UNIVERSIDAD DEL AZUAY

Facultad de Ciencias de la Administración

Carrera de Ingeniería en Ciencias de la Computación

Ciberataques al Active Directory: Medidas de Mitigación, Prevención y Seguimiento. Una Revisión Sistemática de Literatura

Trabajo de titulación previo a la obtención del grado de Ingeniero en Ciencias de la Computación

Autor:
Mateo Julián Guillén Idrovo

Director:
Paúl Esteban Crespo Martínez

Cuenca – Ecuador
2026

DEDICATORIA

Dedico este trabajo a mi madre, quien con su constante esfuerzo y amor me ha permitido formarme tanto personal como académicamente; así como a mi familia cercana, quienes han sido un soporte y apoyo incondicional.

AGRADECIMIENTO

Agradezco a mi tutor de tesis, Esteban Crespo, quien ha sido un apoyo fundamental en este proceso.

Asimismo, agradezco a mi familia: a mi madre, quien es mi más grande ejemplo de perseverancia y amor; a mi padre, quien siempre me recuerda el objetivo de la vida; y a mis abuelos maternos, quienes han sido como mis segundos padres, con quienes me he criado.

También agradezco a mis abuelos paternos, Gloria C. y Guillermo G.; a mis hermanos, Martina I., quien es mi apoyo incondicional; Renata G., Jhosua G., Ismael G. y Vida G.

A Isabel A., quien estuvo conmigo brindándome ayuda y apoyo desde el inicio; a mis compañeros de clase, Josué L. y Mateo J., quienes siempre me impulsan a ser mejor; y a mis amigos cercanos, Juan P., Pedro M., Edwin P., Sebas C. y Juan C.

Finalmente, agradezco a toda mi familia, quienes siempre velan por mi bienestar y crecimiento.

Índice de Contenidos

Índice de Figuras

Índice de Tablas

Índice de Anexos

RESUMEN

El trabajo tuvo como objetivo identificar los ataques más comunes dirigidos a entornos de Active Directory (AD), los factores facilitadores y las estrategias de detección, respuesta y monitoreo aplicadas tras el acometimiento de amenazas. La investigación se enmarca en el campo de la ciberseguridad corporativa, considerando que el AD de Microsoft constituye el servicio central de gestión de identidades y control de acceso en la mayoría de las organizaciones a nivel mundial, y que su compromiso representa una vía de acceso a toda la infraestructura. Para alcanzar los objetivos planteados, se realizó una revisión sistemática de literatura siguiendo el protocolo PRISMA, consultando las bases de datos Scopus, IEEE Xplore, Web of Science, Springer, SAGE, Emerald, Taylor & Francis y SciELO, dentro de un periodo de diez años, entre 2016 y 2026. Los estudios seleccionados fueron procesados mediante un análisis textométrico con el software IRaMuTeQ. Este análisis permitió identificar cuatro agrupaciones temáticas: prevención y defensa, optimización y seguimiento, servicios del Active Directory y estrategias de mitigación. Los hallazgos evidenciaron que los principales vectores de ataque son la escalación de privilegios, el movimiento lateral y la explotación del protocolo Kerberos, facilitados principalmente por configuraciones permisivas y la ausencia de monitoreo continuo. Como conclusión principal, se propuso una guía estructurada en tres etapas: aseguramiento preventivo, mitigación activa y continuidad operativa, fundamentada en evidencia científica y orientada a ofrecer acciones prácticas y aplicables para administradores y equipos de seguridad que gestionan entornos de Active Directory.

Palabras clave: AD, ciberataques, directorio activo, gestión, kerberos, revisión sistemática de literatura, seguridad

ABSTRACT

This study aimed to identify and analyze the most common attacks targeting Active Directory (AD) environments, the factors that facilitate them, and the detection, response, and monitoring strategies applied after such incidents. The research is framed within the field of corporate cybersecurity, considering that Microsoft AD serves as the central identity management and access control service in most organizations worldwide, and that its compromise represents a gateway to the entire infrastructure. It also examined how these measures can strengthen organizational resilience against increasingly sophisticated cyber threats. To achieve the stated objectives, a systematic literature review was conducted following the PRISMA protocol, consulting the Scopus, IEEE Xplore, Web of Science, Springer, SAGE, Emerald, Taylor & Francis, and SciELO databases, within a ten-year period from 2016 to 2026. The selected studies were processed through a textometric analysis using IRaMuTeQ software. This analysis identified four thematic clusters: prevention and defense, optimization and monitoring, Active Directory services, and mitigation strategies. The findings revealed that the predominant attack vectors are privilege escalation, lateral movement, and exploitation of the Kerberos protocol, primarily facilitated by permissive configurations and the absence of continuous monitoring mechanisms. As the main conclusion, a structured guide was proposed comprising three stages: preventive hardening, active mitigation, and operational continuity, grounded in scientific evidence and designed to provide practical and actionable measures for system administrators and security teams managing Active Directory environments in the face of the current evolving threat landscape worldwide.

Keywords: AD, active directory, cyberattacks, kerberos, management, security, systematic literature review

1. Introducción

El Active Directory (AD) de Microsoft es uno de los sistemas más utilizados en el mundo para administrar usuarios, contraseñas, accesos y recursos dentro de las organizaciones (Krishnamoorthi & Carleton, 2020). Sin embargo, al concentrar un gran volumen de información crítica en un solo servicio, se convierte en un objetivo de ataque atractivo para los atacantes, ya que comprometer el AD puede significar el acceso a toda la red corporativa. A pesar de su importancia, existe una escasez notable de investigaciones que aborden de forma integral tanto los ataques dirigidos a este sistema como las medidas para prevenirlos, contenerlos y dar seguimiento después de un incidente. Por esta razón, el presente trabajo resulta relevante, ya que ofrece información organizada y actualizada para investigadores, administradores de sistemas y profesionales de ciberseguridad que busquen comprender y enfrentar estas amenazas.

El objetivo general de este trabajo es identificar y analizar, mediante una revisión sistemática de literatura con el protocolo PRISMA y un análisis textométrico con IRaMuTeQ, los ataques más frecuentes al AD, los factores que los facilitan y las estrategias de detección, respuesta y monitoreo que se han aplicado. El principal aporte diferenciador de esta investigación es la propuesta de una guía de estrategias de aseguramiento, mitigación y continuidad operativa, construida a partir de evidencia científica y pensada para conectar los hallazgos académicos con acciones prácticas aplicables en entornos reales.

Como objetivo general de esta investigación se plantea identificar y analizar, a través de una revisión sistemática de la literatura, los ataques más comunes dirigidos a Active Directory y los factores que los facilitan, así como las estrategias de detección, respuesta y monitoreo aplicadas después de dichos ataques. Para soportar este objetivo se proponen los siguientes objetivos específicos: (1) realizar una revisión sistemática de literatura aplicando el método PRISMA para identificar fuentes de ataque y técnicas de mitigación y continuidad de operaciones de entornos Active Directory; (2) realizar un análisis textométrico para clasificar los factores y mecanismos de ataque más comunes, así como las técnicas de restablecimiento de operaciones más aplicadas; y (3) concluir con la estructura de una guía de estrategias de detección, respuesta y seguimiento post-incidente reportadas en estudios y buenas prácticas de AD.

De esta manera, este artículo está dividido de la siguiente manera: (1) en el capítulo 1 se aborda el marco teórico y estado del arte con respecto a trabajos que comparten un propósito similar, (2) la metodología aplicada, considerando PRISMA como guía metodológica para realizar el trabajo de revisión literaria; (3) los resultados y la discusión, indicando lo obtenido tras el cribado de información científica y análisis textométrico ejecutado en Iramuteq, (4) la propuesta de la guía de aseguramiento, prevención y monitoreo de entornos Active Directory. Finalmente se exponen (5) las conclusiones, limitaciones y trabajos futuros.

1.2 Marco Teórico y Estado del Arte

Actualmente, Microsoft Active Directory (AD) se ha consolidado como una de las tecnologías más utilizadas por las empresas a nivel mundial (Krishnamoorthi & Carleton, 2020). Este sistema ha sido fundamental, ya que permite a las organizaciones centralizar la gestión de la información de los usuarios, contraseñas, dispositivos, servicios, entre otros aspectos críticos, lo que posibilita un control integral de los recursos (Velu et al., 2013).

El Active Directory (AD), según Dias (2002) se fundamenta en una arquitectura lógica jerárquica compuesta por dominios, árboles y bosques, diseñada para almacenar millones de objetos de red y facilitar su búsqueda mediante un Catálogo Global. En este esquema, el dominio actúa como la unidad atómica de seguridad y administración, estableciendo límites donde las políticas y derechos no se transfieren automáticamente a otros dominios, mientras que la integración con el Sistema de Nombres de Dominio (DNS) resulta crítica, ya que los espacios de nombres de ambos servicios deben coincidir para garantizar la localización de recursos y controladores de dominio.

Sin embargo, esta misma centralización de los recursos dentro de un sistema propio convierte a este en un objetivo para diversos ataques, especialmente porque al comprometerse este servicio, se crea una vía de entrada al resto de la infraestructura e información corporativa (Mokhtar et al., 2022).

En el ámbito de la seguridad y la gestión operativa, Dias (2002) comenta que, los Objetos de Política de Grupo (GPO) constituyen el mecanismo principal para la administración de cambios y configuraciones, permitiendo aplicar reglas de seguridad uniformes, como políticas de contraseñas o restricciones de IPSec, a todos los usuarios y equipos de un dominio.

Para optimizar la administración, sin incrementar la complejidad de la infraestructura, se utilizan las Unidades Organizativas (OU), las cuales funcionan como contenedores dentro de los dominios que permiten la delegación granular de la autoridad; esto faculta a los administradores para asignar permisos específicos a subgrupos sin necesidad de otorgar control total sobre el dominio, reduciendo así los costos operativos y la necesidad de crear múltiples dominios por razones puramente administrativas (Goel et al., 2025).

Para comprender con precisión los riesgos y amenazas que enfrenta el AD, es necesario revisar ciertos conceptos fundamentales. Un directorio es una estructura que permite almacenar información sobre los activos dentro de una red. En este contexto, el Active Directory o AD, es un servicio de directorio desarrollado por Microsoft. Este servicio permite gestionar objetos de una organización, como nombres de usuario, credenciales, contraseña y ponerlos a disposición de grupos específicos, los cuales también son creados y administrados desde el mismo sistema. De esta manera, solo los usuarios con ciertas políticas de acceso pueden utilizar funcionalidades previamente establecidas por un administrador (Microsoft, 2025b).

En la evaluación de la seguridad de un Active Directory, se utiliza comúnmente el término Tácticas, Técnicas y Procedimientos (TTP). Este enfoque implica la simulación, con diferentes métodos y objetivos, de un ataque común hacia el AD. De esta manera, se puede observar la respuesta del sistema frente al ataque y determinar las mejores configuraciones posibles (Abo-alian et al., 2025).

En cuanto a los ataques, Domain Enumeration hace referencia a la fase en la que el atacante, inicialmente, intenta obtener la mayor cantidad de información posible y disponible del AD objetivo, enfocándose principalmente en usuarios con accesos superiores. Posteriormente, se suele llegar al escalamiento de estos privilegios, donde el objetivo del atacante es obtener las credenciales de un administrador de dominio, ya que con acceso a estas credenciales se puede acceder a información más sensible. Algunos ataques siguen esta estructura son: *Pass the hash* o *Kerberoasting* (Mokhtar et al., 2022).

Otros de los ataques comunes es el ransomware, un tipo de ciberataque que se centra en secuestrar datos importantes de la organización, con el propósito de, posteriormente, solicitar

un pago a cambio de su la liberación de esta información obtenida (IBM, 2024; Yan & Talaei Khoei, 2025).

En el contexto del AD el ransomware tiene como objetivo comprometer los datos obtenidos a través del propio sistema. En este entorno, los ataques son especialmente críticos, ya que la información almacenada en el AD suele ser de naturaleza sensible, como, por ejemplo, las credenciales de los usuarios (McIntosh et al., 2024).

Dentro de los ataques de ransomware, Phipps & Nurse (2025) ha descrito lo que se conoce como un movimiento lateral o *Lateral Movement,* en su traducción al inglés. Esto implica que el atacante comienza en nodos "bajos" del AD, es decir, con pocos privilegios, y luego avanza hacia activos de mayor valor. A diferencia del escalamiento de privilegios, en este caso el atacante no necesariamente se desplaza de un nodo con menos privilegios a uno con más, por lo que se considera un movimiento horizontal, en contraste con el movimiento vertical que caracteriza al escalamiento de privilegios (Herranz-Oliveros, Tejedor-Romero, et al., 2024).

El ransomware se ha convertido en una de las amenazas más utilizadas. En el entorno de los servicios de Microsoft, como Active Directory, se ha evidenciado que este tipo de ataques no siempre afecta por completo el funcionamiento general de sistema. No obstante, puede provocar la desactivación de determinadas operaciones luego de la "captura" de archivos, alterando o interrumpiendo algunos de los servicios y funciones que el sistema proporciona (McDonald et al., 2022).

Otro ataque que ha resultado especialmente complejo de identificar es el *Silver Ticket Attack.* En el estudio de Matsuda et al. (2025) se señaló que este tipo de ataque ha sido recurrente y difícil de detectar debido a la ausencia de registros (logs) en el sistema. Además, se indicó que puede mantener al sistema vulnerable durante periodos prolongados, incluso por varios años. En dicho estudio también se propuso reducir la duración de los tickets Kerberos y correlacionar los registros del *Domain Controller* con los de Azure AD en entornos híbridos.

