación desde la Metodología del Ciclo de Evaluación de Vulnerabilidad. La ingeniería social es una técnica de ataque que se ha vuelto cada vez más común en el mundo de la ciberseguridad; en el contexto de sistemas transaccionales, la ingeniería social puede ser particularmente peligrosa, ya que se enfoca en manipular a las personas para que revelen información confidencial o realicen acciones que ponen en riesgo la seguridad de los datos y las transacciones.

Un ataque de ingeniería social es un tipo de ataque que busca explotar la vulnerabilidad humana, en lugar de debilidades técnicas en un sistema. En un sistema transaccional, un ataque de ingeniería social implica engañar a los usuarios o empleados para que revelen información confidencial, como contraseñas o datos de tarjetas de crédito, o para que realicen acciones que comprometen la seguridad, como transferir fondos de manera fraudulenta; los atacantes utilizan tácticas de persuasión y manipulación para engañar a las personas y obtener acceso no autorizado a sistemas o datos.

Fases del Ciclo de Evaluación de Vulnerabilidad en Ataques de Ingeniería Social. La evaluación de vulnerabilidades en ataques de ingeniería social se puede analizar siguiendo las fases del ciclo de evaluación de vulnerabilidad:

Reconocimiento. El atacante investiga el sistema transaccional para identificar a las personas involucradas y sus roles. Busca información pública sobre los usuarios, como nombres, cargos y redes sociales.

Exploración. El atacante planifica y diseña el ataque de ingeniería social, identificando posibles víctimas y desarrollando tácticas persuasivas. Utiliza la información recopilada en la fase de reconocimiento para personalizar el ataque.

Explotación. El atacante ejecuta el ataque, ya sea enviando correos electrónicos de phishing, llamando por teléfono o utilizando otros métodos de manipulación. El objetivo es engañar a las víctimas para que revelen información confidencial o realicen acciones no deseadas.

Mantenimiento del Acceso. Si el atacante tiene éxito, puede mantener el acceso a sistemas o datos mediante la recopilación continua de información y la manipulación de las víctimas.

Reporte y Mitigación. Las organizaciones afectadas deben tomar medidas para mitigar el ataque, como concientizar a los empleados sobre las tácticas de ingeniería social, implementar políticas de seguridad y realizar capacitación en seguridad cibernética.

7.5 FACTORES DE SEGURIDAD EN LOS SISTEMAS TRANSACCIONALES

La seguridad en los sistemas transaccionales representa un aspecto prioritario que se debe implementar en las empresas donde se emplee algún tipo de sistema transaccional, para estas organizaciones es esencial preservar la confidencialidad, integridad y disponibilidad de la información, así como para asegurar la continuidad del negocio bajo criterios de productividad, eficiencia credibilidad y garantía hacia sus clientes.

El presente apartado pretende explorar de manera concreta la forma cómo se implementan diversos factores de seguridad para alcanzar los objetivos fundamentales de todo sistema transaccional y que de esta manera pueda operar de forma confiable y segura.

El cifrado de datos, es entendido como un proceso donde se codifica los datos o información delicada de la empresa, con el fin de soslayar la intromisión de terceros no autorizados para verla; la forma adecuada para entender el contenido o mensaje enviado originalmente es a través del uso de una llave especial capaz de decodificar la información.

Desde años atrás el cifrado de datos está fundamentado en una ciencia denominada la criptografía, la cual se empleó desde la antigüedad hasta el presente cuando era indispensable para mantener cierto tipo de información secreta. Actualmente, se emplean equipos de cómputo capaces de realizar un cifrado mucho más complejo donde se acude a la implementación de algoritmos complejos que generan una directriz para encriptar y desencriptar la información en el momento que sea requerida; no se debe olvidar que muchos elementos de la tecnología evolucionan constantemente, por ende se hace necesario mencionar el uso de la inteligencia artificial para cifrar datos, como lo expresa el equipo de investigación de Google, “Dos redes neuronales intercambiaron mensajes cifrados de tal manera que sólo ellas entienden”[114], el equipo investigador explica que se crearon dos redes neuronales que interactuaron entre sí enviándose mensajes codificados y que hasta el momento los investigadores no han sido capaces de entender, es un ejemplo del uso de la inteligencia artificial en el cifrado de la información.

La implementación de técnicas de cifrado es crucial para salvaguardar la confidencialidad de la información transmitida y almacenada. Como señalan Stallings y Brown, "el cifrado de datos proporciona una capa adicional de seguridad, protegiendo la información contra accesos no autorizados"[115]. Cabe entender que una capa adicional de seguridad le permite al sistema operar de forma confiable garantizando la seguridad de sus activos. (Kaspersky, 2023).

La autenticación y autorización es otra salvaguarda a implementar como factor de seguridad, como se expresa en la guía N° 8 de MinTIC[116], se deben usar controles de seguridad basados en la norma ISO/IEC 27001 que permitan garantizar la

[114] Mundo, Sputnik. La Inteligencia Artificial crea un método de cifrado y nadie sabe cómo funciona. Sputnik Mundo. Recuperado de: (https://sputniknews.lat/20161029/robot-inteligencia-artificial-google-1064472992.html)

[115] kaspersky, Lab. ¿Qué es el cifrado de datos? Definición y explicación. {17 Agosto de 2023}. Recuperado de: (https://latam.kaspersky.com/resource-center/definitions/encryption)

[116] MinTic. Controles de Seguridad y Privacidad de la Información. Guía No.8. {20 Noviembre de 2023}. Recuperado de: (https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf)

seguridad de los datos; por tanto, la autenticación robusta y la autorización precisa son elementos clave para garantizar que solo usuarios autorizados accedan al sistema. Whitman y Mattord (2005), destacan que "la composición efectiva de entre los procesos de autenticaciones y autorizaciones certifica la identificación idónea del usuario y restringe se acceso a servicios, funciones y datos específicos"[117].

La auditoría y seguimiento; teniendo en cuenta que la auditoria se define como la revisión de procesos y procedimientos que implementa la organización para verificar la existencia de requisitos preestablecidos que permitan salvaguardar la información, es indispensable realizar procesos de auditoría constantes y el seguimiento a los eventos detectados, estos dos factores son esenciales para identificar posibles amenazas. Según el NIST (National Institute of Standards and Technology), "los registros de auditoría permiten rastrear eventos, facilitando la investigación de incidentes y cumpliendo con requisitos de conformidad"[118]. Los registros consignados de los eventos observados permiten a la organización la toma de decisiones con el fin de garantizar el funcionamiento del sistema transaccional.

También se encuentra la protección contra ataques, La implementación de medidas de seguridad contra ataques conocidos es esencial para minimizar la exposición a vulnerabilidades. Chapman y Engebretson (2017),[119] afirman que "***la protección efectiva contra ataques, como inyecciones SQL y cross-site scripting, fortalece la resiliencia del sistema"***; por ello las empresas se ven obligadas a implementar sistemas de protección integrados que contribuyan a la disminución de los ataques y minimice el impacto cuando algún vector de ataque se materialice dentro de un sistema.

Otra acción hace referencia al respaldo y recuperación, se deben implementar políticas de seguridad en la organización, la realización de copias de seguridad periódicas y la planificación de la recuperación ante desastres son fundamentales para garantizar la continuidad del negocio. En este sentido Whitman y Mattord (2005),[120] indican que *"la disponibilidad de datos respaldados reduce el impacto de eventos adversos y facilita la restauración rápida de los servicios".*

Por último, un factor importante es la Seguridad Física; entendida como todas aquellas políticas y acciones que se pueden implementar de forma tangible dentro

[117] WHITMAN, Michael & MATTORD, Herb. (2005). Principles of Information Security.
[118] VILLAMIZAR, Carlos. ¿Qué es NIST Cibersecurity Framework?,. GlobalSuite Solutions {blog, 22 de octubre de 2020}. Recuperado de: (https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/)
[119] CHAPMAN y ENGEBRETSON. Amazon Web Services, Inc. «Qué es un ataque DDOS y cómo proteger su sitio contra uno». Accedido 22 de noviembre de 2023. https://aws.amazon.com/es/shield/ddos-attack-protection/)
[120] Whitman, M. E. & Mattord, H. J. (2018). Can blockchain make risk management more secure?.

de la empresa, La seguridad física de la infraestructura subyacente es tan crítica como las medidas digitales. Harris argumenta que una estrategia efectiva de seguridad es limitar el uso físico de los equipos que almacenan activos críticos, se encarga de planear encontrar y minimizar amenazas potenciales, implementa salvaguardas para proteger la integridad de los sistemas transaccionales".

A manera de conclusión preliminar se puede afirmar que la implementación efectiva de estos factores de seguridad en sistemas transaccionales no solo protege la información sensible y asevera prolongación del negocio transaccional en un ambiente empresaria cambiante y dinámica. Al abordar aspectos como el cifrado, la autenticación, la auditoría y la protección contra ataques, las organizaciones pueden construir una base sólida para enfrentar desafíos de seguridad y mantener la integridad de sus operaciones comerciales.

7.6 ESTRATEGIAS DE MITIGACIÓN PARA PREVENIR ATAQUES A LA SEGURIDAD DE LOS SISTEMAS TRANSACCIONALES

La mitigación de los efectos que puede ocasionar la materialización de un vector de ataque implica la implementación de estrategias y medidas para reducir o eliminar el impacto de una amenaza de seguridad, a continuación, se describen algunas estrategias comunes de mitigación que las empresas pueden implementar en aras de proteger el activo más importante, la información.

La actualización y aplicación de parches de software, son prácticas fundamentales en la gestión de la seguridad informática, destinadas a mantener la integridad y proteger los sistemas contra vulnerabilidades conocidas; esta estrategia se basa en la premisa de que, con el tiempo, los desarrolladores de software identifican y corrigen fallos de seguridad en sus productos, las actualizaciones y parches son entregados a los usuarios para cerrar estas brechas y fortalecer la resistencia contra posibles amenazas.

En lenguaje coloquial, una actualización de software implica la instalación de nuevas versiones o revisiones de un programa, sistema operativo o aplicación, estas actualizaciones pueden abordar una variedad de problemas, desde mejoras en la funcionalidad hasta correcciones de errores críticos, lo más importante en el contexto de la seguridad, la solución de vulnerabilidades descubiertas.

El proceso de aplicación de parches, por otro lado, se centra específicamente en corregir fallas y vulnerabilidades de seguridad identificadas en el software existente, los parches son fragmentos de código diseñados para reemplazar o actualizar porciones específicas del software afectado, cerrando así las brechas de seguridad y reduciendo el riesgo de explotación por parte de actores malintencionados.

Esta estrategia se alinea con el principio de "Defense in Depth"[121] (defensa en profundidad), donde múltiples capas de seguridad se implementan para proteger un sistema, la actualización y parcheo de software constituyen una capa esencial en este enfoque, ya que abordan directamente las vulnerabilidades conocidas, una vez que han sido identificadas y resueltas por los desarrolladores.

Otra acción importante es la implementación de firewalls y filtros de red, esta salvaguarda busca garantizar la integridad de las redes informáticas contra amenazas cibernéticas. En consonancia con Stallings y Brown (2018),[122] quienes destacan en su obra "Computer Security: Principles and Practice," los firewalls actúan como barreras defensivas, controlando el tráfico de red y regulando el acceso a los recursos del sistema, estos dispositivos, situados estratégicamente en la arquitectura de red, examinan el tráfico entrante y saliente, permitiendo o bloqueando la comunicación en función de reglas predefinidas.

