ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO DE UNA METODOLOGÍA PARA OBTENER LA SUPERFICIE DE ATAQUE CIBERNÉTICO DE UNA EMPRESA DE TELECOMUNICACIONES”

TESIS DE GRADO

Previa a la obtención del Título de:

MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. PAOLO STEFANO LARA TILUANO

ING. CHRISTIAN DAVID OÑA SALAZAR

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Mi más sincero agradecimiento al tutor de este proyecto, el Ing. Lenin Freire, por la guía aportada a través de su desarrollo. A mis colegas de Telconet, quienes me brindaron su total apertura y comprensión.

Ing. Paolo Stefano Lara Tiluano

Agradezco la calidad de este trabajo a mi compañero de tesis Paolo Lara, cuyo compromiso y dedicación han sido esenciales para alcanzar este objetivo. Su apoyo incondicional y su manera de colaborar fueron clave para el desarrollo exitoso de este proyecto. También quiero expresar mi profunda gratitud a Andrés, Patricio y Alfonso, quienes me abrieron las puertas hacia el fascinante mundo de la ciberseguridad. Gracias a ellos, tuve la oportunidad de demostrar mis habilidades, ampliar mis conocimientos y desarrollarme profesionalmente en este campo que tanto me apasiona.

Ing. Christian David Oña Salazar

DEDICATORIA

El presente proyecto se lo dedico a toda mi familia: a mi madre, a mi padre y a mi hermano por demostrarme a diario su amor y su constante motivación a ser mejor cada día. A mi novia Madelyne, por apoyarme en cada una de las etapas importantes de mi vida.

Ing. Paolo Stefano Lara Tiluano

Dedico este trabajo a mi familia, quienes siempre están a mi lado brindándome su amor y apoyo en cada paso de mi vida. A mis padres, por ser mi guía y fortaleza, por enseñarme el valor del esfuerzo y la perseverancia. A mis hermanos, por ser mi inspiración constante y por su confianza en mí. Este logro es tan suyo como mío.

Ing. Christian David Oña Salazar

TRIBUNAL DE GRADUACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

Mgs. Lenin Eduardo Freire Cobo

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

Mgs. Juan Carlos García

REVISOR

DECLARACIÓN EXPRESA

Nosotros, PAOLO STEFANO LARA TILUANO y CHRISTIAN DAVID OÑA SALAZAR, acordamos y reconocemos que: La titularidad de los derechos patrimoniales de autor (derechos de autor) del proyecto de graduación corresponderá al autor o autores, sin perjuicio de lo cual la ESPOL recibe en este acto una licencia gratuita de plazo indefinido para el uso no comercial y comercial de la obra con facultad de sublicenciar, incluyendo la autorización para su divulgación, así como para la creación y uso de obras derivadas. En el caso de usos comerciales se respetará el porcentaje de participación en beneficios que corresponda a favor del autor o autores. El o los estudiantes deberán procurar en cualquier caso de cesión de sus derechos patrimoniales incluir una cláusula en la cesión que proteja la vigencia de la licencia aquí concedida a la ESPOL.

La titularidad total y exclusiva sobre los derechos patrimoniales de patente de invención, modelo de utilidad, diseño industrial, secreto industrial, secreto empresarial, derechos patrimoniales de autor sobre software o información no divulgada que corresponda o pueda corresponder respecto de cualquier investigación, desarrollo tecnológico o invención realizada por mí/nosotros durante el desarrollo del proyecto de graduación, pertenecerán de forma total, exclusiva e indivisible a la ESPOL, sin perjuicio del porcentaje que me/nos corresponda de los beneficios económicos que la ESPOL reciba por la explotación de mi/nuestra innovación, de ser el caso.

En los casos donde la Oficina de Transferencia de Resultados de Investigación (OTRI) de la ESPOL comunique al/los autor/es que existe una innovación

potencialmente patentable sobre los resultados del proyecto de graduación, no se realizará publicación o divulgación alguna, sin la autorización expresa y previa de la ESPOL.

Firmado electrónicamente por:
PAOLO STEFANO LARA TILUANO

ING. PAOLO STEFANO LARA TILUANO

Firmado electrónicamente por:
CHRISTIAN DAVID OÑA SALAZAR

ING. CHRISTIAN DAVID OÑA SALAZAR

RESUMEN

Los profesionales de ciberseguridad son responsables de identificar los riesgos que afectan a las empresas y por eso utilizan herramientas informáticas en sus operaciones para la identificación de vulnerabilidades. A pesar de contar con las estas, los profesionales de ciberseguridad no disponen de un producto que les permita monitorear y ampliar la visibilidad de sus activos tecnológicos en función de las tácticas empleadas por los ciberdelincuentes, y resulta necesario diseñar una solución que esté basada en los estándares de la industria y aborde la problemática.

En el presente trabajo se utilizaron herramientas de reconocimiento de activos tecnológicos como Nessus, Spiderfoot e IntelligenceX, con enfoque a las tácticas, técnicas y procedimientos más utilizados por los ciberdelincuentes.

Durante el proyecto se pudo observar que sí es factible diseñar una metodología que pueda ser implementada en un proveedor de servicios gestionados, de tal forma que pueda mejorar su postura de ciberseguridad. Finalmente se realizó una validación sobre la efectividad de la metodología propuesta.

Con los resultados, se concluyó que la herramienta producida puede beneficiar a los ingenieros de ciberseguridad para la obtención de la superficie de ataque, de tal forma que pueda ser replicado para otras empresas como servicio.

Palabras clave: Ciberseguridad, Superficie de Ataque, Brechas de Datos

ÍNDICE GENERAL

ABREVIATURAS

SAC	Superficie de Ataque Cibernético
COVID-19	Coronavirus Disease 2019
GCI	Global Cybersecurity Index
SANS	Sysadmin Audit Networing Security Institute
SBOM	Software Bill of Materials
CNT	Corporación Nacional de Telecomunicación
ARCOTEL	Agencia de Regulación y Control de las Telecomunicaciones
TI	Tecnologías de la Información
NVD	National Vulnerability Database
OSVDB	Open Source Vulnerability Database
SIEM	Security Information and Event Management
IDS	Intrusion Detection Systems
IOA	Indicadores de Ataque
IOC	Indicadores de Compromiso
IOE	Indicadores de Exposición
NIST	National Institute of Standards and Technology
CISO	Chief Information Security Officer

MTTD	Tiempo Medio de Detección
CAASM	Ciber Asset Attack Surface Management
CIS	Center for Internet Security
VPN	Virtual Private Network
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
TTP	Tácticas, Técnicas y Procedimientos
TOR	The Onion Router
ISP	Internet Service Provider
ONG	Organización Sin Fines De Lucro
GBPS	Gybabite por segundo
SSH	Secure Shell
SMB	Server Message Block
RDP	Remote Desktop Protocol
SNMP	Simple Network Management Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
DoS	Denial-of-Service

CSIS	Center for Strategic and International Studies
BEC	Business Email Compromise
IoT	Internet de las cosas
OT	Operative Technology
AiTM	Ataques de adversario en el Medio
CVSS	Common Vulnerability Scoring System
FIRST	Forum of Incident and Response Teams
OSINT	Open Source Intelligence
ASN	Autonomous System Numbers
SMTP	Simple Mail Transfer Protocol
DNS	Domain Name Service
HTML	HyperText Markup Language

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El panorama digital contemporáneo está lleno de desafíos, el principal de ellos es la gestión y seguridad de los activos cibernéticos. En las últimas décadas, el ciberdelito ha emergido como una amenaza global, generando un aumento significativo en el interés por la investigación en ciberseguridad. En la extensa competencia entre quienes atacan y quienes defienden, la identificación de vulnerabilidades se ha consolidado como un paso crucial para ambas partes. La naturaleza dinámica del panorama tecnológico ha dado como resultado un sistema complejo de soluciones, lo que dificulta la selección e implementación estructurada de herramientas compatibles de manera estructurada.

El incremento de brechas de seguridad tanto a nivel local como internacional, así como la evolución en las tácticas de los actores de amenazas, resaltan la necesidad urgente de una enfoque integral y estratégico de la ciberseguridad. Por ello, el enfoque de este trabajo es examinar la Superficie de Ataque Cibernético (SAC) como un método para abordar los peligros que aquejan la industria. Esta tesis se enfoca en un aspecto crucial de la SAC, el cual es la visibilidad. Al explorar la relación entre ciberseguridad y visibilidad, esta tesis busca responder dos interrogantes claves en esta investigación: cuáles es el rol de esta visibilidad y qué aplicación puede tener en la industria.

Esta tesis está dividida en cinco capítulos, cada uno de ellos contribuye a una respuesta integral a las interrogantes de investigación. El capítulo uno realiza una introducción al problema de estudio, los objetivos y el alcance del proyecto. El capítulo dos proporciona una revisión teórica sobre la seguridad informática, la superficie de ataque y los marcos de trabajo empleados en la industria. El capítulo tres realiza una revisión literaria sobre los reportes de seguridad emitidos por reconocidas firmas de seguridad a nivel nacional e internacional, bajo la premisa de identificar cuáles son los riesgos actuales a los que se enfrentan las empresas. El capítulo cuatro presenta un diseño para la obtención de la superficie de ataque cibernético, aplicando los criterios teóricos y prácticos previamente identificados, y generando una herramienta de fácil aplicación para las empresas y de gran poder consultivo. Finalmente, el capítulo cinco aborda un caso de uso en donde se aplica esta metodología a una empresa de telecomunicaciones.

Para validar el diseño propuesto, se tomó en cuenta los criterios de validación obtenidos previamente y fueron plasmados en una prueba de concepto que evidencia la utilidad de implementar esta metodología en ambientes reales. Este diseño demostró que el proyecto es viable porque existe una base de conocimiento y tecnología para la detección de la superficie de ataque. Además, se pudo implementar la prueba de concepto en un período de tiempo razonable ya que el alcance se encuentra limitado al diseño y desarrollo del marco de trabajo, mas no a un despliegue masivo. Este trabajo constituye una síntesis de los criterios esenciales que representan una consultoría estratégica para todas aquellas entidades que consideran adoptar una metodología de

reconocimiento de la superficie de ataque cibernético, así como propuestas de futuras investigaciones y aplicaciones.

CAPÍTULO 1: GENERALIDADES

1.1 Antecedentes

Una compañía especializada en soluciones tecnológicas con sede en Guayaquil, Ecuador se ha destacado por ofrecer servicios de conectividad y seguridad especialmente diseñados para el sector corporativo durante más de veinticinco años. Con un personal de planta que abarca un total aproximadamente de cinco mil empleados, la empresa ha manifestado cuestionamientos sobre la seguridad de su ecosistema digital.

El impacto de la pandemia de COVID-19 ha transformado drásticamente la dinámica empresarial, especialmente en el ámbito tecnológico. La abrupta transición hacia modalidades de trabajo remoto y el aumento exponencial en la demanda de servicios digitales han generado un crecimiento desmedido en el ecosistema tecnológico de la empresa. Este cambio acelerado ha creado un entorno propicio para la proliferación de riesgos cibernéticos, ya que la expansión no planificada

de la infraestructura digital ha dejado vacíos en términos de seguridad. La necesidad urgente de adaptarse a estas circunstancias ha aumentado la complejidad y la amplitud de la superficie de ataque, generando una preocupación adicional para la empresa.

Un detonante en la preocupación de la compañía sobre la identificación de riesgos se puso en evidencia con la reconocida amenaza de seguridad denominada Log4Shell. Publicada en diciembre de 2021, este fallo de seguridad afectó a una amplia cartera de soluciones tecnológicas, y según Ars Technica es la vulnerabilidad más severa jamás descubierta [1].

Su reconocimiento significó una ardua tarea, debido a la complejidad de no poderse identificar a nivel de servicios sino en la implementación de estos. Ello implicaba que los proveedores de servicios debían contar con un inventario de activos tecnológicos, mediante el cual pudieran realizar un control de seguridad y una auditoría de los componentes de desarrollo empleados en sus plataformas, conocido como Software Bill Of Materials (SBOM). La empresa se ha visto confrontada con la necesidad crítica de reevaluar su postura de seguridad, comprendiendo la importancia de una metodología eficaz para la identificación y gestión proactiva de riesgos cibernéticos.

En el contexto de las amenazas cibernéticas, la empresa involucrada ha experimentado carencias específicas en la ausencia de una herramienta fácilmente accesible y de rápida implementación. La identificación de riesgos críticos, como vulnerabilidades no parchadas y fugas de credenciales, se ha visto obstaculizada por la falta de una solución

integral, instando a la empresa a buscar métodos más eficientes para salvaguardar su infraestructura.

En conclusión, la falta de herramientas accesibles para identificar riesgos cibernéticos críticos ha resaltado la urgencia de implementar un mecanismo que brinde una visibilidad más efectiva, permitiendo a la empresa abordar de manera proactiva los desafíos emergentes en materia de seguridad.

1.2 Descripción del Problema

En la actualidad, todas las organizaciones se enfrentan a una creciente complejidad de amenazas cibernéticas. Factores como el tamaño de la organización y su actividad comercial no son limitantes ni decisivas a la hora de ser víctimas de un ciberataque. La rápida evolución de las tecnologías digitales ha expandido las superficies de ataque, proporcionando a los ciberdelincuentes un terreno fértil para explorar y explotar vulnerabilidades.

En este contexto, las empresas se encuentran en una constante batalla para salvaguardar sus activos digitales y datos confidenciales. Según el informe Security Report 2023 de la firma de seguridad ESET, el 69% de las empresas de Latinoamérica ha sufrido algún incidente de seguridad, siendo Ecuador víctima de ataques informáticos como phishing y ransomware [2]. Por otro lado, el Global Cybersecurity Index (GCI), métrica de referencia que evalúa el compromiso de las naciones en materia de ciberseguridad a nivel global, ubica a Ecuador en la posición 19 de 45 en el ranking de países de América Latina y el Caribe. En los

criterios de evaluación, las debilidades identificadas fueron el aumento de capacidad, las medidas y las acciones adoptadas, tanto técnicas como organizacionales [3]. Entre los parámetros evaluados, también se encuentran Costa Rica, Colombia y Uruguay, los tres países mejor posicionados de la región, ocupan los puestos 1, 2 y 3, respectivamente. Ecuador está por debajo de estos países en todos los parámetros evaluados.

A pesar de los avances en ciberseguridad, existe una brecha significativa en la capacidad de las entidades públicas y privadas para detectar de manera eficiente y automatizada las diversas superficies de ataque. Uno de los factores que inciden en esta problemática son los recursos disponibles. En el reporte 2023, de ESET, se afirma que el 65% de las organizaciones latinoamericanas no poseen un presupuesto suficiente para ciberseguridad. Por otro lado, el Sysadmin Audit Networking Security Institute (SANS) afirma que entre 2015 y 2025, el impacto financiero del cibercrimen crecerá globalmente en un 250%, representado en 10.5 trillones de dólares americanos, y que tan solo el 10% de las empresas estarán dispuestas asignar recursos para mejorar su seguridad informática con un crecimiento en 2023 del 11%, representado en tan solo 188 billones de dólares [4].

El impacto negativo que ocasiona un incidente de seguridad no es ajeno a la realidad ecuatoriana. Existe evidencia como el estudio realizado por la empresa de ciberseguridad ESET en 2022, encontró que Ecuador fue uno de los países de América Latina con mayor número de ataques de ransomware en el primer trimestre de ese año. El estudio también

encontró que la mayoría de estos ataques se aprovecharon de vulnerabilidades técnicas que podrían haberse evitado con una metodología adecuada de detección de superficie de ataque [5]. Esto demuestra que la ausencia de una metodología de detección de superficie de ataque resulta nociva para la correcta gestión de vulnerabilidades técnicas. Uno de los casos con mayor repercusión en Ecuador fue el ataque ransomware a la Corporación Nacional de Telecomunicaciones (CNT) en julio de 2021, el cual afectó a los sistemas de atención al cliente, agencias y contact center [6] [7]. La Agencia de Regulación y Control de las Telecomunicaciones de Ecuador (ARCOTEL), levantó una alerta nacional dirigida a los administradores de sistemas de Tecnologías de la Información (TI), por los equipos comprometidos con un ransomware de la familia RANSOMEXX. Esta amenaza afectó los ecosistemas de virtualización que alojan a los activos tecnológicos críticos para las operaciones de instituciones públicas [7].