Para enfrentar el aumento de ataques a este tipo de sistemas, se han explorado distintas alternativos. Una de ellas ha sido la implementación de sistemas *password-less*, es decir, entornos que no requieren el uso de contraseñas. *Windows Hello for Business* se ha planteado

como una de las herramientas para llevar a cabo este tipo de configuraciones. En una etapa inicial, ha sido posible recuperar u obtener contraseñas y permisos; no obstante, una vez completada la transición hacia un entorno sin contraseñas, estos sistemas se han mostrado más resistentes frente a ataques de fuerza bruta, reutilización o robo de credenciales. En este contexto, también ha resultado beneficioso el uso de autenticación de doble factor, PIN seguro y biometría (Haddad et al., 2023).

El Kerberoasting se ha consolidado como uno de los ataques más frecuentes dirigidos al Active Directory, principalmente por su capacidad de obtener contraseñas de cuentas de servicio sin requerir permisos administrativos. En el estudio de Kotlaba et al. (2020) se planteó la implementación de mecanismos de monitoreo y detección temprana apoyados en la auditoría nativa de Windows, junto con estrategias como la creación de cuentas honeypot para atraer intentos de explotación. La aplicación conjunta de estas medidas ha contribuido a disminuir los falsos positivos y a mejorar la identificación de este tipo de ataques.

Además, Kotlaba et al. (2021) abordaron la detección del ataque Kerberoasting mediante técnicas de aprendizaje automático centradas en la identificación de anomalías. En su revisión de estudios previos señalaron limitaciones en los métodos basados en firmas o reglas estáticas, ya que estos generaban altos niveles de falsos positivos. Por esta razón, propusieron el uso de algoritmos como One-Class SVM y LOF (Local Outlier Factor) con el objetivo de reducir dichos falsos positivos.

Sobre ataques, Liu, Bao, & Hagenmeyer (2025) explica que, las amenazas persistentes avanzadas (APT) han evolucionado estrategias *Low and Slow*[1], donde los atacantes evitan los sistemas de detección tradicionales dividiendo sus ataques en múltiples fases y con técnicas de persistencia. En este contexto, el robo de las credenciales y el movimiento lateral son tácticas donde los atacantes pueden obtener accesos iniciales y luego generan un escalamiento con las herramientas de Windows

A lo largo del tiempo se identificaron diversas formas de comprometer el Active Directory y, debido a que ha sido un sistema de administración ampliamente adoptado a nivel global,

[1] Estrategia de ataque en la que el adversario opera con baja intensidad y de forma prolongada para imitar tráfico legítimo, evitar umbrales de detección y mantener acceso persistente a la red objetivo durante meses o años sin ser detectado (Liu, Bao, & Hagenmeyer, 2025).

esto se convirtió en una preocupación para la comunidad. En este sentido, informes como el del Australian Government (2025) permitieron reconocer al menos diecisiete de los ataques más frecuentes, entre ellos los ya mencionados Kerberoasting y Silver Ticket. De igual forma, se advirtió sobre las configuraciones predeterminadas del Active Directory, las cuales fueron consideradas débiles y excesivamente permisivas.

De igual manera, se desarrollaron distintos sistemas orientados a mitigar este tipo de ataques; uno de ellos fue HADES, aunque no llegó a ser desplegado. Este sistema utilizó un enfoque basado en el análisis de procedencia y trazabilidad entre máquinas. A través de la correlación de eventos, inicios de sesión y registros del sistema, el modelo fue capaz de reconstruir el ataque desde su fase inicial hasta el escalamiento de privilegios. En comparación con soluciones SIEM tradicionales, mostró un rendimiento superior; sin embargo, no se implementó, en parte porque el análisis detallado de logs podía afectar las políticas de privacidad de los usuarios (Liu, Bao, Hassan, et al., 2025).

Otro estudio que abordó estrategias de mitigación y prevención fue el de (Nebbione & Calzarossa, 2023), en el cual se presentó un marco metodológico asistido por inteligencia artificial para la evaluación automatizada de la seguridad en entornos de Active Directory. En este trabajo se integraron enfoques basados en teoría de grafos y aprendizaje automático con el fin de identificar y clasificar rutas de ataque que evidenciaban vulnerabilidades o configuraciones incorrectas dentro de la red.

Por otra parte, se identificaron estudios como el de (Guo et al., 2023), en el cual se modeló la estructura del Active Directory como un grafo de ataque. En este modelo, los nodos representaron cuentas y equipos, mientras que las aristas describieron las relaciones de acceso o privilegios que permitían escalar hasta obtener un Domain Admin. El problema se planteó mediante la simulación de un juego de tipo Stackelberg entre un atacante y un defensor. Además, se propusieron algoritmos para el bloqueo de aristas basados en descomposición en árboles, programación entera mixta y aprendizaje por refuerzo.

Ante la necesidad de fortalecer la seguridad de estos servicios, algunas recomendaciones se estructuraron en tres ejes principales: la superficie de ataque, los privilegios administrativos y los controladores de dominio. Dentro de estos enfoques se plantearon medidas como la aplicación del principio de privilegio mínimo para cuentas administrativas y la restricción

de inicio de sesión en equipos no confiables. También se recomendó limitar el tiempo de membresía permanente en cuentas con altos privilegios, implementar autenticación multifactor en tareas de mayor riesgo y reforzar la seguridad física y lógica de los controladores de dominio (Microsoft, 2025a).

2. Metodología

Para el desarrollo de la SLR se siguió el método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), el cual permitió estructurar la selección, identificación y análisis de los estudios relevantes. Este enfoque permitió organizar de manera sistemática el proceso de búsqueda, filtrado y evaluación de la literatura (Page et al., 2021).

2.1 Criterios de Elegibilidad

Los criterios de inclusión para este trabajo abarcan los siguientes ámbitos: (1) El enfoque principal del trabajo debe estar estrechamente relacionado con el tema a tratar, es decir, enfocado en ciberataques al AD, así como (2) las medidas de mitigación, prevención y seguimiento de los ataques hacia estos sistemas, por esto se han considerado únicamente investigaciones que se encuentren dentro de este ámbito.

De igual manera, (3) se ha tomado en cuenta los artículos que hayan presentado diseños metodológicos claramente definidos, ya sean estudios experimentales, empíricos, estudios de caso, análisis técnico, entre otros.

Otro criterio es, que (4) sea un caso generalizable dentro de los entornos reales, también se aceptaron investigaciones desarrolladas en servicios de directorio compatibles, como LDAP en entornos Linux, siempre que los hallazgos fueran transferibles y relevantes para el contexto de Active Directory.

Además, (5) se seleccionaron únicamente artículos que contribuyeran de manera total o parcial a responder la pregunta de investigación planteada, permitiendo identificar tipos de ciberataques, mecanismos de mitigación, estrategias de prevención o enfoques de monitoreo y seguimiento en Active Directory. El nivel de contribución fue considerado durante el proceso de selección.

En cuanto a las características formales de las fuentes, se incluyeron artículos científicos, artículos de conferencias, capítulos de libros y libros académicos publicados en los últimos diez años, con el fin de asegurar la actualidad de la información. Los estudios debían estar escritos en inglés, español o portugués y haber sido sometidos a revisión por pares, verificando este proceso a través de las políticas de cada base de datos utilizada.

Finalmente, se consideraron únicamente estudios indexados en bases de datos científicas reconocidas, puntualmente se llevó a cabo en: Scopus, IEEE Xplore, Web of Science, Springer, SAGE y SciELO, con el objetivo de garantizar la calidad y la fiabilidad de las fuentes seleccionadas.

2.2 Información de Recursos

Las bases de datos consultadas, junto a sus respectivas fechas de última búsqueda son: Scopus (8 de enero de 2026), IEEE Xplore (15 de enero de 2026), Web of Science (14 de enero de 2026), Springer (10 de enero de 2026), SAGE (10 de enero de 2026), Taylor & Francis (16 de enero de 2026), Emerald (22 de enero de 2026) y SciELO (14 de enero de 2026). Además, las búsquedas literarias para este trabajo fueron realizadas por los autores de forma manual y con acceso institucional proporcionado por la Universidad del Azuay en Cuenca, Ecuador.

2.3 Estrategias de Búsqueda

Siguiendo el protocolo PRISMA, la estrategia de búsqueda se aplicó de manera sistemática en todas las bases de datos seleccionadas. En cada una de ellas se utilizó una cadena de búsqueda que permita identificar estudios relacionados con Active Directory, servicios de directorio y ciberseguridad, enfocándose en ataques, vulnerabilidades y medidas de mitigación.

En la cadena de búsqueda se consideraron términos relacionados con Active Directory y LDAP. Además, se incluyeron palabras asociadas al ámbito de la seguridad, como security, hardening, protection, attacks, exploits, silver ticket, ransomware y malware infection. Finalmente, también se incorporaron términos orientados a la gestión y reducción de riesgos, como vulnerabilities, barriers y mitigation. Estos términos fueron aplicados específicamente al campo del resumen *abstract* de los documentos.

Tabla 1
Cadenas de búsqueda

Base	Cadena	Artículos Recopilados
Scopus	((("Abstract" : "Active Directory") OR ("Abstract" :LDAP)) AND (("Abstract" :Security) OR ("Abstract" :Hardening) OR ("Abstract" :Protection) OR ("Abstract" :Attacks) OR ("Abstract" :Exploits) OR ("Abstract" :Silver Ticket) OR ("Abstract" :Ransomware) OR ("Abstract" :Malware Infection)) AND (("Abstract" :vulnerabilities) OR ("Abstract" :barriers) OR ("Abstract" :mitigation)))	137
Emerald	((("Abstract":"Active Directory") OR ("Abstract":LDAP)) AND (("Abstract":Security) OR ("Abstract":Hardening) OR ("Abstract":Protection) OR ("Abstract":Attacks) OR ("Abstract":Exploits) OR ("Abstract":Silver Ticket) OR ("Abstract":Ransomware) OR ("Abstract":Malware Infection)) AND (("Abstract":vulnerabilities) OR ("Abstract":barriers) OR ("Abstract":mitigation)))	23
IEEExplore	("Abstract":"Active Directory" OR "Abstract":LDAP) AND ("Abstract":Security OR "Abstract":Hardening OR "Abstract":Protection OR "Abstract":Attacks OR "Abstract":"Silver Ticket" OR "Abstract":Ransomware OR "Abstract":"Malware Infection") AND ("Abstract":vulnerabilities OR "Abstract":barriers OR "Abstract":mitigation)	15
Web Of Science	AB=("Active Directory" OR "LDAP") AND AB=("Security" OR "Hardening" OR "Protection" OR "Attacks" OR "Silver Ticket" OR "Ransomware" OR "Malware Infection") AND AB=("vulnerabilities" OR "barriers" OR "mitigation")	4
SciELO	ab:("Active Directory" OR "LDAP") AND ab:("Security" OR "Hardening" OR "Protection" OR "Attacks" OR "Exploits" OR "Silver Ticket" OR "Ransomware" OR "Malware Infection") AND ab:("vulnerabilities" OR "barriers" OR "mitigation" OR "prevention")	0
Taylor & Francis	ab:("Active Directory" OR "LDAP") AND ab:("Security" OR "Hardening" OR "Protection" OR "Attacks" OR "Exploits" OR "Silver Ticket" OR "Ransomware" OR "Malware Infection") AND ab:("vulnerabilities" OR "barriers" OR "mitigation" OR "prevention")	0
Springer	ab:("Active Directory" OR "LDAP") AND ab:("Security" OR "Hardening" OR "Protection" OR "Attacks" OR "Exploits" OR "Silver Ticket" OR "Ransomware" OR "Malware Infection") AND ab:("vulnerabilities" OR "barriers" OR "mitigation" OR "prevention")	0
SAGE	abstract:("Active Directory" OR "LDAP") AND abstract:("Security" OR "Hardening" OR "Protection" OR "Attacks" OR "Exploits" OR "Silver Ticket" OR "Ransomware" OR "Malware Infection") AND abstract:("vulnerabilities" OR "barriers" OR "mitigation" OR "prevention")	

Cada una de estas cadenas de búsqueda fueron aplicadas a las respectivas bases de datos científicas, tal como se indica en la tabla 1. Como criterios de filtrado, en todas las búsquedas se estableció un límite temporal de los últimos diez años, así como una restricción por idioma, considerando únicamente estudios publicados en inglés, español y portugués, con el fin de garantizar la actualidad, relevancia y accesibilidad de los trabajos incluidos en la revisión.

El límite temporal de diez años (2016-2026) se estableció considerando que Windows Server 2016 marcó un punto de inflexión en la seguridad de Active Directory, al introducir mecanismos como Privileged Access Management (PAM) y autenticación mutua obligatoria mediante Kerberos, que redefinieron el panorama de amenazas y defensas que esta revisión busca analizar (Microsoft, 2016).

2.4 Proceso de Selección

El proceso de selección de los estudios se realizó de manera estructurada, posterior a la aplicación de la cadena de búsqueda en las bases de datos definidas. Los resultados obtenidos fueron exportados a una hoja de cálculo en Excel, donde inicialmente se procedió a la eliminación de registros duplicados.

Posteriormente, se llevó a cabo una revisión por etapas. En una primera fase se evaluaron los títulos y resúmenes de los artículos recuperados, con el objetivo de determinar su pertinencia en relación con la temática de Active Directory y ciberseguridad. En una segunda fase, cuando fue necesario, se realizó la revisión del texto completo para confirmar el cumplimiento de los criterios de inclusión previamente establecidos.

La selección fue realizada por un único revisor, aplicando de forma consistente los criterios definidos para la revisión. Aquellos estudios que no cumplían con los requisitos establecidos fueron descartados antes de pasar a la etapa de evaluación metodológica.