La función principal de los firewalls es evitar el acceso no autorizado a la red y proteger contra amenazas como intrusiones y ataques de denegación de servicio (DDoS), este control riguroso del tráfico de red contribuye a prevenir el ingreso de códigos maliciosos y a impedir que actores no autorizados comprometan la seguridad de los sistemas.

En términos de filtros de red, estos constituyen una extensión de la estrategia de seguridad al ofrecer un mecanismo adicional para examinar, clasificar y gestionar el flujo de datos en la red. Stallings y Brown (2018), resaltan que los filtros de red permiten a los administradores establecer políticas específicas para filtrar o bloquear determinados tipos de tráfico, lo que resulta crucial para mitigar amenazas y mantener un entorno de red seguro.

Finalmente, la implementación de firewalls y filtros de red se erige como un pilar esencial en la protección de sistemas informáticos, controlando la comunicación de manera efectiva y aplicando medidas preventivas para salvaguardar la integridad de la red.

Otra acción que garantiza reducir el riesgo de ataques cibernéticos es la implementación de Sistemas de Detección y Prevención de Intrusiones (IDS/IPS) constituye una estrategia esencial para fortalecer la seguridad de las redes informáticas, según se destaca en las palabras de Stallings y Brown (2018),[123] en su obra "Computer Security: Principles and Practice". Estos sistemas desempeñan un papel crucial en la identificación temprana y mitigación de actividades sospechosas o maliciosas dentro de una red.

[121] STALLINGS, W., BROWN, L. 2018. Computer Security: Principles and Practice. Pearson.
[122] Ibid., p. 259
[123] Ibid., p. 276

En este contexto, los Sistemas de Detección de Intrusiones (IDS) monitorizan activamente el tráfico de red en busca de patrones y comportamientos anómalos que puedan indicar posibles amenazas, al identificar eventos no autorizados o anómalos, los IDS generan alertas que alertan a los administradores sobre la potencial intrusión, permitiéndoles tomar medidas correctivas de manera proactiva.

Por otro lado, los Sistemas de Prevención de Intrusiones (IPS) van más allá de la detección y tienen la capacidad de tomar acciones automáticas para bloquear o mitigar las amenazas identificadas. Según Stallings y Brown (2018), los IPS se configuran con reglas específicas que les permiten bloquear el tráfico malicioso en tiempo real, evitando así que las intrusiones tengan éxito y minimizando el impacto en la seguridad de la red.

En conjunto, la implementación de IDS/IPS ofrece una capa adicional de defensa en profundidad, permitiendo una respuesta más rápida y eficaz ante posibles amenazas. Estos sistemas son esenciales para la protección proactiva de las redes, brindando a los administradores la capacidad de anticiparse a las intrusiones y mantener la integridad del entorno de red.

La estrategia de seguridad en capas, también conocida como "Defense in Depth" (Defensa en Profundidad), se erige como un enfoque fundamental para fortalecer la seguridad informática, según lo destacado por Stallings y Brown (2018),[124] en su obra "Computer Security: Principles and Practice". Esta metodología se fundamenta en la idea de que la implementación de múltiples capas de seguridad proporciona una defensa más sólida contra amenazas cibernéticas, ya que cada capa contribuye de manera complementaria a la protección global del sistema.

En esencia, la Seguridad en Capas implica la aplicación de diversas medidas de seguridad a lo largo de la arquitectura de una red o sistema. Cada capa está diseñada para abordar específicamente diferentes tipos de amenazas, y su combinación sinérgica reduce las posibilidades de un compromiso de seguridad exitoso.

Stallings y Brown (2018), resaltan que esta estrategia va más allá de depender exclusivamente de una única medida de seguridad, reconociendo que ninguna solución única puede ofrecer una protección completa, en cambio, la Defensa en Profundidad abarca la implementación de firewalls, sistemas de detección y prevención de intrusiones, controles de acceso, encriptación, entre otras medidas, en distintos niveles de la infraestructura.

Al adoptar la Seguridad en Capas, se crea un entorno donde la superposición de medidas de seguridad mejora la resistencia del sistema ante ataques diversos, este enfoque estratégico afianza la premisa de que la seguridad debe ser un

[124]Ibid., p. 302

esfuerzo integral y continuo, adaptándose a la evolución constante de las amenazas cibernéticas.

Quizás el factor más débil de la cadena de seguridad es el factor humano, en este caso, la educación y concientización del Usuario, según la perspectiva de Stallings y Brown (2018),[125] en "Computer Security: Principles and Practice", representa una piedra angular en la fortificación de la seguridad informática, este enfoque reconoce que los usuarios desempeñan un papel crucial en la prevención de amenazas y la protección de los sistemas, y por lo tanto, se destaca la importancia de brindarles conocimientos y conciencia respecto a las buenas prácticas de seguridad.

En este contexto, la educación del usuario implica proporcionar información detallada sobre los riesgos potenciales en línea, las tácticas de ingeniería social y las prácticas de seguridad recomendadas. Stallings y Brown (2018), señalan que, al elevar el nivel de conocimiento de los usuarios, se reduce significativamente la probabilidad de caer en trampas cibernéticas y se fomenta un comportamiento en línea más seguro.

La concientización del usuario va más allá de la mera transmisión de conocimientos, abordando la importancia de desarrollar una actitud proactiva hacia la seguridad, esto implica cultivar una mentalidad crítica y reflexiva entre los usuarios, alentándolos a cuestionar la autenticidad de correos electrónicos, enlaces y solicitudes de información sensible.

La obra de Stallings y Brown (2018), destaca que, mediante programas de concientización, se puede fomentar una cultura de seguridad en la que los usuarios se conviertan en defensores activos de la integridad de los sistemas, este enfoque preventivo no solo reduce el riesgo de incidentes de seguridad, sino que también contribuye a la creación de un entorno cibernético más seguro y resiliente.

Otra acción importante es la implementación de sistemas de Control de Acceso, según Stallings y Brown (2018),[126] en "Computer Security: Principles and Practice", se presenta como una estrategia clave en la protección de sistemas informáticos, este enfoque se centra en la gestión y restricción de los permisos de acceso a recursos, asegurando que solo aquellos usuarios autorizados tengan la capacidad de interactuar con determinadas áreas o información sensible.

En palabras sencillas, los Controles de Acceso buscan garantizar que los usuarios solo puedan acceder a los recursos para los cuales tienen permisos explícitos. Stallings y Brown (2018), resaltan que esta restricción se implementa a través de la autenticación y la autorización, la autenticación verifica la identidad del usuario,

[125] Ibid., p. 504
[126] Ibid., p. 545

mientras que la autorización determina qué recursos específicos están disponibles para ese usuario después de la autenticación.

La obra subraya que el principio fundamental de los Controles de Acceso es minimizar el riesgo asociado con la potencial explotación por parte de usuarios no autorizados. Esto se logra mediante la aplicación de políticas y reglas que definen quién puede acceder a qué recursos y bajo qué condiciones.

El Control de Acceso no solo se limita a la autenticación de usuarios, sino que también se extiende a la gestión de privilegios, garantizando que los usuarios solo tengan acceso a funciones y datos esenciales para sus responsabilidades. Este enfoque proactivo contribuye significativamente a la prevención de accesos no autorizados y a la protección de la confidencialidad e integridad de la información.

Por último, La gestión de vulnerabilidades, según la perspectiva de Stallings y Brown (2018),[127] en su obra "Computer Security: Principles and Practice", es una estrategia integral que busca identificar, evaluar y mitigar las debilidades en los sistemas de información, este enfoque proactivo reconoce que las vulnerabilidades constituyen puntos críticos de riesgo y que la gestión eficaz de estas es esencial para mantener la seguridad de los sistemas.

La Gestión de vulnerabilidades implica un ciclo continuo de actividades que comienza con la identificación de posibles debilidades en el software, hardware o la configuración de un sistema. Stallings y Brown (2018), resaltan que esta identificación puede llevarse a cabo mediante la aplicación de escaneos de seguridad, análisis de código fuente y evaluaciones de configuración.

Posteriormente, la evaluación de vulnerabilidades implica clasificar y priorizar estas debilidades en función de su impacto potencial y la probabilidad de explotación. la obra señala que esta fase permite a los administradores de seguridad focalizar sus recursos en la mitigación de las vulnerabilidades más críticas y urgentes.

La mitigación de vulnerabilidades comprende la implementación de parches, actualizaciones de software y configuraciones de seguridad adicionales para eliminar o reducir el riesgo asociado con las debilidades identificadas. Stallings y Brown (2018), destacan que este proceso no es estático; más bien, es un ciclo continuo que se adapta a la evolución de las amenazas y a la dinámica de los sistemas.

Para finalizar, la Gestión de Vulnerabilidades representa un componente esencial de la seguridad cibernética, abordando proactivamente las debilidades potenciales y contribuyendo a la creación de entornos informáticos más robustos y resistentes.

[127] Ibid., p 598

7.7 PANORAMA ACTUAL ACERCA DE LA MATERIALIZACION DE VECTORES DE ATAQUE EN EL ENTORNO EMPRESARIAL

Con el fin de abordar la temática se propone a los lectores el siguiente informe que pretende hacer el análisis de la situación actual, describiendo un panorama que responda al interrogante ¿Por qué se materializan vectores de ataque en las empresas o en los sistemas transaccionales? En este orden de ideas se tiene el siguiente informe:

7.7.1 Informe Sobre Motivos Específicos De Ataques Cibernéticos En El Entorno Empresarial

Fecha: 20 de noviembre de 2023

Destinatario: Lectores de la monografía vectores de ataque en los sistemas transaccionales

Remitente: Adriano Gutiérrez Poche

Resumen Ejecutivo

Este informe se centra en los motivos específicos que impulsan la materialización de ataques cibernéticos en el entorno empresarial actual, se destacan diversos escenarios, desde amenazas tradicionales como el *phishing* y *ransomware* hasta tácticas más avanzadas que involucran tecnologías emergentes como la inteligencia artificial y el metaverso.

Phishing y *Ransomware* en Constante Evolución

Los ataques de *phishing* y *ransomware* continúan en aumento, y su sofisticación se incrementa de manera constante, los ciberdelincuentes adaptan sus tácticas para eludir las medidas de seguridad, aprovechando la ingeniería social y la vulnerabilidad humana.

Transformación Digital sin Dirección Estratégica

La falta de una transformación digital planificada y sin argumentos sólidos puede dejar a las empresas expuestas a riesgos cibernéticos, la adopción de tecnologías sin una estrategia clara puede resultar en la implementación de sistemas mal configurados y vulnerables.

Empleados Despedidos con Acceso a Información Valiosa

La terminación de empleados sin una gestión adecuada de los accesos y la información puede generar riesgos significativos. Los ex empleados pueden convertirse en amenazas internas al poseer información valiosa y sentirse descontentos.

