Universidad Cenfotec

Escuela de Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 2

Tema:

Creación de un plan de *hardening* y monitoreo continuo de Directorio Activo para mitigar técnicas de persistencia y escalamiento de privilegios

Elaborado por:

Angie Abarca Moreno

Mayo,2026

Dedicatoria

Dedico este trabajo, en primer lugar, a Dios, por darme la fortaleza, la sabiduría y la perseverancia necesarias para culminarlo. A pesar de los momentos difíciles, siempre estuvo ahí para mí, sosteniéndome y ayudándome a no caer.

A mi hija, mi enana preciosa, por tenerme paciencia mientras estudiaba, por saber esperar a que terminaran mis clases para poder compartir tiempo con ella y por ser esa niña tan especial que Dios me envió. Ella es mi motor para seguir adelante; este esfuerzo también es para brindarle un mejor futuro y para que vea en su mamá a una persona esforzada, perseverante y que no se rinde ante las circunstancias.

A mi mamá, por ser mi soporte y por estar presente en los momentos más difíciles.

Hay personas que llegan a nuestras vidas sin esperarlo, nos llenan de luz y alegría, y nos muestran un mundo diferente, en el que somos capaces de lograr aquello que nos proponemos. A esa persona especial que apareció en mi vida, que cada vez que podía me lanzaba una indirecta para que iniciara la maestría, que me escuchaba cuando lo llamaba para contarle sobre temas de ciberseguridad y veía cómo se desbordaba en mí la pasión por esta disciplina, también le dedico esta tesis. No sabes lo importante que eres en mi vida ni cuánto me has ayudado a crecer, tanto personal como profesionalmente.

(JCZM)

Agradecimiento

Agradezco profundamente a mi tutor, Miguel Pérez, por su orientación, compromiso, pasión y comprensión durante el desarrollo de este trabajo.

A mi familia, por su apoyo incondicional, por acompañarme en cada etapa de este proceso y por brindarme la fortaleza necesaria para continuar.

Finalmente, agradezco de manera especial a la persona que me impulsó a iniciar esta maestría, por estar siempre presente, por creer en mí y por motivarme a seguir creciendo personal y profesionalmente.

Tabla de Contenido

Tabla de Figuras

Índice de Tablas

Abstract

El Directorio Activo (AD) constituye el núcleo de la gestión de identidades en la mayoría de las infraestructuras corporativas, convirtiéndose en el objetivo principal de los adversarios que buscan establecer persistencia y escalar privilegios. A pesar de su importancia crítica, muchas organizaciones carecen de una estrategia integral que combine el *hardening* proactivo del entorno con mecanismos de detección continúa alineados al comportamiento del adversario. Este trabajo presenta la creación de un plan de *hardening* y monitoreo continuo para entornos de Directorio Activo *on-premise*, orientado a mitigar cinco técnicas de alto impacto catalogadas en las tácticas de Persistencia(TA0003) y Escalamiento de Privilegios (TA0004) del marco MITRE ATT&CK, La metodología adoptó un enfoque cualitativo, evaluativo y propositivo, fundamentado en la revisión sistemática de literatura, análisis documental de marcos de referencia como CIS Benchmark y MITRE ATT&CK, además de validación empírica mediante la herramienta Purple Knight en un entorno de producción real. La propuesta se estructura en tres componentes: diagnóstico de seguridad, plan de *hardening* con 25 controles técnicos, y 34 reglas de detección personalizadas en Wazuh con telemetría extendida mediante Sysmon. La implementación de los controles de menor impacto operativo elevó la postura de seguridad del entorno de 68% a 82%, resolviendo cinco de los indicadores críticos. La validación del componente de monitoreo continuo, mediante las ilustraciones del dashbord de Wazuh en un entorno productivo, afirman que las reglas diseñadas generan alertas activas clasificadas por táctica de MITRE ATT&CK, y las métricas de autenticación con estadísticas de 2.682 inicios de sesión exitosos y 470 fallidos en 24 horas son capturas y correlacionadas de forma continua. Los resultados confirman que la integración congruente de *hardening* y monitoreo, donde cada componente retroalimenta al otro, representa un enforque más efectivo que abordar ambas disciplinas de forma independiente.

Palabras Clave: Directorio Activo, *hardening*, monitoreo continuo, MITRE ATT&CK, persistencia, escalamiento de privilegios, Wazuh, CIS Benchmark, Purple Knight, ciberseguridad.

Capítulo 1. Introducción

1.1 Generalidades

En la actualidad, es necesario comprender y combatir las amenazas cibernéticas. Por ello, existen marcos, como MITRE ATT&CK, que ofrecen una estandarización de las tácticas y técnicas utilizadas por los adversarios, mientras que CIS Benchmark ofrece una serie de guías de *hardening*[1] que se pueden implementar en los entornos Windows. Asimismo, el personal de ciberseguridad publica de forma constante análisis detallados, herramientas y recomendaciones de *hardening*.