2.4.1 Evaluación de calidad Metodológica

Una vez identificados los estudios potencialmente relevantes, se procedió a realizar una evaluación de calidad metodológica mediante una matriz estructurada en Excel. En esta matriz se definieron cinco dimensiones principales: diseño de la investigación, adecuación del método empleado, generalizabilidad de los hallazgos, enfoque en las áreas de interés de la revisión y nivel en que el estudio responde a la pregunta de investigación.

Cada uno de estos criterios fue calificado utilizando una escala de 0, 0.5 y 1, donde el valor 0 indica que el criterio no se cumple, 0.5 que se cumple de manera parcial, y 1 que se cumple de forma adecuada.

El puntaje total de cada estudio se calculó mediante el promedio de las calificaciones obtenidas en las cinco dimensiones evaluadas. Considerando que cada criterio podía tomar un valor máximo de 1, el puntaje total posible osciló entre 0 y 5.
La decisión de inclusión final se estableció mediante el siguiente criterio:

$Si\ \sum_{i=1}^{5} C_i \geq 2.5$ *entonces Estudio Aceptado*

$Si\ \sum_{i=1}^{5} C_i < 2.5$ *entonces Estudio Rechazado*

Donde C_i representa la calificación asignada a cada uno de los cinco criterios evaluados.

2.5 Proceso de Obtención de Información

Una vez definidos los estudios aceptados tras el proceso de selección y evaluación metodológica, se procedió a la obtención y organización de la información mediante una matriz estructurada en Excel.

En dicha matriz se registraron las siguientes variables generales de identificación: autores, título del estudio, año de publicación, revista o conferencia de procedencia, resumen o abstract, tipo de documento, DOI y enlace de acceso. Estas variables permitieron sistematizar la información bibliográfica y garantizar la trazabilidad de cada estudio incluido en la revisión.

Adicionalmente, la matriz incorporó las cinco columnas correspondientes a los criterios de evaluación metodológica previamente definidos, así como un campo destinado a indicar el estado final del estudio (aceptado o rechazado). En los casos en que un artículo fue excluido, se registró de manera explícita la razón de eliminación, conforme a los criterios de exclusión establecidos.

Finalmente, los resúmenes de los estudios aceptados fueron extraídos y consolidados en un archivo de texto estructurado, con el propósito de conformar el corpus utilizado en el análisis textométrico posterior mediante el software IRaMuTeQ.

2.6 Elementos de los Datos

En la presente revisión se definieron como salidas principales aquellos relacionados con los ataques dirigidos a entornos de Active Directory y las medidas de mitigación o endurecimiento propuestas para su protección. Dentro de estos se incluyeron: tipos de ataque

reportados, técnicas de explotación descritas, mecanismos de defensa implementados y resultados asociados a la mejora de la seguridad del entorno.

Además, se consideraron como salidas secundarias los efectos reportados en términos de reducción de superficie de ataque, fortalecimiento del controlador de dominio, gestión de privilegios y mejoras en monitoreo y detección.

Las salidas definidas también orientaron la interpretación de los patrones léxicos identificados en el análisis textométrico, permitiendo relacionar los resultados estadísticos del corpus con las categorías temáticas de interés.

2.7 Riesgo de Sesgo

La evaluación del riesgo de sesgo de los estudios incluidos se realizó mediante la misma matriz de calidad metodológica descrita previamente. Se consideró que un estudio presentaba mayor riesgo de sesgo cuando obtenía puntuaciones bajas en criterios relacionados con el diseño de la investigación, adecuación metodológica y capacidad de generalización de los resultados.

2.8 Medidas de Efecto

Dado que la presente investigación corresponde a una RSL de carácter descriptivo y técnico, no se emplearon medidas de efecto cuantitativas como razón de riesgo, diferencia de medias u otras métricas estadísticas comparativas.

2.9 Métodos de Síntesis

2.9.1 Elegibilidad para la Síntesis

Todos los estudios que superaron el proceso de selección fueron incluidos en la síntesis final. No se establecieron subgrupos independientes para análisis diferenciados porque el objetivo de la investigación fue realizar una síntesis global de los ataques dirigidos a Active Directory y las medidas de mitigación propuestas.

El texto de análisis estuvo conformado por los títulos, resúmenes (abstracts) y palabras clave de los estudios aceptados, los cuales fueron consolidados en un único archivo de texto para su procesamiento posterior.

2.9.2 Preparación de los Datos

Los registros, anteriormente mencionados, fueron organizados y unificados en un corpus textual estructurado. Antes del análisis, se realizó una revisión manual para formatear los resúmenes y títulos de los documentos seleccionados con el fin de poder realizar el procesamiento automatizado de manera eficaz.

Durante el análisis textométrico, se estableció un criterio de frecuencia mínima para la visualización de resultados. En determinados análisis, se consideraron únicamente las 25 palabras con mayor frecuencia de aparición, con el fin de reducir el ruido léxico y facilitar la identificación de los términos más representativos del corpus. Esta decisión no implicó la exclusión de documentos del análisis general, sino únicamente un ajuste en la presentación de resultados.

2.9.3 Síntesis de Resultados

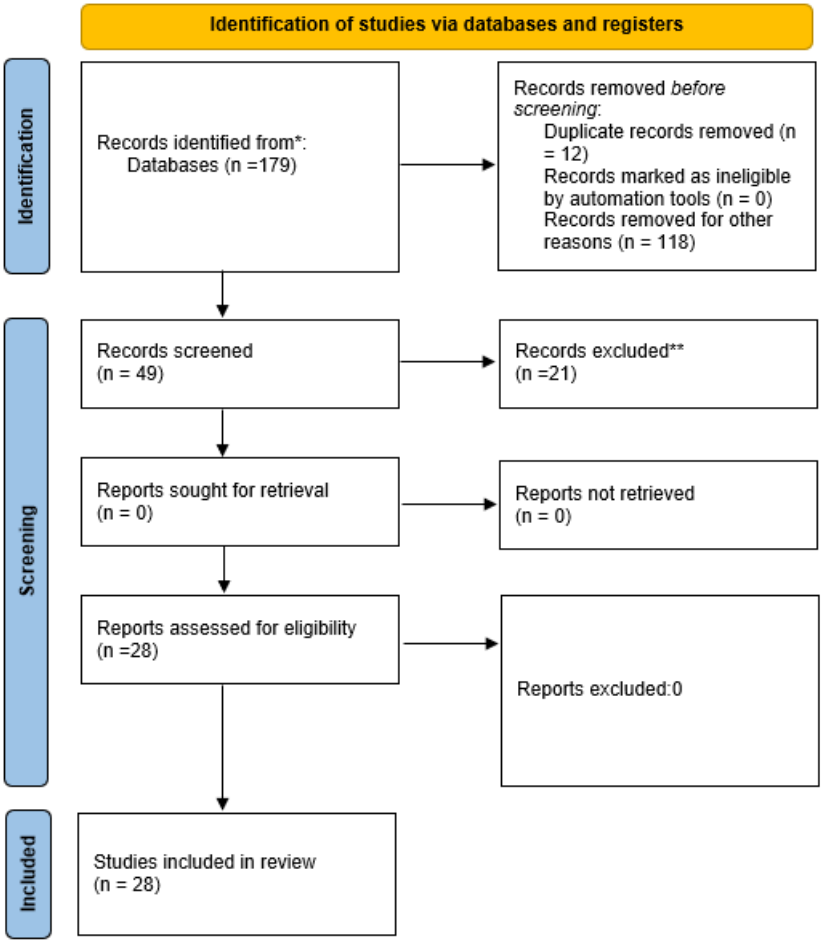
La síntesis se realizó mediante un análisis textométrico, utilizando el software IRaMuTeQ, el cual es como una interfaz del entorno estadístico R. Este método permitió identificar estructuras léxicas dominantes, agrupaciones temáticas y relaciones relevantes dentro del conjunto de estudio.

2.9.4 Heterogeneidad

En el estudio se aborda la heterogeneidad de los resultados basado en los resultados del análisis textométrico, dentro de las clases léxicas generadas, así como los clústeres generados y el dendograma.

Figura 1

Diagrama de flujo del proceso de selección de estudios según PRISMA 2020

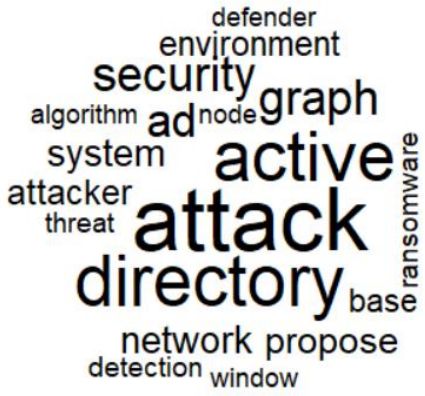


Nota: Diagrama de Flujo adaptado de PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analyses), 2020 https://www.prisma-statement.org/prisma-2020-flow-diagram. En dominio público

3. Resultados y Discusión

Con la herramienta IRaMuTeQ mediante el proceso de análisis textométrico se encontraron las 25 palabras con mayor frecuencia, como se muestra en la nube de palabras (figura 2).

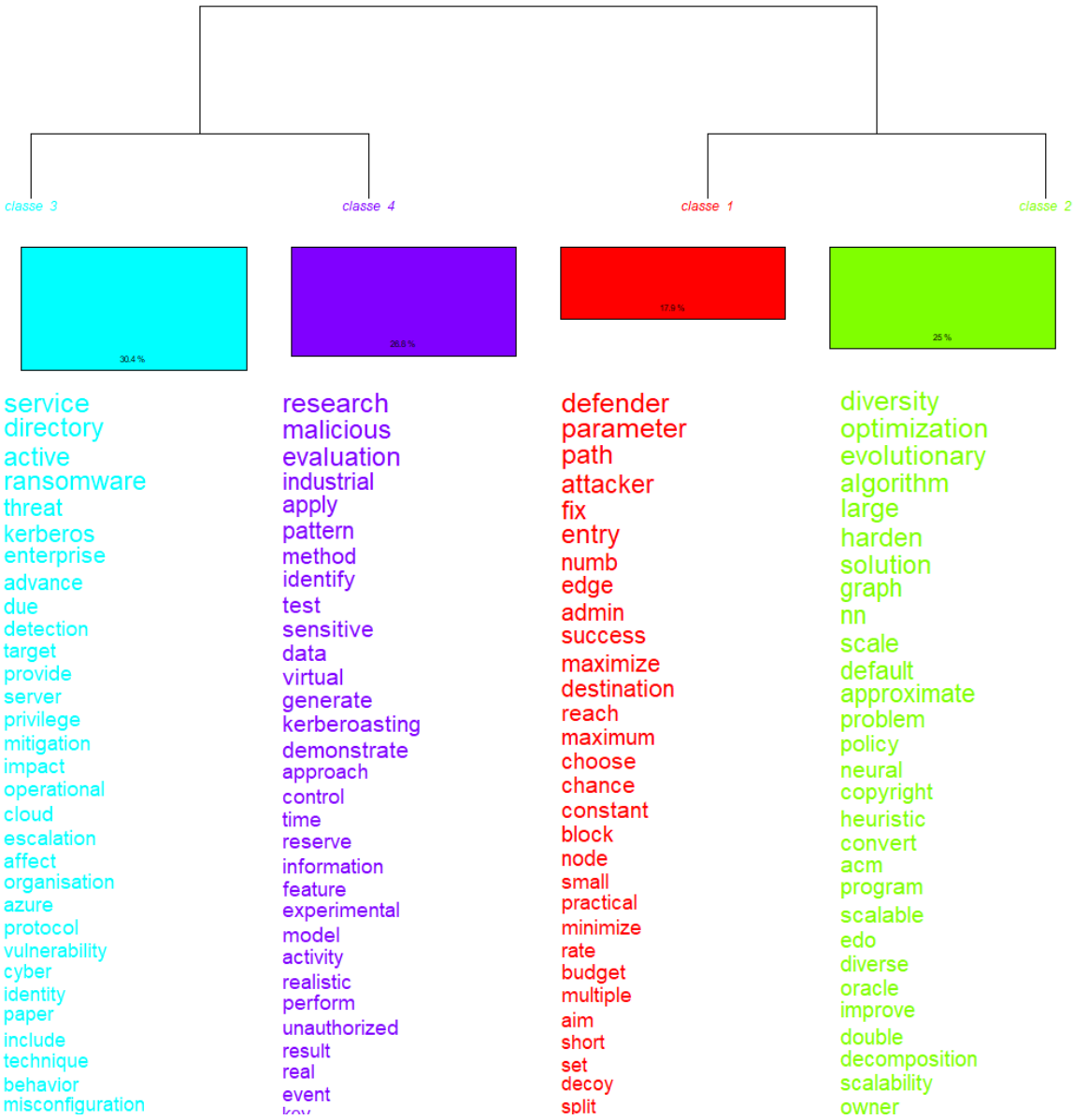
Figura 2
Nube de palabras obtenida de IRaMuTeQ



Se identificaron los siguientes ataques y las técnicas de mitigación propuestas por los diferentes autores. Esto se refleja em la tabla número 1. De acuerdo con lo que refleja el dendograma (figura 3) obtenido tras el análisis textométrico realizado con IRaMuTeQ, además de 4 clases que describen: 1) Prevención y defensa, 2) mitigación 3) defensa y 4) mitigación. A continuación, se detallan los hallazgos del dendograma.

Figura 3

Dendograma obtenido de IRaMuTeQ



3.1 Clúster 1 Prevención y Defensa

La Clase 1, siendo la más pequeña de todas (rojo, 17.9%), visualiza una inclinación hacia una prevención proactiva, además de un refuerzo estructural de la red, mostrado por ejemplo con el término *hardening*[2]. Esta clase también destaca una interacción entre un atacante y un defensor (*defender, attacker, path, Edge, block, decoy).*

[2] Proceso de reducción de la superficie de ataque de un sistema mediante la eliminación de servicios innecesarios, el cierre de puertos no utilizados, la aplicación de parches y la implementación de controles de acceso estrictos, con el fin de minimizar los vectores de entrada disponibles para un atacante (Echeverría et al., 2021).