Con base en lo expuesto, se evidencia que Ecuador presenta una brecha significativa en la detección y comprensión de las superficies de ataque, lo cual representa un riesgo significativo para la integridad, confidencialidad y disponibilidad de los sistemas informáticos. La falta de una metodología de obtención de la superficie de ataque dificulta la identificación temprana de vulnerabilidades y amenazas informáticas, comprometiendo así la postura de ciberseguridad y limitando la capacidad de respuesta ante posibles amenazas.

1.3 Solución propuesta

La solución propuesta es diseñar una metodología de superficie de ataque cibernético, basado en los riesgos cibernéticos identificados en la actualidad, y que pueda ser generada de forma consistente, modular y sistemática. El enfoque del proyecto será de tipo cualitativo con un alcance descriptivo, que permitirá explorar la ciberseguridad y sus implicaciones en cuanto a la ausencia de mecanismos de control y monitoreo.

En primer lugar, se ejecutará un análisis de contenido cualitativo sobre los incidentes de seguridad presentados a nivel nacional e internacional, tomando en cuenta los vectores de ataque presentados en las organizaciones y los esfuerzos utilizables según lo determinado en el estado del arte. Los instrumentos utilizados para el presente estudio serán reportes de ciberseguridad de firmas reconocidas y entidades de la industria de la ciberseguridad. Estos elementos facilitarán el planteamiento de una base de conocimiento sobre los escenarios de riesgos que presentan las empresas. Luego, se analizará el marco de trabajo más reconocidos en la ciberseguridad, MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK), que cuenta con una amplia gama tácticas, técnicas y procedimientos (TTP) relacionados a los escenarios de ataque aprovechados por los cibercriminales, y se escogerán aquellas tácticas, técnicas y procedimientos que permitan enfocar los esfuerzos en la detección de superficie.

Finalmente, se utilizará la metodología obtenida para realizar una implementación en una empresa de telecomunicaciones, para analizar los resultados obtenidos y evaluar la utilidad que ofrece frente a la postura de ciberseguridad de la organización.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar una metodología para la obtención de la superficie de ataque cibernético de una empresa de telecomunicaciones, basado en los reportes anuales de reconocidas firmas de seguridad nacionales y extranjeras, utilizando el marco de trabajo MITRE ATT&CK, para mejorar la postura de ciberseguridad y fortalecer la capacidad de respuesta ante amenazas.

1.4.2 Objetivos específicos

- Identificar los riesgos cibernéticos con mayor presencia en la actualidad, utilizando los reportes de ciberseguridad de una empresa local y una empresa multinacional, para identificar patrones de ataque de los actores de amenazas.
- Analizar el marco de trabajo MITRE ATT&CK para identificar qué tácticas, técnicas y procedimientos se adaptan mejor a la detección de superficies de ataque cibernético.
- Diseñar una metodología basada en los criterios de seguridad y marcos de trabajo estudiados, para la obtención de la superficie de ataque cibernético.

- Validar la metodología diseñada en una empresa de telecomunicaciones.

1.5 Metodología

El enfoque del proyecto será de tipo cualitativo con un alcance descriptivo, que permitirá explorar la ciberseguridad y sus implicaciones en cuanto a la ausencia de mecanismos de control y monitoreo. En primer lugar, se ejecutará un análisis de contenido cualitativo sobre los incidentes de seguridad presentados a nivel nacional e internacional, tomando en cuenta los vectores de ataque presentados en las organizaciones y los esfuerzos utilizables según lo determinado en el estado del arte. Los instrumentos utilizados para el presente estudio serán reportes de ciberseguridad de firmas reconocidas y entidades de la industria de la ciberseguridad. Estos elementos facilitarán el planteamiento de una base de conocimiento sobre los escenarios de riesgos que presentan las empresas, y con ello determinar aquellos puntos de dolor que deben ser considerados en la propuesta del diseño de la superficie de ataque.

Luego, se analizará el marco de trabajo con más reconocimiento en cuanto a ciberseguridad, como es MITRE ATT&CK, que cuenta con una amplia gama de tácticas, técnicas y procedimientos relacionados estrechamente a los escenarios de ataque aprovechados por los actores de amenazas. Posterior al análisis de estudio, se escogerán aquellas tácticas, técnicas y procedimientos que permitan enfocar los esfuerzos en la detección de superficie de ataque cibernético, para

finalmente establecer su incidencia sobre los ecosistemas tecnológicos analizados y así preparar el diseño de la metodología.

Finalmente, se utilizará la metodología obtenida para realizar una implementación en una empresa de telecomunicaciones, para analizar los resultados obtenidos y evaluar la utilidad que ofrece frente a la postura de ciberseguridad de la organización. Esto permitirá contextualizar el diseño propuesto frente a los casos de uso relacionados a las operaciones de ciberseguridad, los mismos que a criterio de la empresa corresponden a los más relevantes de acuerdo con sus necesidades.

CAPÍTULO 2: Marco Teórico

En este capítulo se presentarán los fundamentos conceptuales sobre la ciberseguridad, vulnerabilidades e inteligencia de amenazas. También se revisarán conceptos de la superficie de ataque, su importancia y cuáles son los dominios de análisis más importantes. Finalmente, se realizará una introducción sobre los marcos de trabajo utilizados en la industria de la ciberseguridad, su propósito de aplicación, así como sus ventajas y desventajas.

2.1 Fundamentos

2.1.1 Seguridad informática

La seguridad informática nace como como la necesidad de salvaguardar los sistemas tecnológicos que utilizan, almacenan y transmiten información, de accesos no autorizados, exfiltración, alteración y destrucción. La información es un activo crítico que las organizaciones deben proteger, ante el riesgo latente de ataques cibernéticos. En este escenario, muchas empresas han

surgido como figuras destacadas en esta industria. Una de ellas es EC-Council, una firma de ciberseguridad con más de 20 años de actividad, en constante búsqueda de soluciones efectivas y líderes de la industria para contrarrestar las crecientes amenazas cibernéticas, así como una amplia cartera de servicios como entrenamiento, certificaciones y servicios profesionales. Con un enfoque resiliente, EC-Council en su curso de preparación para ser un Certified Ethical Hacker [8] define la seguridad informática como un estado de bienestar de la información y la infraestructura, donde la amenaza de robo, manipulación o interrupción de los servicios es mantenida a niveles bajos o tolerables. Según su definición, la seguridad informática basa su funcionamiento en tres pilares fundamentales, conocidos como la tríada CID:

- *Confidencialidad*: Es la garantía de que la información es accesible solo para aquellos elementos autorizados. Las brechas que afectan a la confidencialidad ocurren principalmente por el manejo inadecuado o por un intento de ciberataque dirigido. Los controles enfocados a la confidencialidad incluyen segmentación, encriptación y gestión segura de los datos, físicos y digitales.
- *Integridad*: Es la confianza de los datos o recursos en la prevención de cambios inapropiados y no autorizados, esto es la confianza de que la información es suficientemente confiable para su propósito. Entre las medidas para mantener

la integridad de la data se encuentran: el uso de códigos de integridad para identificar de forma única a los elementos de información, y controles de acceso para asignar privilegios únicamente a aquellos elementos que lo requieren.

- *Disponibilidad*: es la garantía de que los sistemas responsables de la entrega, almacenamiento y procesamiento de la información sean accesibles cuando sean requeridos. Entre las medidas para mantener la disponibilidad de la información se incluyen: almacenamiento redundante y protección contra ataques de denegación de servicio (DoS).

2.1.2 Gestión de Vulnerabilidad Técnica

La gestión de vulnerabilidad técnica es la práctica iterativa de identificar, clasificar, remediar y mitigar vulnerabilidades [9]. En este apartado se introducen los conceptos de vulnerabilidad y los posibles mecanismos de seguridad que se pueden implementar, tanto para evitarlas como para solucionarlas cuando se presenten. Shirey define una vulnerabilidad como "una falla o debilidad en el diseño, implementación u operación y administración de un sistema que podría ser explotado para violar la política de seguridad del sistema". Desde su creación y descubrimiento inicial hasta su eliminación final, las vulnerabilidades pasan por varias etapas descritas en el ciclo de vida de la vulnerabilidad:

- *Hora de creación*: este es el momento en que se cometió el error durante el desarrollo del software. Se desconoce la fecha

exacta de este evento, ya que aún no se ha descubierto la vulnerabilidad. Podría haber una excepción en la que un actor malintencionado cree una vulnerabilidad a propósito; en este caso, la creación y el descubrimiento de la vulnerabilidad ocurren al mismo tiempo.

- *Tiempo de descubrimiento*: esta es la primera vez que se encuentra una vulnerabilidad en un software o sistema. La vulnerabilidad puede ser descubierta por los propios desarrolladores o proveedores, por actores malintencionados o investigadores de seguridad.
- *Tiempo de explotación*: esta es la primera vez que está disponible un exploit que aprovecha esa vulnerabilidad. A partir de este momento del ciclo de vida, el software vulnerable queda expuesto a un riesgo de seguridad, a veces sin el conocimiento del propietario del código.
- *Momento de divulgación*: este es el momento en que una persona confiable e independiente divulga públicamente una vulnerabilidad. Los canales comunes para dichas divulgaciones incluyen repositorios como el National Vulnerability Database (NVD) y el Open Source Vulnerability Database (OSVDB).
- *Tiempo disponible del parche*: este es el momento en que un proveedor lanza un parche que corrige la vulnerabilidad. Esto puede suceder tanto antes como después del momento de divulgación pública. Las medidas que podrían mitigar la

vulnerabilidad, como herramientas antivirus o sistemas de prevención de intrusiones, no se consideran parches porque no eliminan la causa raíz.

- *Tiempo de instalación del parche*: este es el momento en el que el usuario instala el parche, finalizando con la vulnerabilidad y por tanto con su ciclo de vida. Esta fecha puede variar mucho dependiendo de la prioridad del parche en cuanto al riesgo que supone o la política de parcheo de una organización.

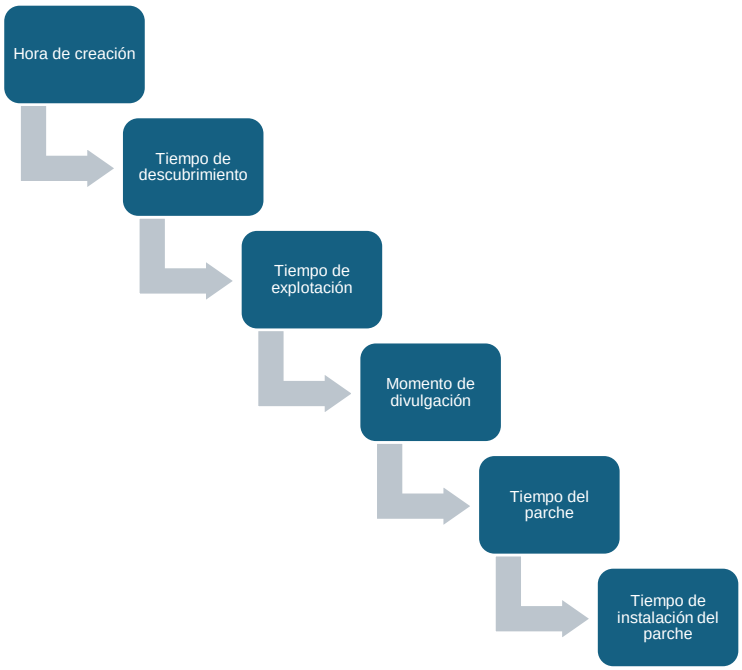


Figura 1: Proceso de gestión de una vulnerabilidad encontrada. Fuente: P. Foreman.

Por su parte, el ciclo de gestión de vulnerabilidades comienza en la definición de efectividad de las políticas y procedimientos actualmente implementados. Si una compañía ya tiene un sistema de gestión de seguridad de la información es importante establecer aquellos riesgos que pudieran estar asociados a esta

implementación, así como posibles puntos ciegos no contemplados. Para una mejor visualización, se recomienda tomar la perspectiva de un atacante externo, así como uno interno. Sobre esa premisa, se puedan definir objetivos, establecer alcances, hacer un control de seguimiento de los ejercicios, entre otras actividades. Para este propósito, se tomó como referencia la propuesta de EC-Council [10] para el estudio del ciclo de gestión de vulnerabilidades:

- *Definición de línea base*: este primer paso sirve para definir el plan de acción, alcance de las pruebas, objetivos principales y procedimientos.
- *Evaluación de Vulnerabilidades:* en esta fase se ejecuta un escaneo de vulnerabilidades para identificar todos aquellos fallos de seguridad a nivel de sistema operativo, plataformas web y otros servicios expuestos. Esta etapa suele involucrar pruebas de Penetración, que son ejercicios que involucran un nivel técnico más especializado y que son aplicables en función del alcance provisto.
- *Evaluación de Riesgos:* en esta fase se identifican y clasifican los riesgos basados en técnicas de control. Las vulnerabilidades son categorizadas en función de su nivel de impacto, para luego presentar los resultados en reportes que identifiquen los problemas y el plan de tratamiento de riesgos correspondiente.

- *Remediación*: se refiere a la ejecución de los pasos para mitigar las vulnerabilidades en función de su nivel de impacto. En esta fase, el equipo de respuesta diseña el proceso de mitigación para solventar las vulnerabilidades.
- *Verificación*: esta fase ayuda a verificar si todas las fases anteriores han sido correctamente aplicadas, además de validar si las remediaciones fueron aplicadas. Es aquí donde se debe presentar evidencias que respalden que la ejecución del plan de tratamiento de riesgos ha sido efectiva y ha corregido fallos.
- *Monitoreo*: es importante recordar que los controles de seguridad deben ser monitorizados apropiadamente y actualizados mediante un plan de gestión de vulnerabilidad técnica. Herramientas como los SIEM (Security Information and Event Management), IDS (Intrusion Detection Systems) y Firewalls son útiles para este propósito.

2.1.3 Inteligencia de Amenazas

Frente a este panorama de vulnerabilidades, la obtención de una Inteligencia de Amenazas se erige como un componente esencial. Mientras que la Gestión de Vulnerabilidades se enfoca en identificar y corregir debilidades, la Inteligencia de Amenazas amplía esta perspectiva. Gartner, empresa consultora líder en investigación de las tecnologías de la información, lo define como el conocimiento basado en evidencia que incluye contexto, mecanismos, indicadores, implicaciones y consejos prácticos

sobre una amenaza o peligro existe o emergente hacia los activos, que puede utilizarse para informar decisiones sobre la respuesta ante estas amenazas o peligros [11]. Esta inteligencia ayuda a las organizaciones a identificar y mitigar varios riesgos en las compañías, al convertir amenazas desconocidas en peligros conocidos, a la vez que facilita a la implementación de estrategias integrales y avanzadas para la mejora de la postura de ciberseguridad [8] .

Se consideran dos tipos de enfoques [12] en cuanto al tipo de datos con los que se operan en la Inteligencia de Amenazas:

- *Indicadores de Ataque (IOA)***:** representan un punto de vista proactivo, pues corresponden a una serie de acciones que un adversario debe realizar para tener éxito. Es posible ilustrar este indicador mediante la táctica más común y aún más exitosa de adversarios decididos: el phishing. Un correo electrónico de phishing exitoso debe persuadir al objetivo a hacer clic en un enlace o abrir un documento que infectará la máquina. Una vez comprometido, el atacante ejecutará silenciosamente otro proceso, se ocultará en la memoria o en el disco y mantendrá la persistencia durante los reinicios del sistema. El siguiente paso es ponerse en contacto con un sitio de comando y control, informando a sus responsables que espera más instrucciones. Los IOA se preocupan por la ejecución de estos pasos, la intención del adversario y los resultados que intenta lograr. Los IOA no se centran en las

herramientas específicas que utiliza para lograr sus objetivos. Al monitorear estos puntos de ejecución, recopilar los indicadores y consumirlos a través de un motor de inspección de ejecución con estado, es posible determinar cómo un actor obtiene acceso exitosamente a la red e inferir su intención.