Descuido en la Reconfiguración de Usuarios y Contraseñas

Cuando se retiran los accesos de empleados, es crucial reconfigurar el sistema para evitar posibles riesgos de seguridad, la falta de esta directriz en gran medida puede desencadenar potencialmente en accesos no acreditados (autorizados) vulnerando la integridad de los datos y la confiabilidad de la información

Insiders Buscando Beneficio Monetario

La amenaza interna se agrava cuando empleados actuales buscan ganancias personales infectando los sistemas de la empresa. La conciencia y la monitorización constante son esenciales para prevenir estos actos malintencionados.

Nuevos Ataques con APT e Inteligencia Artificial

El uso de APT (Amenazas Persistentes Avanzadas) y la inteligencia artificial para suplantar personas, incluso mediante tecnologías de Deep Face en videoconferencias en tiempo real, presenta una nueva frontera en la ciberdelincuencia, requiriendo enfoques de defensa más avanzados.

Utilización del Metaverso y Avatares para Suplantación

La creciente adopción del metaverso introduce nuevos riesgos, con la posibilidad de suplantación de identidad mediante avatares, las empresas deben anticipar y abordar estas amenazas emergentes en entornos virtuales.

Riesgos en el Uso de Canales de Redes Sociales Empresariales

La utilización de canales de redes sociales de la empresa, como WhatsApp, puede convertirse en una vulnerabilidad si no se implementan medidas de seguridad adecuadas. La comunicación por estos medios debe ser monitorizada y protegida contra posibles amenazas.

Como conclusión se afirma que, en el panorama actual de amenazas cibernéticas, es imperativo que las empresas adopten estrategias integrales de ciberseguridad, la concientización, la educación continua, la implementación de medidas de seguridad avanzadas y la adaptación constante a las nuevas tecnologías son esenciales para mitigar los riesgos y proteger la integridad de la información empresarial.

Este informe pretende proporcionar una visión detallada de los motivos específicos detrás de los ataques cibernéticos en el entorno empresarial y se recomienda una evaluación constante de las amenazas y la implementación proactiva de medidas de seguridad.

7.8 SISTEMAS TRANSACCIONALES ATACADOS EN COLOMBIA, ANÁLISIS DE CASOS

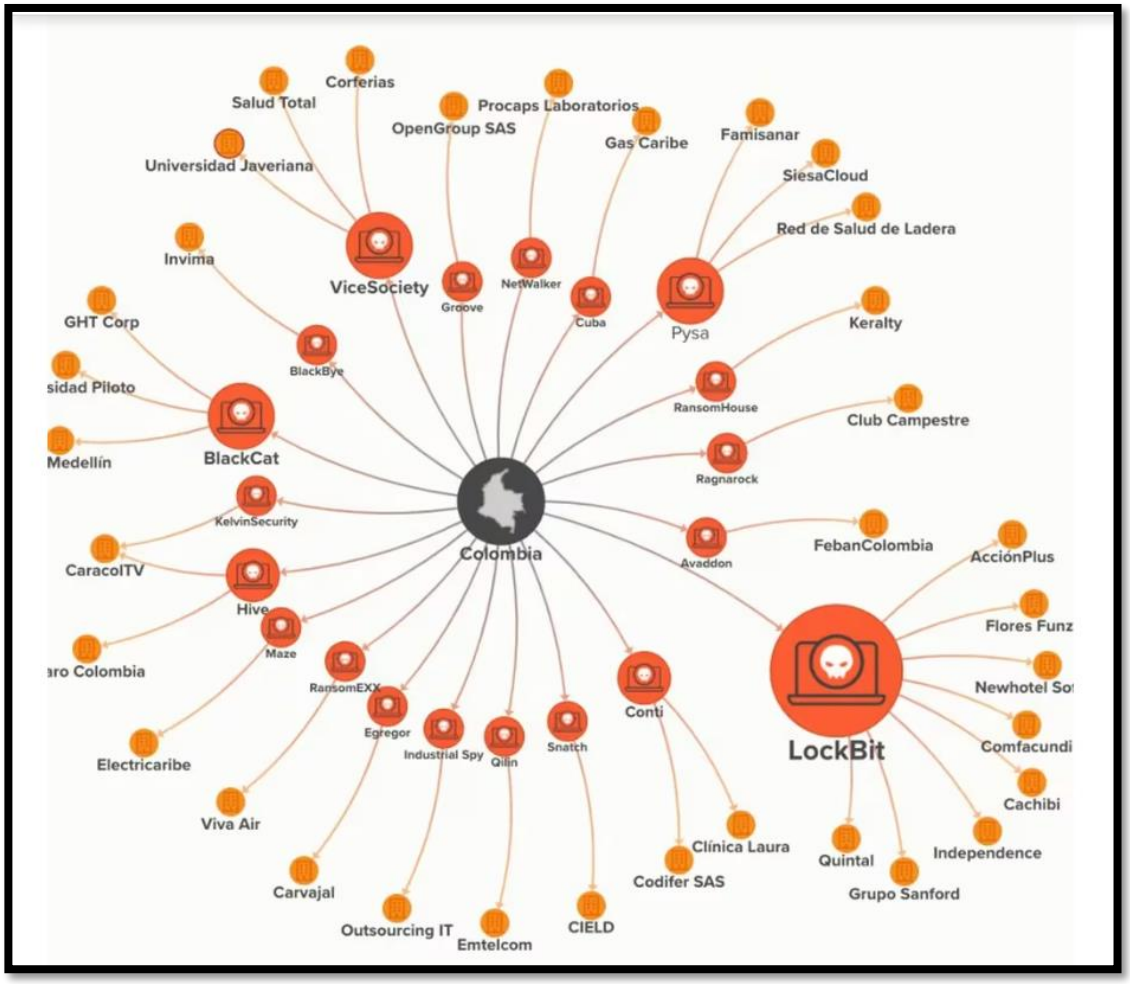
Teniendo en cuenta los diferentes medios de comunicación escritos radicados en Colombia muchos lectores observan con preocupación el siguiente titular “Las 34 empresas que fueron hackeadas en Colombia durante 2022”[128], es preocupante que al finalizar el 2022 las empresas de Colombia fueron blanco del cibercrimen, donde se observa la materialización de vectores de ataque en prestigiosas entidades del país como EPM y la EPS Sanitas. Según Lumu Technologies[129], se incrementó en un 133% la cantidad de empresas afectadas; donde el vector de ataque predominante fue el ransomware. Cuyo objetivo es secuestrar datos, mediante la infección por un malware, con el fin de pedir un rescate a las empresas para que los recuperen.

De forma ilustrativa se muestra la figura 1, donde aparecen las 34 empresas vulneradas en sus sistemas de ciberseguridad para el año 2022.

Cabe destacar que en la mayoría de ataques el vector predominante fue el *Phising, ransonware* y la ingeniería social en donde se el factor humano continúa siendo el eslabón más débil en la cadena de la ciberseguridad, por tanto, es necesario sugerir a las empresas y lectores de esta obra proponer e implementar políticas tendientes a la capacitación del talento humano en todos los temas relacionados con las buenas prácticas de ciberseguridad.

[128] INFOBAE. “Las 34 empresas que fueron hackeadas en Colombia durante 2022”. {2 de enero de 2023}. (https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/)
[129] Ibid., p. 1

Ilustración 2 Empresas atacadas en Colombia durante el 2022



Fuente: 1 INFOBAE. Las 34 empresas que fueron hackeadas en Colombia durante 2022, 2 de enero de 2023. https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/.

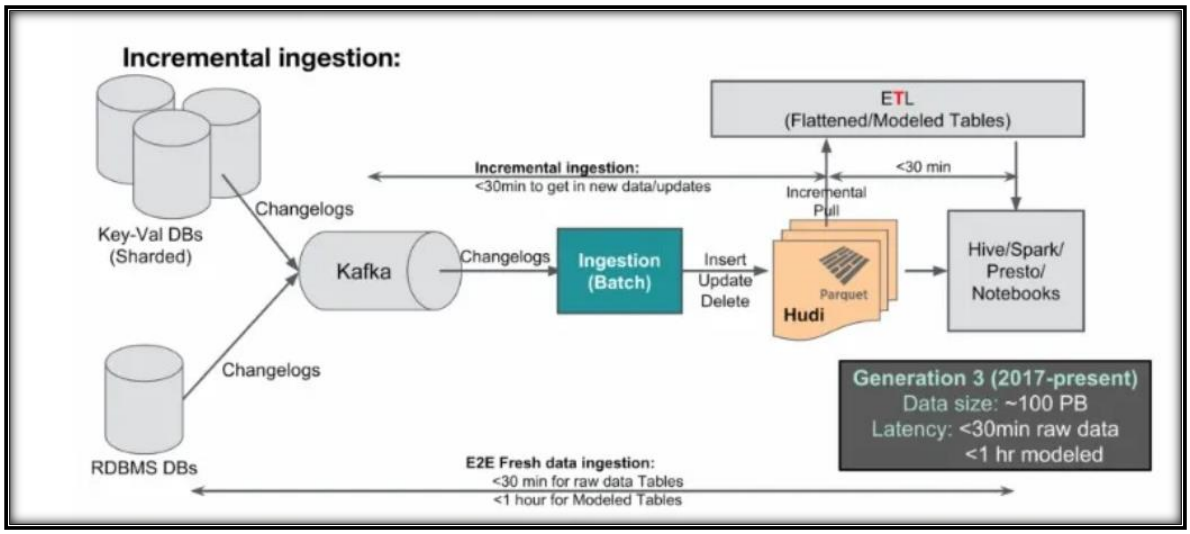
Para entender cómo funciona, o para descubrir cual es proceso empleado en un ataque a un sistema transaccional se analiza el caso del ataque cibernético efectuado en contra de la empresa UBER

7.9 ANALISIS DEL CASO DE CIBERATAQUE A LA PLATAFORMA UBER

Se inicia el análisis definiendo que UBER se reconoce como una empresa de tecnología, donde se usa la aplicación para que los usuarios que requieren transporte, lo consiguen de forma rápida y fácil haciendo uso de la aplicación en su dispositivo móvil socios conductores y clientes interactúan para ofrecer y acceder a un servicio a través de un sistema transaccional que permite la oferta y el pago del servicio en tiempo real además de otras funcionalidades que ofrece la

plataforma; en la siguiente figura se muestra la estructura de red con la cual funciona la plataforma UBER