Esto sin duda refleja la necesidad de estrategias de prevención frente a los ataques dirigidos al AD. La asociación léxica se correlaciona con los modelos teóricos recientes que abordan la seguridad del AD como un juego de *Stackelberg* [3]entre un atacante y el defensor (Goel et al., 2025; Guo et al., 2022). En estos modelos el entorno AD se representa generalmente como un grafo donde los nodos son los activos empresariales, así como cuentas de servicio o de personal y las aristas dirigidas son los accesos posibles o las vulnerabilidades existentes (Ngo et al., 2025). Para estas mismas debilidades del sistema, se propone un endurecimiento de la red mediante un bloqueo de estas aristas, eliminando configuraciones erróneas y accesos innecesarios, además implementando nodos señuelo (*Honeypots o Decoys)* para así maximizar el tiempo de respuesta defensiva. Puesto que calcular una política óptima de defensa en grafos a gran escala es un problema computacionalmente complejo, se destaca el uso de heurísticas escalables, redes neuronales y algoritmos de Optimización de Diversidad Evolutiva (EDO) para generar planes de bloqueo eficaces (Goel et al., 2025).

3.2 Clúster 2 Optimización y Seguimiento

En cuanto a la optimización, los autores tratan la defensa del AD como un problema de optimización, donde el objetivo es reducir la probabilidad de éxito del atacante con un presupuesto de defensa limitado (Zhang et al., 2023). Para redes de gran escala, se propone combinar la Optimización de Diversidad Evolutiva (EDO) con Aprendizaje por Refuerzo (RL) y Redes Neuronales, lo que permite generar múltiples planes de bloqueo de rutas de ataque sin caer en soluciones locales poco efectivas. Además, la optimización no solo se enfoca en lo matemático, sino también en reducir la carga del administrador de TI. Para esto, algunos estudios proponen modelos adaptativos que, en lugar de pedir al administrador que bloquee aristas individuales, le presentan rutas de ataque completas como opciones de selección múltiple (Goel et al., 2025). Este enfoque garantiza que el atacante quede desconectado efectivamente y reduce el tiempo de validación manual (Ngo et al., 2025).

Por otro lado, la literatura señala que esta optimización debe ir acompañada de un seguimiento riguroso para detectar Amenazas Persistentes Avanzadas (APT). Dado que estos atacantes usan tácticas lentas y sigilosas, los Sistemas de Detección de Intrusiones basados en Procedencia (PIDS) han tomado relevancia (Radah et al., 2023). Herramientas como Commander o HADES aplican un rastreo por sesión de inicio de sesión, lo que permite

[3] Modelo de teoría de juegos en el que un líder (atacante) actúa primero y un seguidor (defensor) responde de forma óptima, usado para modelar estrategias de ataque y defensa en seguridad informática.

seguir la actividad maliciosa a través de varias máquinas y vincularla a una sola identidad, incluso cuando el atacante utiliza credenciales robadas para moverse lateralmente. Estos sistemas también integran detectores para identificar técnicas de evasión, como el secuestro de sesiones o ataques de persistencia, reconstruyendo el grafo de ataque completo a nivel de red (Liu, Bao, & Hagenmeyer, 2025).

Este seguimiento se complementa con análisis estadístico y monitoreo de registros en tiempo real. Se propone evaluar la rareza estadística del Evento ID 4624 (inicios de sesión exitosos en Windows) para detectar patrones de autenticación inusuales que indiquen movimiento lateral. De manera similar, el monitoreo del Evento ID 4769 (solicitudes de tickets Kerberos) permite identificar anomalías como la solicitud masiva de tickets con cifrados débiles, que es una señal característica de ataques como Kerberoasting (Kotlaba et al., 2020).

3.3 Clúster 3 Active Directory

El Clúster 3 agrupa la literatura que analiza los servicios que conforman el Active Directory, representando el 30.4% del texto analizado. Los términos más frecuentes en esta clase incluyen: Kerberos, Ransomware, Mitigation, Detection, Privilege y Protocol.

En la arquitectura de redes corporativas modernas, el Active Directory actúa como el servicio central de gestión de identidades, autenticación y control de acceso. Esta centralización lo convierte en el objetivo principal de las Amenazas Persistentes Avanzadas (APT), ya que comprometer el AD equivale a obtener control total sobre la infraestructura de la organización (Nebbione & Calzarossa, 2023).

Dentro de los servicios del AD, la autenticación depende principalmente de Kerberos, que es el protocolo por defecto en entornos Windows. La literatura agrupada en esta clase (Goel et al., 2025; Lee et al., 2024; Motero et al., 2021) revela la manera en que los atacantes aprovechan configuraciones permisivas de este protocolo para extraer credenciales desde la memoria y falsificar tickets de acceso. Técnicas como Kerberoasting, Pass-the-Ticket o la creación de Golden y Silver Tickets permiten evadir los controles de seguridad convencionales sin generar alertas inmediatas(Motero et al., 2021).

El objetivo de explotar estos servicios es el escalamiento de privilegios. Los atacantes avanzan desde nodos con accesos básicos hasta obtener credenciales de alto valor, como las

del Administrador de Dominio. Una vez alcanzado este nivel, el entorno centralizado del AD facilita la propagación de Ransomware. Variantes como Clop o TeslaCrypt aprovechan el acceso administrativo y protocolos de red como SMB para distribuir cargas maliciosas, cifrar datos críticos y comprometer la continuidad operativa de la organización(Lee et al., 2024).

3.4 Clúster 4 Estrategias de Mitigación

El análisis de textométrico de la Clase 4 identifica la mitigación y el seguimiento como una estrategia estructural y operativa, no como una medida aislada. Los estudios coinciden en que la protección efectiva del AD requiere un enfoque de defensa en profundidad que combina el endurecimiento de la red (*hardening)*, la restricción de privilegios y el monitoreo continuo (Hmiddouch et al., n.d.; Senturk & Irmak, 2024).

Una de las estrategias más destacadas es la segmentación de la red mediante modelos de administración por niveles. En estos modelos, los activos más críticos como el Controlador de Dominio y sus administradores (Tier 0) se aíslan lógicamente de los servidores empresariales (Tier 1) y de las estaciones de trabajo de los usuarios (Tier 2) (Lee et al., 2024; Nguyen et al., 2024). Esta separación, alineada con marcos como el modelo Purdue, limita el movimiento lateral de los atacantes y contiene la propagación de amenazas como el ransomware. Complementando este enfoque, la mitigación proactiva también exige el bloqueo sistemático de configuraciones erróneas y accesos innecesarios en el grafo del AD, eliminando las rutas de ataque más directas hacia el Administrador de Dominio (Goel et al., 2025).

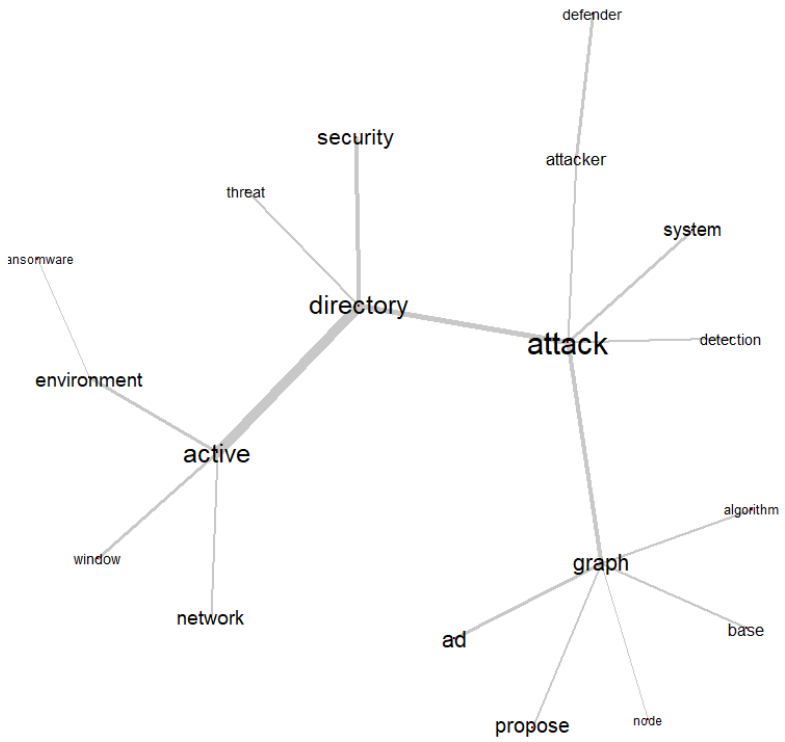
Además, en la literatura se observó la presencia de dos estrategias de mitigación: con BUDGETFTP y DP (dynamic programation) en grafos acíclicos, y por otro lado los SPLITFTP, los cuales pueden ser controlados sobre nodos de bifurcación y Heurística GCN.

A nivel de gestión de identidades, la mitigación se centra en proteger los protocolos de autenticación y prevenir el escalamiento de privilegios. Para esto, la integración de la Gestión de Identidades y Accesos (IAM) con la Gestión de Accesos Privilegiados (PAM) es fundamental, asegurando que todos los usuarios y servicios operen bajo el principio de menor privilegio (Parveen et al., 2021). Frente a ataques como Golden Ticket o Silver Ticket, las medidas preventivas incluyen reducir al mínimo las cuentas con privilegios

administrativos, usar contraseñas complejas y aleatorias para cuentas de servicio, y rotarlas periódicamente. En particular, la literatura señala la importancia de cambiar regularmente la contraseña de la cuenta krbtgt [4] y, ante cualquier evento sospechoso, restablecerla dos veces consecutivas para invalidar cualquier ticket Kerberos forjado por un atacante (Hmiddouch et al., n.d.; Senturk & Irmak, 2024).

En el ámbito técnico, las estrategias de mitigación requieren deshabilitar protocolos heredados como SMBv1 y forzar el uso de versiones más seguras como SMBv2 o superior. Además, se recomienda auditar regularmente las Listas de Control de Acceso (ACL) y revisar los permisos de objetos protegidos como AdminSDHolder, para evitar que los atacantes manipulen plantillas de seguridad y establezcan persistencia. Todas estas medidas deben estar respaldadas por sistemas EDR configurados para rastrear Indicadores de Compromiso (IoC) específicos y plataformas SIEM que monitoreen los registros de eventos de Windows desde servidores aislados y protegidos con autenticación multifactor (Lee et al., 2024).

Figura 4
Gráfico de similitud de texto obtenido de IRaMuTeQ



[4] Cuenta de servicio integrada en Active Directory que cifra y firma todos los tickets Kerberos del dominio; su compromiso permite forjar tickets de autenticación para cualquier usuario (Lee et al., 2024).

3.5 Análisis de Similitud

El gráfico de similitud obtenido mediante IRaMuTeQ refleja las relaciones léxicas más representativas del corpus analizado. En el centro de la red se ubican los términos *attack*, *directory* y *active*, que actúan como nodos principales y concentran la mayor cantidad de conexiones. Esto confirma que la literatura revisada gira en torno a los ataques dirigidos específicamente al Active Directory como servicio.

La fuerte conexión entre *active* y *directory* era esperada, ya que ambos términos conforman la unidad conceptual central de toda la revisión. A su vez, attack se vincula con términos como *attacker, detection, system* y *graph*, lo que refleja que los estudios no solo describen los ataques, sino que también proponen modelos de representación, como grafos, y mecanismos de detección para enfrentarlos. Por otro lado, "active" se conecta con *network, environment* y *window*, indicando que la literatura contextualiza el AD dentro de entornos Windows en red.

Finalmente, la presencia de *ransomware* y *threat* en la periferia del grafo, vinculados a *active*, sugiere que estos términos aparecen como consecuencias o vectores de ataque asociados al AD, pero con menor densidad léxica en comparación con los conceptos centrales.