- *Indicadores de Compromiso (IOC)***:** representan a una perspectiva reactiva, ya que menudo se describe en el mundo forense como evidencia en una computadora que indica que se ya ha violado la seguridad de la red. Los investigadores suelen recopilar estos datos después de ser informados de un incidente sospechoso, de forma programada o después de descubrir llamadas inusuales de la red. Idealmente, esta información se recopila para crear herramientas "más inteligentes" que puedan detectar y poner en cuarentena archivos sospechosos en el futuro.

De manera complementaria, aparecen un nuevo tipo de artefactos llamado Indicadores de Exposición (IOE), los cuales consideran todas aquellas debilidades propias de la infraestructura de las empresas que pueden ser usadas como vías de explotación para los actores de amenazas [13]. Algunos de los elementos considerados IOE son:

- *Vulnerabilidades*: son aquellas debilidades en aplicaciones, complementos, sistemas operativos, bases de datos y demás herramientas de gestión tecnológica, volumen considerable de fallos de seguridad.

- *Configuraciones inadecuadas*: a nivel perimetral, controles de acceso parcial o totalmente permisivas hacia la infraestructura crítica; a nivel de usuarios finales, hardware y software sin controles de acceso que faciliten el uso no autorizado de dichas herramientas.

2.2 Superficies de ataque

2.2.1 Definiciones

El análisis de la Superficie de Ataque juega un rol crucial en la gestión de la seguridad informática. Según el National Institute of Standards and Technology (NIST) se define como el conjunto de posibles puntos o vectores de ataque en la frontera de un sistema o de sus componentes, donde un usuario mal intencionado, denominado ciber atacante, puede intentar ingresar y extraer datos [14]. El propósito del análisis de la superficie de ataque es comprender las áreas de riesgos de los activos informáticos, para concientizar a los administradores de sistemas y especialistas de ciberseguridad sobre aquellos, encontrar vías para minimizar el impacto y evidenciar cuándo y cómo la superficie de ataque cambia y lo que esto representa en términos de gestión de riesgos [15].

2.2.2 Obtención de la superficie de ataque

La obtención de la superficie de ataque es un proceso iterativo y cíclico [16], y normalmente funciona mediante los siguientes pasos que se pueden apreciar en la Figura 2.

Figura 2: Proceso de obtención de superficie de ataque.
Fuente: Scrut Automation

- *Levantamiento de activos*: el primer paso es descubrir todos los activos dentro del entorno de una organización, lo que implica identificar hardware, software y datos presentes. Se crea un inventario preciso de todos los activos y se desarrolla un programa sólido para agregar nuevos activos al inventario y eliminar o aislar aquellos que no cumplen con las normativas o representan una amenaza de seguridad. Esta fase ayuda a comprender la superficie de ataque y tomar decisiones informadas sobre cómo asegurarla.

- *Evaluación de vulnerabilidades*: el siguiente paso consiste en identificar y evaluar las vulnerabilidades en los activos de la organización, lo cual implica escanear sistemas, aplicaciones y bases de datos en busca de vulnerabilidades conocidas, y evaluar el impacto potencial de cada vulnerabilidad en caso de un ataque.
- *Inteligencia de Amenazas*: en este proceso también recopilar y analizar datos para comprender los tipos de amenazas a los que se enfrenta la organización, a la vez que se integra la utilización de fuentes internas, como registros y tráfico de red, o fuentes externas, como feeds de inteligencia de amenazas [17].
- *Monitoreo continuo*: completados los primeros tres pasos, el proceso evoluciona hacia el monitoreo continuo de los activos de la organización para detectar y responder rápidamente a posibles amenazas, reduciendo el tiempo medio de detección (MTTD) y respuesta ante una amenaza de varios días a solo algunas horas.
- *Gestión de riesgos*: capacitar a los Chief Information Security Officer (CISO), o Gerentes de Seguridad Informática, para evaluar y gestionar de manera efectiva los riesgos asociados con sus activos. Este proceso incluye cuantificar el impacto de cada vulnerabilidad y evaluar la probabilidad de un ataque exitoso. Posteriormente, se emplean esfuerzos de remediación priorizados y se toman decisiones informadas

sobre los activos que requieren protección inmediata. Un proceso integral de gestión de riesgos capacita a los gerentes de seguridad para minimizar el riesgo de ataques exitosos y preservar la confidencialidad, integridad y disponibilidad de sus activos.

- *Remediación*: implementar controles de seguridad apropiados para mitigar los riesgos asociados con los activos implica aplicar parches de software, configurar firewalls e implementar políticas y procedimientos de seguridad. Además, los activos con riesgos de seguridad conocidos pueden ser aislados para prevenir una mayor exposición.
- *Mejora continua*: este proceso iterativo y en curso asegura que los CISOs monitoreen y reevalúen continuamente los activos de su organización para mantener una postura de seguridad sólida. Involucra la actualización del inventario de activos, la reevaluación de vulnerabilidades e implementación de nuevos controles de seguridad. Las soluciones CAASM (Cyber Asset Attack Surface Management) permiten a las organizaciones asegurar la seguridad de sus activos con confianza.

2.2.3 Obstáculos para su diseño

Resulta comprensible que las organizaciones pueden protegerse de los ciberataques únicamente siguiendo las buenas prácticas, como el despliegue de escáneres de vulnerabilidades, aplicación de parches de actualización y seguridad, e implementación

robusta de controles de seguridad [18]. Varias de estas medidas están fundamentadas en los controles del Center of Internet Security (CIS). Sin embargo, existen varios motivos que sugieren que la aplicación de estas medidas, por sí mismas, rara vez suelen ser poco efectivas.

- *Volumen masivo de datos:* actualmente las empresas manejan un volumen considerable de vulnerabilidades en sus ecosistemas. Si no existe una adecuada gestión de vulnerabilidad técnica, los equipos de ciberseguridad no podrán identificar y priorizar los hallazgos, y por consecuencia aumentar los tiempos de respuesta ante nuevas amenazas avanzadas.
- *Topología compleja*: se origina como consecuencia del punto anterior, en adición a las existentes vulnerabilidades y configuraciones inadecuadas de seguridad, lo cual expone a las organizaciones a ataques que no pueden ser detectados por soluciones tradicionales de ciberseguridad, ocasionando varios puntos ciegos en la topología. Por ejemplo, un virus informático puede ingresar a la red corporativa a través de una conexión de terceros, incluso si las conexiones están protegidas por soluciones como Virtual Private Networks (VPN) y control de accesos.
- *Ausencia sistemática de la reducción:* muchas compañías carecen de las herramientas para obtener y correlacionar eventos útiles para la visualización de la superficie de ataque,

lo cual evidencia una limitación tecnológica para identificar los riesgos más críticos, estableciendo prioridades para la gestión de remediaciones y destinando recursos a las áreas más vulnerables.

2.3 Marcos de trabajo

2.3.1 Adversarios

Para comprender lo que se debe proteger, es crucial conocer a los adversarios que llevan a cabo ataques contra nuestra organización. Los objetivos de un adversario pueden variar, desde robo de datos, espionaje, sabotaje hasta extorsión [19]. La distribución de los adversarios se presenta en una pirámide mostrada en la Figura 3, donde en la cima se encuentran los "script kiddies" que utilizan herramientas preconstruidas, mientras que en la base se sitúan el crimen organizado y las Advanced Persistent Threats (APT) [20].

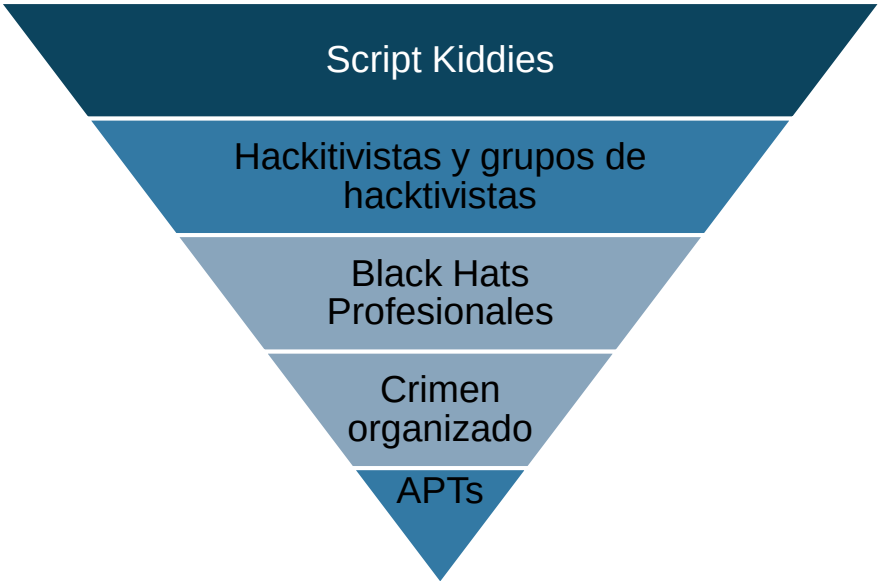


Figura 3: Distribución de los adversarios. Fuente: Wiley.

La atribución de incidentes de seguridad puede ser desafiante, ya que los ataques, como el espionaje o los ciberataques, pueden disfrazarse fácilmente como acciones de otro país o grupo. La atribución se basa en el método de ataque, las herramientas utilizadas y el análisis del código de malware encontrado. La falta de regulaciones internacionales y la privacidad de la información complican la recopilación y el intercambio de datos para realizar la atribución [21].

Comprender las motivaciones de los atacantes es crucial para defenderse eficazmente. Las motivaciones intrínsecas y extrínsecas dividen los impulsos detrás de un ataque, ya sea personalmente gratificante (intrínseco) o con recompensas externas, como el pago por el ataque (extrínseco) [22].

Cuando los atacantes comprometen infraestructuras, dejan IOCs como direcciones IP, nombres de dominio, URL, valores hash

SHA-256 y MD5, o cambios en la configuración del sistema operativo [23]. La "Pirámide del Dolor" de David Bianco muestra la relación entre estos indicadores, destacando que los valores hash son los más efectivos, ya que cualquier cambio en el archivo altera el valor hash [24].

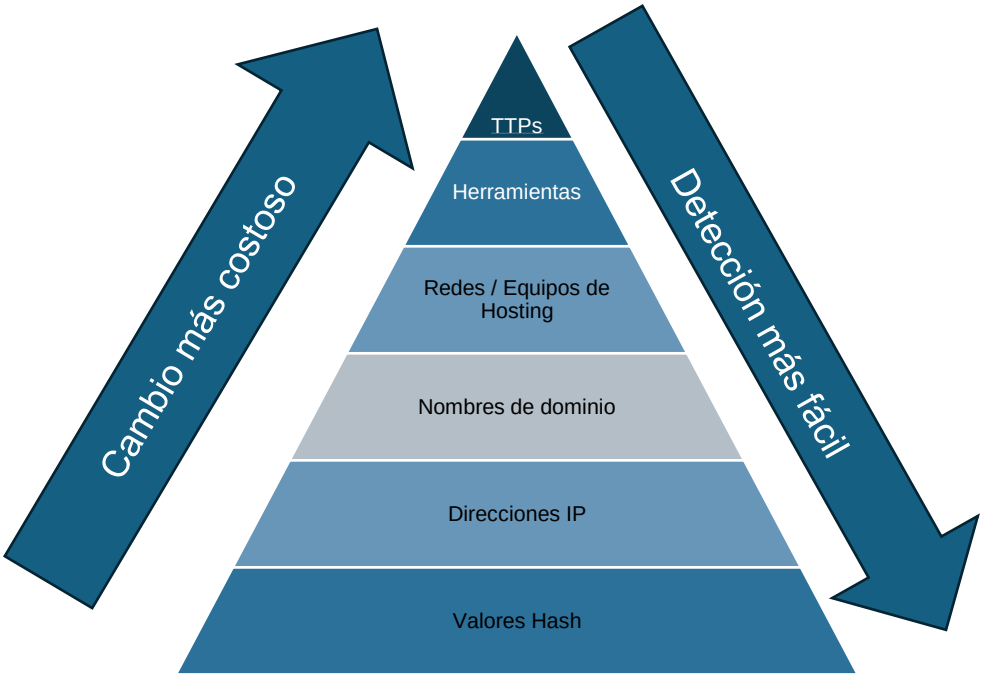


Figura 4: Pirámide del dolor. Fuente: David Bianco

La pirámide también destaca que las direcciones IP son fáciles de cambiar o falsificar mediante el uso de VPN, proxys anónimos, The Onion Router (Tor) u otras infraestructuras capturadas [25]. Los nombres de dominio son más costosos para cambiar, ya que requieren registro y pago, lo que lleva tiempo [24]. Los artefactos de red y host implican la comunicación del adversario con entidades externas, y las tácticas y procedimientos son la cima de la pirámide, representando la inteligencia más valiosa para los defensores [26].

La motivación del atacante influye en la elección de herramientas. El malware, un término amplio para software malicioso, abarca desde gusanos hasta troyanos y keyloggers [27]. Detectar el uso de herramientas específicas puede impactar significativamente al adversario, forzándolo a cambiarlas y, potencialmente, aumentando el tiempo requerido para preparar el próximo ataque [24].

2.3.2 Postura defensiva por capas

Los controles defensivos de seguridad engloban personas, procesos y tecnologías que protegen las redes organizativas contra intrusiones [28]. La estrategia de defensa en profundidad busca salvaguardar el entorno contra ciberataques y ralentizar al adversario [29]. Se necesita más de un control defensivo para detectar los pasos del adversario en los sistemas de la organización, y si uno falla, otro debería detener o detectar el ataque en la siguiente etapa [29]. Dada la diversidad de adversarios y sus métodos, no hay un método, herramienta o solución única para detener ataques [30]. Es crucial aumentar el costo para el atacante en cada recurso posible, ya que podría haber comprometido diversos recursos dentro de la organización [23].

El diseño de defensa en profundidad describe tres tipos de controles:

(1) Técnicos, como antivirus, firewalls y herramientas de monitoreo de red, el foco principal de este trabajo [29].
(2) Procedimentales, incluyendo políticas empresariales y directrices sobre el uso de dispositivos y datos.
(3) Físicos, como puertas cerradas con llave o cercas para limitar el acceso físico [29].

Estos controles se clasifican en tres esquemas:

(1) Detectores proporcionan visibilidad sobre incidentes, ya sea técnicos o físicos.
(2) Preventivos pueden detener incidentes, ya sea con seguridad física o sistemas de prevención de intrusiones.
(3) Correctivos procedimentales, incluyen planes de respuesta a incidentes y continuidad del negocio [31].

Chapple y Seidl sugieren el diseño de seguridad en capas en defensa en profundidad, enfocándose en proteger el activo más crítico: la seguridad de datos [29].

La eficacia de la seguridad en capas se respalda mediante soluciones de monitoreo y detección bien diseñadas, como los SIEM [29]. Es crucial comprender el entorno para que el monitoreo sea efectivo [32]. La investigación de Khalid et al. (2021) [33] destaca que la detección exitosa de un ataque de APT implica correlacionar todas las etapas del proceso, señalando que esto sigue siendo un problema de investigación abierto.

2.3.3 MITTRE ATT&CK Framework

Lockheed Martin desarrolló el primer modelo de adversario llamado Cyber Kill Chain en 2011, trazando los pasos específicos de un adversario al atacar a una organización, desde el reconocimiento hasta el despliegue de armas y acciones de comando y control [34]. MITRE Corporation, mediante ATT&CK Framework, amplió una base de conocimientos que rastrea el comportamiento de los adversarios en diversas fases del ciclo de ataque. La versión 10 contiene 14 tácticas y más de 500 técnicas y subtécnicas combinadas [35]. En comparación con el modelo Lockheed Martin, el marco MITRE ATT&CK es más completo, proporcionando un mayor nivel de abstracción para ilustrar el comportamiento del adversario y está en constante evolución con el respaldo de la comunidad [36].