Este trabajo de investigación tiene como propósito crear un plan integral de *hardening* y monitoreo con el fin de mitigar técnicas de persistencia y escalamiento de privilegios en el Directorio Activo (AD). Esta investigación surge de la inquietud del autor por la escasez de metodologías relacionadas con el tema y se construye sobre una base de información disponible, con un valor agregado de su integración, validación práctica y adaptación en un plan aplicable.

1.2 Antecedentes del Problema

En los últimos años, el panorama de amenazas ha evolucionado hacia campañas sofisticadas de *ransomware* y robo de datos, donde los entornos corporativos son el objetivo principal. Dentro de estos entornos, el Directorio Activo se establece como el vector de ataque crítico por excelencia, dado su función central en la gestión de identidades y el control de accesos. Si el Directorio Activo se logra ver comprometido permite a los atacantes lograr sus objetivos finales: la persistencia encubierta en la red y el escalamiento de privilegios para moverse lateralmente.

Las estadísticas reflejan esta tendencia. El informe de Inteligencia de CrowdStrike (2024) documentó 291 víctimas de filtración de datos y *ransomware* en Latino América, lo que representa un aumento del 15% interanual. Si bien esta cifra es el 5% del total global (5.276 incidentes), evidencia una clara tendencia hacia el aumento de estos ataques. Este escenario se atribuye principalmente a la debilidad de las configuraciones por defecto del Directorio Activo y la falta de controles de *hardening* proactivo, lo que amplía la superficie de ataque.

Por otro lado, investigaciones como la de Grillenmeire (2023) demuestran que una configuración robusta del Directorio Activo impacta directamente en la dificultad que encuentran los atacantes durante las fases de reconocimiento, movimiento lateral y escalamiento de privilegios, técnicas catalogadas y detalladas en la matriz MITRE ATT&CK. Sin embargo, solamente la implementación de *hardening* es insuficiente sin un marco de monitoreo continuo que detecte y responda a las actividades anómalas que intentan eludir estos controles.

---

[1] Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas. (Grupo Smartekh, 2025)

Por lo tanto, se evidencia una necesidad crítica en las organizaciones: la falta de una estrategia integral y estandarizada que combine un plan de *hardening* para mitigar las configuraciones vulnerables desde el origen, con un plan de monitoreo continuo especifico diseñado para detectar las TTPs (tácticas, técnicas y procedimientos), que indica MITRE ATT&CK, relacionadas con la persistencia y el privilegio en el Directorio Activo. Esta falencia deja a los entornos corporativos expuestos a brechas de seguridad prolongadas y de alto impacto.

1.3 Definición y Descripción del Problema

El Directorio Activo constituye un componente crítico y, por ende, un objetivo de alto valor para los ciber atacantes. Al centralizar la información de identidades, accesos y recursos de una organización, su compromiso concede a un adversario el control efectivo sobre la infraestructura de TI, lo que inevitablemente conduce a pérdidas económicas sustanciales, filtración de datos sensibles y un severo daño reputacional.

Este trabajo aborda el problema específico de la exposición de los entornos del Directorio Activo a técnicas de persistencia encubierta y escalamiento de privilegios, tal como se documenta en el marco MITRE ATT&CK. La raíz del problema se encuentra en una serie de factores:

1. Configuraciones débiles o permisivas.
2. La ausencia de un monitoreo efectivo y continuo
3. El desconocimiento o subestimación.

Como indican Al-Sada et al. (2024), la correcta aplicación del marco MITRE ATT&CK, centrada en el modelado del comportamiento adversario, la detección automatizada de amenazas y la mejora continua del marco de defensa es fundamental para contrarrestar estas amenazas. No obstante, existe una gran brecha entre la existencia de este marco y la implementación práctica de un plan integral que conjugue de manera estandarizada el *hardening* proactivo del entorno con las capacidades de detección y respuesta necesarias para mitigar estas técnicas de forma continua.

1.4 Justificación

El Directorio Activo constituye el núcleo principal de la mayoría de las infraestructuras empresariales modernas, siendo responsable de la autenticación, autorización y gestión de identidades dentro de los entornos corporativos. En efecto posee las “llaves del reino”, ya que controla el acceso a los recursos críticos de toda la organización. Esta centralidad lo convierte en un blanco prioritario para actores maliciosos que buscan persistencia y elevar privilegios para penetrar en una red comprometida.