Ilustración 3 Esquema de red de la plataforma UBER



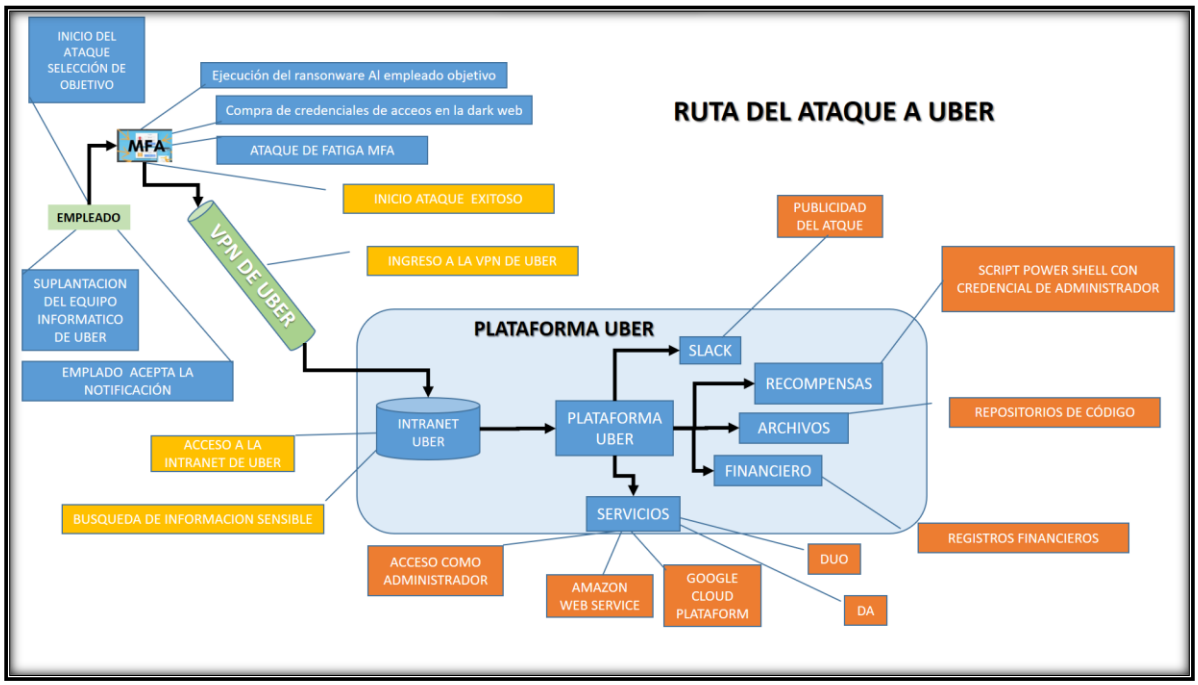
Fuente: 2. UBER, Equipo. «Pero al fin de cuentas, ¿Qué es Uber y cómo se usa?» Uber Blog, 29 de julio de 2015. https://www.uber.com/es-CL/blog/que-es-uber/.

la literatura consultada indica que el ataque fue ejecutado por un joven de 18 años, quien, usando credenciales de acceso robadas, realiza múltiples peticiones de autenticación multifactor al servidor y mensajería falsa a uno de los empleados de la empresa con el fin de que alguien le dé respuesta.

El empleado de UBER, abrumado por tanta insistencia, de las ventanas emergentes y mensajería falsa, acepta una de las solicitudes y de este modo se inicia el ataque a la seguridad de la plataforma UBER, cuando el joven atacante, logra ingresar al sistema eleva privilegios y accede a la información crítica y envía mensajes afirmando que la plataforma está bajo ataque.

Ruta del ataque. Según lo que se afirma en la documentación y videos revisados todo inicia con la selección de un objetivo, a quien se infecta con un ransonware pero el ataque no es efectivo, en vista de ello, se procede a iniciar un ataque de peticiones multifactor al mismo objetivo, luego para lograr el ataque es necesario suplantar al equipo informático de UBER con el fin de generar confianza en el empleado, posterior al mensaje por WhatasApp el usuario acepta una solicitud y desde allí se inicia el ataque a la plataforma; el atacante ingresa a la VPN, luego eleva privilegios de administrador ingresando a la intranet de la empresa, accede al sistema ingresando a los servicios de la empresa, publica mensajes dentro de la plataforma informando a los empleados acerca del ataque, y descarga archivos con vulnerabilidades del sistema. En la siguiente figura se traza la ruta del ataque indicando las acciones que realizó el atacante.

Ilustración 4 Ruta del ataque realizado a la plataforma UBER



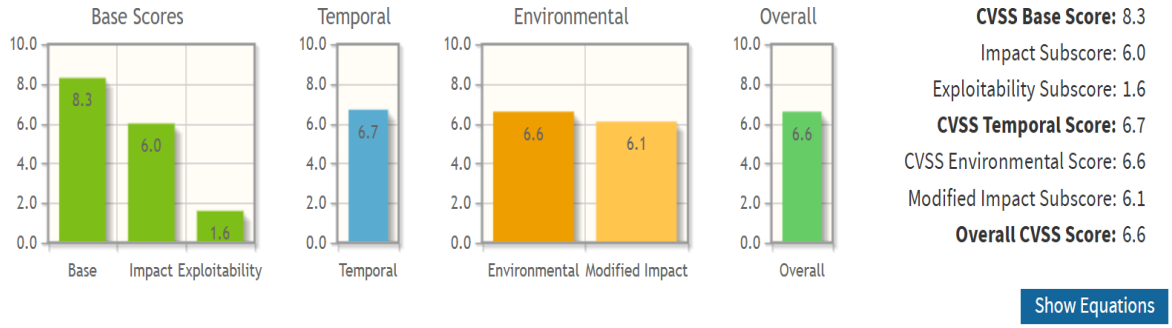
Como conclusión del análisis del caso se estable lo siguiente:

Atacante: joven de 18 años
Objetivo: empleado de la empresa
Vector de ataque: *Ransonware*, sobrecarga de peticiones de autenticación, suplantación de identidad, ingeniería social, programación inadecuada.
Resultados del ataque: saboteo a la plataforma, robo de información, robo de archivos con informe de vulnerabilidades, beneficio económico para el atacante, desprestigio de la empresa.
Aprendizajes: formulación de políticas para fortalecer la educación en ciberseguridad para los empleados de la empresa (factor humano)
Implementar acciones y dispositivos para filtrar el tráfico de los datos.
Implementar acciones y dispositivos que impidan la sobrecarga del sistema
Implementar acciones tendientes a las buenas prácticas de programación.
Invertir en ciberseguridad

Puntuación CVSS del ataque a UBER. Teniendo en cuenta los párrafos anteriores donde se describe el ataque a la plataforma UBER se establece la vulnerabilidad identificada como CVE-2021-44228 (la vulnerabilidad de Log4Shell), que fue ampliamente explotada y afectó a sistemas como los de Uber si no estaban adecuadamente parcheados.

Ahora bien, se analiza la vulnerabilidad identificada y se establece el nivel de criticidad usando los CVSS, en este caso se usa la calculadora CVSS Versión 3.1; según la información existente se puede inferir que en el caso concreto de la CVE-2021-44228 el vector de ataque es la inserción de código malicioso la cual permite la conexión con el servidor. En la figura siguiente se muestra las gráficas del puntaje base, el puntaje temporal y el puntaje del entorno cuando se le adicionan los parámetros según el caso de estudio

Ilustración 5. puntaje CVSS 1



Fuente 3. National Vulnerability Database.. 12 de noviembre de 2024. **https://nvd.nist.gov/vuln-metr 1**

Atendiendo a la clasificación del nivel de criticidad según la CVSS SCORE 3.1 se observa que el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS) es
Baja: Si la puntuación está entre 0.1 y 3.9
Medio: Si la puntuación está entre 4,0 y 6.9
Alta: Si la puntuación está entre 7.0 y 8.9 y
Crítica: Si la puntuación está entre 9.0 y 10.0

En la anterior ilustración se muestra que el vector de ataque explotado tiene una puntuación base de 8.3 lo cual indica que el sistema presenta una vulnerabilidad de nivel alto, por tanto, es indispensable promover acciones para mitigar la vulnerabilidad

8 FASE 3: ELABORACION DE RECOMENDACIONES GENERALES APLICABLES A SISTEMAS TRANSACCIONALES

8.1 RECOMENDACIONES PARA EVITAR CIBERATAQUES EN LOS SISTEMAS TRANSACCIONALES

En un entorno empresarial altamente dependiente de sistemas transaccionales, la seguridad de la información es fundamental; los vectores de ataque pueden poner en peligro la integridad, confidencialidad y disponibilidad de los datos, así como la continuidad de las operaciones, para evitar la materialización de estos vectores de ataque, las empresas deben implementar sólidas prácticas de ciberseguridad; en el presente texto, se presentan recomendaciones esenciales para fortalecer la seguridad de los sistemas transaccionales y prevenir la materialización de vectores de ataque.

Dentro de las recomendaciones esenciales para la Prevención de Vectores de Ataque se tienen las siguientes

8.1.1 Auditoría de Seguridad Regular. Realizar auditorías periódicas de seguridad para identificar posibles vulnerabilidades en los sistemas transaccionales.
Contratar profesionales de seguridad o empresas de seguridad cibernética para realizar pruebas de penetración y análisis de vulnerabilidades.

8.1.2 Gestión de Vulnerabilidades. Establecer un proceso de gestión de vulnerabilidades que incluya la identificación, evaluación, priorización y corrección de vulnerabilidades de manera oportuna. Actualización constante y recurrente de Hardware y software, parcheándolos con las últimas actualizaciones de seguridad.

8.1.3 Políticas de Contraseñas Fuertes. Implementar políticas de contraseñas sólidas que requieran contraseñas complejas y cambiantes con regularidad. Fomentar el uso de autenticación de dos factores (2FA) para aumentar la seguridad de las cuentas.

8.1.4 Control de Acceso. Establecer controles de acceso basados en roles y privilegios para limitar el acceso a los sistemas transaccionales. Implementar un principio de "menor privilegio", donde los usuarios solo tienen acceso a las funciones necesarias para su trabajo.

8.1.5 Educación y Concienciación de los Empleados. Proporcionar capacitación en seguridad cibernética a todos los empleados para que estén al tanto de las amenazas y sepan cómo identificar posibles ataques, como el *phishing*. Fomentar una cultura de seguridad cibernética en la empresa.

8.1.6 Protección contra *Malware*. Utilizar software antivirus y antimalware actualizado en todos los sistemas. Implementar políticas de restricción de software para evitar la ejecución de programas no autorizados.

8.1.7 Respuesta a Incidentes. Desarrollar y probar un plan de respuesta a incidentes que permita una rápida detección y mitigación de ataques. Establecer procedimientos claros para notificar y gestionar incidentes de seguridad.

8.1.8 Monitorización Continua. Implementar sistemas de monitorización y detección de amenazas en tiempo real para identificar actividades anómalas o sospechosas. Utilizar registros de seguridad para el seguimiento de eventos y actividades.

8.1.9 Encriptación de Datos. Utilizar encriptación para proteger los datos en reposo y en tránsito, especialmente en transacciones financieras y transferencias de datos sensibles.

8.1.10 Actualización de Políticas y Procedimientos. Revisar y actualizar regularmente las políticas y procedimientos de seguridad para adaptarse a las amenazas cambiantes y a las mejores prácticas de seguridad.

A manera de conclusión se afirma que la prevención de vectores de ataque en sistemas transaccionales es fundamental para garantizar la seguridad de la información y la integridad de las operaciones empresariales. Implementar estas recomendaciones ayudará a fortalecer la seguridad y reducir la exposición a amenazas cibernéticas. La seguridad de la información debe ser un esfuerzo continuo y debe ser parte integral de la cultura organizacional.

Las empresas que priorizan la seguridad cibernética están mejor preparadas para enfrentar y mitigar los riesgos de vectores de ataque, protegiendo así sus activos críticos y la confianza de sus clientes.