El ATT&CK Framework describe cómo los adversarios obtienen acceso inicial, se mueven lateralmente, escalan privilegios y evaden las defensas de una organización. Organiza estos comportamientos en tácticas, técnicas y procedimientos, permitiendo a los defensores comprender los métodos específicos utilizados en actividades maliciosas [37]. Hallberg demostró en su tesis de maestría cómo el marco MITRE ATT&CK se utiliza para visualizar y detectar intrusiones [38]. Este marco respalda los artefactos creados en esta tesis basados en investigaciones anteriores.

2.3.3.1 Tácticas

Las tácticas representan el nivel más abstracto de la matriz ATT&CK. Describen por qué un atacante opera, mientras que las Técnicas y Subtécnicas explican cómo lo hacen [37]. En la versión 10 de MITRE ATT&CK Matrix for Enterprise, hay 14 tácticas diferentes, cada una con un identificador único para facilitar el uso programático [39]. Por ejemplo, el objetivo estratégico de un adversario podría ser obtener beneficios mediante ransomware, y este objetivo táctico residiría en TA0040 – Impacto [40].

2.3.3.2 Técnicas

Las Técnicas MITRE ATT&CK describen cómo los adversarios logran objetivos tácticos al realizar una actividad, abordando el "cómo" y, en algunos casos, el "qué" obtiene el adversario al completar una acción [35]. La Versión 10 incluye 188 Técnicas, y las diferencias entre Tácticas, Técnicas y Subtécnicas se ilustran en la matriz [39]. Por diseño, las acciones de los adversarios pueden mapearse a múltiples Técnicas, como el uso de código malicioso, que puede vincularse a varias Técnicas ATT&CK [41]. Una única técnica puede formar parte de diversas tácticas, como por ejemplo T1078 - Cuentas Válidas, presente en cuatro tácticas diferentes [39]. Los adversarios priorizan la identificación de cuentas administrativas en la fase de Acceso Inicial para su uso

posterior en movimiento lateral, persistencia y cumplimiento de misiones [32].

2.3.3.3 Procedimientos

Las Procedimientos describen cómo el adversario implementa Técnicas o Subtécnicas, detallando el uso específico en entornos reales y señalando comportamientos adicionales. Pueden indicar el uso de herramientas específicas cuando se alcanzan objetivos tácticos [35].

CAPÍTULO 3: IDENTIFICACIÓN DE RIESGOS CIBERNÉTICOS

La ciberseguridad es un tema de creciente importancia hoy, debido al aumento de los ataques cibernéticos. Estos ataques pueden tener un impacto significativo en las organizaciones, tanto en términos económicos como reputacionales.

Para identificar los riesgos cibernéticos y poder integrar el estado del arte con el desarrollo de una metodología de reconocimiento de superficie externa, se realizó una revisión exhaustiva de la literatura especializada en ataques cibernéticos, focalizándose en la identificación de los más relevantes contemporáneos.

Los informes seleccionados para este trabajo son "Reporte Tráfico Malicioso Ecuador 2022" de Telconet [42] y "Microsoft Digital Defense Report: Building and improving cyber resilience" de Microsoft [43], que ofrecen una visión única y valiosa de la situación actual de la ciberseguridad. Por un lado, el informe de Microsoft proporciona una perspectiva global, abordando los desafíos cibernéticos a nivel internacional, mientras que el reporte de Telconet se

enfoca en la realidad específica de las amenazas y tráfico malicioso en Ecuador.

La incorporación de perspectivas locales e internacionales busca entender los desafíos de las organizaciones en el panorama cibernético actual, permitiendo así una estrategia de seguridad más robusta y adaptada a las circunstancias específicas de la entidad en la que se probará la metodología desarrollada.

Esta revisión comprende los siguientes aspectos de manera detallada:

- Estado del cibercrimen.
- Los tipos de ataques cibernéticos más comunes.
- Las vulnerabilidades explotadas en estos ataques.
- Los impactos potenciales de estos ataques.
- Retos que enfrenta la ciberseguridad en la actualidad.

3.1 Revisión de Literatura

3.1.1 Análisis del reporte de tráfico malicioso en Ecuador 2022 por Telconet

3.1.1.1 Estado del cibercrimen en Ecuador

El informe revela un panorama preocupante en cuanto a la ciberseguridad en Ecuador durante el año 2022. Se destaca un aumento en la cantidad de ataques cibernéticos y una variedad de amenazas dirigidas tanto al sector empresarial como al residencial.

En este informe se expone una tabla donde se muestra los ataques y vulnerabilidades generadas en Ecuador a organizaciones por tipo de actividad comercial donde se observa que todos los negocios

comerciales están en riesgo de incidentes de seguridad incluso servicios delicados como energías y petróleo y que los más atacados son los dedicados al Comercio.

Tipo de negocio	Vulnerabilidad	Incidente
Comercio	20.20%	16.11%
Servicios	17.56%	18.07%
Carrier Proveedor de Servicio de Internet (ISP)	5.39%	19.73%
Empresa	7.05%	7.68%
Telecomunicaciones	5.54%	3.77%
Gobierno	4.96%	4.37%
Industria	3.93%	1.51%
Financiero	3.70%	2.41%
Transporte	3.33%	1.81%
Educación Organización Sin Fines de lucro (ONG)	2.85%	4.07%
Retail	2.85%	1.96%
Educación	2.79%	1.51%
Salud	2.01%	1.36%
Agroindustria	1.92%	0.30%
Social	1.59%	0.45%
Hotelería	1.01%	0.30%
Negocio	0.81%	1.20%
Construcción	0.56%	0.60%
Energía y Petróleo	0.36%	0.15%

Tabla 1: Vulnerabilidades e incidentes reportados por tipo de negocio.
Fuente: Telconet

En este informe se indica que los ataques de DoS crecieron en gran cantidad y fueron los más recurrentes en 2022 con el mayor ataque detectado uno de 787.54 gigabytes por segundo (Gbps).

Los tipos de ataques cibernéticos más comunes reportados por Telconet fueron de tipo DoS y fuerza bruta. Se puede leer más información a detalle en Tabla 2.

Evento	Detalles
DoS	• Número de Eventos: 26,289 eventos de DoS de severidad alta. • Mayor Ataque: 787.54 Gbps • Duración del Ataque: 7 días.
Ataques de fuerza bruta	• Puerto Más Atacado: TCP/22 Secure Shell (SSH) indicando intentos de acceso no autorizado. • Tipos de Ataques: Conexión SSH, Conexión Server Message Block (SMB), Conexión Remote Desktop Protocol (RDP), entre otros.

Tabla 2: Tipos de ataque más comunes. Fuente: Telconet

Este incremento se justifica, según la publicación de ENISA THREAT LANDSCAPE 2023 que, en los últimos años, el COVID-19 primero y la invasión rusa de Ucrania después modificaron sustancialmente la amenaza [44]. Asimismo, el hacktivismo (con fines políticos) aumentó esta detección.

3.1.1.2 Vulnerabilidades explotadas en estos ataques

Las principales vulnerabilidades detectadas fueron los puertos expuestos y las vulnerabilidades empresariales. Se detalla a continuación el detalle de ellas:

- Puertos expuestos
  - Se detectó una alta exposición de puertos en pequeñas y medianas empresas.
  - Puerto 161 sobre User Datagram Protocol (UDP), servicio Simple Network Management Protocol (SNMP) y Puerto 22 sobre Transmission Control Protocol (TCP), servicio SSH fueron los más expuestos.

- Vulnerabilidades Empresariales:
    - Sectores más afectados: Comercio, Servicios, ISP/Carrier.
    - Vulnerabilidades asociadas a Microsoft Office (CVE-2017-11882), esta vulnerabilidad podría permitir ejecución remota de código. Este tipo de vulnerabilidad representa un riesgo sustancial para la seguridad, con posibles consecuencias como la instalación de malware o el robo de datos. Además, se destaca la presencia de ataques de fuerza bruta, táctica agresiva empleada por actores malintencionados para obtener acceso no autorizado a sistemas.

3.1.1.3 Impactos potenciales de estos ataques

El reporte revela que el sector residencial, seguido por la educación y el financiero, experimentó el mayor impacto de ataques en 2022 por ataques DoS y compromisos empresariales. En el informe, se reporta que el impacto de los ataques DoS disminuyó y el número total de ataques aumentó en un 20% respecto al año anterior [42]. La presencia del malware de tipo MSIL/Kryptik causó gran impacto en el sector empresarial. Este malware está caracterizado por su capacidad para ocultar su presencia y ejecutar acciones dañinas en sistemas Windows, así como

el malware de tipo W32/Injector, que se especializa en inyectar código malicioso en procesos en ejecución [45].

3.1.1.4 Retos que enfrenta la ciberseguridad

El aumento en la diversidad y frecuencia de ataques se destaca los retos actuales en ciberseguridad en los siguientes puntos:

- Escaneo Activo:
  - Estados Unidos, Rusia y Alemania lideran los escaneos al sector empresarial ecuatoriano.
- Ingeniería Social y Correos Electrónicos Maliciosos:
  - Se destaca la continua amenaza de phishing y correos fraudulentos como vectores de ataque exitosos.
- Dispositivos Android:
  - El incremento del 8% al 36% en compromisos de dispositivos Android indica un cambio en las estrategias de ataque.

3.1.2 Análisis del informe de protección digital 2023 por Microsoft

3.1.2.1 Estado del cibercrimen global

Según el Informe de protección digital de Microsoft 2023, el estado del cibercrimen sigue siendo una amenaza importante para las empresas y los individuos en todo el mundo. El informe destaca que los ataques cibernéticos están en constante evolución y se están volviendo cada vez

más sofisticados, lo que hace que sea cada vez más difícil para las empresas y los individuos protegerse contra ellos.

Uno de los hallazgos clave del informe es que el panorama de amenazas cibernéticas está evolucionando hacia ataques más efectivos y dañinos, a menudo a gran escala. Según los datos presentados en el informe, las organizaciones enfrentaron un aumento general en los ataques de ransomware en comparación con el año anterior, mientras que el número de ataques de ransomware operados por humanos casi se triplicó [43]. Según el Center for Strategic and International Studies (CSIS), el ransomware fue la principal amenaza cibernética en 2023, representando el 60% de todos los ataques cibernéticos e incrementándose más del 45% durante el primer semestre del año en comparación al 2022 [46].

Algunos de los resultados presentados en este informe indican que los ataques de ransomware han crecido en gran cantidad y más específicamente indican que del 80 al 90% de ataques exitosos de ransomware se originan en dispositivos no administrados o identificados expuestos en la web. También indican que no solo grandes empresas son objetivos de este tipo de ataques, sino que incluso organizaciones con menos de quinientos empleados han sido víctimas de estos ataques. Esto resalta la importancia de implementar medidas de seguridad sólidas para todos

los dispositivos, incluidos los dispositivos personales utilizados para fines laborales.

El informe también indica que los ciberdelincuentes están utilizando una variedad de técnicas para comprometer sistemas y robar información valiosa. Están utilizando técnicas de ingeniería social como phishing y Business Email Compromise (BEC) para engañar a los usuarios y obtener acceso a sistemas y datos valiosos. El informe también destaca el creciente uso del cibercrimen como servicio por parte de los ciberdelincuentes para lanzar ataques a gran escala [43].

Éste enfatiza que los ataques cibernéticos están afectando una amplia gama de sectores, incluyendo gobierno, salud, educación y manufactura. Los ataques también están afectando una amplia gama de dispositivos, incluyendo computadoras, dispositivos móviles, dispositivos de internet de las cosas (IoT) y dispositivos de tecnología operativa (OT). Gartner indica que "los dispositivos IoT son cada vez más vulnerables a los ataques cibernéticos”. Estos dispositivos suelen estar conectados a Internet y tienen acceso a datos confidenciales. Los atacantes pueden explotar estas vulnerabilidades para robar datos, interrumpir el funcionamiento de los dispositivos o incluso causar daños físicos." [47]

En general, cabe destacar la importancia de la ciberseguridad hoy en día y la necesidad de que las empresas y las personas tomen medidas para protegerse contra las amenazas cibernéticas en constante evolución. Es importante mantenerse actualizado sobre las últimas técnicas y tendencias de ciberseguridad para adaptarse rápidamente a las nuevas amenazas.

3.1.2.2 Tipos de ataques cibernéticos más comunes

En cuanto a los tipos de ataques cibernéticos más comunes, el informe destaca que los atacantes continúan buscando el método más fácil para obtener acceso no autorizado a cualquier sistema a través de ataques de identidad, como intentos de fuerza bruta tradicionales, intentos sofisticados de rociado de contraseñas en múltiples países y direcciones IP, y ataques de adversario en el medio (AiTM). El phishing no desaparece y los atacantes utilizan tanto el phishing de malware para comprometer dispositivos como el phishing de AiTM para robar identidades que pueden ser utilizadas en actividades criminales adicionales, como el compromiso de correo electrónico empresarial [43]

El informe también destaca la creciente tendencia de los ataques de DoS y la creciente sofisticación de los ataques de ingeniería social, como el phishing y el BEC. Además, se mencionan los ataques de ransomware, que han

aumentado en número y sofisticación en los últimos años [43].

En general, el informe destaca la importancia de estar al tanto de los tipos de ataques cibernéticos más comunes y de implementar medidas de seguridad sólidas para protegerse contra ellos. Es importante que las empresas y las personas estén al tanto de las últimas técnicas y tendencias de ciberseguridad para adaptarse rápidamente a las nuevas amenazas y protegerse contra los ataques cibernéticos.

3.1.2.3 Vulnerabilidades explotadas en estos ataques

En cuanto a las vulnerabilidades explotadas en estos ataques, el informe destaca que los ciberdelincuentes están aprovechando una amplia variedad de vulnerabilidades en sistemas y dispositivos para comprometerlos y robar información valiosa. Por ejemplo, el informe menciona que los atacantes pueden explotar vulnerabilidades en el servidor web Boa para obtener acceso a redes y recopilar información sensible de archivos antes de moverse lateralmente en la red o iniciar ataques adicionales en un dispositivo. Además, muchas de las direcciones IP asociadas con los servidores web estaban asociadas con dispositivos IoT que tenían vulnerabilidades críticas sin parchear, lo que los convierte en un vector de ataque accesible para los operadores de malware [43].

El informe también destaca que los atacantes están explotando vulnerabilidades en software y sistemas operativos desactualizados, así como en aplicaciones y servicios en la nube. Además, los atacantes están utilizando técnicas de ingeniería social, como el phishing y el compromiso de correo electrónico empresarial, para engañar a los usuarios y obtener acceso a sistemas y datos valiosos [43].

En general, el informe destaca la importancia de mantener los sistemas y dispositivos actualizados con los últimos parches de seguridad y de implementar medidas de seguridad sólidas para protegerse contra las vulnerabilidades conocidas. También es importante estar al tanto de las últimas técnicas y tendencias de ciberseguridad para adaptarse rápidamente a las nuevas amenazas y protegerse contra los ataques cibernéticos.

3.1.2.4 Impactos potenciales de estos ataques

En cuanto a los impactos potenciales de estos ataques, el informe destaca que los ciberdelincuentes pueden causar una amplia gama de daños a las organizaciones y a los individuos. Por ejemplo, los ataques de ransomware pueden cifrar archivos y sistemas, lo que impide que los usuarios accedan a ellos hasta que se pague un rescate. Los ataques de phishing y compromiso de correo electrónico empresarial pueden permitir a los atacantes

acceder a información confidencial, como contraseñas y datos financieros, que pueden ser utilizados para cometer fraude o robo de identidad [43].