Errores de configuración, cuentas con privilegios excesivos y vulnerabilidades sin parchear no solo facilitan el compromiso de toda la red, sino que también generan consecuencias severas a nivel financiero, operativo y reputacional. A pesar de su importancia crítica, muchas organizaciones carecen de un plan estructurado y actualizado para el *hardening* y monitoreo continuo del servicio.

Este trabajo es importante porque propone la creación de un plan de *hardening* y monitoreo continuo del Directorio Activo, fundamentado en técnicas de ataques reales, como las descritas en MITRE ATT&CK. Aportando una visión práctica, actualizada y aplicable a entornos corporativos reales, cerrando la brecha entre configuraciones inseguras y la defensa activa. Su relevancia radica en el creciente número de ataques dirigidos a controladores de dominio, la complejidad de la administración del Directorio Activo y la necesidad de adoptar marcos de protección que favorezcan un enfoque proactivo en lugar de reactivo frente a las amenazas emergentes.

1.5 Viabilidad

1.5.1 Punto de Vista Técnico.

Para llevar a cabo este proyecto se cuenta con las competencias, el conocimiento fundamental y la experiencia práctica necesarios para el desarrollo exitoso. Se posee conocimientos exhaustivos de la arquitectura interna del Directorio Activo, que abarca no solo desde la administración básica de usuarios y equipos, sino también la comprensión de su estructura física y lógica, como dominios, bosques, sitios y controladores de dominio, Asimismo, se tiene dominio técnico de los protocolos de autenticación Kerberos y NTLMv2 y experiencia en la administración de grupo de políticas, incluyendo creación, vinculación y priorización para aplicar las configuraciones de seguridad.

Además, se ha adquirido experiencia directa en procesos de *hardening* de servidores y en la configuración de controles de seguridad. Por último, se cuenta con la capacidad para monitorear, detectar y analizar logs de seguridad, lo que resulta esencial para la fase de diseño del plan de monitoreo continuo.

1.5.2 Punto de Vista Operativo.

La ejecución de este proyecto se fundamenta en metodologías de análisis y diseño que no invasivas y se llevarán a cabo en un entorno de laboratorio controlado y aislado.

Se tiene planeado llevar a cabo una investigación exhaustiva de las técnicas de persistencia y escalamiento de privilegios incluidas en MITRE ATT&CK, así como las mejores prácticas de *hardening* y monitoreo para el Directorio Activo. Una vez identificadas las medidas más efectivas, se diseñará el plan, y por medio de una simulación de adversarios, en un entorno de laboratorio, se procederá a validar su eficacia.

Posteriormente se realizará la creación del plan y monitoreo realizado con base en los resultados de las pruebas controladas.

Por lo tanto, esta investigación no altera de ninguna manera la infraestructura de ninguna compañía ni consume recursos de productivos.

1.5.3 Punto de Vista Económico.

Los costos de inversión estimados para el desarrollo de este trabajo provienen del capital intelectual, el tiempo y el esfuerzo del investigador, los cuales se aportan como parte del requisito académico. Por lo tanto, el costo es asumido en su totalidad por el investigador. Es importante aclarar que las herramientas utilizadas en el desarrollo de este trabajo son completamente de código abierto (*open source*), por lo que no implican un costo económico**.**

1.6 Objetivos

Se utiliza la taxonomía de Bloom de 1956 debido a su amplia documentación y aceptación en el ámbito educativo. Su estructura jerárquica facilita la definición de los objetivos desde los niveles más generales a más específicos por su amplia utilización.

1.6.1 Objetivo General.

- Crear un plan de *hardening* y monitoreo continuo de Directorio Activo para mitigar técnicas de persistencia y escalamiento de privilegios.

1.6.2 Objetivos Específicos.

- Identificar técnicas de ataques comunes asociadas al Directorio Activo según MITTRE ATT&CK para reconocer amenazas relevantes.
- Comprender el estado de seguridad actual del Directorio Activo mediante la herramienta Purple Knight para interpretar hallazgos y debilidades en la configuración.
- Elaborar un plan de *hardening* basado en CIS Benchmark para fortalecer la seguridad del Directorio Activo.
- Clasificar reglas por medio de Wazuh para detectar comportamientos anómalos que puedan comprometer la integridad del Directorio Activo.

1.7 Alcances y Limitaciones

1.7.1 Alcances.

El proyecto de investigación se centra en la creación de un plan de *hardening* y monitoreo continuo para entornos de Directorio Activo *on-premise*[2]. El plan está dirigido a mitigar un conjunto seleccionado de técnicas de las tácticas de persistencia (TA0003) y

escalamiento de privilegios (TA0004) del marco MITRE ATT&CK, clasificadas por su alta prevalencia e impacto en entornos corporativos.