CONCLUSIONES

Con el desarrollo de la presente monografía se logró abordar la temática relacionada con los vectores de ataque que afectan los sistemas transaccionales. A nivel nacional y global, bajo esta perspectiva se observa la necesidad de proponer criterios que maximicen la seguridad en sistemas transaccionales, mediante la revisión sistemática que incorpore un enfoque integral para mitigación de riesgos de ciberataques

La revisión bibliográfica llevada a cabo proporcionó una visión crítica y actualizada de la amenaza constante que enfrentan los sistemas transaccionales en el entorno digital. A través del análisis de casos documentados de sistemas vulnerados, se revelan procedimientos empleados, el alcance de los ataques y se generan recomendaciones que pueden ser aplicadas a futuro.

En primer lugar, se desarrolló una revisión sistemática de un centenar de documentos entre artículos científicos y la literatura especializada relacionada con el problema de estudio donde se identificó que los vectores de ataque prevalentes, como el *phishing*, el *malware*, la ingeniería social y las vulnerabilidades de *software*, el correo electrónico siguen siendo las principales amenazas para la seguridad de los sistemas transaccionales, lo anterior se evidencia en los resultados de la evaluación del impacto generado por los ataques materializados a los sistemas.

En segundo lugar, se evaluó el impacto generado en cuatro sistemas transaccionales que han sido vulnerados en los últimos cinco años mediante la materialización de ataques de tipo *ransonware*, denegación de servicios y ataques de *phishing*; en donde se logró implementar la metodología de evaluación de vulnerabilidades que determinó en todos los casos un impacto de nivel crítico con calificación entre 9.0 y 10.0 en los CVSS, consecuencia de ello la confidencialidad, la disponibilidad y la integridad de la información y el funcionamiento y operatividad de los sistemas fueron altamente afectados ocasionando fugas de información y perdidas económicas y debilitando el factor de credibilidad ante los clientes; de igual forma la evaluación efectuada a estos sistemas permite establecer que el factor humano es altamente responsable de los fallos de seguridad en los sistemas

En tercer lugar, se redactó un decalogo con las recomendaciones para implementar en las empresas que administran sistemas transaccionales con el fin de minimizar la ocurrencia de situaciones de riesgo; la implementación de las

recomendaciones está enfocada en garantizar la seguridad y confiabilidad las plataformas y de igual manera garantizar confidencialidad, la disponibilidad y la integridad de la información contenida

Por último, la colaboración y el intercambio de información entre empresas y con las autoridades de ciberseguridad también son fundamentales. Compartir inteligencia sobre amenazas y vulnerabilidades permite una respuesta más efectiva a los ciberataques, las empresas deben establecer redes de colaboración y estar dispuestas a comunicar incidentes de seguridad de manera responsable y coordinada.

RECOMENDACIONES

Teniendo en cuenta el contenido presentado en la presente monografía la cual es resultado de la revisión de muchas fuentes bibliográficas referentes al tema, resulta preocupante descubrir que muchos de los sistemas transaccionales actuales están propensos a los ataques cibernéticos.

A manera de recomendación se plantea que se debe confirmar que los vectores de ataque típicos, como el *phishing*, el *malware*, la ingeniería social y las vulnerabilidades de *software*, siguen siendo las principales fuentes de amenazas para la seguridad de los sistemas transaccionales; estos ataques explotan la tecnología y la ingeniería con el fin de comprometer la integridad y la confidencialidad de las transacciones digitales y la información contenida en los sistemas transaccionales.

Por otra parte es necesario recomendar que la metodología del ciclo de Evaluación de Vulnerabilidades es una herramienta efectiva para identificar y comprender las debilidades en los sistemas transaccionales, este enfoque sistemático permite a las organizaciones llevar a cabo una evaluación exhaustiva de su infraestructura y aplicaciones, identificando posibles puntos de vulnerabilidad que podrían ser explotados por actores maliciosos; al comprender estas vulnerabilidades, las organizaciones pueden priorizar la asignación de recursos y tomar medidas proactivas para abordarlas.

Por último, minimizar el riesgo de la materialización de los vectores de ataque se constituye como una función esencial en la adopción de medidas proactivas en este sentido es importante que las empresas deben estar preparadas para enfrentar ciberamenazas que están en constante evolución, se debe destacar la importancia de la educación y la capacitación continua de los empleados quienes son el eslabón vital en la cadena de seguridad, y su conocimiento y vigilancia pueden ayudar a prevenir ciberataques; las empresas deben invertir en programas de concienciación en ciberseguridad y garantizar que los empleados estén al tanto de las últimas amenazas y buenas prácticas de seguridad.

BIBLIOGRAFÍA

¿QUÉ ES LA INGENIERÍA SOCIAL Y CÓMO ME PROTEJO?,. Argentina.gob.ar [En línea]. 2020. [Consultado: 9 May 2023]. Disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte.

¿QUÉ ES UN ATAQUE DDOS?,. Akamai [En línea]. [Consultado: 9 May 2023]. Disponible en: https://www.akamai.com/es/our-thinking/ddos.

¿QUÉ ES UN VECTOR DE ATAQUE? | Cloudflare. [En línea]. [Consultado: 9 May 2023]. Disponible en: https://www.cloudflare.com/es-es/learning/security/glossary/attack-vector/.

2021 SECURITY AWARENESS REPORT | SANS SECURITY AWARENESS. [En línea]. [Consultado: 9 May 2023]. Disponible en: https://www.sans.org/security-awareness-training/resources/reports/sareport-2021/.

25 TIPOS DE ATAQUES INFORMÁTICOS Y CÓMO PREVENIRLOS. CIBERSEGURIDAD. [En línea]. 2018. [Consultado: 12 May 2023]. Disponible en: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/.

A. A. MALIK AND D. K. TOSH, "Towards Developing a Scalable Cyber Risk Assessment and Mitigation Framework [En línea]. IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 2024, p. 1-8, doi: 10.1109/SysCon61195.2024.10553535.

AGUINIS, H., y GLAVAS, A. What We Know and Don't Know About Corporate Social Responsibility [En línea]. Journal of Management, p. 46(4), 1454-1488.

ALEGSA, L. Definición de Sistema transaccional (sistema de procesamiento de transacciones) [En línea]. 2018. Disponible en: https://www.alegsa.com.ar/Dic/sistema_transaccional.php.

ALEGSA, Leandro. Definición de Sistema transaccional (sistema de procesamiento de transacciones). [En línea]. 2018. [Consultado: 8 April 2023]. Disponible en: https://www.alegsa.com.ar/Dic/sistema_transaccional.php.

AMAZON WEB SERVICES, Inc. «Qué es un ataque DDOS y cómo proteger su sitio contra uno». [En línea]. Consultao 22 de noviembre de 2023. Disponible en: https://aws.amazon.com/es/shield/ddos-attack-protection/.

AMERICAN BAR ASSOCIATION. (2019). Health Care Fraud and Abuse Laws Affecting Medicare and Medicaid: An Overview. [En línea]. Consultado el 15 de abril de 2023, Disponible en:

https://www.americanbar.org/groups/health_law/section-news/2019/06/health-care-fraud-and-abuse-laws-affecting-medicare-and-medicaid-an-overview/.

ANDERSON, R., y MOORE, T. The economics of information security. Science. 2009. p.. 314(5799), 610-613.

ANDREASEN, J y YENKINSON, C. Understanding Denial-of-Service Attacks | CISA. [En línea]. 2021. [Consultado: 9 May 2023]. Disponible en: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.

ANDREASEN, J. y JENKINSON, C. Distributed Denial-of-Service (DDoS) Attacks. En The Computer Security Handbook 2015 (pp. 703-725).

APEDANICA. Seguridad en la red: principales preocupaciones de los usuarios de Internet en todo el mundo. [En línea]. 2018. Disponible en: https://www.apedanica.org/seguridad-en-la-red-principales-preocupaciones-de-los-usuarios-de-internet-en-todo-el-mundo/.

APLICACIÓN DE LA TEORÍA DEL PORTAFOLIO EN EL MERCADO ACCIONARIO COLOMBIANO. [En línea]. [Consultado: 9 May 2023]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-47722003000200007.

ARROW, K. J. Essays in the theory of risk-bearing. North-Holland Pub. Co. 1971.

ASOBANCARIA. (La reinvencion financiera en la era digital 2022 (primera edición ed.). [Consultado: el 28 de julio de 2024]. Disponible en: https://asobancaria.com/wp-content/uploads/La_reinvencion_financiera_en_la_era_digital-2022.pdf

BABCOCK, J. C., GREEN, C. E., y ROBIE, C. (). Does batterers' treatment work? A meta-analytic review of domestic violence treatment. Clinical Psychology Review, 2004 p. 23(8), 1023-1053.

BANISAR, David. Data Protection Laws Around the World Map. SSRN Electronic Journal [En línea]. 2011. DOI 10.2139/ssrn.1951416. Disponible en: http://www.ssrn.com/abstract=1951416. [Consultado: 10 May 2023].

BAUER, D. Decision-making under risk: Theory and application. Springer International Publishing. 2019

BISHOP, M. Computer security: Art and science. Addison-Wesley. 2002

BLACK, S. Mitigating DDoS Attacks. Communications of the ACM, 2018 61(2), p.70-78.

BLOOMBERG. Capital one Financial Corporation. [En línea]. 2023. Disponible en: https://www.bloomberg.com/profile/company/COF:US

BROWN, R. Phishing: Creating Fake Websites to Steal Personal Information. Journal of Cybersecurity, 2017.10(3), p. 123-136.

CAO, J., CHEN, X., y YAN, Y. A Survey on Authentication Mechanisms in Cybersecurity. [En línea]. 2020. Journal of Information Security, p. 11(2), 81-96. doi: 10.4236/jis.2020.112007

CAPITAL ONE. Official Website. [En línea].2023. Disponible en: https://www.capitalone.com/.

CHÁVEZ, C. A. C. La encriptación de datos empresariales: Ventajas y desventajas. 2019

Ciberseguridad ante el Crimen transnacional y la Ciberdelincuencia [Parte 1/4]. LISA Institute [En línea]. [Consultado: 10 May 2023]. Disponible en: https://www.lisainstitute.com/blogs/blog/ciberseguridad-crimen-transnacional-ciberdelincuencia.

CLARKE-SALT, J. SQL injection attacks and defense. SANS Institute. 2004.

CLOUDFLARE. ¿Qué es un vector de ataque?,. Cloudflare [En línea]. 2023. [Consultado: 9 April 2023]. Disponible en: https://www.cloudflare.com/es-es/learning/security/glossary/attack-vector/.

CLOUDFLARE. Cloudflare's DDoS trends report: Q1 [En línea].2021. Disponible en: https://www.cloudflare.com/zh-tw/learning/ddos/ddos-trends-report-q1-2021/

COLOMBIA Ley 1273 de 2009. Diario Oficial No. 47.365, 5 de enero de 2009.

COMISIÓN EUROPEA. La estrategia de ciberseguridad de la UE: hacia un enfoque de seguridad cibernética más fuerte y resiliente. [En línea].2018. Luxembourg: Publications Office of the European Union. Disponible en: https://ec.europa.eu/digital-single-market/en/news/strategia-de-ciberseguridad-de-la-ue-hacia-un-enfoque-de-seguridad-cibernetica-mas-fuerte-y-resiliente.

COMISIÓN FEDERAL DE COMERCIO DE ESTADOS UNIDOS. Fraude en línea: cómo evitar convertirse en una víctima. FTC. 2004.