Además, los ataques pueden causar daños a la reputación de una organización, ya que los clientes y los socios pueden perder la confianza en la capacidad de la organización para proteger sus datos. Los ataques también pueden interrumpir las operaciones comerciales y causar pérdidas financieras significativas. En algunos casos, los ataques pueden tener consecuencias graves para la seguridad pública, como cuando se dirigen a infraestructuras críticas, como sistemas de energía y transporte [43].

En general, el informe destaca la importancia de tomar medidas para protegerse contra los ataques cibernéticos y minimizar los impactos potenciales. Es importante implementar medidas de seguridad sólidas, como la autenticación multifactor y la detección de comportamiento anómalo, para protegerse contra los ataques. También es importante tener planes de respuesta a incidentes en su lugar para minimizar los daños en caso de un ataque exitoso.

3.1.3 Comparativa entre riesgos cibernéticos locales y globales con enfoque en la identificación de superficie externa

La identificación de la superficie externa, entendida como la exposición digital de una organización, emerge como una estrategia clave para reducir vulnerabilidades y minimizar ataques cibernéticos. Al comparar los informes "Reporte Tráfico Malicioso Ecuador 2022" de Telconet y "Microsoft Digital Defense Report Building and improving cyber resilience," se destaca cómo esta aproximación se traduce en ventajas tangibles tanto a nivel local como global en cada uno de los puntos en los que se analizaron previamente.

3.1.3.1 Estado del cibercrimen

La identificación de la superficie externa permite una evaluación detallada de la situación cibernética ecuatoriana, destacando aumentos significativos en ataques. La visibilidad externa facilita la anticipación de posibles amenazas locales. A nivel mundial, la comprensión de la superficie externa es crucial para enfrentar amenazas en constante evolución. La identificación temprana de ataques de ransomware destaca la importancia de monitorear la exposición digital global.

La identificación de la superficie externa proporciona una visión proactiva tanto a nivel local como global,

permitiendo respuestas anticipadas a las amenazas emergentes.

3.1.3.2 Tipos de ataques cibernéticos

A nivel nacional, los ataques DoS y los ataques de fuerza bruta son detectados y mitigados más eficazmente mediante la evaluación de la superficie externa, con una atención específica a la exposición de puertos. La diversificación de los ataques a nivel mundial, desde ataques de identidad hasta ataques de DoS, resalta la necesidad de una comprensión holística de la superficie externa. La identificación proactiva de vulnerabilidades externas es esencial para contrarrestar tanto los ataques locales específicos como los desafíos cibernéticos más amplios.

3.1.3.3 Vulnerabilidades explotadas

En Ecuador, la exposición de puertos y las vulnerabilidades empresariales son abordadas eficientemente mediante una evaluación detallada de la superficie externa, especialmente en sectores específicos como Comercio y Servicios. A nivel global, la explotación de vulnerabilidades en servidores web y dispositivos IoT destaca la importancia de abordar la exposición externa a nivel global. Esto permite deducir que la identificación temprana de vulnerabilidades externas proporciona una ventaja crítica,

ya sea para proteger sectores locales específicos o abordar amenazas a escala global.

3.1.3.4 Impactos potenciales

En Ecuador, la comprensión de la superficie externa contribuye a la mitigación de impactos significativos en sectores residenciales y educativos, especialmente en ataques DoS y compromisos empresariales Globalmente, la prevención de pérdida de datos, interrupciones comerciales y daños a la reputación se ve facilitada por la identificación temprana de amenazas a través de la superficie externa. La gestión efectiva de impactos cibernéticos ya sea a nivel local o global, depende en gran medida de la capacidad para evaluar y reducir la exposición digital.

3.1.3.5 Retos de la ciberseguridad

Los desafíos locales como el escaneo activo son mejor abordados mediante una identificación precisa de la superficie externa, permitiendo respuestas focalizadas. Mundialmente, la sofisticación de ataques y la falta de personal capacitado se enfrentan mejor con una estrategia global que incluya la comprensión de la superficie externa. La identificación de la superficie externa emerge como un componente esencial para superar desafíos locales y globales, permitiendo respuestas adaptativas.

3.2 Análisis de los reportes de ciberseguridad

En la exploración detallada de los informes "Reporte Tráfico Malicioso Ecuador 2023" de Telconet y "Microsoft Digital Defense Report Building and improving cyber resilience," emerge un patrón claro: el estado de los ataques cibernéticos, tanto a nivel local como global, presenta similitudes notables. Este paralelismo no solo destaca la universalidad de las amenazas cibernéticas, sino también la necesidad crítica de estrategias unificadas para mitigar estos riesgos.

Ambos informes subrayan la creciente sofisticación de los ataques, desde ataques de fuerza bruta hasta intrusiones altamente especializadas, afectando no solo a empresas sino también a usuarios individuales. La convergencia de estos desafíos resalta la importancia de soluciones holísticas que aborden tanto las preocupaciones locales como globales.

En este contexto, el reconocimiento de la superficie externa se plantea como una herramienta indispensable. Al evaluar y comprender la exposición digital de una organización, se logra una visión integral que abarca desde vulnerabilidades locales específicas hasta amenazas cibernéticas globales en constante evolución.

La identificación temprana de ataques DoS y ataques de fuerza bruta en el ámbito local, así como la sofisticación creciente de ataques de ransomware a nivel global, destacan la necesidad de un enfoque estratégico y proactivo. La superficie externa no solo proporciona visibilidad sobre vulnerabilidades concretas, sino que también se

convierte en un facilitador clave para anticipar y mitigar los impactos potenciales.

La gestión efectiva de la exposición digital no solo se presenta como una solución sino como una necesidad urgente. La colaboración internacional para compartir las mejores prácticas en el reconocimiento de superficie emerge como un paso esencial. Al unificar esfuerzos y adoptar enfoques similares hacia la identificación proactiva de amenazas, se puede fortalecer la resiliencia cibernética en una era donde la interconexión global se traduce en desafíos compartidos. En última instancia, reconocer y gestionar la superficie externa no solo es una estrategia, sino la clave para una ciberseguridad eficaz en un mundo digital.

CAPÍTULO 4: EVALUACIÓN Y TRATAMIENTO DE RIESGO

En este capítulo se presenta un diseño de metodología para la obtención de superficie de ataque cibernético. El diseño fue desarrollado tanto en alto como en bajo nivel, y está alineado al ecosistema actual de riesgos en la ciberseguridad presentado en el capítulo tres. El diseño será validado por un oficial de ciberseguridad de la empresa de telecomunicaciones, que proveerá de retroalimentación y posteriormente aprobación para que la propuesta esté alineada a las necesidades de la empresa e implementarla.

El presente proyecto facilita a la empresa de telecomunicaciones tener a su disposición una herramienta útil y reproducible, para uso tanto interno como para clientes, que permita obtener un diagnóstico rápido acerca de la postura de ciberseguridad de una entidad, basado en su exposición pública.

4.1 Diseño en alto nivel

4.1.1 Análisis de vulnerabilidades

4.1.1.1 Propósito

Según como lo define la revista especializada en tecnologías de la información, TechTarget, la evaluación de vulnerabilidades, también conocida como análisis de vulnerabilidades, es el proceso de definir, identificar, clasificar y priorizar vulnerabilidades en sistemas informáticos, aplicaciones e infraestructuras de red [48]. Esta herramienta también provee a una organización del conocimiento necesario para tener un mejor entendimiento de sus activos tecnológicos y responder ante las amenazas cibernéticas que puedan afectarlos, reduciendo así la posibilidad que un cibercriminal pueda ganar acceso no autorizado a dichos sistemas.

4.1.1.2 Procedimiento

Para comenzar, es importante aclarar cuál será el alcance de este análisis. Tomando como referencia la ubicación de un atacante, se identificaron dos tipos de análisis de vulnerabilidades [49]:

- Evaluación Externa: es llevada a cabo desde la perspectiva de un atacante externo, en donde se analizan todos los activos digitales y sistemas informáticos accesibles desde Internet.

- Evaluación Interna: se ejecuta desde el plano de un atacante con acceso privilegiado al ambiente interno, en donde se estudian todos los activos y sistemas accesibles desde la red interna.

Para este proyecto se tomará en cuenta el caso externo, ya que es el punto de entrada principal de los atacantes, según lo descrito en el capítulo 3. Asimismo, se llevarán a cabo diversas etapas en el análisis de vulnerabilidades.

En el contexto del análisis de vulnerabilidades de la superficie externa, es importante alinearse con el marco de referencia MITRE ATT&CK para comprender cómo los actores maliciosos pueden llevar a cabo ataques desde el exterior de una organización. El enfoque principal se centrará en las técnicas y tácticas relacionadas con el reconocimiento y la explotación de activos accesibles externamente.

Dentro de la matriz MITRE ATT&CK, las tácticas que se aplican específicamente al reconocimiento de la superficie externa incluyen las siguientes TTPs:

T1071.001 - Reconocimiento a través de comandos externos: Los atacantes pueden utilizar herramientas de red, como *ping*, *traceroute* y *whois*, para identificar la estructura de la red, rangos IP y servidores expuestos públicamente.

T1595 - Active Scanning (Escaneo activo): Los actores maliciosos ejecutan escaneos de puertos (TCP y UDP) y servicios para detectar puertos abiertos, tecnologías expuestas y servicios mal configurados o vulnerables. Esto puede incluir el uso de herramientas como Nmap, Masscan y Shodan, que les permite mapear la superficie de ataque y determinar posibles puntos de entrada.

T1590.001 - Gather Victim Network Information: External Network Domains: Los atacantes pueden realizar búsquedas públicas para identificar nombres de dominio, subdominios, direcciones IP y otros activos accesibles desde el exterior, con el objetivo de entender mejor la superficie de exposición y su relación con los sistemas críticos de la empresa.

T1586.001 - Compromiso de Infraestructura Externa (Email Domains): En algunos casos, los actores maliciosos intentan comprometer dominios de correo electrónico asociados a la organización para llevar a cabo ataques de phishing o spear-phishing contra usuarios internos, lo que les permite acceder a la infraestructura interna.

T1596 - Search Open Websites/Domains for Victim Information: Los atacantes pueden usar sitios públicos y servicios como certificados Secure Sockets Layer (SSL) registros de Domain Name System (DNS), y otras fuentes

abiertas de información para obtener detalles sobre los servidores, aplicaciones web o bases de datos expuestas al exterior.

Primero, se realizará el despliegue de recursos, que implica la preparación de los servidores destinados al escáner de vulnerabilidades y la elección cuidadosa de la herramienta de escaneo que se utilizará. Esta fase es esencial para garantizar una evaluación efectiva y precisa.

A continuación, se procederá a la definición de parámetros, lo que implica identificar el alcance de las pruebas, los activos involucrados, perfiles de escaneo, tiempos de respuesta y otros elementos clave que influirán en el proceso de evaluación.

El despliegue de escaneos de puertos y servicios será una fase crucial, ya que se llevarán a cabo escaneos exhaustivos de todos los puertos TCP y UDP, validando los servicios activos y las tecnologías asociadas. Esto proporcionará una visión detallada de la superficie de ataque y las posibles vulnerabilidades.

Posteriormente, se ejecutarán los escaneos de vulnerabilidades, recopilando métricas importantes como la capacidad de explotación de las vulnerabilidades, el puntaje Common Vulnerability Scoring System (CVSS) asociado, la severidad de las vulnerabilidades, entre otros aspectos clave.

Finalmente, en la fase de análisis de resultados, se realizará un resumen detallado de los hallazgos, identificando los riesgos más prioritarios que requerirán una gestión inmediata. Este enfoque estructurado y metodológico se alinea con las prácticas recomendadas para realizar análisis de vulnerabilidades de manera efectiva. En esta propuesta, conviene disponer de una herramienta que permita categorizar los resultados obtenidos, priorizando así su respectivo tratamiento. Para ello, se tomó como referencia CVSS [50], el cual es un sistema de puntuación gratuito y abierto desarrollado por el Forum of Incident and Response Teams (FIRST).

Ampliamente considerado como el estándar de la industria para determinar la gravedad de las vulnerabilidades, el CVSS asigna una puntuación en una escala de 0.0 a 10.0.

Para el cálculo del puntaje CVSS, se utilizan los siguientes criterios:

- Vector de Acceso:
  - Red: La vulnerabilidad es explotable de forma remota a través de la pila de red, extendiéndose a posibles atacantes hasta incluir toda la Internet.
  - Adyacente: La vulnerabilidad está limitada a una topología lógicamente adyacente, compartiendo red física o lógica.

- Local: El componente vulnerable no está vinculado a la pila de red y el ataque puede ser local o remoto a través de capacidades de lectura/escritura/ejecución.
- Físico: El ataque requiere contacto físico con el componente vulnerable.

- Complejidad del Acceso
  - Bajo: No hay condiciones especiales. Un atacante puede tener éxito repetidamente.
  - Alto: Un ataque exitoso depende de condiciones fuera del control del atacante, requiriendo esfuerzo medible en preparación o ejecución antes de esperar éxito
- Privilegios Requeridos
  - Ninguno: El atacante no está autorizado antes del ataque y no requiere acceso a configuraciones o archivos.
  - Bajo: El atacante está autorizado con privilegios básicos que afectan configuraciones o archivos del usuario.
  - Alto: El atacante está autorizado con privilegios significativos, como administrativos, que afectan configuraciones y archivos a nivel de componente.
- Interacción del Usuario:
  - Ninguno: El sistema vulnerable puede ser explotado sin interacción alguna del usuario.

- Requerido: La explotación exitosa de esta vulnerabilidad requiere que un usuario realice alguna acción antes de que pueda ser aprovechada.

- Alcance:
  - No cambiado: Una vulnerabilidad explotada solo puede afectar recursos gestionados por la misma autoridad de seguridad. En este caso, el componente vulnerable y el componente afectado son iguales o ambos son gestionados por la misma autoridad de seguridad.
  - Cambiado: Una vulnerabilidad explotada puede afectar recursos más allá del alcance de seguridad gestionado por la autoridad de seguridad del componente vulnerable. En este caso, el componente vulnerable y el componente afectado son diferentes y están gestionados por diferentes autoridades de seguridad.
- Confidencialidad:
  - Ninguno: No hay pérdida de confidencialidad dentro del componente afectado.
  - Bajo: Existe cierta pérdida de confidencialidad. Se obtiene acceso a información restringida, pero el atacante no tiene control sobre qué información se obtiene, o la pérdida es limitada en cantidad o tipo.
  - Alto: Hay una pérdida total de confidencialidad, lo que resulta en que todos los recursos dentro del componente afectado se divulguen al atacante.

- Integridad:
  - Ninguno: No hay pérdida de integridad dentro del componente afectado. Bajo: Es posible la modificación de datos, pero el atacante no tiene control sobre las consecuencias de la modificación, o la cantidad de modificación es limitada.
  - Alto: Hay una pérdida total de integridad o una pérdida completa de protección. Por ejemplo, el atacante puede modificar todos los archivos protegidos por el componente afectado.
- Disponibilidad:
  - Ninguno: Sin impacto en disponibilidad.
  - Bajo: Reducción de rendimiento o interrupciones. El atacante no puede negar completamente el servicio.
  - Alto: Pérdida total de disponibilidad, el atacante puede negar completamente el acceso o causar interrupciones sostenidas o persistentes con graves consecuencias.

En la Tabla 3 se describe el desglose de la asignación de puntajes a los resultados encontrados.