1.7.2 Limitaciones.

Con el fin de asegurar la profundidad y viabilidad del estudio, el proyecto se limita de la siguiente manera:

- **Técnicas MITRE ATT&CK:** El análisis se centra en cinco técnicas consideradas de alto impacto y con controles de mitigación correctamente definidos. Las técnicas son las siguientes:
  - **T1078.002:** Valid Accounts – Domain Accounts (se utiliza como técnica sombrilla donde se cubren aspectos de T1098 – Account Manipulation).
  - **T1484.002:** Domain Policy Modification.
  - **T1134.002:** Token Impersonation/Theft.
  - **T1547.002:** Boot or Logon Autostart Execution.
  - **T1574.001:** Hijack Execution Flow – DLL Side-Loading.
- **Entorno:** El estudio se limita a entornos de Directorio Activo *on-premise*. Quedan por fuera del análisis los entornos híbridos (Azure AD Connect) o nativo de la nube (Azure Entra ID), ya que estos presentan vectores de ataques y controles de seguridad distintos.
- **Herramientas:** Se despliega una arquitectura de monitoreo unificado para la detección de amenazas, integrando la telemetría del sistema. Complementariamente, se ejecutan auditorías de seguridad especializadas sobre el Directorio Activo, reportando su nivel de exposición, salud general y las técnicas de ataque potenciales catalogadas por marcos de base de conocimientos de acceso universal y actualizados.

1.8 Marco de Referencia Organizacional y Socioeconómico

El proyecto se enmarca en el contexto de un panorama de ciber amenazas en constante evolución, donde organizaciones de todos los tamaños y sectores se enfrentan a riesgos crecientes contra sus infraestructuras. Estas organizaciones, en su afán de evolucionar digitalmente y adoptar distintos modelos de trabajo híbridos, dependen de manera esencial de servicios de identidad del Directorio Activo, convirtiéndose en un objetivo importante para actores maliciosos. Este trabajo aborda el desafío de proteger el entorno del Directorio Activo de manera proactiva, dejando de lado la cultura reactiva, proporcionando un plan accionable que ayude a mitigar riesgos operativos, financieros y los más relevantes: reputacionales.

1.8.1 Historia.

En sus inicios, la seguridad se basaba en *firewalls* y antivirus, conforme ha avanzado la tecnología, su evolución ha ido creciendo, pasando de un enfoque perimetral y una cultura reactiva a uno centrado en la gestión de identidades y una cultura proactiva.

En el año 2000, con el lanzamiento de Windows Server 2000, se empezó a dar una adopción masiva del Directorio Activo como el núcleo para la gestión de identidades en entornos corporativos, siendo una característica llamativa que los atacantes cambiaron la mayoría de sus objetivos hacia este servicio, aprovechando su estructura para robar credenciales, vulnerar servicios que se ejecutan en este entorno, con el fin de propagar *ransomware* directamente a la red. Incidentes recientes de alto nivel incluyen el Barts Health NHS Trust de Londres, que atienden a más de 2 millones de pacientes, que fue víctima de un ataque de BlackCat/ALPHV, así como Dish Network informó de un ataque de *ransomware* que logró comprometer el Directorio Activo y luego su infraestructura en WMware, afectando a millones de abonados. Esto demuestra que el Directorio Activo está siendo un punto que permite a los atacantes moverse lateralmente y escalar privilegios hasta tomar el control total de la infraestructura.

Con la aparición de marcos de conocimiento como MITRE ATT&CK en el 2013, se llegó a marcar un antes y un después, al proporcionar un lenguaje común y una taxonomía detallada de las técnicas adversarias. Este proyecto se basa en esta evolución, traduciendo el conocimiento del marco en un plan concreto de *hardening* y monitoreo para las técnicas más críticas.

1.8.2 Tipo de Negocio y Mercado Meta.

Este proyecto se dirige principalmente a organizaciones que gestionan sus identidades basadas en Directorio Activo, abarcando tres niveles:

- Instituciones públicas
- Empresas privadas
- Pymes.

El mercado meta incluye empresas privadas de banca y finanzas, Pymes, y servicios gubernamentales, todos ellos altamente dependientes de la integridad, confidencialidad y disponibilidad de su información, la cual depende de sus sistemas de autenticación. El valor socioeconómico de esta investigación radica en fortalecer la Ciber resiliencia organizacional, además de contribuir a la estabilidad socioeconómica de las organizaciones al evitar impactos que pueden traducirse en pérdidas millonarias, afectación a ciudadanos y la continuidad operacional de servicios esenciales.