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION. Intellectual Property Rights Enforcement and Cybersecurity Act. [En línea]. 2015Consultado el 15 de abril de 2023, desde https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/16/ipr-enforcement-cybersecurity-act-2012.pdf.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - la información y los datos - y se tipifican nuevas conductas delictivas, [En línea]. [Consultado: 15 de abril de 2023]. Disponible en: https://www.mintic.gov.co/portal/604/articles-5622_documento.pdf.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.462 de 17 de octubre de 2012. [En línea]. [Consultado: 10 May 2023]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4981.

CONSTITUCIÓN POLÍTICA DE COLOMBIA. [En línea]. 1991. [Consultado el 15 de abril de 2023]. Disponible en: https://www.constitucioncolombia.com/.

COPPOLA, Maria. Frontend y backend: qué son, en qué se diferencian y ejemplos. [En línea]. 2022. [Consultado: 9 April 2023]. Disponible en: https://blog.hubspot.es/website/frontend-y-backend.

CROWDSTRIKE. Global Threat Report 2021. [En línea]. Disponible en: https://go.crowdstrike.com/rs/281-OBQ-266/images/ReportCrowdStrikeGlobalThreatReport2021.pdf.

DATA PROTECTION. GOV.UK [En línea]. [Consultado: 10 May 2023]. Disponible en: https://www.gov.uk/data-protection.

DEFINICIÓN DE SISTEMA TRANSACCIONAL (SISTEMA DE PROCESAMIENTO DE TRANSACCIONES). [En línea]. [Consultado: 9 May 2023]. Disponible en: https://www.alegsa.com.ar/Dic/sistema_transaccional.php#gsc.tab=0.

DELGADO Jefferson. Sistemas transaccionales, sistemas de apoyo a las decisiones y sistemas estratégicos. [En línea]. 2015. Disponible en: https://www.gestiopolis.com/sistemas-transaccionales-sistemas-de-apoyo-a-las-decisiones-y-sistemas-estrategicos/.

DELITOS INFORMÁTICOS Y ENTORNO JURÍDICO VIGENTE EN COLOMBIA. [En línea]. [Consultado: 10 May 2023]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003.

DENNING, D. E. Denial of service in computer networks. ACM Press. 1987.

DIFFIE, W., Y HELLMAN, M. (). New directions in cryptography. IEEE Transactions on Information Theory. 1976, p 22(6), 644-654.

DOE, J. El impacto del phishing en los sistemas transaccionales. [En línea]. 2019. Revista de Seguridad Informática, p. 15(2), 45-56.

DOMINGUEZ, Estefanía. Tipos de Hackers. [En línea]. [Consultado: 9 mayo 2023]. Disponible en: https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers.

ELMASRI, R., y NAVATHE, S. B. Fundamentals of database systems. Pearson Education India. 2010

ESCOBAR, Ruth. Modelado del proceso de gestion financiera mediante BPM [En línea]. 2018. [Consultado: 8 April 2023]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/18459/55305916.pdf?sequence=1&isAllowed=y.

ÉTICA HACKER EN LA ACTUALIDAD. BLOG IDA CHILE | ESTRATEGIA PARA EL ÉXITO DE TU NEGOCIO [En línea]. 2019. [Consultado: 9 May 2023]. Disponible en: https://blog.ida.cl/seguridad/la-etica-hacker-en-la-actualidad/.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. European Cybersecurity Policy Framework. [En línea]. 2019Consultado el 15 de abril de 2023, desde https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/european-cybersecurity-policy-framework.

F5 NETWORKS. TLS/SSL vulnerabilities & best practices. [En línea]. 2020. Disponible en: https://www.f5.com/services/resources/guides/tls-ssl-vulnerabilities-best-practices.

FORBES. Capital one. [En línea]. 2022. Disponible en: https://www.forbes.com/companies/capital-one-financial/.

FRIEDBERG, Barbara. Personal Finance: An Encyclopedia of Modern Money Management: An Encyclopedia of Modern Money Management. ABC-CLIO, 2015. ISBN 978-1-4408-3032-7.

FRONTEND Y BACKEND: QUÉ SON, EN QUÉ SE DIFERENCIAN Y EJEMPLOS. [En línea]. [Consultado: 9 May 2023]. Disponible en: https://blog.hubspot.es/website/frontend-y-backend.

GARCÍA, C. Y GONZÁLEZ, J. Análisis de vectores de ataque en sistemas transaccionales: un enfoque basado en el análisis de amenazas. Monografía de grado. Universidad Nacional de Colombia. 2017

GAVRIĆ, Željko and SIMIĆ, Dejan. Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. Ingeniería e Investigación. [En línea]. [Consultado: 9 May 2023]. v. 38, n. 1, p. 130–138.

2018. DOI 10.15446/ing.investig.v38n1.65453. Disponible en: https://revistas.unal.edu.co/index.php/ingeinv/article/view/65453.

GÓMEZ, D. Análisis de vectores de ataque en sistemas transaccionales basados en blockchain. [En línea]. 2020. Revista de Tecnología, Información y Comunicación en Educación, p. 10(1), 1-10.

GRAMM-LEACH-BLILEY ACT | FEDERAL TRADE COMMISSION. [En línea]. [Consultado: 10 May 2023]. Disponible en: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

GREEN, A. Phishing Evolution: From Simple Attacks to Spear Phishing and Whaling. 2021. Journal of Computer Security, p. 12(4), 321-336.

GREENE, J., OLIVER, J. E., y BRODIE, N. The opinion-policy nexus in a representative democracy. Journal of Politics, 2008. p. 70(3), 717-736.

HACKERS: NINGÚN SISTEMA ES SEGURO. Cineplex. [En línea]. Disponible en: https://cineplex.com.co/peliculas/hackers-ningun-sistema-es-seguro/.

HADNAGY, C. Social Engineering: The Art of Human Hacking. Wiley. 2018.

HAN, Y., y HAN, K. A Review of Authentication Techniques for Cloud Computing. International Journal of Network Security, 2019 p. 21(3), 468-478.

HERNÁNDEZ SAMPIERI, R.; FERNÁNDEZ COLLADO, C., y BAPTISTA LUCIO, P. Metodología de la Investigación (5ta ed.). México: McGraw-Hill. 2010.

HERNÁNDEZ, Martín, y E Aldana. Delitos Transnacionales y su Impacto en Cinco Localidades Críticas del Distrito Capital de Bogotá en el Período 2009 – 2018.

HOOVER'S. Capital one Financial Corporation. [En línea]. 2023 Disponible en: https://www.hoovers.com/company-information/cs/company-profile.capital_one_financial_corporation.68d8a86c3c73958b.html.

ICOVE, D., SEGER, K., y VONSTORCH, W. Computer crime: A crimefighter's handbook. O'Reilly. 1995.

INCIBE. Los 10 vectores de ataque más utilizados por los ciberdelincuentes. [En línea]. 2022. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/los-10-vectores-ataque-mas-utilizados-los-ciberdelincuentes.

INFOBAE. Las 34 empresas que fueron hackeadas en Colombia durante 2022. [En línea]. 2022. [Consultado: 2 de enero de 2023]. Disponible en: https://www.infobae.com/america/tecno/2023/01/02/las-34-empresas-que-fueron-hackeadas-en-colombia-durante-2022/.

INSTITUTO NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES. NICT desarrolla medidas de seguridad para proteger a ciudadanos y organizaciones de la ciberdelincuencia. [En línea]. 2019. Disponible en: https://www.nict.go.jp/en/press/2019/02/25-1.html.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (). Information Technology - Security Techniques - Information Security Management Systems - Requirements. [En línea]. 2013. Disponible en: https://www.iso.org/standard/54534.html.

ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization. 2013

ITAA. Information Security Committee's Malware Definitions. [En línea]. Disponible en: https://www.isc2.org/-/media/ISC2/Certifications/Tech-Resources/ITAA_Definitions_Malware.ashx.

JIMÉNEZ, Junior Andrés. La Implementación De Un Sistema Automatizado Reduce Los Tiempos De Atención En Los Procesos Aplicables a La Ventanilla Única De Turismo En La Municipalidad Provincial Del Callao. Industrial Data [En línea]. v. 23, n. 2. 2020. [Consultado: 8 May 2023]. Disponible en: https://www.redalyc.org/journal/816/81665362003/html/.

JOHNSON, M. Phishing Attacks via Email: Techniques and Countermeasures. International Journal of Information Security, 2020. p. 15(2), 145-162.

JONES, A. DDoS Attacks and Countermeasures: Trends, Challenges, and Opportunities. Journal of Cybersecurity. 2019. p. 3(2), 123-136.

KAHNEMAN, D. y TVERSKY, A. Choices, values, and frames. Cambridge University Press. 2000.

KAHNEMAN, Daniel and TVERSKY, Amos. Choices, values, and frames. Cambridge University Press: New York, NY, US, 2000. ISBN 978-0-521-62172-4.

KASPERSKY. Kaspersky Security Bulletin: Story of the Year, 2020. [En línea]. 2021. Disponible en: https://securelist.com/kaspersky-security-bulletin-story-of-the-year-2020/100404/.

KINDERVAG, J. The future of encryption. Forrester Research. 2018

KIZZA, J. M. Ethical and social issues in the information age. Springer Science & Business Media. 2012

KOSINSKI, M., y FORREST, A. Topics vulnerability scanning. [En línea]. [Consultado: 15 de diciembre de]. IBM. Disponible en: https://www.ibm.com/mx-es/topics/vulnerability-scanning

KOUROUXOUS, Thomas y BAUER, Thomas. Violations of dominance in decision-making. Business Research [En línea]. v. 12, n. 1, p. 209–239. 2019. DOI 10.1007/s40685-019-0093-7. [Consultado: 9 May 2023]. Disponible en: https://doi.org/10.1007/s40685-019-0093-7

KREBS, B. Capital one Data Theft Impacts 100M People; Woman Arrested. KrebsOnSecurity. 2019.

KSHETRI, N. Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 2018. p.. 39, 80-89.

LATAM.KASPERSKY.COM. ¿Qué es el cifrado de datos? Definición y explicación. [En línea]. [Consultado: 17 de agosto de 2023]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/encryption.

LAUDON, K. C., y LAUDON, J. P. Management Information Systems: Managing the Digital Firm. Pearson Education. 2016.

LAZAR, J.; FENG, J. H., y HOCHHEISER, H. Research methods in human-computer interaction. Elsevier. 2015.

LEHTINEN, R., y WILLEMS, G. T. Computer security basics. O'Reilly. 1989.

LEVY, Steven. Hackers: Heroes of the Computer Revolution - 25th Anniversary Edition. O'Reilly Media, Inc., 2010. ISBN 978-1-4493-9374-8.

LI, X.; LIANG, X. y CHEN, W.. Security and privacy in crowdsourcing: A survey. IEEE Transactions on Parallel and Distributed Systems, 2019. p.. 30(3), 662-682.

LIU, Zhiyong. Proximal Operator Splitting for Multi-Constraint Dictionary Learning. International Journal of Hybrid Information Technology [En línea]. v. 10, n. 2, p. 107–116. 2017. DOI 10.14257/ijhit.2017.10.2.11. [Consultado: 9 May 2023]. Disponible en: http://gvpress.com/journals/IJHIT/vol10_no2/11.pdf.