Tabla 2

Ataques y Respuestas propuestas por los Autores

Autor	Ataque	Mitigación	Prevención	Seguimiento
Guo	Identity snowball attack y phishing	Bloquear aristas con BUDGETFTP, DP en grafos acíclicos, SPLITFTP sobre nodos de bifurcación y Heurística GCN	Bloqueo preventivo de aristas de alto riesgo. Reducir aristas administradoras, convertir grafos cíclicos en acíclicos	Monitoreo de longitud máxima de las rutas de ataque. Seguir aristas bloqueables con BloodHound/SharpHound
Zhang	Identity snowball attack, ransomware	Eliminación de aristas con algoritmo Double Oracle, corte de rutas de ataque de menor longitud ponderada	Hardening del AD, no depender de weakest links de GoodHound, eliminar aristas para cubrir rutas	Auditoría continua de rutas más cortasponderadas, detección deunblockable paths
Nebbione	Amenazas Genéricas	Corrección de configuraciones erróneas, Actualización constante de CVEs identificados en nodos del grafo de ataque, eliminar relaciones críticas innecesarias	Asignación de scores de vulnerabilidades a nodos y aristas del grafo AD, deshabilitar SO obsoletos con *score CRITICAL*, control de contraseñas no expirantes	Evaluaciones de rutas con Random Forest, extracciones de rutas con Neo4j, reclasificación de rutas vulnerables, actualizar *scores*
Simon	Pass-the-hash, Golden Ticket, Kerberoasting, Credential-based attacks, APTs	Respuesta automatizada vía SOAR, reset forzado de contraseñas y deshabilitación de cuentas comprometidas	Baselining comportamental de usuarios/entidades con Open XDR, políticas de acceso, control de cuentas huérfanas, integración con IGA	Correlación de telemetría multifuente, endpoints, red, nube e identidad AD; monitoreo en tiempo real de Event IDs 4624/4625, 4728/4729/4732, 4768/4769; mapeo de cadenas de eventos a tácticas MITRE ATT$CK
Nicholas	Varios tipos de ransomware	Reglas de detección comportamental, aislamiento de endpoints, revocación de credenciales	Restricción de Event ID 7045 (instalación de servicios no autorizados), control estricto de hardening de gestión de servicios	Monitoreo de varios Event IDs, seguimiento de estos eventos, clasificación con Random Forest
Goel	Identity snowball attack, phishing	Bloqueo de aristas, uso de EDO para planes de bloqueo	Bloqueo preventivo de aristas block-worthy con presupuesto k, eliminación de aristas con privilegios	Simulacro Monte Carlo, monitorear rutas de ataque con BloodHound
Ngo	Ataques por rutas de escalamiento de niveles	Eliminación interactiva de rutas de ataque con DPR	Eliminación de conexiones cross-tier no autorizadas, implementar el modelo de tiering	Revisión de rutas de ataque, auditorías periódicas de nodo con tier indefinido usando ImproHound
Nguyen	Identity snowball attack, escalamiento de privilegios	No hay	Separación de objetos por tier, Aplicación del principio de mínimo privilegio	Facilita el testing no propone
Mokthar	Pass-the-hash, kerberoasting, silver ticket, golden ticket, Skeleton key, Delegation abuse	Proteger la memoria del proceso LSASS, reestablecer contraseña de krbtgt dos veces para detener Golden ticket activo, Deshabilitar cuenta de	Políticas de contraseña fuerte, habilitar cifrado Kerberos AES	Monitoreo constante de eventos, monitoreode estado del servicio DNS

		acceso DSRM, limitar número de Domains Admins		
Lee	Clop ransomware, spear phishing	Implementar EDR, Aplicar MFA, Segmentar la red	Control estricto de cuentas administradoras, capacitar el personal para identificar phishing, backups offline regulares	Monitoreo en tiempo real de procesos terminados por el ransomware, vigilancia de modificaciones de archivos, ejercicios periódicos de red teaming y simulaciones de ransomware.
Liu	APT multi-fase y multi-máquina	Integración de detectores especializados contra persistencia	Hardening de registros	Rastreo de proveniencia por sesión de login en toda la red, reglas TTP sobre MITRE ATT&CK
Nguyen demo	Movimiento lateral	No se menciona	Generación de grafos de AD sintéticos con ADSynth para evaluar y optimizar	No se menciona
Radah	Movimiento lateral	No se menciona	No se menciona	Análisis de rareza estadística
Lukas O	Movimiento lateral	No se menciona	Inserción de honeyusers en posiciones orgánicas con DAG-RNN VAE	Monitoreo de accesos a cuentas señuelo para identificación de los atacantes
Younisse	Kerberoasting, fuerza bruta	No se menciona	Deshabilitar la opción, *do not require Kerberos pre-authentication*	Detetcción temprana por etapa del ciclo de vida del ataque, escaneo masivo de puertos, usar SharpHound en campo *info* de los logs de red
Hmiddouch	AS-REP Roasting, Kerberoasting, movimiento lateral, ransomware	Aislamiento inmediato del nodo comprometido, despliegue de reverse Shell, monitoreo de tráfico con Wireshark	Activar pre-autenticación Kerberos en todas las cuentas de dominio, segmentación de la red, control de servicios SSH expuestos	Capturar tráfico de red con Wireshark, análisis de procesos y cambios con Sysinternals Suite
Bu Haimed	Escalamiento horizontal de privilegios, escalamiento vertical de privilegios	Revocar privilegios de Owner en la identidad administrada y limitar el alcance, corrección inmediata de condiciones de grupo	Evitar condiciones de grupos dinámicos basados en atributos que el usuario	Evaluación de vulnerabilidades con el marco CCSS, monitoreo continuo de accesos y roles asignados a identidades administradas
Liu et al	AS-REP Roasting, kerberoasting , pass-the-hash, pass-the-Ticket, overpass-the-hash, silver ticket, golden ticket, movimiento lateral	Triaje automático con *threat score*, generación de grafos de ataque de bajo nivel con trazado cross-machine	Particionado con sesión de logon para reducir falsas dependencias, configuración de Windows logs	Detección de anomalías de autenticación, trazado de procedencia cross-machine, puntuación de amenazas por grafo considerando credential Access, Discovery.
Goel 2025	Identity snowball attack	Bloqueo de aristas, RL+C-EDO (Critic network-Assisted Evolutionary Diversity Optimization), bloqueo de aristas mediante política NNDP+EDO , selección del plan de bloqueo óptimo por EDO	Bloqueo preventivo de k aristas block-worthy, reducción del grafo AD a grafo condensado via kernelización, aplicación del modelo Stackelberg	Evaluación periódica mediante simulaciones Monte Carlo , reentrenamiento continuo , monitoreo del grafo AD con BloodHound/SharpHound

Parveen	Robo de credencniales	Terminación autpomática de sesiones sospechosas, grabación de sesiones	Integración de IAM con PAM, implementar RBAC, evaluación periódica de derechos de acceso	Grabación continua de sesiones privilegiadas de auditoría, registro y monitoreo de toda actividad
Abo alian	ATP sobre AD	Priorizar TTPs	Emular atacantes con ATI	No menciona
Kotlaba	Kerberoasting	Honeypots, filtrado de cuentas	Deshabilitar suites con cifrado	Monitoreo de eventos
Diaz Montero	Overpass-the-Hash, Pass-the-Ticket, Golden Ticket, Silver Ticket, Kerberoasting	Reseteo doble de contraseña KRBTGT; Credential Guard; grupo 'Protected Users'; gMSA;	Deshabilitar delegación irrestricta; deshabilitar RC4, forzar AES256; no otorgar privilegios admin	Monitoreo de eventos
Ngo	Identity snowball attack en grafos temporales de AD	Colocación óptima de decoys/honeypots en nodos estratégicos	No menciona	No menciona
McDonald et al. (2022)	Ransomware WannaCry Ransomware TeslaCrypt Ransomware Jigsaw	Restauración desde snapshots de VMs, uso de directorios críticos (system32) y separación de file share para limitar cifrado	Deshabilitar SMBv1, aplicar parches (MS17-010), mantener Windows Defender, usar backup DC y restringir extensiones en file share	Monitoreo con Process Monitor, verificación de servicios AD (Logon, DNS, DHCP, IIS, GPO) y detección de vssadmin.exe
Guo et al. (2023)	Identity snowball attack, phishing	Bloqueo de aristas con TDCYCLE (DP), IP/kernelización y MIP-F + ITERLP para minimizar éxito del atacante	Eliminación de aristas no esenciales (AdminTo, MemberOf, HasSession) y hardening cercano al DA	Evaluación con Dijkstra en grafos AD, uso de BloodHound y seguimiento de rutas de ataque
Herranz-Oliveros et al. (2023)	Lateral movement, identity snowball attack, ransomware automatizado tipo WannaCry, APTs	Inmunización reactiva de super-spreaders y reconfiguración de red	Inmunización selectiva (SImS) con DBSCAN, basada en centralidad (betweenness, closeness, K-shell)	Simulación SI, medición MTHC y análisis de shortest paths
Goel et al. (2024)	Identity snowball attack, movimiento lateral hacia Domain Admin	Bloqueo dinámico con RL-EDO y reentrenamiento del defensor	Selección de aristas block-worthy (k limitado), optimización de diversidad y poda de NSPs	Evaluación con RL critic network, simulación en grafos (r1000 a r4000) y análisis de cobertura

4. Propuesta

La presente guía propone un marco integral para el aseguramiento de entornos AD, esta guía está orientada en las etapas de: (1) prevención o aseguramiento; (2) mitigación; y (3) seguimiento o continuidad. Además, está conformada usando como bases principales los estudios seleccionados previamente, lo que permite que estructura sea sólida y el enfoque científico este garantizado. Para la propuesta los estudios considerados fueron los que se visualizan en la tabla 3.

Tabla 3

Estudios seleccionados con los objetivos de cada estudio.

Título	Autores	Objetivo
Hardening Active Directory Graphs via Evolutionary Diversity Optimization-based Policies	Goel, Diksha Ward, Max Neumann, Aneta Neumann, Frank Nguyen, Hung Guo, Mingyu	Políticas defensivas basadas en NN y RL para bloquear rutas de ataque en grafos AD.
COMMANDER: A robust cross-machine multi-phase Advanced Persistent Threat detector via provenance analytics	Liu, Qi Bao, Kaibin Hagenmeyer, Veit	PIDS capaz de detectar ataques APT multi-fase y entre múltiples máquinas en redes industriales.
Adaptive Wizard for Removing Cross-Tier Misconfigurations in Active Directory	Ngo, Huy Guo, Mingyu Nguyen, Hung.X Ngo, Q.	Minimizar el esfuerzo manual del administrador en la eliminación iterativa de rutas de ataque en AD.
HADES: Detecting and Investigating Active Directory Attacks via Whole Network Provenance Analytics	Liu, Qi Bao, Kaibin Hassan, Wajih Ul Hagenmeyer, Veit	PIDS con trazabilidad causal entre máquinas para detectar ataques APT en entornos AD.
Active Directory Open XDR Cyber Security Techniques to Detect Anomalies	Simon, Judy Mohanakumar, Anoop Kapileswar, Nellore	Detectar anomalías y ataques en AD mediante integración de XDR y correlación de eventos de seguridad.
A Behavioral Analysis of Ransomware in Active Directory: A Case Study of BlackMatter, Conti, LockBit, and Midnight	Bhandary, Prajna Nicholas, Charles	Analizar patrones de comportamiento de ransomware en AD para mejorar su detección y mitigación.
Enhancing Industrial Cybersecurity with Virtual Lab Simulations	Hmiddouch, Hamza Villafranca, Antonio Castro, Raul Dubetskyy, Volodymyr Cano, Maria-Dolores	Framework AD + Open XDR para detectar movimiento lateral, escalada de privilegios y abuso de credenciales.
Clop Ransomware in Action: A Comprehensive Analysis of Its Multi-Stage Tactics	Lee, Yongjoon Lee, Jaeil Ryu, Dojin Park, Hansol Shin, Dongkyoo	Analizar comportamiento de cuatro familias de ransomware en AD mediante modelado n-gram sobre Event Logs.
Demo: Synthesizing Realistic Enterprise Active Directory Attack Graphs with ADSynth	Nguyen, Nhu Long Falkner, Nickolas Nguyen, Hung	Entorno virtual ICS/AD para entrenar profesionales en detección y mitigación de vulnerabilidades.
Optimizing Cyber Response Time on Temporal Active Directory Networks Using Decoys	Ngo, Huy Guo, Mingyu Nguyen, Hung	Analizar técnicas multi-paso del ransomware Clop enfocadas en servidores AD.

Surgical immunization strategies against lateral movement in Active Directory environments	Herranz-Oliveros, David Marsa-Maestre, Ivan Jimenez-Guzman, Jose Manuel Tejedor-Romero, Marino de la Hoz, Enrique	Herramienta open source para generar grafos AD realistas para investigación y pruebas de seguridad.
A Scalable Double Oracle Algorithm for Hardening Large Active Directory Systems	Zhang, Yumeng Ward, Max Guo, Mingyu Nguyen, Hung	Maximizar el tiempo de respuesta del defensor mediante colocación óptima de señuelos en grafos AD temporales.
Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks	Haimed, Ibrahim Bu Albahar, Marwan Alzubaidi, Ali	Técnicas de inmunización selectiva sobre relaciones de confianza en AD para mitigar movimiento lateral.
Scalable Edge Blocking Algorithms for Defending Active Directory Style Attack Graphs	Guo, Mingyu Ward, Max Neumann, Aneta Neumann, Frank Nguyen, Hung	Algoritmo escalable basado en Double Oracle para endurecer sistemas AD de gran escala.
AN EARLY DETECTION MODEL FOR KERBEROASTING ATTACKS AND DATASET LABELING	Younisse, Remah Alkasassbeh, Mouhammad Almsedein, Mohammad Abdi, Hamza	Identificar y evaluar vulnerabilidades por mala configuración en Azure AD que derivan en escalada de privilegios.
Detecting Unconventional and Malicious Windows Authentication Activities Through Statistical Rarity Assessment	Radah, Tarek Chaoui, Habiba Saadi, Chaimae	Algoritmos que explotan la estructura tipo árbol de grafos AD para bloquear rutas de ataque eficientemente.
Disrupting Active Directory Attacks with Deep Learning for Organic Honeyuser Placement	Lukas, Ondrej Garcia, Sebastian	Método para etiquetar datasets de ataques multi-etapa y predecir ataques Kerberoasting en AD.
A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments	Nebbione, Giuseppe Calzarossa, Maria Carla	Análisis estadístico de eventos de autenticación para identificar accesos maliciosos en entornos AD.
Active Directory Attacks—Steps, Types, and Signatures	Mokhtar, Basem Ibrahim Jurcut, Anca D. ElSayed, Mahmoud Said Azer, Marianne A.	Modelo basado en autoencoder variacional para ubicar honeypots orgánicos e indetectables en AD.
Defending active directory by combining neural network based dynamic program and evolutionary diversity optimisation	Goel, Diksha Ward-Graham, Max Hector Neumann, Aneta Neumann, Frank Nguyen, Hung Guo, Mingyu	Framework IA con grafos y ML para evaluar automáticamente la seguridad de entornos AD.
Practical Fixed-Parameter Algorithms for Defending Active Directory Style Attack Graphs	Guo, Mingyu Li, Jialiang Neumann, Aneta Neumann, Frank Nguyen, Hung	Revisión de ataques AD, su criticidad, impacto y detección con experimentos sobre escalada de privilegios.