1.9 Revisión de literatura

1.9.1 Estado de la cuestión

La seguridad del Directorio Activo ha sido objeto de múltiples estudios, especialmente en lo relacionado con ataques dirigidos que explotan debilidades de configuración y monitoreo. Diversas investigaciones internacionales han abordado la necesidad de reforzar este componente, y existen esfuerzos por catalogar las técnicas más utilizadas por atacantes mediante marcos como MITRE ATT&CK.

A pesar de esto, se observa una carencia de propuestas prácticas que integren *hardening* con reglas de detección específicas para las técnicas de persistencia (TA0003) y escalamiento de privilegios (TA0004). En particular, son escasos los estudios aplicados al contexto de organizaciones en América Latina o entornos gubernamentales, donde estas vulnerabilidades pueden tener un impacto crítico.

1.9.2 Revisión sistemática

La revisión sistemática se planifica con el propósito de identificar, evaluar y sintetizar las estrategias defensivas, tanto de *hardening* como de monitoreo continuo que han demostrado efectividad para mitigar ataques mediante las técnicas de MITRE ATT&CK en entornos de Directorio Activo *on-premise*. Esta etapa contempla la definición de los objetivos, preguntas de investigación, criterios de inclusión y exclusión, fuentes de información y métodos de extracción y análisis de datos.

1.9.3 Planificación de la revisión

Se planifica realizar una revisión sistemática de literatura enfocada en las siguientes líneas:

1.9.3.1 Formulación de la pregunta

¿Qué controles de *hardening* y mecanismos de monitorio continuo han sido propuestos o aplicados para mitigar, de manera efectiva, las técnicas de persistencia y escalamiento de privilegios, expuestas en MITRE ATT&CK, en entornos de Directorio Activo *on-premise*?

1.9.3.1.1 Foco de la pregunta

Se centra en el análisis de estudios o documentos técnicos que describen configuraciones seguras (*hardening*) y mecanismos de monitoreo asociados a AD, que hayan sido diseñados o evaluados en relación con MITRE ATT&CK.

1.9.3.1.2 Amplitud y calidad de la pregunta

Para delimitar la revisión, se establecen los siguientes componentes:

- Problema: Las organizaciones carecen de controles específicos para prevenir técnicas de persistencia y escalamiento de privilegios en AD.
- Pregunta: ¿Qué estrategias efectivas se han documentado para prevenir y detectar estas técnicas?
- Palabras clave: Active Directory, hardening, monitoring, persistence, privilege escalation, MITRE ATT&CK, TTPs.
- Intervención: Análisis de controles y herramientas aplicables.
- Control: Estudios que utilicen como base MITRE ATT&CK.
- Medida de salida: Nivel de efectividad, cobertura y aplicabilidad de las soluciones.
- Población: Entornos organizacionales con implementación del Directorio Activo.
- Aplicación: Equipos de ciberseguridad y administradores de infraestructura.

1.9.3.2 Selección de fuentes

1.9.3.2.1 Criterios de selección

Se priorizan fuentes académicas y técnicas reconocidas, tales como:

- Whitepapers de Microsoft, SpecterOps, RedCanary, Semperis.
- Artículos de conferencias como BlackHat, SANS, DefCon.
- Repositorios como IEEE, ACM, EBSCO y MITRE.org.

1.9.3.2.2 Lenguaje

Se utilizan textos en inglés y español.

1.9.3.2.3 Cadena de búsqueda

- “Active Directory” AND “MITRE ATT&CK”
- “persistence” OR “privilege escalation”
- “hardening” OR “monitoring” OR “detection”

1.9.3.3 Criterios de inclusión y exclusión

Inclusión:

- Estudios que incluyan Directorio Activo *on-premise* y tácticas TA0003 y TA0004.
- Propuestas o evaluaciones de controles técnicos.

- Casos prácticos o herramientas de monitoreo asociadas.

Exclusión:

- Investigaciones sin relación a Directorio Activo o que aborden exclusivamente Azure Directorio Activo.
- Estudios teóricos sin propuestas aplicables, que se centren solamente en concienciación o phishing.

1.9.4 Ejecución de la revisión

Durante esta etapa se ejecutó la búsqueda en las fuentes seleccionadas. El proceso incluyó:

1. Aplicación de cadenas de búsqueda.
2. Revisión del título, resumen y palabras clave de cada resultado.
3. Aplicación de los criterios de inclusión y exclusión.
4. Lectura detallada de los textos completos seleccionados.
5. Extracción estructurada de información relevante: tácticas TA0003 y TA0004, controles aplicados, métricas, herramientas utilizadas.

1.9.5 Evaluación de la ejecución

La revisión fue validada mediante:

- Registro de cada fuente y artículo procesado.
- Documentación de las decisiones de inclusión/exclusión.
- Análisis de saturación: se observó que, tras revisar 40 documentos, ya no se obtenía nueva información significativa (saturación teórica).
- Clasificación de la calidad de los estudios con base en el tipo de publicación, citaciones y validación técnica.