LÓPEZ, J. M. H., y LÓPEZ, M. F. J. Herramientas de análisis de vulnerabilidad en sistemas operativos para mejorar la seguridad en la industria. Procesamiento de Señales, Imágenes y Redes de Comunicaciones, 2019, p. 127-133.

MADYANINGRUM, Ali. MUSTIKA Sari, Developing a Blockchain-Based Data Storage System Model to Improve Government Agencies' Organizational Performance. IJTech - International Journal of Technology. [En línea]. [Consultado:

22 de noviembre de 2023]. Disponible en: https://ijtech.eng.ui.ac.id/article/view/5237.

MAHJABIN, Tasnuva; XIAO, Yang, SUN., Guang y JIANG, Wangdong. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks [En línea]. v. 13, n. 12, p. 1550147717741463. 2017. DOI 10.1177/1550147717741463. [Consultado: 9 May 2023]. Disponible en: https://doi.org/10.1177/1550147717741463.

MALWAREBYTES. The State of Malware 2020. [En línea]. 2020. Disponible en: https://resources.malwarebytes.com/files/2020/02/2020_State_of_Malware_Report.pdf.

MARKOWITZ, H. Portfolio selection: Efficient diversification of investments. John Wiley & Sons. 2014.

MARTINEZ, Jeferson y SANDINO, Pedro. Creación de un ataque ddos utilizando http-get flood a partir de la metodología cyber kill chain. [En línea]. [Consultado: 9 May 2023]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-17982019000100041.

MAY, K. O. Intransitivity, utility and the aggregation of preference patterns. Econometrica, 1954. p. 22(1), 1-13.

MCAFEE. Crimen financiero en línea. [En línea]. 2018. Disponible en: https://www.mcafee.com/es/resources/reports/rp-economic-cybercrime-on-the-rise.pdf

MCCLURE, S.; SCAMBRAY, J., y KURTZ, G. Hacking exposed 5th edition. McGraw-Hill. 2005.

MICROSOFT. Análisis de vulnerabilidades y herramientas de seguridad. [En línea]. 2021. [Consultado: 18 de mayo de 2021]. Disponible en: https://docs.microsoft.com/es-es/windows-server/administration/server-core/server-core-server-security-and-guidance/vulnerability-scanning-and-security-tools.

MICROSOFT. Security Signals Report. [En línea]. 2020. Disponible en: https://info.microsoft.com/ww-landing-Security-Signals-Report-2020.html.

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Red País Digital, Delitos informáticos. [En línea]. 2019. Disponible en: http://www.redpais.gov.co/delitos-informaticos.

MISHRA, R. y GUPTA, N. K. Literature Review: Detection of Distributed Denial of Service Attack. International Journal of Computer Science and Mobile Computing, 2016. p. 5(6), 38-43.

MITNICK, K. D., y SIMON, W. L. The Art of Deception: Controlling the Human Element of Security. Wiley. 2002.

MUNDO, SPUTNIK. La Inteligencia Artificial crea un método de cifrado y nadie sabe cómo funciona. [En línea]. Sputnik Mundo. Disponible en: https://sputniknews.lat/20161029/robot-inteligencia-artificial-google-1064472992.html.

NAKAMOTO, S.. Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf. 2008.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information systems and Organizations. Washington, DC: National Institute of Standards and Technology. 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST Special Publication 800-131A rev. 2: Transitioning the use of cryptographic algorithms and key lengths. U.S. Department of Commerce. 2016.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Security and Privacy Controls for Federal Information Systems and Organizations. [En línea]. 2013. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

NATIONAL SECURITY AGENCY. (). Identity and Access Management. [En línea]. 2014. Disponible en: https://www.nsa.gov/Portals/70/documents/resources/cybersecurity-technical-best-practices-23july2014.pdf.

NELSON, B., y PHILLIPS, A. Guide to computer forensics and investigations. Cengage Learning. 2008.

NEVINS, Catherine, y YOUNG B Choi. Can Blockchain Make Risk Management More Secure?, 2018. p. 15, No. 2

NIST. SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology. 2020.

NOTI_INFOSEGURA: Qué es el cifrado de datos y cuál es su utilidad – Seguridad de la información. [En línea]. [Consultado: 20 de noviembre de 2023]. Disponible en: https://www.uv.mx/infosegura/general/noti_cifradodatos/.

O'BRIEN, J. A., y MARAKAS, G. M. Management Information Systems. McGraw-Hill Education. 2011

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. (). Estrategia Interamericana de Ciberseguridad. [En línea]. 2016. Disponible en: https://www.oas.org/es/csh/estrategiainteramericana.asp.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. (). Seguridad de la Información y Tecnología de la Información (TI). [En línea]. 2021. Disponible en: https://www.oas.org/es/seguridadinfo/.

OSPINA, M. R.; SANABRIA, P. E. y Sanabria Rangel, P. E. (). Desafíos nacionales frente a la ciberseguridad en el escenario global: Un análisis para Colombia. [En línea]. 2020. Revista Criminalidad, 62(2), 199-217. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S1794-31082020000200199&lng=en&nrm=iso&tlng=es.

PACHÓN, Camila. 10 reconocidas instituciones de Colombia hackeadas en el 2022. [En línea]. [Consultado: 10 de enero de 2023]. Disponible en: https://www.nsit.com.co/10-reconocidas-instituciones-de-colombia-hackeadas-en-el-2022/.

PARLAMENTO EUROPEO. (). Convenio sobre Ciberdelincuencia. [En línea]. 2001. Disponible en: https://www.europarl.europa.eu/cmsdata/122461/Proyecto%20Budapest_2017_es%20(3).pdf.

PÉREZ, L. Y RODRÍGUEZ, R. Estudio de los vectores de ataque en sistemas transaccionales [En línea]. 2019. Revista Científica de Tecnología e Innovación, p.. 5(1), 1-12.

PHRACK MAGAZINE [En línea]. [Consultado: 9 May 2023]. Disponible en: http://phrack.org/issues/54/8.html.

PODDEBNIAK, D. Y ZALEWSKI, M. (). Back doors vs. front doors: Attacks and defenses in modern operating systems. [En línea]. 1999. Disponible en: http://phrack.org/issues.html?issue=54&id=8.

PORTFOLIO SELECTION: Efficient Diversification of Investments, 2nd Edition | Wiley. Wiley.com [En línea]. [Consultado: 9 May 2023]. Disponible en: https://www.wiley.com/en-us/Portfolio+Selection%3A+Efficient+Diversification+of+Investments%2C+2nd+Edition-p-9781557861085.

POSITIVE TECHNOLOGIES. Cybersecurity Threatscape 2020. Disponible en: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity-Threatscape-2020.pdf. 2020.

Principales problemas de las empresas en Ciberseguridad, 2022. https://www.youtube.com/watch?v=GPsORgO2_kU.

RAMAKRISHNAN, R., y GEHRKE, J. (2003). Database management systems. McGraw-Hill Education.

RASTREA CRIMINALES COMO FBI: HERRAMIENTAS DE INFORMÁTICA FORENSE, 2021. [En línea]. Disponible en: https://www.youtube.com/watch?v=5tMkYvR2ZM4.

RAYMOND, E. S. The Cathedral and the Bazaar. O'Reilly Media, Inc. 1999

RAYMOND, Eric S. Cómo ser un hacker. [En línea]. [Consultado: 9 May 2023]. Disponible en: https://www.smaldone.com.ar/documentos/docs/comoserhacker.shtml.

RECIMUNDO [En línea]. v. 3, n. 2, p. 980–997. 2019. DOI 10.26820/recimundo/3.(2).abril.2019.980-997. Disponible en: https://recimundo.com/index.php/es/article/view/487. [Consultado: 11 April 2023].

REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [En línea]. 2016. [Consultado el 15 de abril de 2023]., Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

RIGHTS (OCR), Office for Civil. Health Information Privacy. HHS.gov [En línea]. 2021. [Consultado: 10 May 2023]. Disponible en: https://www.hhs.gov/hipaa/index.html.

ROUSE, M. Attack vector. TechTarget. Disponible en: https://searchsecurity.techtarget.com/definition/attack-vector. 2021.

RSA. How the RSA breach happened. [En línea]. 2017. Disponible en: https://www.rsa.com/en-us/company/newsroom/company-news/how-the-rsa-breach-happened.

SÁNCHEZ CRESPO, Luis Enrique. Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020 [En línea]. 2020. Universidad del Rosario, 2020. [Consultado: 9 May 2023]. ISBN 978-958-784-433-7. Disponible en:

https://editorial.urosario.edu.co/seguridad-informatica-editorial-universidad-del-rosario.html.

SANS INSTITUTE. Attack vectors. [En línea]. 2021. Disponible en: https://www.sans.org/security-awareness-training/ouch-newsletter/2013/attack-vectors.

SCHNEIER, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. 2013.

SEGURIDAD DIGITAL | Colombia Aprende. [En línea]. [Consultado: 9 de abril de 2023]. Disponible en: https://www.colombiaaprende.edu.co/recurso-coleccion/seguridad-digital.

SEMANA. Gravísimo: EPS Sanitas confirmó que fue víctima de un potente ciberataque; mientras, pacientes inundan las redes de quejas y hay aglomeraciones en centros. Semana.com Últimas Noticias de Colombia y el Mundo [En línea]. 2022. [Consultado: 12 May 2023]. Disponible en: https://www.semana.com/salud/articulo/la-eps-sanitas-confirmo-que-fue-victima-de-un-ciberataque-los-pacientes-inundan-las-redes-de-quejas/202228/.

SENTINELONE. Informe de Verizon sobre investigaciones de fugas de datos 2020 – Guía rápida para los CISO. SentinelOne ES [En línea]. 2020. [Consultado: 12 May 2023]. Disponible en: https://es.sentinelone.com/blog/the-cisos-quick-guide-to-verizons-2020-data-breach-investigations-report/.

SHABTAI, A., FLEDEL, Y., y ELOVICI, Y. Attacking industrial control systems: a chain reaction approach. IEEE Transactions on Industrial Informatics, 10(4), 2290-2299. 2014.

SHARMA, N., y DAHIYA, R. A Comprehensive Review of Authentication Mechanisms in Network Security. International Journal of Computer Sciences and Engineering, 2020. p. 8(3), 7-13. doi: 10.1109/IEMTRONICS48171.2020.9123550.

SILBERSCHATZ, A., KORTH, H. F., y SUDARSHAN, S. 2010.

SILBERSCHATZ, A., KORTH, H. F., y SUDARSHAN, S. Database system concepts. McGraw-Hill Education. 2010

SMITH, A. La ingeniería social como táctica de phishing. En Congreso Internacional. 2018.

SMITH, J. Understanding DDoS Attacks: Types, Vectors, and Mitigation Strategies. International Journal of Information Security and Cybercrime, 2018. p. 7(1), 15-22.

SNODGRASS, R. T., y AHUJA, A. Security issues in database systems. ACM Press. 1986

SONICWALL. (). 2021 SonicWall cyber threat report. [En línea]. 2021. Disponible en: https://www.sonicwall.com/techdocs/pdf/SonicWall-2021-Cyber-Threat-Report.pdf.