Tabla 3: Clasificación de puntaje de vulnerabilidades. Fuente: CVSSv3

Rango de puntaje	Detalle
 CRITICO 9.0 – 10.0	Un intruso puede ganar control sobre el activo de información o existe una fuga potencial de información sensible de acuerdo con las políticas y regulaciones de seguridad de la información. La vulnerabilidad es explotable con un grado de complejidad de ataque medio o bajo y tiene un impacto mayor al activo vulnerable en la confidencialidad, integridad y disponibilidad.
 ALTO 7.0 – 8.9	Un intruso puede ganar acceso a cierta información específica almacenada en el activo de información incluyendo configuraciones de seguridad. Esto puede llevar al uso indebido del activo. La vulnerabilidad es explotable con un grado de complejidad de ataque medio y compromete al menos a dos de las propiedades de la seguridad de la información. El impacto es igual o superior al activo vulnerable.
 MEDIO 4.0 – 6.9	Un intruso puede obtener información acerca del activo como versiones precisas del software instalado. Esto puede ser utilizado para explotar las vulnerabilidades existentes específicas de cada versión. La vulnerabilidad puede ser explotable o no. Tiene un impacto igual al activo vulnerable. Afecta al menos a una propiedad de la seguridad de la información.
 BAJO 0.1 – 3.9	Los intrusos pueden recolectar información acerca del activo, por ejemplo, puertos abiertos y servicios en ejecución, que pueden utilizarse para encontrar otras vulnerabilidades. La vulnerabilidad no es explotable. Solo podría afectar a una de las propiedades de la seguridad de la información. El impacto abarca solo al activo vulnerable y puede ser corregido de forma inmediata con los recursos disponibles.

4.1.2 Análisis de Huella Digital

4.1.2.1 Propósito

En el contexto de ciberseguridad, es de vital importancia determinar la presencia que poseen las compañías en Internet. Por ello se destaca la importancia del manejo e integración de la inteligencia en las operaciones de ciberseguridad. La información es más valiosa cuando

contribuye al proceso de toma de decisiones, proporcionando una percepción razonada ante eventuales incidencias de ciberseguridad. Este análisis se enfoca en la transformación de datos en inteligencia mediante el análisis y la comparación, permitiendo que se aborden adecuadamente escenarios futuros. Se destaca la necesidad de evaluar el nivel de exposición de las compañías y el riesgo que ello implica, relevante para mitigar posibles fallos de seguridad. La inteligencia no es un fin en sí mismo, sino un medio para entender el entorno operativo y facilitar decisiones informadas. Este enfoque estratégico puede aplicarse al análisis de huella digital para prever y contrarrestar operaciones adversarias en el ciberespacio.

4.1.2.2 Procedimiento

En el contexto de ciberseguridad, el documento oficial JP 2-0 Joint Intelligence proporciona una guía valiosa sobre el proceso de inteligencia, específicamente en la Operación de Recopilación de Open Source Intelligence (OSINT). De origen militar y emitido por el Estado Mayor Conjunto de los Estados Unidos, describe un ciclo bien definido de las etapas clave del proceso de inteligencia, que se pueden aplicar de manera efectiva en la ciberseguridad y en particular para el presente proyecto [51].

La Planificación y Dirección es esencial para un análisis OSINT efectivo en ciberseguridad. Aquí, los analistas determinan las necesidades del cliente, establecen estrategias y métodos de recopilación, y preparan la plataforma de análisis OSINT.

La Recopilación es crucial en el Análisis de Huella Digital. Los analistas buscan términos clave, recopilan imágenes y medios, y exploran contenido web y bases de datos, registrando todos los datos relevantes.

El Procesamiento y Explotación se relaciona con la organización y agregación de datos brutos recopilados, preparándolos para el análisis detallado en la siguiente fase.

El Análisis y Producción es central en el contexto de ciberseguridad. Aquí, los analistas examinan los datos adquiridos, aplican la comprensión de las necesidades del cliente y clasifican la información en categorías útiles. La capacidad de identificar "seguimientos" y "pivotes" permite a los analistas profundizar en el tema o cambiar de enfoque según sea necesario.

Finalmente, en la Etapa de Diseminación e Integración, los analistas comparten los productos de inteligencia finales, que incluyen datos, análisis y brechas identificadas. Este intercambio de información permite que el cliente integre los resultados en sus operaciones de ciberseguridad. Además,

es importante identificar cuáles serán los resultados que se esperan obtener de este proceso. Para ello, se plantean cuatro dominios de información que establecerán el alcance del análisis:

- *Superficie de los Servicios IT*: la infraestructura pública del objetivo es uno de los principales puntos de entrada a la investigación, permitiendo conocer el tipo de operaciones que realiza, qué tecnologías anuncia al mundo, así como posibles rastros remanentes de servidores que pueden no estar contemplados por su departamento técnico y que, como consecuencia, se vuelvan un potencial vector de ataque. Las tácticas técnicas y procedimientos MITRE relacionadas a este punto del procedimiento son:
  - T1595 – Active Scanning
    - T1595.002 – Vulnerability Scanning
  - T1590 – Gather Victim Network Information
    - T1590.001 – Domain Properties
    - T1590.002 – DNS
    - T1590.003 – IP Addresses
- *Sistemas de Reputación*: además de las vulnerabilidades, es importante evaluar la salud de las direcciones IP analizadas, en términos de su reputación. Existen diversos motores de búsqueda que ofrecen una rápida categorización para reconocer si una IP tiene baja

reputación. Una categorización negativa de la IP está potencialmente vinculada a un compromiso parcial o total del servidor. Las tácticas técnicas y procedimientos MITRE relacionadas a este punto del procedimiento son:

- T1590 – Gather Victim Network Information
  - T1590.001 - Domain Properties
  - T1590.002 – DNS
  - T1590.003 – IP Addresses
- T1596 – Search Open Technical Databases
  - T1596.001 – Reputation Services

- *Internet Superficial*: es importante identificar la información indexada en Internet sobre los motores de búsqueda, los cuales clasifican e indexan los contenidos web, almacenando la información en bases de datos. Los canales de comunicación del cliente facilitan su reconocimiento en el Internet superficial. Las tácticas técnicas y procedimientos MITRE relacionadas a este punto del procedimiento son:
  - T1590 – Gather Victim Network Information
    - T1590.002 – DNS
    - T1590.003 – IP Addresses
  - T1589 – Gather Victim Identity Information
    - T1589.002 – Open-Source Intelligence
- *Fuga de Información*: corresponden a incidentes de seguridad que exponen datos sensibles, confidenciales o

protegidos, a una persona no autorizada. Estas fugas de datos son generalmente publicadas en foros dedicados al cibercrimen, que pueden estar en la web (Red común) como también en la red oscura (redes TOR). Las tácticas técnicas y procedimientos MITRE relacionadas a este punto del procedimiento son:

- T1597 – Search Closed Sources
  - T1597.001 – Credential Leaks
- T1589 – Gather Victim Identity Information
  - T1589.003 - Leaked Data

Dado que este enfoque no involucra explotación activa, sino únicamente la recopilación de información externa y el reconocimiento pasivo, las tácticas MITRE relacionadas con fases posteriores de explotación o intrusión no se aplican en este contexto.

Finalmente, resulta importante detallar de qué forma se categorizarán los resultados obtenidos, priorizando así su respectivo tratamiento. Para ello, se tomó como referencia el estándar JP 2-0 previamente analizado. En dicho documento se ofrece una visión acerca de la confianza de las decisiones a tomarse en función de los resultados, siendo estos clasificados en niveles altos, medios y bajos. Para el presente proyecto y con base en la experiencia empírica, se consideraron dos criterios: el esfuerzo que requiere un ciber atacante para obtener la información y la

relevancia de dicha información. En la Tabla 4 se muestra el desglose de la asignación de puntajes a los resultados encontrados.

		Relevancia			
		Bajo	**Medio**	**Alto**	**Muy Alto**
Complejidad	**Bajo**	**1**	**3**	**3**	**4**
	Medio	**1**	**2**	**3**	**4**
	Alto	**1**	**1**	**3**	**4**
	Muy Alto	**1**	**1**	**2**	**4**

Tabla 4: Matriz de severidad de la huella digital. Fuente: Los autores.

4.2 Diseño en bajo nivel

El presente proyecto tiene previsto llevar a cabo un despliegue manual de los análisis de vulnerabilidades y huella digital. Los resultados de estos análisis se presentarán a la empresa de telecomunicaciones en un formato de informe ejecutivo junto con un anexo técnico que detallará los criterios técnicos aplicados y las herramientas utilizadas en profundidad. La implementación inicial manual permitirá una comprensión detallada de los procesos y la identificación precisa de vulnerabilidades. Posteriormente, la transición a un sistema automatizado optimizará el proceso, agilizando las evaluaciones y mejorando la capacidad de respuesta a posibles amenazas. Tanto el Análisis de Vulnerabilidades como el Análisis de Huella Digital pueden llevarse a cabo bajo tres modalidades [52]:

- *Caja Negra*: buscan replicar lo que enfrentaría un atacante real. Los consultores no tienen acceso ni información sobre el entorno, por lo que deben recopilar información, descubrir vulnerabilidades y avanzar en la infraestructura o sistemas como lo haría un atacante.
- *Caja Blanca*: se realizan con pleno conocimiento de la tecnología a estudiarse. Los consultores suelen disponer con información como diagramas de red, listas de sistemas y rangos de red IP, e incluso credenciales para los sistemas que están evaluando.
- *Caja Gris:* son una combinación de las pruebas de caja negra y blanca, ya que pueden proporcionar cierta información sobre el entorno a los evaluadores sin otorgar acceso completo o detalles de configuración. Esto permite enfocar el tiempo y esfuerzo de los evaluadores, brindando una vista más precisa de lo que realmente encontraría un atacante, sin revelar toda la información del entorno.

Para el presente proyecto fue escogida la modalidad Caja Gris, puesto que el alcance de las pruebas debe ser acordado previamente con la empresa de telecomunicaciones, debido a la naturaleza de información sensible que se maneja.

4.2.1 Análisis de vulnerabilidades

Previo al despliegue del análisis, se estudió el cuadro comparativo de Gartner sobre escáneres de vulnerabilidades, en donde participaron alrededor de veinte firmas de ciberseguridad [53].

Nessus, desarrollado por Tenable, lidera sobre las demás soluciones siendo una de más populares del mercado [54].

Confiable a nivel mundial, Nessus resalta por su exhaustiva capacidad de escaneo, amplia cobertura de complementos y sólidas características de informes y análisis

Nessus desempeña un papel crucial al ayudar a las organizaciones a identificar vulnerabilidades, priorizar esfuerzos de remedio y fortalecer su postura de seguridad global. Entre sus fortalezas se destaca su detección integral de vulnerabilidades gracias a una amplia base de datos de complementos actualizados continuamente. Además, ofrece informes detallados y personalizables que proporcionan percepciones accionables para que los profesionales de seguridad aborden las amenazas de manera efectiva. Nessus también se distingue por su capacidad de integración con diversas herramientas y plataformas de seguridad de terceros, lo que mejora su versatilidad y su capacidad para integrarse en ecosistemas de seguridad existentes. Asimismo, incorpora el sistema de puntaje CVSS para vulnerabilidades, lo cual facilita la clasificación y priorización de los resultados. Para el presente proyecto se utilizó Tenable Nessus licenciado en su versión Professional.

4.2.2 Análisis de huella digital

Previo al despliegue del análisis, se estudió el documento OSINT Handbook [55] que ofrece una lista exhaustiva de todas las herramientas y recursos de OSINT disponibles. Para el presente proyecto se escogieron dos herramientas que facilitan la obtención

de información sobre el objetivo de estudio tanto a nivel superficial como a nivel de red oscura:

- *Spiderfoot*: Es una herramienta para automatización y auditoria de OSINT diseñado para ser altamente modular y proporcionar las funciones necesarias para la manipulación y almacenamiento de datos [56]. La ventaja significativa de Spiderfoot frente a otras herramientas OSINT es la cantidad de módulos que implementa, más de 150. Posee una interfaz de línea de comandos y una interfaz web. Spiderfoot puede usar como punto de partida datos como son nombres de dominio, direcciones IP, nombres de host y subdominios, subredes, Autonomous System Numbers (ASN), direcciones de correo electrónico, números de teléfono y nombres de personas. La versión de pago Spiderfoot HX incluye integración con el navegador Tor, escaneo de la web profunda, escaneo de múltiples objetivos, monitoreo continuo con alertas y notificaciones por correo electrónico, y un motor de correlación que busca anomalías y resultados notables. La interfaz web de Spiderfoot facilita la configuración de la aplicación y los módulos, integración con fuentes OSINT adicionales, la selección de módulos para un escaneo, la depuración y la visualización de los resultados en forma de tabla y gráfico. Los resultados seleccionados pueden marcarse como falsos positivos, lo que también marca elementos secundarios y los elimina del gráfico. Spiderfoot HX puede ejecutar la

recopilación de datos paso a paso para inspeccionar cómo se descubre cada resultado.

- *IntelligenceX*: es una empresa tecnológica europea independiente fundada en 2018 por Peter Kleissner, con sede en Praga, República Checa. Su misión es desarrollar y mantener el motor de búsqueda y archivo de datos [57]. Se diferencia de otros motores de búsqueda de manera única: utiliza selectores, como direcciones de correo electrónico, dominios, URL, direcciones IP, segmentos de red, direcciones de Bitcoin, hashes, etc. A través de dichos selectores, es posible realizar búsquedas en lugares como la red oscura, sitios de pegado, plataformas de intercambio de documentos, datos de los registros whois, filtraciones de datos públicos y otros. Además, mantiene un archivo histórico de resultados, de la misma forma como Wayback Machine almacena copias históricas de sitios web.

Finalmente, en la Tabla 5, Tabla 6, Tabla 7 y Tabla 8 se detalla un desglose específico de los criterios de puntajes a utilizarse para categorizar los resultados obtenidos en cada uno de los dominios de estudio.

Parámetros	Severidad	Matriz
Registros DNS declarados	Media	Complejidad media Relevancia media
Registros DNS no declarados	Alta	Complejidad media Relevancia alta
Sitios comprometidos por ransomware	Muy Alta	Complejidad media Relevancia muy alta

Tabla 5: Resultados obtenidos en superficies de servicios IT.
Fuente: Los autores

Parámetros	Tiempo – Fuentes	Severidad
Última detección (tiempo)	< 6 meses	Muy Alta
	6 meses – 1 año	Alta
	1 año – 2 años	Media
	> 2 años	Baja
Detecciones (frecuencia)	1	Baja
	2 – 3	Media
	4 – 5	Alta
	> 5	Muy Alta
Conocimiento	Sí	Media
	No	Alta

Tabla 6: Resultados obtenidos por la reputación. Fuente: Los autores

Parámetro	Detalle	Severidad	Matriz
Números de teléfono	Contactos corporativos públicos	Baja	Complejidad Baja Relevancia Baja
	Contactos del personal de la empresa	Media	Complejidad Baja Relevancia Media
	Contactos del personal crítico de la empresa	Alta	Complejidad Baja Relevancia Alta
Correos electrónicos	Contactos corporativos públicos	Baja	Complejidad Baja Relevancia Baja
	Contactos del personal de la empresa	Media	Complejidad Baja Relevancia Media
	Contactos del personal crítico de la empresa	Alta	Complejidad Baja Relevancia Alta
Personal de la empresa	Cuentas externas – no usa correo corporativo	Media	Complejidad Media Relevancia Media
	Cuentas externas – sí usa correo corporativo	Alta	Complejidad Media Relevancia Alta

Tabla 7: Resultados obtenidos en internet superficial. Fuente: Los autores

Parámetro	Severidad	Matriz
Cuentas expuestas	Media	Complejidad Media Relevancia Media
Cuentas comprometidas (contraseñas en hash)	Alta	Complejidad Media Relevancia Alta
Cuentas comprometidas (contraseñas en texto plano)	Muy alta	Complejidad Media Relevancia Muy alta
Filtración de documentos	Muy Alta	Complejidad Media Relevancia Muy alta

Tabla 8: Resultados obtenidos en filtración de información sensible. Fuente: Los autores

CAPÍTULO 5: Resultados

5.1 Implementación en empresa de telecomunicaciones

La implementación de la solución propuesta en la empresa de telecomunicaciones en Ecuador se basó en una metodología integral para la obtención de la superficie de ataque cibernético desarrollada y alineada con el ecosistema de riesgos actual en ciberseguridad. Esta metodología, detallada en el capítulo 4, se validó con la colaboración de un oficial de ciberseguridad de la empresa para asegurar que la implementación estuviera alineada con las necesidades específicas de la empresa y su infraestructura tecnológica.