1.9.6 Análisis de resultados

Se identificaron patrones clave entre los estudios seleccionados:

- Las técnicas más documentadas y de mayor impacto incluyen T1558.003 (Golden Ticket), T1098 (Account Manipulation), T1484.002 (Domain Policy Modification) y T1003.006 (DCSync). No obstante, se observó que para otras técnicas de alta criticidad no hay tanta cobertura.
- Las configuraciones a nivel de *hardening* en el Directorio Activo más efectivas se relacionan con el menor privilegio en la delegación de permisos, limpieza periódica de usuarios privilegiados, protección de cuentas de servicio y des habilitación de protocolos obsoletos.
- Se logró identificar una dependencia de las herramientas nativas de Windows como el visor de eventos potenciadas por Sysmon.

- Se identifica una desconexión entre el *hardening* y el monitoreo, muchos estudios solo abordan un tema o el otro, pero no los dos en conjunto, donde la configuración de *hardening* optimice las reglas de detección y viceversa. Este hallazgo valida la necesidad y originalidad de la presente investigación.

Capítulo 2. Marco Teórico o Conceptual

Con el fin de identificar los conceptos más recurrentes en los artículos revisados para el estado de la cuestión, se generó la siguiente nube de palabras que representa gráficamente los términos de mayor relevancia.

Ilustración 1 Nube de palabras Fuente: Elaboración propia. Elaborado usando el sitio https://www.nubedepalabras.es

A continuación, se presentan las definiciones de los conceptos más mencionados y relevantes para la presente investigación. Es importante destacar que, con el propósito de ofrecer un mejor contexto sobre el tema abordado, los conceptos se organizan desde un enfoque general hacia aspectos más específicos, necesarios para comprender los distintos elementos relacionados con Directorio Activo y MITRE ATT&CK.

2.1 Seguridad de la Información

Según Microsoft, la seguridad de la información también conocida como “Infosec” se trata de un conjunto de procedimientos y herramientas de seguridad diseñados para proteger de manera integral la información confidencial de la empresa contra usos indebidos, accesos no autorizados, interrupciones del servicio y destrucción de datos.