SSMA: ¡acciones que debes implementar ahora mismo!,. [En línea]. [Consultado: 10 May 2023]. Disponible en: https://blog-es.checklistfacil.com/ssma/.

STALLINGS, W. Seguridad en la era de la información. México: Pearson. 2014.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. (). ¿Qué es la protección de datos personales? [En línea]. 2019. [Consultado: el 15 de abril de 2023]. Disponible en: https://www.sic.gov.co/proteccion-de-datos-personales.

SWAN, M. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc. 2015

SYMANTEC. (). Internet Security Threat Report. [En línea]. 2019. Disponible en: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

THE BELMONT REPORT: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. [En línea]. 1979. [Consultado: 15 de abril de 2023].

THE DATA PROTECTION Act 2018. [En línea]. 2018. [Consultado: 15 de abril de 2023]. Disponible en: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf.

THE FULL STORY OF THE STUNNING RSA Hack Can Finally Be Told | WIRED. [En línea]. [Consultado: 9 May 2023]. Disponible en: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/.

THOMPSON, M. Impacto y consecuencias de los ataques DDoS en las organizaciones. [En línea]. 2020. Revista de Seguridad Informática, p. 8(2), 45-56.

TORRES, A. Seguridad en sistemas transaccionales: análisis de vectores de ataque y propuestas de mitigación. Trabajo de fin de grado. Universidad de Salamanca. 2018.

UBER SUFRE UN ATAQUE INFORMÁTICO - Un Hacker de 18 años Vulnera todo los Sistemas de la Empresa, [En línea]. 2022. Disponible en: https://www.youtube.com/watch?v=NxNsYVXyQGE.

UBER, Equipo. Pero al fin de cuentas, ¿Qué es Uber y cómo se usa? [En línea]. 2015. Disponible en: https://www.uber.com/es-CL/blog/que-es-uber/.

UNDERSTANDING DENIAL-OF-SERVICE ATTACKS | CISA. [En línea]. 2021. [Consultado: 9 May 2023]. Disponible en: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.

VERIZON. Data Breach Investigations Report. [En línea]. 2021. Disponible en: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.

VILLAMIZAR, Carlos. ¿Qué es NIST Cibersecurity Framework? GlobalSuite Solutions [En línea]. 2020. Disponible en: https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/.

WALSH, A., y ELLIS, L. Criminology: An interdisciplinary approach. [En línea]. 2007. Thousand Oaks, CA: SAGE Publications.

WARREN, H. S. Hacker's delight. Addison-Wesley. 2003.

WHITE, J. Mitigating Distributed Denial of Service Attacks. En S. J. Schmidt (Ed.),. Advances in Digital Forensics XIII. 2017. (pp. 129-142). Springer.

YOUNIS, M., y ALWAN, A. (). Design and Implementation of an IoT-based TransactionalSystem forQuality Management. Iraqi Journal of Science. 2021. Doi:0.24996/ijs.2021.62.2.30

ANEXOS

ANEXO A: RAE: Maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques.

1. Información General	
Tema	Maximización de la seguridad en sistemas transaccionales mediante una revisión sistemática y un enfoque integral para la mitigación de riesgos de ciberataques
Titulo	Maximización de la seguridad en sistemas transaccionales: revisión sistemática y enfoque integral para mitigación de riesgos de ciberataques.
Autor	Adriano Gutiérrez Poche.
Fuente bibliográfica	Para la elaboración de la monografía fue necesario consultar más de un centenar de fuentes bibliográficas las cuales enriquecieron el documento, a continuación, se relacionan algunas de ellas: ARROW, K. J. Essays in the theory of risk-bearing. 1971. North-Holland Pub. Co. CIBERSEGURIDAD ANTE EL CRIMEN TRANSNACIONAL Y LA CIBERDELINCUENCIA [PARTE 1/4]. LISA Institute [En línea]. [Consultado: 10 May 2023]. Disponible en: https://www.lisainstitute.com/blogs/blog/ciberseguridad-crimen-transnacional-ciberdelincuencia. COMISIÓN EUROPEA (2018). La estrategia de ciberseguridad de la UE: hacia un enfoque de seguridad cibernética más fuerte y resiliente. [En línea]. 2018. Luxembourg: Publications Office of the European Union. Disponible en: https://ec.europa.eu/digital-single-market/en/news/strategia-de-ciberseguridad-de-la-ue-hacia-un-enfoque-de-seguridad-cibernetica-mas-fuerte-y-resiliente. DELGADO Jefferson. Sistemas transaccionales, sistemas de apoyo a las decisiones y sistemas estratégicos. [En línea]. Disponible en: https://www.gestiopolis.com/sistemas-transaccionales-sistemas-de-apoyo-a-las-decisiones-y-sistemas-estrategicos/.

	GARCÍA, C. Y GONZÁLEZ, J. Análisis de vectores de ataque en sistemas transaccionales: un enfoque basado en el análisis de amenazas. Monografía de grado. (2017) Universidad Nacional de Colombia.
Año	2024
Resumen	El documento analiza la seguridad en sistemas transaccionales, enfocándose en mitigar los riesgos de ciberataques a través de una revisión sistemática y un enfoque integral. Identifica los principales vectores de ataque, como phishing, malware, y denegación de servicio, y evalúa cómo estos explotan vulnerabilidades en sistemas informáticos. Se plantea como problema central la necesidad de garantizar transacciones seguras debido al impacto económico y social de los ciberataques. A pesar de las medidas de seguridad actuales, los ciberdelincuentes emplean técnicas cada vez más sofisticadas, destacando la importancia de estrategias de prevención y mitigación. El documento emplea una metodología cualitativa basada en revisión documental y de entrevistas a expertos; el marco teórico aborda teorías sobre el riesgo y la ciberseguridad, subrayando conceptos clave como autenticación, autorización y encriptación. También describe vectores de ataque y amenazas como la ingeniería social y el malware. Desde un enfoque metodológico, se utilizan técnicas cualitativas para analizar casos documentados de ataques y vulnerabilidades en sistemas transaccionales. Las conclusiones preliminares destacan la vulnerabilidad persistente de estos sistemas, a pesar de los esfuerzos de ciberseguridad. Se propone una serie de recomendaciones, como la educación del usuario, el fortalecimiento de medidas de seguridad y la implementación de prácticas como autenticación multifactor y monitoreo continuo. Por último, aunque las empresas buscan la implementación de medidas de seguridad los atacantes utilizan técnicas cada vez más sofisticadas para comprometer los sistemas, como resultado el estudio proporciona un análisis exhaustivo de los riesgos asociados con los sistemas transaccionales y ofrece estrategias para fortalecer su seguridad y minimizar los riesgos destacando la importancia de una combinación de herramientas tecnológicas,

	mejores prácticas y educación continua con el fin de promover la confiabilidad en un entorno empresarial cada vez más digitalizado.
Palabras Claves	Sistema transaccional, ciberseguridad, vectores de ataque, phishing, malware, vulnerabilidades, DDoS, autenticación, encriptación
Contenidos	Introducción al problema de investigación. Definición y antecedentes del problema. Marco teórico: conceptos clave y teorías relevantes. Metodología: revisión bibliográfica y análisis de casos. Identificación de vectores de ataque prevalentes. Evaluación de vulnerabilidades en sistemas transaccionales. Recomendaciones y estrategias para mitigar riesgos. Conclusiones.

2. Descripción del problema de investigación

La creciente sofisticación de los ciberataques compromete la seguridad de los sistemas transaccionales, usados ampliamente en sectores empresariales y financieros. Estos sistemas son vulnerables a una variedad de vectores de ataque, lo que hace necesario identificar vulnerabilidades y fortalecer las medidas de protección para garantizar la integridad y confidencialidad de la información.

3. Objetivos

General:

Maximizar los factores de seguridad en los sistemas transaccionales y mitigar los riesgos de ciberataques a través de la revisión sistemática de literatura y la implementación de un enfoque integral de análisis, evaluación de vulnerabilidades y recomendaciones para organizaciones y usuarios

Específicos:

- Desarrollar un estado del arte de los vectores de ataque prevalentes que comprometen la seguridad de los sistemas transaccionales por medio del análisis de casos documentados de sistemas vulnerados estableciendo características y nivel de impacto.

- Evaluar las vulnerabilidades en los sistemas transaccionales mediante la aplicación de la metodología del ciclo de Evaluación de Vulnerabilidades y la puntuación de los CVSS para que organizaciones y usuarios implementen medidas de seguridad para minimizar los riesgos.

- Elaborar recomendaciones para las empresas que emplean sistemas transaccionales con el fin de que implementen factores de seguridad que permitan prevenir los ciberataques mediante la materialización de los vectores.

4. Metodología

Bajo la premisa que en la monografía no aplica un diseño metodológico, de forma general la revisión documental plantea los siguientes criterios para el proceso de revisión bibliográfica.

Se empleó un enfoque cualitativo exploratorio-descriptivo, basado en:

Revisión de literatura científica y técnica.
Selección de fuentes relevantes sobre vectores de ataque.
Análisis de casos documentados y entrevistas a expertos.
Aplicación del ciclo de evaluación de vulnerabilidades para categorizar riesgos.

5. Referentes teóricos

En el marco teórico se expone información de los siguientes temas:

Teoría del Riesgo: Fundamenta la evaluación de incertidumbres y riesgos en sistemas informáticos.

Teoría del Ataque Distribuido (DDoS): Examina la capacidad de múltiples sistemas para sobrecargar un objetivo.

Teoría de Ingeniería Social: Explora la manipulación psicológica como vector de ataque.
Teoría del Malware: Clasificación y análisis de software malicioso.

Conceptos Clave: Definición de sistema transaccional, ciberseguridad, vectores de ataque, entre otros.

6. Referentes conceptuales

Conceptos Clave: Definición de sistema transaccional, ciberseguridad, vectores de ataque, entre otros.

7. Resultados

- Identificación de los vectores de ataque más comunes, como phishing, inyección SQL y malware.
- Análisis de vulnerabilidades críticas en componentes de sistemas transaccionales, como bases de datos y autenticación.
- Desarrollo de estrategias de mitigación basadas en herramientas tecnológicas, mejores prácticas y políticas de seguridad.

8. Conclusiones

Los sistemas transaccionales enfrentan riesgos persistentes debido a la sofisticación de los ciberataques. Aunque las organizaciones adoptan medidas preventivas, estas no siempre son suficientes. Es esencial un enfoque integral que combine tecnología avanzada, educación de usuarios y políticas de seguridad robustas para minimizar el impacto de los ataques que se materialicen.

- se desarrolló una revisión sistemática de la literatura especializada donde se identifica que los vectores de ataque prevalentes, como el *phishing*, el *malware*, la ingeniería social y las vulnerabilidades de *software*, el correo electrónico son las principales amenazas para la seguridad de los sistemas transaccionales.

- Se evaluó el impacto generado en sistemas transaccionales vulnerados en los últimos cinco implementando la metodología de evaluación de vulnerabilidades que determina el nivel de criticidad del impacto

- Se redactó un decálogo con las recomendaciones para implementar en las empresas que administran sistemas transaccionales con el fin de minimizar la ocurrencia de situaciones de riesgo, está enfocada en garantizar la seguridad y confiabilidad de las plataformas y de la información que se administra y almacena.