5.1.1 Descripción del escenario de implementación

Para este escenario, se escogió una compañía del grupo empresarial por su exposición digital significativa y alto nivel de riesgo asociado. La compañía posee dos dominios y 14 subdominios que fueron analizados para este escenario. Los

resultados numéricos y estadísticos son analizados en este escenario mientras se mantiene la anonimidad de la compañía.

5.1.2 Herramientas y técnicas utilizadas

La solución utilizó Nessus para realizar escaneos avanzados y autenticados, lo que permitió identificar un amplio espectro de vulnerabilidades críticas y altas. Nessus proporcionó informes detallados que fueron esenciales para priorizar las acciones correctivas, alineándose con el objetivo de descubrir y mitigar las vulnerabilidades críticas en la infraestructura.

Se implementaron las herramientas Spiderfoot e IntelligenceX para la recopilación de datos sobre la huella digital de la empresa. Spiderfoot, integrado con Shodan, permitió la identificación de múltiples subdominios, portales web públicos y datos sensibles expuestos. Esta capacidad de detección continua más allá del descubrimiento inicial ayudó a mantener una visión actualizada de la superficie de ataque, cumpliendo con los objetivos de monitoreo y descubrimiento continuo de activos.

El análisis de huella digital se realizó de manera semiautomática. Aunque muchas tareas fueron automatizadas, algunos resultados requerían un triaje manual. Esto incluyó:

- Validación de Credenciales: Las credenciales encontradas en bases de datos de brechas de seguridad fueron validadas manualmente para confirmar su validez, asegurando que la información utilizada fuera precisa y relevante.

- Verificación de Aplicaciones Web: Se llevó a cabo una verificación manual de las aplicaciones web descubiertas para garantizar que eran válidas y estaban correctamente categorizadas.

5.2 Resultados obtenidos

5.2.1 Análisis de vulnerabilidades

El análisis de vulnerabilidades realizado con Nessus reveló varias brechas de seguridad en la infraestructura de la empresa de telecomunicaciones. En total, se identificaron 150 vulnerabilidades en un total de 14 activos. El promedio del CVSS v3.1 Score de estas vulnerabilidades es 4.2 y la mayoría de ellas están en la categoría baja y media, tal como se aprecia en la Figura 5.

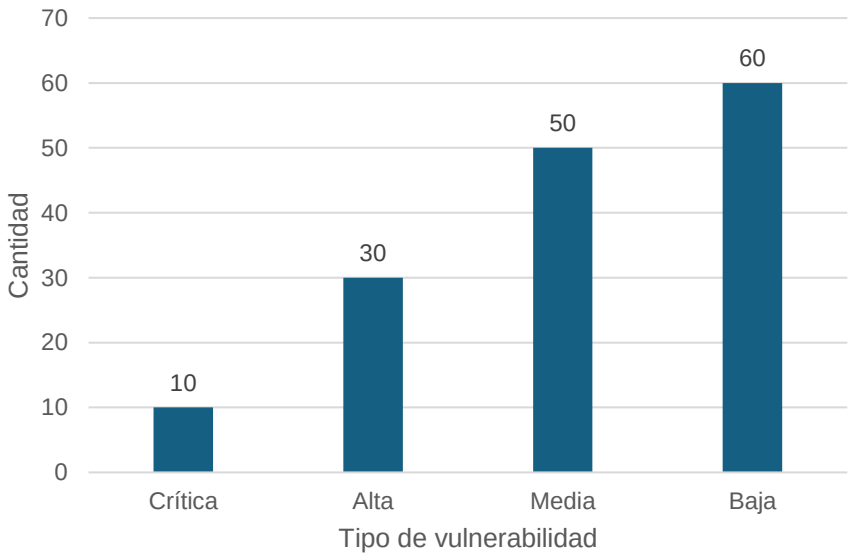


Figura 5: Distribución de vulnerabilidades por severidad. Fuente: Los autores

En la Tabla 9, Tabla 10 y Tabla 11 se presentan las vulnerabilidades encontradas de la compañía:

Tabla 9: Detalle de vulnerabilidad sobre protocolo TLS. Fuente: Los autores

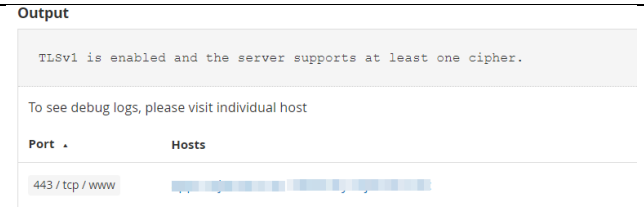
Vulnerabilidad	Detección de protocolo TLS versión 1.0
Descripción	El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas para estos defectos y deben usarse siempre que sea posible.
Activos afectados	Redacted_3, Redacted_4
Puntaje CVSS v3.1	6.5
Severidad	Medio
Criterios CVSS	• Vector de acceso: Red • Complejidad del acceso: Alto • Privilegios requeridos: Ninguno • Interacción del usuario: Ninguno • Alcance: No cambiado
Remediación	Deshabilitar TLS versión 1.0 y habilitar soporte para TLS versión 1.2 y 1.3.
Evidencia	

Tabla 10: Detalle sobre vulnerabilidad sobre servicio SMTP. Fuente: Los autores

Vulnerabilidad	Servicio Simple Mail Transfer Protocol (SMTP) permite inicio de sesión en texto plano
Descripción	El host remoto está ejecutando un servidor SMTP que permite inicios de sesión de texto claro a través de conexiones sin cifrar. Un atacante puede descubrir nombres de usuario y contraseñas rastreando el tráfico al servidor si se utiliza un mecanismo de autenticación menos seguro.
Activos afectados	Redacted_5
Puntaje CVSS v3.1	3.7
Severidad	Bajo
Criterios CVSS	• Vector de acceso: Red • Complejidad del acceso: Alto • Privilegios requeridos: Ninguno • Interacción del usuario: Ninguno

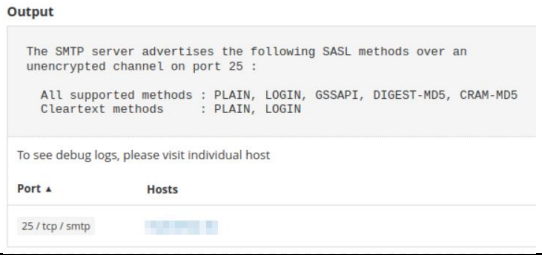
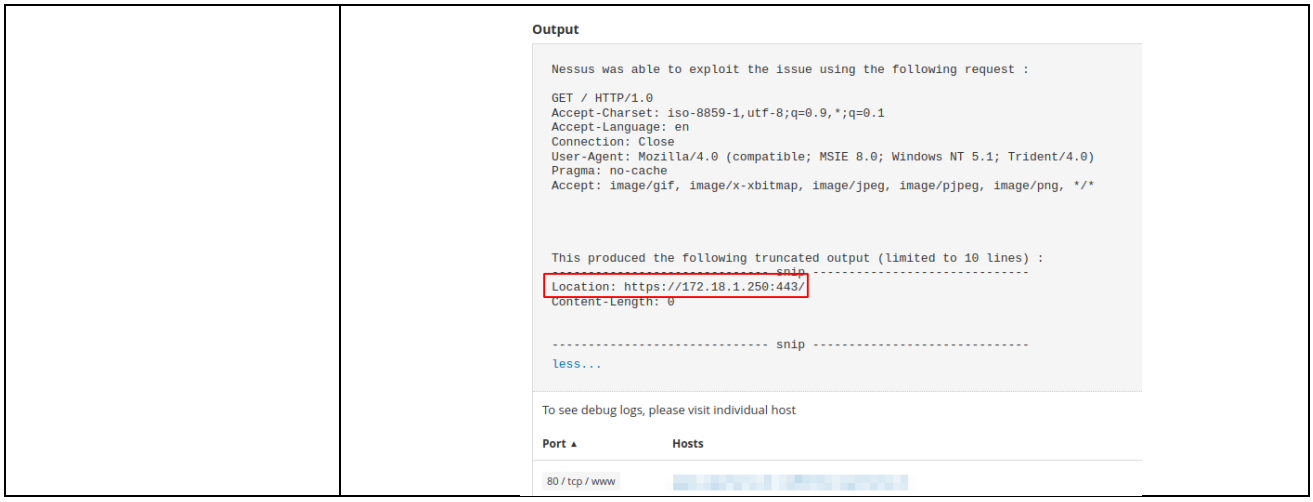
	• Alcance: No cambiado • Confidencialidad: Bajo • Integridad: Ninguno • Disponibilidad: Ninguno
Remediación	Configurar el servicio para admitir mecanismos de autenticación menos seguros solo a través de un canal cifrado.
Evidencia	

Tabla 11: Detalle de vulnerabilidad sobre exposición de IP interna.
Fuente: Los autores

Vulnerabilidad	Exposición de IP interna en encabezado HTTP de servidor web
Descripción	Esto puede exponer direcciones IP internas que generalmente están ocultas o enmascaradas detrás de un firewall de traducción de direcciones de red (NAT) o un servidor proxy.
Activos afectados	Redacted_3, Redacted_4
Puntaje CVSS v3.1	3.1
Severidad	Bajo
Criterios CVSS	• Vector de acceso: Red • Complejidad del acceso: Alto • Privilegios requeridos: Ninguno • Interacción del usuario: Ninguno • Alcance: No cambiado • Confidencialidad: Bajo • Integridad: Ninguno • Disponibilidad: Ninguno
Remediación	Configurar los encabezados para evitar revelar información que pueda comprometer al servidor
Evidencia	



5.2.2 Análisis de Huella Digital

Para el análisis de huella digital, se analizaron catorce subdominios de la compañía. En este análisis, se evaluó el nivel de presencia que tiene la compañía en Internet. Entre los hallazgos se incluyen: infraestructura pública, reputación de IP, información en la internet superficial y fugas de información sensible.

5.2.2.1 Superficie de servicios IT

Para un reconocimiento inicial, se procedió a enumerar los subdominios asociados al objetivo por sus registros DNS. Se encontraron catorce subdominios que están catalogados con una severidad media ya que requiere un nivel de complejidad medio para encontrarlos, y su nivel de relevancia es bajo.

Con los subdominios identificados, se encontraron diecinueve portales web con diferentes niveles de severidad como se aprecia en la Figura 6.

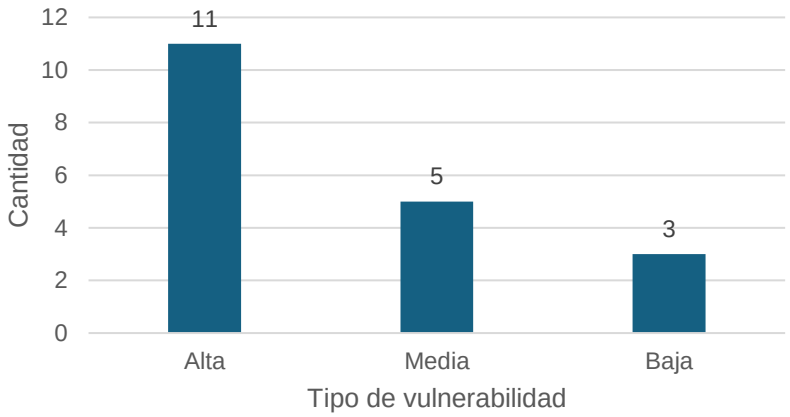


Figura 6: Distribución de portales web identificados.
Fuente: los autores

5.2.2.2 Sistema de reputación

No se encontraron direcciones catalogadas como maliciosas según las firmas de seguridad.

5.2.2.3 Internet superficial

Se encontraron diez números de teléfono relacionados con la compañía. De éstos, siete son nacionales, correspondientes a empleados, vendedores y otros contactos internos, y tres son extranjeros, asociados con posibles clientes o socios internacionales. Además, utilizando los dominios de la compañía, se identificaron 71 correos electrónicos de trabajadores indexados en motores de búsqueda, que incluyen direcciones de empleados, personal de ventas, soporte técnico, y otros roles asociados con la organización.

5.2.2.4 Fuga de información sensible

Se encontraron doce brechas de datos con 260 resultados, de los cuales 163 son de carácter corporativo en el que su contraseña está en texto plano. Estos resultados están catalogados con una severidad muy alta, ya que requiere un nivel de complejidad media para encontrarlos y un nivel de relevancia muy alto. Una cuenta identificada destaca por su gran cantidad de apariciones en las brechas, teniendo en total 73 resultados.

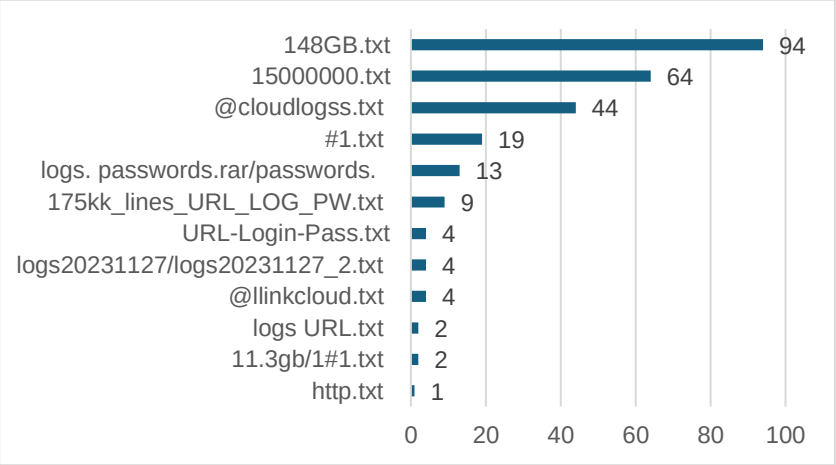


Figura 7: Total de resultados por brecha. Fuente: Los autores.

Los archivos mostrados en la Figura 7 representan compilaciones de datos provenientes de actores de amenaza que buscan robar credenciales y otra información sensible. Los nombres sugieren una variedad de formatos y fuentes, reflejando las técnicas utilizadas para recolectar y almacenar credenciales y datos comprometidos. Se validó que las contraseñas de algunas cuentas

encontradas en las brechas eran débiles, lo que permitió comprometer las cuentas en pruebas controladas.

En la Figura 8 se aprecia el total de brechas que cuentan con filtraciones tanto de usuarios corporativos como de usuarios personales.

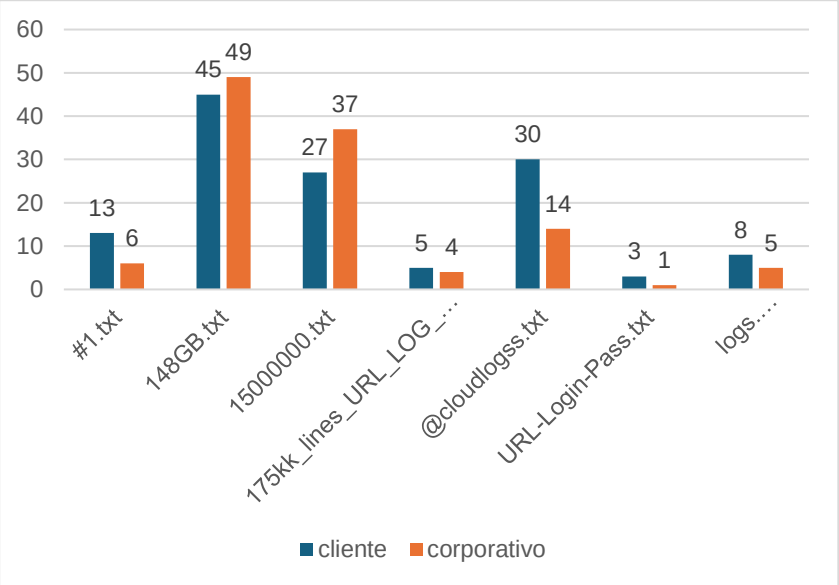


Figura 8: Total de brechas identificadas por tipo de usuario.
Fuente: los autores.