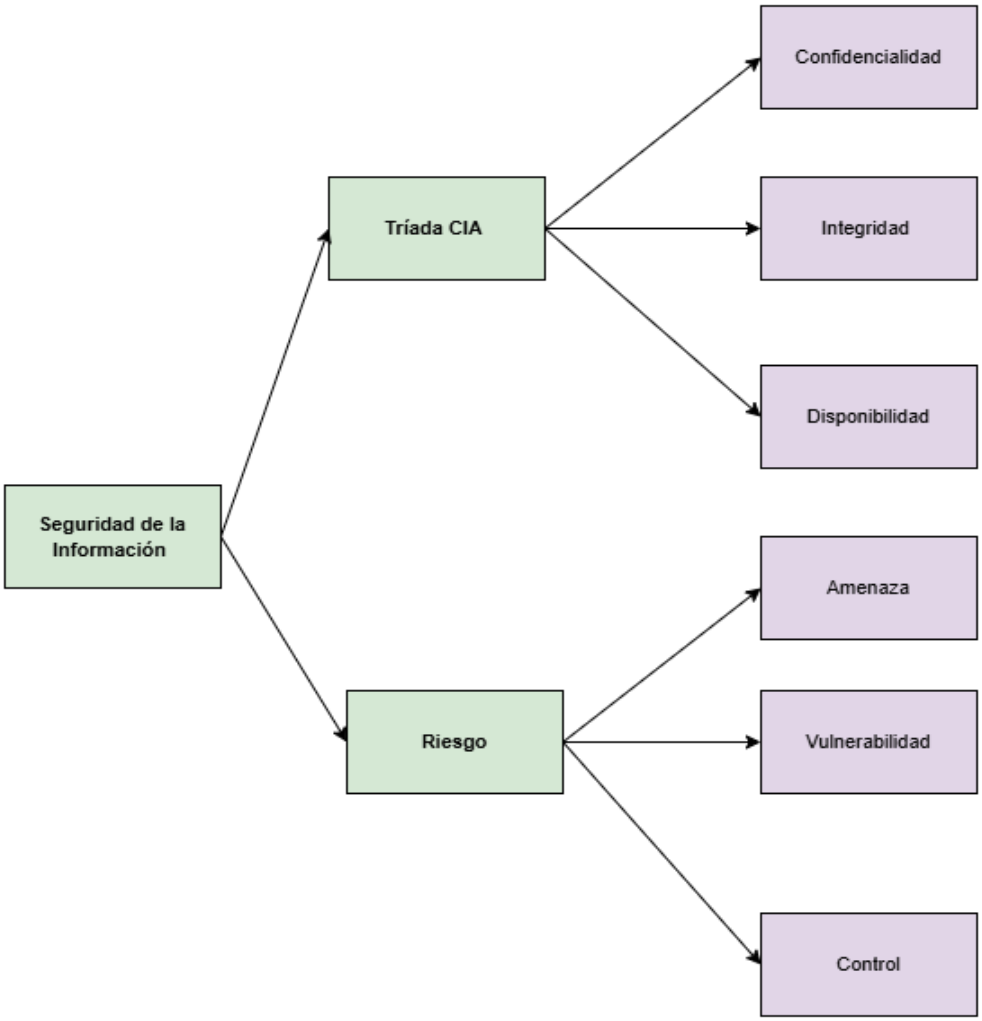

Ilustración 2 Diagrama de Seguridad de la Información Fuente: Elaboración Propia utilizando el sitio web https://app.diagrams.net/

2.1.1 Tríada CIA

La tríada se conoce como los tres pilares solidos que crean la base sólida de la seguridad de la información. LA Tríada CIA ofrece estos tres conceptos como bases al momento de su implementación (Microsoft,2026)

2.1.1.1 Confidencialidad

Significa garantizar que las partes no puedan acceder a datos a los que no están autorizados. Este principio define un espectro de usuarios que va desde empleados internos con acceso privilegiado a gran parte de la información empresarial, hasta personas

autorizadas únicamente para consultar datos de carácter público. Cuando una persona no autorizada obtiene acceso a datos protegidos, como contraseñas se produce una violación de la confidencialidad (IBM,2026).

2.1.1.2 Integridad

Implica que toda la información contenida en las bases de datos de la empresa sea completa, precisa y confiable. Los procesos de integridad tienen como objetivo evitar la manipulación de datos mediante alteraciones o eliminaciones no autorizadas.

2.1.1.3 Disponibilidad

Equivale a asegurar que los usuarios puedan acceder a la información cuando lo necesiten. La disponibilidad incluye aspectos como garantizar la robustez del hardware y software con el fin de evitar interrupciones en los servicios y sitios web de la empresa.

2.1.2 Riesgo

La ISO 27005:2012 define el riesgo de la seguridad de la información como el potencial con el que las amenazas aprovecharán las vulnerabilidades de un activo o de un grupo activos de información, y de este modo causar daño a la organización.

2.1.2.1 Amenaza

Se define como la causa potencial de un incidente no deseado, que puede resultar en un daño para un sistema u organización. A nivel de Directorio Activo se busca comprometer la identidad y accesos a la red empresarial.

2.1.2.2 Vulnerabilidad

Es considerada como la debilidad de un activo o control que puede ser explotada por una o varias amenazas. En el ámbito del Directorio Activo pueden estar incluidas en configuraciones inseguras de grupo de políticas, permisos excesivos o contraseñas débiles a nivel de cuentas de servicio.

2.1.2.3 Control

Los controles para la seguridad de la información incluyen cualquier proceso, política, procedimiento, directriz, práctica o estructura organizacional, que pueden ser de naturaleza administrativa, técnica, de gestión o legal, que modifican los riesgos. (ISO 27005:2012)

2.2 Directorio Activo

El Directorio Activo es un servicio de directorio propietario que permite a los administradores controlar los permisos de los recursos de red, inicialmente estuvo disponible en el sistema operativo Windows Server 2000, con el paso de los años se ha expandido hasta convertirse en una estructura completa para la administración centralizada de diversos elementos de red, como usuarios, equipos, grupos y diferentes recursos de la organización. (Simister, A, 2025).

El Directorio Activo funciona como la base centralizada para la gestión de identidades, autenticación, autorización y administración de recursos de red en un dominio, incluyendo usuarios, equipos, grupos y políticas entre otros. Además, proporciona una manera de que los usuarios autorizados de la misma red accedan a esta información. (Microsoft,2025).