Ransomware: Analysing the Impact on Windows Active Directory Domain Services	McDonald, Grant Papadopoulos, Pavlos Pitropakis, Nikolaos Ahmad, Jawad Buchanan, William J.	Aproximar el problema del atacante en AD con NN entrenada mediante optimización evolutiva diversificada.
Integration of Identity Governance and Management Framework within Universities for Privileged Users	Parveen, Shadma Ahmad, Sultan Khan, Mohammad Ahmar	Maximizar la longitud esperada de la ruta de ataque más corta mediante interdición de aristas en grafos AD.
Active Directory Kerberoasting Attack: Monitoring and Detection Techniques	Kotlaba, Lukáš Buchovecka, Simona Lőrincz, Róbert	Analizar mediante análisis dinámico cómo tres variantes de ransomware afectan servicios de Windows Server y AD.
A data-driven approach to prioritize MITRE ATT&CK techniques for active directory adversary emulation	Alshaimaa Abo-alian, Mahmoud Youssef Nagwa L. Badr	Enfoque integrado IAM + PAM sobre AD para proteger datos sensibles de accesos no autorizados.
On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey	Carlos Díaz Motero Juan Ramón Bermejo Higuera Javier Bermejo Higuera Juan Antonio Sicilia Montalvo Nadia Gámez Gómez	Reglas de detección del ataque Kerberoasting usando capacidades nativas de auditoría de AD.
ADSynth: Synthesizing Realistic Active Directory Attack Graphs	Nguyen, N.L.; Falkner, N.; Nguyen, H.	Generar grafos de ataque realistas de AD para evaluar y probar estrategias de defensa.
Optimizing Cyber Defense in Dynamic Active Directories Through Reinforcement Learning	Goel, D.; Moore, K.; Guo, M.; Wang, D.; Kim, M.; Camtepe, S.	Optimizar estrategias defensivas en AD dinámicos mediante aprendizaje por refuerzo.

4.1 Estrategia de Aseguramiento

Esta etapa se centra en la prevención, el endurecimiento de la arquitectura y la identificación de vulnerabilidades antes que sean explotadas.

Nebbione & Calzarossa (2023) proponen automatizar las evaluaciones de seguridad del AD modelando la red como un grafo y aplicando técnicas de machine learning, específicamente random forest, para clasificar rutas de ataque y asignar puntuaciones de vulnerabilidad a nodos y aristas. Esto permite a los administradores identificar sistemas operativos obsoletos con puntuación crítica, contraseñas sin expiración y relaciones innecesarias entre objetos, corrigiendo configuraciones de forma proactiva antes de que sean aprovechadas.

Abo-alian et al. (2025) plantean que la mejor forma de preparar el entorno es mediante la simulación de adversarios basada en datos reales. Su enfoque combina *Toma de Decisiones Multicriterio con Inteligencia de Amenazas Operacional* para priorizar dinámicamente las técnicas del marco MITRE ATT&CK que tienen mayor impacto y menor probabilidad de detección en el AD, evitando invertir recursos en simulaciones estáticas o manuales que no reflejan el comportamiento real del atacante.

Hmiddouch et al. (2025) sostienen que una práctica fundamental para evitar interrupciones en los sistemas productivos es el uso de laboratorios virtuales que funcionen como gemelos digitales del entorno real. Esto permite probar la segmentación de red y descubrir errores críticos de configuración, como la ausencia de autenticación kerberos, antes que provoquen incidentes en producción. Complementan esto recomendando activar la preautenticación kerberos en todas las cuentas de dominio y controlar los servicios SSH expuestos innecesariamente.

Goel et al. (2025) y Zhang et al., (2023) mencionan que para el endurecimiento del AD la estrategia más sólida es la inhabilitación de bordes, es decir, el bloqueo preventivo de rutas de acceso. Proponen la defensa como un juego de Stackelberg donde el defensor actúa primero y utilizan algoritmos de *Optimización de Diversidad Evolutiva* y aprendizaje por refuerzo para determinar matemáticamente qué aristas del grafo deben bloquearse para reducir al máximo la tasa de éxito del atacante dentro de un presupuesto limitado, luego el atacante realiza su movimiento teniendo en cuenta estas restricciones y así sucesivamente.

Esto se traduce en eliminar aristas de tipo AdminTo, MemberOf y HasSession que no sean estrictamente necesarias, reducir la cantidad de objetos con privilegios administrativos y convertir grafos cíclicos en acíclicos para limitar los caminos disponibles hacia el Domain Admin.

Goel et al., (2025) y Zhang et al., (2023) refuerzan este enfoque indicando que la separación de objetos por niveles mediante el modelo de *tiering*[5], combinado con el principio de mínimo privilegio, reduce de forma significativa la superficie de ataque disponible antes de que un adversario intente moverse lateralmente.

Haimed et al. (2023), enfocados en entornos de Azure AD, comentan que para asegurar el sistema en la nube se debe implementar un modelo riguroso y preciso de permisos basados en alcances. Recomiendan no depender de atributos controlables por el usuario para configurar grupos dinámicos y restringir severamente el uso de identidades administradas en máquinas virtuales, ya que estas pueden ser explotadas para escalar privilegios de forma horizontal y vertical.

Parveen et al. (2021) señala que integrar la gestión de identidades y accesos (IAM) con plataformas de gestión de acceso privilegiado (PAM), junto con la implementación de control de acceso basado en roles (RBAC) y evaluaciones periódicas de derechos de acceso, constituye una base sólida para reducir el riesgo antes de cualquier ataque.

McDonald et al. (2022) aportan medidas concretas de endurecimiento orientadas a la prevención del ransomware: (1) deshabilitar SMBv1 para eliminar el vector de propagación usado por WannaCry, (2) mantener actualizadas las correcciones críticas del sistema, (3) conservar Windows Defender activo en los equipos cliente e implementar un controlador de dominio de respaldo, lo que permite prevenir una eventual caída del DC.

4.2 Estrategia de Mitigación

Esta etapa define las acciones para interrumpir un ataque en curso, limitar el movimiento lateral y aislar los activos comprometidos de la mejor manera posible.

[5] Estrategia de defensa en ciberseguridad que organiza los activos y controles de seguridad en capas jerárquicas según su nivel de criticidad, permitiendo priorizar la protección de los recursos más sensibles de la organización.

En este sentido, Herranz-Oliveros, Marsa-Maestre, et al. (2024) proponen lo que denominan “inmunización quirúrgica”. Utilizando modelos epidemiológicos y métricas de centralidad de grafos como betweenness centrality, closeness y número de descendientes, demuestran que es posible frenar la propagación de un ataque endureciendo menos del 0.1% de los nodos de la red, concentrándose exclusivamente en los nodos que actúan como propagadores del movimiento lateral. Esto paraliza la infección con un impacto mínimo en el rendimiento operativo, que es lo que se busca en la práctica.

Por otro lado, Lukas & Garcia, (2023) y Ngo et al., (2025), coinciden en que el despliegue de señuelos (Honeypots) es una de las herramientas más efectivas para mitigar el avance del atacante. Proponen el uso de autoencoders DAG-RNN para insertar cuentas falsas en posiciones estructuralmente orgánicas dentro del grafo del AD, de forma que resulten creíbles para el atacante. Ngo et al. (2025) demuestra que ubicar estos señuelos de manera estratégica maximiza el tiempo de respuesta del defensor, permitiendo detectar y aislar al atacante antes de que alcance el controlador de dominio.

Motero et al. (2021), junto con Mokhtar et al. (2022), especifican que, para mitigar ataques de robo de credenciales como Golden Ticket, Pass the Hash, Pass the Ticket o Kerberoasting, las acciones más efectivas son: deshabilitar el cifrado débil RC4 y forzar el uso de AES256; añadir las cuentas sensibles al grupo de Usuarios Protegidos y habilitar Windows Defender Credential Guard para proteger la memoria del proceso LSASS. Si un controlador de dominio resulta comprometido, la acción de respuesta crítica es restablecer dos veces la contraseña de la cuenta KRBTGT para invalidar cualquier ticket Kerberos falsificado que esté activo. Además, recomiendan deshabilitar la delegación son restricciones, limitar el número de Domain Admins y deshabilitar la cuenta de acceso DSRM.

Además, Simon et al. (2025) argumentan que integrar plataformas Open XDR con el AD permite implementar playbooks de automatización mediante SOAR que, al detectar una anomalía, ejecutan respuestas instantáneas como el aislamiento de sistemas afectados, el reset forzado de contraseñas o la exigencia de autenticación multifactor, reduciendo drásticamente el tiempo medio de respuesta ante incidentes.

Lee et al. (2024) indican que ante la presencia de ransomware como Clop, las acciones de contención deben incluir la implementación de EDR, la aplicación de MFA y la segmentación de red para limitar el alcance del cifrado. McDonald et al. (2022) complementan esto indicando que, en caso de infección, es viable restaurar desde snapshots de máquinas virtuales y que los archivos de servicios críticos como DNS y DHCP ubicados en directorios del sistema suelen ser respetados por el ransomware, lo que permite mantener servicios básicos activos durante la respuesta.

Hmiddouch et al. (2025) añaden que ante un nodo comprometido se debe proceder al aislamiento inmediato del mismo, al despliegue de herramientas de análisis de tráfico como Wireshark y al monitoreo activo de procesos con Sysinternals Suite para contener el incidente.

4.3 Estrategia de Continuidad

Esta etapa se enfoca en la monitorización persistente, la auditoría forense, la resiliencia operativa y el rastreo de amenazas a largo plazo.

En este contexto, Liu, Bao, & Hagenmeyer (2025) y Liu, Bao, Hassan, et al. (2025) establecen que para rastrear ataques sigilosos y de múltiples etapas como las APT, la mejor herramienta es el uso de sistemas de detección basados en procedencia, como HADES o Commander. Estos sistemas dividen la ejecución según las sesiones de inicio de sesión de los usuarios y permiten reconstruir el grafo completo del ataque vinculando causalmente alertas que, de forma aislada, parecerían no relacionadas entre sí.

Además, Bhandary & Nicholas (2025) señalan que la continuidad en la detección temprana del ransomware exige un análisis de comportamiento continuo. Proponen monitorizar los registros de eventos de Windows usando modelos de secuencias de n-gramas, con enfoque en eventos como el 4624 y el 4688, para identificar patrones repetitivos de control de servicios o acceso a credenciales antes de que comience el cifrado.

A esto, Radah et al. (2023) sugieren aplicar evaluaciones de rareza estadística sobre el Evento 4624 de Windows para rastrear actividades de inicio de sesión no convencionales. Asignando puntuaciones de rareza a los accesos, los analistas pueden priorizar la

investigación de patrones anómalos en la red sin necesidad de revisar manualmente todos los registros.

Por su parte, Kotlaba et al. (2020) destacan que para el seguimiento específico de amenazas como kerberoasting se deben implementar filtros en herramientas como Splunk orientados al monitoreo continuo del Evento 4769, prestando especial atención a solicitudes de tickets de servicio que utilicen tipos de cifrado débiles o que provengan de puertos inusuales. El uso de listas blancas reduce los falsos positivos y hace el monitoreo más operativo.

El aporte de Simon et al. (2025) lo complementa indicando que la correlación de telemetría proveniente de múltiples fuentes, como endpoints, red, nube e identidad en el AD, junto con el monitoreo en tiempo real de Event IDs como 4624, 4625, 4728, 4729, 4732, 4768 y 4769, y el mapeo de cadenas de eventos a tácticas del marco MITRE ATT&CK, permite construir una visión completa y contextualizada de las amenazas activas.

Por otro lado, McDonald et al. (2022) aportan que el monitoreo de procesos con Process Monitor es útil para detectar la terminación de servicios clave del AD como Logon, DNS, DHCP, IIS y Group Policy, y que la detección de la terminación del proceso vssadmin.exe constituye un indicador confiable de ejecución de ransomware.

También, Parveen et al. (2021) refuerza la importancia de mantener una grabación continua de sesiones privilegiadas como parte de la auditoría permanente, junto con el registro de toda actividad relacionada con cuentas de alto privilegio.

En la misma línea, Lee et al. (2024) concluyen que la resiliencia administrativa frente al ransomware requiere realizar auditorías regulares, mantener copias de seguridad estrictamente fuera de línea y ejecutar simulacros de phishing de forma periódica para mantener al personal preparado ante el vector de ataque más común. Complementan esto recomendando ejercicios periódicos de red teaming y simulaciones de ransomware para evaluar la capacidad real de respuesta de la organización.

Por otra parte, Egho-Promise et al. (2025) señalan que las estrategias de respaldo constituyen un componente crítico en la mitigación del ransomware, destacando que las organizaciones deben mantener copias de seguridad regulares, cifradas y aisladas de la red, almacenadas en

múltiples ubicaciones incluyendo entornos fuera de línea y en la nube. Los autores agregan que las pruebas regulares de los planes de recuperación ante desastres son esenciales para garantizar que los sistemas y datos puedan restaurarse con rapidez ante un ataque, dado que optimizar los tiempos de recuperación es fundamental para reducir el tiempo de inactividad y restablecer los servicios críticos sin necesidad de pagar el rescate.

Asimismo, Perin (2025) complementa esto al afirmar que los mecanismos de recuperación tienden a estar insuficientemente probados, con escasos criterios estandarizados o pruebas de rendimiento a escala, y que no debe asumirse que la recuperación está correctamente validada, sino que debe garantizarse de forma continua mediante simulacros periódicos de recuperación.

En el trabajo de Derick Musundi Kesa (2023) se establece que la planificación de recuperación ante desastres en TI requiere el desarrollo de estrategias, políticas y procedimientos para restaurar la infraestructura y los servicios de TI dentro de plazos predefinidos, y que dicha planificación debe incluir la definición de objetivos de tiempo de recuperación (RTO) y de punto de recuperación (RPO), los cuales determinan el tiempo máximo de inactividad tolerable y la cantidad máxima aceptable de pérdida de datos respectivamente.