5.3 Análisis y contraste de resultados

Para validar la efectividad de la solución implementada, se llevó a cabo una entrevista con un especialista en ciberseguridad. El objetivo fue comparar los resultados obtenidos con los objetivos iniciales del proyecto. Para este propósito se utilizó la guía de SANS para evaluación de gestión de superficie de ataque [58], que cuenta con criterios de funcionalidad para las soluciones que cumplan este propósito. El especialista en ciberseguridad de la empresa validó que las herramientas utilizadas no solo detectaron vulnerabilidades y expusieron datos

Funcionalidad	Atributo	Capacidad	Criterio del Especialista
Descubrimiento Automático	Descubrimiento Externo	La solución requiere información mínima para iniciar el descubrimiento.	Sí, porque Spiderfoot funciona con una entrada mínima.
	Descubrimiento Integral	La solución descubre y monitorea automáticamente en segmentos IPv4 e IPv6, así como infraestructura de centro de datos y en la nube.	Sí, porque Spiderfoot se integra con herramientas como Shodan.
	Descubrimiento detallado de servicios	La solución enumera servicios detalladamente, incluyendo sus nombres y versiones.	Sí, porque incorpora Nessus.
	Descubrimiento detallado de artefactos	La solución obtiene artefactos detallado como certificados, capturas de pantalla y encabezados de servicio.	Sí, porque incorpora Nessus.
	Descubrimiento de rutas	La solución provee detalles acerca de cómo un activo fue descubierto.	Sí, porque incorpora Nessus, pero debería incorporar otras herramientas como Nuclei.
Monitoreo Continuo	Descubrimientos nuevos	La solución permite descubrir nuevos activos.	Sí, porque Spiderfoot se integra con herramientas como Shodan
	Monitoreo de cambios	La solución provee de paneles interactivos para realizar cambios en el monitoreo.	No, no están contemplados los cambios temporales en el diseño.
	Alertas	La solución provee de mecanismos para alertas de cambios críticos.	No, las alertas no están contempladas en el diseño.
	Falsos positivos y reducción de ruido	La solución limita el ruido y ofrece resultados altamente confiables.	No, porque Nessus no contempla los falsos positivos, esta actividad es manual.
Gestión basada en riesgos	Evaluación externa	La solución ofrece evaluaciones automatizadas de riesgo.	No, porque extrae todo lo que se toma, pero se prioriza según el contexto.
	Puntaje de impacto	La solución permite el ajuste de los niveles de riesgo basado en criterios alineados al negocio.	Sí, porque tienes reglas definidas a nivel de vulnerabilidades y huella digital.
Validación de riesgos	Control de activos	La solución provee la capacidad de controlar el alcance de los activos para la validación de postura de ciberseguridad.	Sí, porque el ejercicio inicia con esta validación.
	Validación de activos	La solución provee de automatización para ataques de credenciales, pruebas de phishing y malas configuraciones.	No, porque las validaciones son manuales debido al riesgo.
	Equipo de investigación	El proveedor de la solución está compuesto de un equipo dedicado a la investigación de desarrollo de pruebas de concepto para nuevas vulnerabilidades.	No, porque no realiza adaptaciones técnicas especializadas.

Tabla 12 Evaluación de la solución con los criterios de SANS. Fuente: los autores

sensibles, sino que también proporcionaron una visión detallada y continua de la infraestructura de la empresa. Algunos puntos clave de la validación incluyeron:

- Eficacia en la Detección: Nessus fue eficaz en la identificación de vulnerabilidades críticas, permitiendo priorizar la remediación de las amenazas más significativas.
- Descubrimiento Continuo: La integración de Spiderfoot con Shodan facilitó el descubrimiento continuo de activos, superando las expectativas iniciales de monitoreo estático.
- Artefactos Detallados: La recopilación de artefactos detallados por parte de Nessus proporcionó una comprensión profunda de los activos monitoreados, cumpliendo con el objetivo de una evaluación completa y precisa.
- Vulnerabilidades Críticas: La identificación y corrección de vulnerabilidades críticas mitigaron el riesgo de explotación por parte de atacantes, reduciendo significativamente la exposición a amenazas.
- Datos Expuestos: La mejora en las políticas de seguridad de la información y la implementación de controles de acceso robustos ayudaron a prevenir futuros incidentes de filtración de datos.

CONCLUSIONES

- Se identificaron los riesgos cibernéticos con mayor presencia en la actualidad, utilizando los reportes de ciberseguridad de una empresa local y una empresa multinacional, para identificar patrones de ataque de los actores de amenazas.
- Se analizó el marco de trabajo MITRE ATT&CK para identificar qué tácticas, técnicas y procedimientos se adaptan mejor a la detección de superficies de ataque cibernético.
- Se logró diseñar una metodología basada en los criterios de seguridad y marcos de trabajo estudiados, para la obtención de la superficie de ataque cibernético.
- Se pudo validar la metodología diseñada en una empresa de telecomunicaciones.

RECOMENDACIONES

- Asignar al departamento de Tecnologías de la Información funciones relacionadas con seguridad de la información, y éste a su vez pueda realizar auditorías de forma periódica y planificada del cumplimiento de las políticas y controles de seguridad de accesos que fueron creados. Esto incluye realizar análisis de forma semestral o anual, para mejorar la visibilidad de la superficie de ataque y mejorar su postura de ciberseguridad.
- Adicionar funciones relacionadas con seguridad de la información como: realizar auditorías periódicas y calendarizadas, llevar control de inventario de sus activos tecnológicos, aplicar políticas y controles de seguridad en los dispositivos de usuarios finales.
- Capacitar a todos los colaboradores de la empresa en aspectos de seguridad de la información, mediante charlas continuas y enfocadas en las buenas prácticas de uso de herramientas corporativas y credenciales de acceso.
- Realizar el mismo esquema a empresas de diferentes tamaños y sector económico, con el propósito de medir la robustez del modelo propuesto.

REFERENCIAS

[1] D. Goodin, «As Log4Shell wreaks havoc, payroll service reports ransomware attack,» Ars Technica, 2021. [En línea]. Available: https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack/.

[2] ESET, «Security Report: Latinoamérica 2023,» ESET, 2023.

[3] International Telecommunication Union, «Global Cybersecurity Index 2020 - Measuring commitment to cybersecurity,» ITU, 2021.

[4] B. Entel, «The New Financial Metric for Cybersecurity,» SANS, 17 03 2023. [En línea]. Available: https://www.sans.org/blog/the-new-financial-metric-for-cybersecurity/.

[5] ESET, spool s.r.o., «Threat Report: Primer Cuatrimestre de 2022,» ESET, 2022.

[6] M. Orozco, «CNT apaga todas sus computadoras tras fuerte ataque informático,» El Comercio, 16 7 2021. [En línea]. Available: https://www.elcomercio.com/actualidad/negocios/cnt-ataque-informatico-ransomware-fiscalia.html.

[7] El Universo, «‘Ransomware’: el secuestro de información es una tendencia cada vez más fuerte,» El Universo, 27 07 2021. [En línea]. Available:

https://www.eluniverso.com/larevista/tecnologia/ransomware-el-secuestro-de-informacion-es-una-tendencia-cada-vez-mas-fuerte-nota/.

[8] EC-Council, «The All-New C|EHv12 with New Learning Framework,» 7 9 2022. [En línea]. Available: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/cehv12-new-learning-framework/.

[9] P. Foreman, Vulnerability Management, New York: Auerbach Publications, 2019.

[10] G. Mandefu, «Vulnerability Assessment: 6 Best Steps to Better Security,» 2020.

[11] Gartner Research, «Definition: Threat Intelligence,» 2013. [En línea]. Available: https://www.gartner.com/en/documents/2487216.

[12] Crowdstrike, «IOA VS IOC,» Crowdstrike, 5 10 2022. [En línea]. Available: https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/ioa-vs-ioc/.

[13] M. Rani, «What are INDICATORS OF EXPOSURE (IOE) ?,» Luminis India, [En línea]. Available: https://luminisindia.com/cybersecurity-prism/281-what-are-indicators-of-exposure-ioe.

[14] NIST | Computer Security Resource Center CSRC, «attack surface,» NIST, [En línea]. Available: https://csrc.nist.gov/glossary/term/attack_surface.

[15] OWASP, «Attack Surface Analysis Cheat Sheet,» OWASP, 2024. [En línea]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html.

[16] Scrut Automation, «CAASM - A must for a CISOs Tech Stack,» Scrut Automation, 2023.

[17] V. L, M. Gowda, G. G. Sindhi y K. V, «Cyber Attack Surface Management System,» *International Journal of Advanced Research in Science Communication and Technology,* vol. 3, nº 8, p. 9, 2023.

[18] J. Friedman, «Attack your attack surface: How to reduce to cyberattacks with an attack surface visualization solution,» Skybox Security, 2016.

[19] Trend Micro, «Understanding Targeted Attacks: Goals and Motive,» Trend Micro, 22 10 2015. [En línea]. Available: https://www.trendmicro.com/vinfo/es/security/news/cyber-attacks/understanding-targeted-attacks-goals-and-motives.

[20] D. Seidl y M. Chappel, «CompTIA PenTest+ Study Guide: Exam PT0-002,» Wiley, 5 10 2021. [En línea].

[21] F. Jaafar, F. Avellaneda y E.-H. Alikacem, «Demystifying the Cyber Attribution: An Exploratory Study,» *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress,* pp. 35-40, 2022.

[22] C. Mark, «Understanding cyber attacker motivations to best apply controls,» AT&T Business, 19 2 2020. [En línea]. Available: https://cybersecurity.att.com/blogs/security-essentials/understanding-cyber-attacker-motivations-to-best-apply-controls.

[23] Y. Diogenes y E. Ozkaya, Cybersecurity – Attack and Defense Strategies - Second Edition, Packt, 2019.

[24] D. Bianco, «The Pyramid of Pain,» 17 1 2014. [En línea]. Available: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

[25] Cyware, «The Concept of Pyramid of Pain,» Cyware, 12 8 2021. [En línea]. Available: https://cyware.com/security-guides/cyberthreat-intelligence/the-concept-of-pyramid-of-pain-f358.

[26] A. Berady, M. Jaume, V. Triem Tong y G. Guette, «From TTP to IoC: Advanced Persistent Graphs for Threat Hunting,» *IEEE Transactions*

on Network and Service Management, vol. 18, nº 2, pp. 1321-1333, 2021.

[27] S. P. Oriyano, CEH™v9 : Certified Ethical Hacker Version 9 Study Guide, John Wiley & Sons, Inc, 2016.

[28] V. Diaz, «We analyzed 80 million ransomware samples – here's what we learned,» Google Cybersecurity Action Team, 13 10 2021. [En línea]. Available: https://blog.google/technology/safety-security/we-analyzed-80-million-ransomware-samples-heres-what-we-learned/.

[29] M. Chapple y D. Seidl, CompTIA CySA+ Study Guide: Exam CS0-001, Sybex, 2017.

[30] T. McGuiness, «Defense In Depth,» SANS Institute, 2021.

[31] D. Walkkowski, «What Are Security Controls?,» F5 Labs, 22 8 2019. [En línea]. Available: https://www.f5.com/labs/learning-center/what-are-security-controls.

[32] M. McWhirt, D. Smith, O. Toor y B. Turner, «Proactive Preparation and Hardening to Protect Against Destructive Attacks | Blog,» Mandiant, 14 1 2022. [En línea]. Available: https://www.mandiant.com/resources/blog/protect-against-destructive-attacks.

[33] A. Khalid, A. Zainal, M. A. Maarof y F. Ghaleb, «Advanced Persistent Threat Detection: A Survey,» *3rd International Cyber Resilience Conference (CRC),* pp. 1-6, 2021.

[34] J. Reiber y C. Wright, MITRE ATT&CK for dummies, Hoboken: John Wiley & Sons, Inc., 2021.

[35] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington y C. Thomas, «MITRE ATT&CKÒ: Design and,» MITRE, 2020.

[36] E. Chow, «Lockheed Martin Cyber Kill Chain vs. MITRE ATTACK Framework,» Medium, 27 6 2021. [En línea]. Available: https://eric-chow.medium.com/lockheed-martin-cyber-kill-chain-vs-mitre-attack-framework-64f8f3bf1e58.

[37] B. Strom, J. Battaglia, M. Kemmerer, W. Kupersanin, D. Miller, C. Wampler, S. Whitley y R. Wolf, «Finding Cyber Threats with ATT&CK™-Based Analytics,» MITRE, 2017.

[38] J. Hallberg, Event-driven Analysis of Cyber Kill, JAMK University of Applied Sciences, 2020.

[39] MITRE, «Enterprise tactics,» MITRE, 2024. [En línea]. Available: https://attack.mitre.org/tactics/enterprise/.

[40] LogRhythm Labs, «Using MITRE ATT&CK™ in Threat Hunting and Detection,» LogRhythm Labs, 2022.

[41] Picus Labs, «The Top Ten MITRE ATT&CK Techniques,» Picus, 13 5 2020. [En línea]. Available: https://www.picussecurity.com/resource/the-top-ten-mitre-attck-techniques.

[42] Telconet Latam, «Reporte de Tráfico Malicioso Ecuador 2022,» Telconet, Guayaquil, 2023.

[43] Microsoft Threat Intelligence, «Microsoft Digital Defense Report,» Microsoft, 2023.

[44] European Union Agency for Cibersecurity (ENISA), «ENISA Threat Landscape 2023 - July 2022 to June 2023,» Enisa, 2023.

[45] F-Secure, «Trojan:W32/Injector,» F-Secure, 2022. [En línea]. Available: https://www.f-secure.com/v-descs/trojan-w32-injector.shtml.

[46] CSIS, «A Discussion of the 2023 Counter Ransomware Initiative with DNSA Anne Neuberger,» Center for Strategic and International Studies, 2023. [En línea]. Available: https://www.csis.org/analysis/discussion-2023-counter-ransomware-initiative-dnsa-anne-neuberger.

[47] K. Steenstrup y J.-A. Clynch, «Hype Cycle for Managing Operational Technology, 2023,» Gartner, 2023.

[48] L. Rosencrance, «vulnerability assessment (vulnerability analysis),» TechTarget, 9 2021. [En línea]. Available: https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis.

[49] S. Basu, «What is Vulnerability Assessment?,» astra, 8 12 2023. [En línea]. Available: https://www.getastra.com/blog/security-audit/vulnerability-assessment/.

[50] FIRST, «Common Vulnerability Scoring System: Specification Document,» FIRST, 9 11 2023. [En línea]. Available: https://www.first.org/cvss/specification-document.

[51] Chairman of the Joint Chiefs of Staff of the United States of America, «JP 2-0, Joint Intelligence,» 2013.

[52] M. Chappel y D. Seidl, CompTIA PenTest+ Study Guide: Exam PT0-001, Sybex, 2018.

[53] Gartner, «Vulnerability Assessment Review and Ratings,» Gartner, 2023. [En línea]. Available: https://www.gartner.com/reviews/market/vulnerability-assessment.

[54] tenable, «Tenable Nessus,» tenable, 2024. [En línea]. Available: https://www.tenable.com/products/nessus.

[55] A. Bielska, N. R. Kurz, Y. Baumgartnerr y V. Benetis, Open Source Intelligence: Tools and Resources Handbook, I-Intelligence, 2020.

[56] Intel 471, «Attack Surface Monitoring: The three pillars of Spiderfoot 2,» Intel 471, 2022. [En línea]. Available: https://www.Spiderfoot .net/attack-surface-monitoring/.

[57] Intelligence X, «Intelligence X,» Intelligence X, 2024. [En línea]. Available: https://intelx.io/.

[58] P. Lidome, «The SANS Guide to Evaluating Attack Surface Management,» SANS, 2023.

[59] Shirey, Internet Security Glossary, Version 2, RFC Editor, 2007.