Finalmente, Chang et al. (2021) refuerzan esta perspectiva al describir una arquitectura de respaldo en red estructurada en tres capas: (1) cliente, (2) servicio y (3) gestión, donde las operaciones de respaldo realizadas por los clientes deben contemplar explícitamente tanto la configuración de planes de backup como la configuración de pruebas de recuperación, junto con medidas de seguridad como el cifrado y la verificación del proceso de restauración, lo que evidencia que la generación de respaldos y su comprobación constituyen componentes inseparables de una estrategia de protección de datos robusta.

5. Conclusiones

La presente investigación permitió identificar y analizar, mediante una revisión sistemática de literatura bajo el protocolo PRISMA y un análisis textométrico en IRaMuTeQ, los ataques más comunes dirigidos a entornos Active Directory, los factores que los facilitan y las estrategias de detección, respuesta y monitoreo aplicadas tras dichos incidentes. Los resultados evidencian que los vectores de ataque predominantes son la escalación de privilegios, el movimiento lateral y la explotación del protocolo Kerberos, facilitados

principalmente por configuraciones permisivas, el principio de mínimo privilegio no aplicado y la ausencia de mecanismos de monitoreo continuo.

Frente a estos riesgos, la literatura revisada converge en un enfoque estructurado de tres etapas: (1) aseguramiento preventivo; (2) mitigación activa y (3) continuidad operativa. De esta forma, se da respuesta al objetivo general de la investigación, cumpliendo también con los tres objetivos específicos planteados.

En cuanto al primer objetivo específico: realizar una revisión sistemática de literatura aplicando el método PRISMA para identificar fuentes de ataque y técnicas de mitigación y continuidad de operaciones de entornos Active Directory, se llevó a cabo la revisión sistemática de literatura aplicando el protocolo en mención, proceso que permitió seleccionar y analizar un conjunto de fuentes científicas relevantes para identificar las principales fuentes de ataque dirigidas a entornos Active Directory, así como las técnicas de mitigación y continuidad de operaciones documentadas en la literatura.

Respecto al segundo objetivo específico, realizar un análisis textométrico para clasificar los factores y mecanismos de ataque más comunes, así como las técnicas de restablecimiento de operaciones más aplicadas, se realizó el análisis textométrico en IRaMuTeQ utilizando los artículos seleccionados en la fase anterior, lo que permitió clasificar los factores y mecanismos de ataque más comunes, así como las técnicas de restablecimiento de operaciones más aplicadas en contextos reales, identificando los siguientes grupos de palabras: (1) defender, parameter, path, attacker, fix, entry, numb, edge, admin, success, maximize, destination, reach, maximum, choose, chance, constant, block, node, small, practical, minimize, rate, budget, multiple, aim, short, set, decoy, split (2) diversity, optimization, evolutionary, algorithm, large, harden, solution, graph, nn, scale, default, approximate, problem, policy, neural, copyright, heuristic, convert, acm, program, scalable, edo, diverse, oracle, improve, double, decomposition, scalability, owner (3) service, directory, active, ransomware, threat, kerberos, enterprise, advance, due, detection, target, provide, server, privilege, mitigation, impact, operational, cloud, escalation, affect, organisation, azure, protocol, vulnerability, cyber, identity, paper, include, technique, behavior, misconfiguration (4) research, malicious, evaluation, industrial, apply, pattern, method, identify, test, sensitive, data, virtual, generate, kerberoasting, demonstrate, approach, control, time, reserve, information, feature, experimental, model, activity, realistic, perform, unauthorized, result, real, event, key.

Finalmente, en cumplimiento del tercer objetivo específico, concluir con la estructura de una guía de estrategias de detección, respuesta y seguimiento post-incidente reportadas en estudios y buenas prácticas de AD, se consolidó una guía de estrategias de detección, respuesta y seguimiento postincidente, estructurada a partir de los hallazgos de los estudios seleccionados y alineada con las buenas prácticas de seguridad en Active Directory.

El logro de estos tres objetivos específicos da cumplimiento al objetivo general de la investigación, al haber identificado y analizado de manera sistemática y fundamentada los ataques más comunes, los factores que los facilitan y las estrategias aplicadas para su detección, respuesta y monitoreo.

Consecuentemente, la guía de estrategias propuesta constituye un aporte concreto y fundamentado científicamente para administradores y equipos de seguridad que gestionan entornos AD. Al integrar en un marco unificado las buenas prácticas más respaldadas por la literatura, la guía ofrece una referencia estructurada y aplicable para configurar, asegurar y mantener operativo un Active Directory ante el panorama actual de amenazas. Su valor radica en traducir hallazgos académicos en acciones operativas concretas, cerrando la brecha entre la investigación teórica y la gestión práctica de la seguridad en directorio de dominio.

6. Limitaciones

La principal limitación de esta investigación fue el acceso restringido a determinadas bases de datos y repositorios académicos, lo cual redujo el número de artículos disponibles para su inclusión en la revisión. Si bien se consultaron múltiples fuentes como Scopus, IEEE Xplore, Web of Science, Springer, SAGE, Emerald, Taylor & Francis y SciELO, algunas publicaciones relevantes se encontraban en bases de datos de acceso cerrado o bajo suscripciones institucionales no disponibles, lo que limitó la cobertura total de la literatura existente.

7. Trabajos futuros

Se recomienda la continuación de esta línea de investigación mediante la validación práctica de la guía propuesta en entornos reales de Active Directory. Específicamente, se sugiere su implementación y evaluación utilizando diferentes versiones de los sistemas operativos Windows Server, así como en distintos contextos de infraestructura tecnológica, con el fin

de verificar su aplicabilidad y adaptabilidad frente a configuraciones heterogéneas. Este tipo de validación permitiría identificar posibles ajustes necesarios según las particularidades de cada entorno y contribuiría a fortalecer la utilidad práctica de la guía como herramienta de referencia para administradores y equipos de seguridad.

8. Declaratoria de uso de la IA.

Durante el desarrollo de este trabajo, se utilizó inteligencia artificial como herramienta de apoyo en tareas específicas de carácter operativo. En particular, se empleó para la organización alfabética del glosario de términos, la verificación y mejora de la redacción de determinados párrafos, la revisión de la consistencia de las fuentes bibliográficas y el estilo de las referencias conforme al formato requerido, así como para la búsqueda complementaria de artículos académicos relacionados con la temática de estudio. En todos los casos, la IA fue utilizada como un recurso de asistencia y no como generadora de contenido sustantivo; las decisiones metodológicas, el análisis de los resultados y la elaboración de las conclusiones fueron realizados íntegramente por el autor.

9. Referencias

Abo-alian, A., Youssef, M., & Badr, N. L. (2025). A data-driven approach to prioritize MITRE ATT&CK techniques for active directory adversary emulation [Un enfoque basado en datos para priorizar técnicas MITRE ATT&CK en la emulación de adversarios en Active Directory]. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-12948-x

Australian Government. (2025). *Detecting and Mitigating Active Directory Compromises [Detección y mitigación de compromisos en Active Directory]*. https://www.cisa.gov/resources-tools/resources/detecting-and-mitigating-active-directory-compromises

Bhandary, P., & Nicholas, C. (2025). A Behavioral Analysis of Ransomware in Active Directory: A Case Study of BlackMatter, Conti, LockBit, and Midnight [Análisis conductual del ransomware en Active Directory: un estudio de caso de BlackMatter, Conti, LockBit y Midnight]. *ISDFS 2025 - 13th International Symposium on Digital Forensics and Security*. https://doi.org/10.1109/ISDFS65363.2025.11012104

Chang, D., Li, L., Chang, Y., & Qiao, Z. (2021). Cloud computing storage backup and recovery strategy based on secure iot and spark [Estrategia de respaldo y recuperación de almacenamiento en computación en la nube basada en IoT seguro y Spark]. *Mobile Information Systems*, *2021*. https://doi.org/10.1155/2021/9505249

Derick Musundi Kesa. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations [Garantizando la resiliencia: integración de la planificación de recuperación ante desastres de TI y la continuidad del negocio para operaciones sostenibles]. *World Journal of Advanced Research and Reviews*, *18*(3), 970–992. https://doi.org/10.30574/wjarr.2023.18.3.1166

Dias, J. (2002). *A Guide to Microsoft Active Directory (AD) Design [Guía para el diseño de Microsoft Active Directory]*. http://www.llnl.gov/tid/Library.html

Echeverría, A., Cevallos, C., Ortiz-Garces, I., & Andrade, R. O. (2021). Cybersecurity model based on hardening for secure internet of things implementation [Modelo de ciberseguridad basado en hardening para la implementación segura del Internet de las Cosas]. *Applied Sciences (Switzerland)*, *11*(7). https://doi.org/10.3390/app11073260

Egho-Promise, E., Asante, G., Balisane, H., Abiodun, A. O., Salih, A., Aina, F., & Kure, H. (2025). THE EVOLUTION AND MITIGATION OF RANSOMWARE: TECHNIQUES, TACTICS AND RESPONSE STRATEGIES [La evolución y mitigación del ransomware: técnicas, tácticas y estrategias de respuesta]. *International Journal of Research -GRANTHAALAYAH*, *13*(9). https://doi.org/10.29121/granthaalayah.v13.i9.2025.6361

Goel, D., Ward, M., Neumann, A., Neumann, F., Nguyen, H., & Guo, M. (2025). Hardening Active Directory Graphs via Evolutionary Diversity Optimization-based Policies [Fortalecimiento de grafos de Active Directory mediante políticas basadas en optimización evolutiva de diversidad]. *ACM Transactions on Evolutionary Learning and Optimization*, *5*(3). https://doi.org/10.1145/3688401

Guo, M., Li, J., Neumann, A., Neumann, F., & Nguyen, H. (2022). *Practical Fixed-Parameter Algorithms for Defending Active Directory Style Attack Graphs [Algoritmos prácticos de parámetros fijos para defender grafos de ataque estilo Active Directory]*. https://github.com/BloodHoundAD/BloodHound

Guo, M., Ward, M., Neumann, A., Neumann, F., & Nguyen, H. (2023). *Scalable Edge Blocking Algorithms for Defending Active Directory Style Attack Graphs [Algoritmos escalables de bloqueo de aristas para defender grafos de ataque estilo Active Directory]*. www.aaai.org

Haddad, J., Pitropakis, N., Chrysoulas, C., Lemoudden, M., & Buchanan, W. J. (2023). Attacking Windows Hello for Business: Is It What We Were Promised? *Cryptography [Atacando Windows Hello for Business: ¿es lo que nos prometieron?]*, *7*(1). https://doi.org/10.3390/cryptography7010009

Haimed, I. B., Albahar, M., & Alzubaidi, A. (2023). Exploiting Misconfiguration Vulnerabilities in Microsoft's Azure Active Directory for Privilege Escalation Attacks [Explotación de vulnerabilidades de mala configuración en Azure Active Directory de Microsoft para ataques de escalada de privilegios]. *Future Internet*, *15*(7). https://doi.org/10.3390/fi15070226

Herranz-Oliveros, D., Marsa-Maestre, I., Gimenez-Guzman, J. M., Tejedor-Romero, M., & de la Hoz, E. (2024). Surgical immunization strategies against lateral movement in Active Directory environments. *Journal of Network and Computer Applications*, *222*. https://doi.org/10.1016/j.jnca.2023.103810

Herranz-Oliveros, D., Tejedor-Romero, M., Gimenez-Guzman, J. M., & Cruz-Piris, L. (2024). Unsupervised Learning for Lateral-Movement-Based Threat Mitigation in Active Directory Attack Graphs [Estrategias de inmunización quirúrgica contra el movimiento lateral en entornos de Active Directory]. *Electronics (Switzerland)*, *13*(19). https://doi.org/10.3390/electronics13193944

Hmiddouch, H., Villafranca, A., Castro, R., Dubetskyy, V., & Cano, M.-D. (n.d.). Enhancing Industrial Cybersecurity with Virtual Lab Simulations [Mejora de la ciberseguridad industrial mediante simulaciones de laboratorio virtual]. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 16, Number 5). Retrieved www.ijacsa.thesai.org

IBM. (2024, June 4). *¿Qué es el ransomware?* https://www.ibm.com/es-es/think/topics/ransomware

Kotlaba, L., Buchovecká, S., & Lórencz, R. (2020). Active Directory Kerberoasting Attack: Monitoring and Detection Techniques [Ataque Kerberoasting en Active Directory: técnicas de monitoreo y detección]. *International Conference on Information Systems Security and Privacy*, 432–439. https://doi.org/10.5220/0008955004320439

Kotlaba, L., Buchovecká, S., & Lórencz, R. (2021). Active Directory Kerberoasting Attack: Detection using Machine Learning Techniques [Ataque Kerberoasting en Active Directory: detección mediante técnicas de aprendizaje automático]. *International Conference on Information Systems Security and Privacy*, 376–383. https://doi.org/10.5220/0010202803760383

Krishnamoorthi, S., & Carleton, J. (2020). *Active Directory Holds the Keys to your Kingdom, but is it Secure? [Active Directory tiene las llaves de tu reino, ¿pero es seguro?]*

Lee, Y., Lee, J., Ryu, D., Park, H., & Shin, D. (2024). Clop Ransomware in Action: A Comprehensive Analysis of Its Multi-Stage Tactics [El ransomware Clop en acción: un análisis exhaustivo de sus tácticas de múltiples etapas]. *Electronics (Switzerland)*, *13*(18). https://doi.org/10.3390/electronics13183689

Liu, Q., Bao, K., & Hagenmeyer, V. (2025). COMMANDER: A robust cross-machine multi-phase Advanced Persistent Threat detector via provenance analytics [COMMANDER: un detector robusto de amenazas persistentes avanzadas multifase y entre máquinas mediante análisis de procedencia]. *Journal of Information Security and Applications*, *91*. https://doi.org/10.1016/j.jisa.2025.104057

Liu, Q., Bao, K., Hassan, W. U., & Hagenmeyer, V. (2025). HADES: Detecting and Investigating Active Directory Attacks via Whole Network Provenance Analytics [HADES: detección e investigación de ataques a Active Directory mediante análisis de procedencia de toda la red]. *IEEE Transactions on Dependable and Secure Computing*, 1–18. https://doi.org/10.1109/TDSC.2025.3611866

Lukas, O., & Garcia, S. (2023). Disrupting Active Directory Attacks with Deep Learning for Organic Honeyuser Placement [Interrupción de ataques a Active Directory con aprendizaje profundo para la colocación orgánica de usuarios señuelo]. *Communications in Computer and Information Science*, *1854 CCIS*, 111–133. https://doi.org/10.1007/978-3-031-37320-6_6

Matsuda, W., Fujimoto, M., Mitsunaga, T., & Watanabe, K. (2025). Detection of the Silver Ticket for Seamless Single Sign-On Focusing on a Ticket Lifetime [Ransomware: análisis del impacto en los servicios de dominio de Active Directory de Windows]. *Journal of Information Processing*, *33*, 156–167. https://doi.org/10.2197/ipsjjip.33.156

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the Impact on Windows Active Directory Domain Services [Ransomware: análisis del impacto en los servicios de dominio de Active Directory de Windows]. *Sensors*, *22*(3). https://doi.org/10.3390/s22030953

McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., Hao, Y., Ng, A., & Halgamuge, M. (2024). Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration. *ACM Computing Surveys*, *57*(1). https://doi.org/10.1145/3691340

Microsoft. (2016). *What's new in Windows Server 2016 [Novedades en Windows Server 2016]*. https://learn.microsoft.com/en-us/windows-server/identity/whats-new-active-directory-domain-services

Microsoft. (2025a, May 21). *Best practices for securing Active Directory [Mejores prácticas para asegurar Active Directory]*. Https://Learn.Microsoft.Com/En-Us/Windows-Server/Identity/Ad-Ds/Plan/Security-Best-Practices/Best-Practices-for-Securing-Active-Directory---.

Microsoft. (2025b, August 15). *Introducción a Active Directory Domain Services*. https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Mokhtar, B. I., Jurcut, A. D., ElSayed, M. S., & Azer, M. A. (2022). Active Directory Attacks—Steps, Types, and Signatures [Ataques a Active Directory: pasos, tipos y firmas]. *Electronics (Switzerland)*, *11*(16). https://doi.org/10.3390/electronics11162629

Motero, C. D., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., & Gomez, N. G. (2021). On Attacking Kerberos Authentication Protocol in Windows Active Directory Services: A Practical Survey [Sobre el ataque al protocolo de autenticación Kerberos en los servicios de Active Directory de Windows: un estudio práctico]. *IEEE Access*, *9*, 109289–109319. https://doi.org/10.1109/ACCESS.2021.3101446

Nebbione, G., & Calzarossa, M. C. (2023). A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments [Un marco metodológico para evaluaciones de seguridad asistidas por IA en entornos de Active Directory]. *IEEE Access*, *11*, 15119–15130. https://doi.org/10.1109/ACCESS.2023.3244490

Ngo, H. Q., Guo, M., & Nguyen, H. X. (2025). *Adaptive Wizard for Removing Cross-Tier Misconfigurations in Active Directory [Asistente adaptativo para eliminar configuraciones incorrectas entre niveles en Active Directory]*.

Nguyen, N. L., Falkner, N., & Nguyen, H. (2024). ADSynth: Synthesizing Realistic Active Directory Attack Graphs [ADSynth: síntesis de grafos de ataque realistas de Active Directory]. *Proceedings - 2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2024*, 66–74. https://doi.org/10.1109/DSN58291.2024.00021

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews [La declaración PRISMA 2020: una guía actualizada para la presentación de revisiones sistemáticas]. *BMJ*, *372*. https://doi.org/10.1136/bmj.n71

Parveen, S., Ahmad, S., & Khan, M. A. (n.d.). Integration of Identity Governance and Management Framework within Universities for Privileged Users [Integración de un marco de gobernanza y gestión de identidades en universidades para usuarios privilegiados]. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 12, Number 6). https://doi.org/DOI:10.14569/IJACSA.2021.0120664

Perin, L. (2025). Cloud Ransomware Defense and Data Recovery [Defensa contra ransomware en la nube y recuperación de datos]. *International Journal of Advances in Engineering and Management*, *7*(8), 877–894. https://doi.org/10.35629/5252-0708877894

Phipps, A., & Nurse, J. R. C. (2025). Inside Ransomware Groups: An Analysis of their Origins, Structures, and Dynamics [Dentro de los grupos de ransomware: un análisis de sus orígenes, estructuras y dinámicas]. *Computers & Security*, 104705. https://doi.org/10.1016/j.cose.2025.104705

Radah, T., Chaoui, H., & Saadi, C. (2023). Detecting Unconventional and Malicious Windows Authentication Activities Through Statistical Rarity Assessment [Detección de actividades de autenticación de Windows no convencionales y maliciosas mediante evaluación estadística de rareza]. *International Journal of Safety and Security Engineering*, *13*(5), 773–780. https://doi.org/10.18280/ijsse.130501

Senturk, Z., & Irmak, E. (2024). Persistence Techniques in Microsoft Active Directory: Detection and Mitigation Strategies [Técnicas de persistencia en Microsoft Active Directory: estrategias de detección y mitigación]. *12th International Symposium on Digital Forensics and Security, ISDFS 2024*. https://doi.org/10.1109/ISDFS60797.2024.10527234

Simon, J., Mohanakumar, A., & Kapileswar, N. (2025). Active Directory Open XDR Cyber Security Techniques to Detect Anomalies [Técnicas de ciberseguridad Open XDR para Active Directory orientadas a la detección de anomalías]. *Proceedings - 3rd International Conference on Self Sustainable Artificial Intelligence Systems, ICSSAS 2025*, 1860–1865. https://doi.org/10.1109/ICSSAS66150.2025.11081224

Velu, C. K., Madnick, S. E., & Van Alstyne, M. W. (2013). Centralizing data management with considerations of uncertainty and information-based flexibility [Centralización de la gestión de datos con consideraciones de incertidumbre y flexibilidad basada en información]. *Journal of Management Information Systems*, *30*(3), 179–212. https://doi.org/10.2753/MIS0742-1222300307

Yan, P., & Talaei Khoei, T. (2025). Securing the internet of things: A comprehensive review of ransomware attacks, detection, countermeasures, and future prospects [Seguridad en el Internet de las Cosas: una revisión exhaustiva de ataques de ransomware, detección, contramedidas y perspectivas futuras]. In *Franklin Open* (Vol. 11). Elsevier B.V. https://doi.org/10.1016/j.fraope.2025.100256

Zhang, Y., Ward, M., Guo, M., & Nguyen, H. (2023). A Scalable Double Oracle Algorithm for Hardening Large Active Directory Systems [Un algoritmo de doble oráculo escalable para el fortalecimiento de grandes sistemas de Active Directory]. *Proceedings of the ACM Conference on Computer and Communications Security*, 993–1003. https://doi.org/10.1145/3579856.3590343

10. Anexos

Anexo A

Glosario

AES (Advanced Encryption Standard): Algoritmo de cifrado moderno y seguro.

APT (Advanced Persistent Threat): Ataque avanzado, persistente y dirigido, generalmente realizado por grupos organizados.

AS-REP Roasting: Ataque contra cuentas que no requieren preautenticación Kerberos.

Betweenness centrality: Medida que indica cuántas rutas pasan por un nodo.

BloodHound / SharpHound: Herramientas para analizar relaciones en Active Directory y detectar rutas de ataque.

Block-worthy edges: Aristas críticas cuya eliminación reduce significativamente las rutas de ataque.

BUDGETFPT: Algoritmo que bloquea rutas de ataque en grafos AD bajo un presupuesto limitado de cambios.

Closeness centrality: Medida de qué tan cerca está un nodo de todos los demás.

Credential Guard: Mecanismo de seguridad de Windows que protege credenciales en memoria.

Critic Network: Red neuronal que evalúa la calidad de las decisiones en RL.

CVE (Common Vulnerabilities and Exposures): Identificador estándar de vulnerabilidades conocidas.

DAG: Grafo sin ciclos, útil para simplificar análisis de ataques.

DBSCAN: Algoritmo de clustering usado para identificar nodos críticos en grafos.

Decoy: Recurso falso diseñado para atraer y detectar atacantes.

Double Oracle: Algoritmo basado en teoría de juegos (Stackelberg) para optimizar decisiones entre atacante y defensor.

DP (Programación Dinámica): Método algorítmico que resuelve problemas complejos dividiéndolos en subproblemas.

DSRM (Directory Services Restore Mode): Modo de recuperación de Active Directory.

EDO (Evolutionary Diversity Optimization): Algoritmo evolutivo que busca soluciones diversas y óptimas.

EDR (Endpoint Detection and Response): Sistema que detecta y responde a amenazas en dispositivos finales.

Escalamiento de privilegios: Proceso mediante el cual un atacante obtiene mayores permisos.

GCN (Graph Convolutional Network): Modelo de redes neuronales aplicado a grafos para detectar patrones o riesgos.

gMSA (Group Managed Service Account): Cuenta administrada automáticamente para servicios en AD.

Golden Ticket: Ataque que permite acceso total al dominio al falsificar tickets Kerberos.

Grafo de ataque: Representación de posibles caminos que un atacante puede seguir dentro de un sistema.

Honeyuser: Cuenta señuelo utilizada para detectar accesos no autorizados.

IAM (Identity and Access Management): Gestión de identidades y accesos.

Identity Snowball Attack: Ataque donde un atacante va escalando privilegios progresivamente dentro de un sistema, aprovechando relaciones entre cuentas.

IGA (Identity Governance and Administration): Gestión de identidades enfocada en cumplimiento, auditoría y control de accesos.

ImproHound: Herramienta para analizar configuraciones de seguridad en AD con enfoque en tiering.

ITERLP: Heurística basada en programación lineal iterativa para reducir el éxito del atacante.

Kerberoasting: Ataque que obtiene tickets de servicio para luego descifrar contraseñas offline.

Kernelización: Reducción del tamaño del problema manteniendo sus propiedades esenciales para facilitar su solución.

KRBTGT: Cuenta especial en AD usada para firmar tickets Kerberos.

K-shell decomposition: Método para identificar la importancia estructural de nodos en una red.

LSASS: Proceso de Windows que gestiona la autenticación y credenciales de usuarios.

MITRE ATT&CK: Framework que clasifica tácticas y técnicas de ataque.

MIP (Mixed Integer Programming): Método matemático usado para optimizar decisiones como el bloqueo de rutas de ataque.

Modelo SI (Susceptible-Infected): Modelo epidemiológico usado para simular propagación de ataques.

Monte Carlo Simulation: Simulación probabilística para evaluar múltiples escenarios posibles.

Movimiento lateral: Cuando el atacante se mueve dentro de la red, de un equipo a otro, después de haber entrado.

MTHC (Mean Time to Half Compromise): Tiempo promedio para comprometer el 50% de la red.

Neo4j: Base de datos de grafos usada para analizar relaciones complejas.

NSP (Non-Splitting Path): Ruta en el grafo que no se divide y es relevante para análisis de ataques.

Overpass-the-Hash: Variante de Pass-the-Hash que obtiene tickets Kerberos usando hashes.

PAM (Privileged Access Management): Gestión de accesos privilegiados.

Pass-the-Hash: Ataque donde se usa el hash de una contraseña en lugar de la contraseña real para autenticarse.

Pass-the-Ticket: Uso indebido de tickets de autenticación de Kerberos para acceder a recursos.

Phishing: Técnica de engaño donde se roba información (credenciales) haciéndose pasar por una entidad confiable.

Random Forest: Algoritmo de machine learning basado en múltiples árboles de decisión.

RBAC (Role-Based Access Control): Control de acceso basado en roles.

RC4: Algoritmo de cifrado antiguo usado en Kerberos, considerado inseguro.

RL (Reinforcement Learning): Técnica de IA que aprende mediante prueba y error.

RL-EDO: Enfoque que combina aprendizaje por refuerzo con optimización evolutiva para defensa.

Ransomware: Malware que bloquea sistemas o datos y exige un pago para liberarlos.

Silver Ticket: Similar al Golden Ticket, pero con acceso limitado a servicios específicos.

Skeleton Key: Ataque que permite autenticarse con una contraseña maestra en AD.

SOAR (Security Orchestration, Automation and Response): Plataforma que automatiza respuestas ante incidentes de seguridad.

SPLITFPT: Técnica que divide nodos de bifurcación para optimizar el bloqueo de rutas de ataque.

Super-spreader: Nodo que facilita la propagación rápida de un ataque en la red.

TDCYCLE: Algoritmo basado en programación dinámica para bloquear rutas en grafos con estructura tipo árbol.

Tiering model: Modelo que separa niveles de privilegio en AD para reducir riesgos.

Weakest link: Elemento más vulnerable del sistema que puede ser explotado por un atacante.

XDR (Extended Detection and Response): Versión extendida que integra múltiples fuentes (red, nube, endpoints).

Anexo B

Enlace a la matriz de referencias

https://github.com/mateoguillen-26/Ciberataques-al-Active-Directory-Medidas-de-Mitigaci-n-Prevenci-n-y-Seguimiento.-