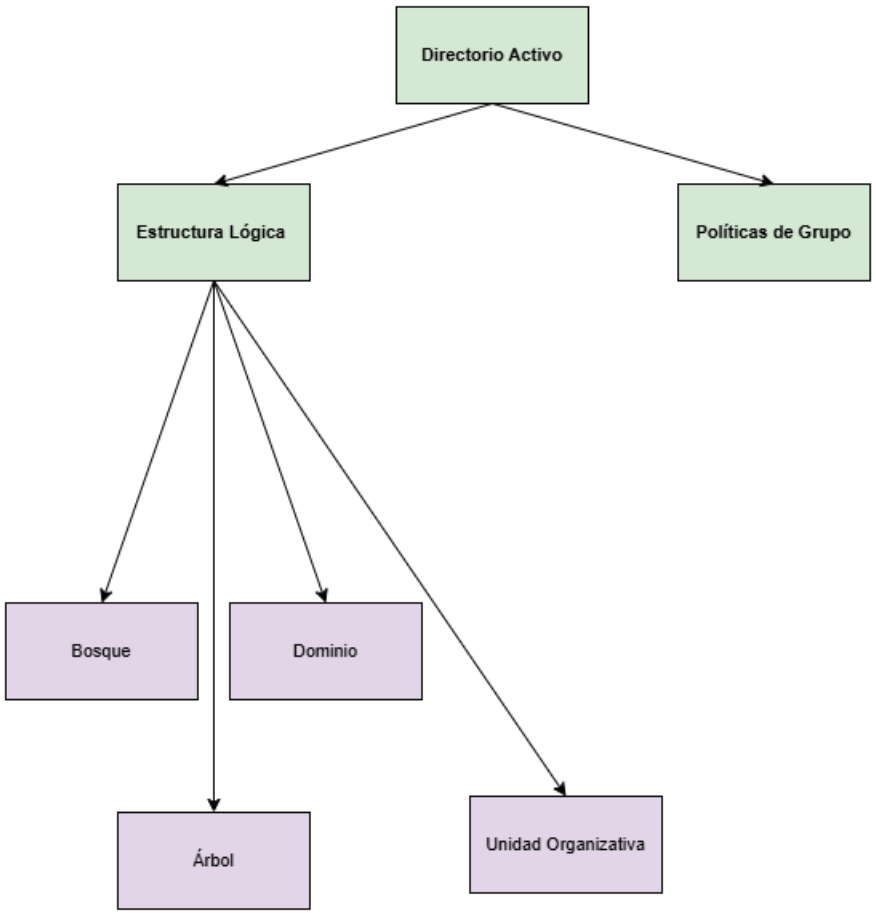

Ilustración 3 Diagrama de Directorio Activo Fuente: Elaboración Propia utilizando el sitio web https://app.diagrams.net/

2.2.1 Estructura del Directorio Activo

Su estructura lógica jerárquica incluye dominios junto con árboles, bosques, unidades organizativas, que definen la función organizativa independiente.

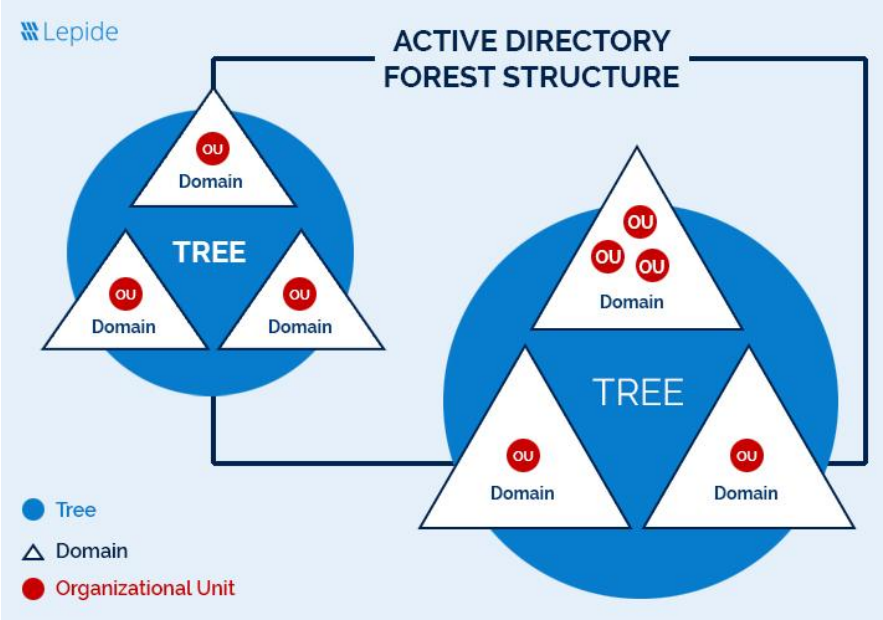

Ilustración 4 Estructura del Directorio Activo.

Fuente Simister, A., & Simister, A. (2025, 3 abril). What is Active Directory? A Comprehensive Guide | Lepide Blog. Lepide Blog: A Guide To IT Security, Compliance And IT Operations. https://www.lepide.com/blog/what-is-_-active-directory/

2.2.1.1 Bosque

Son elementos de nivel más alto a nivel de estructura lógica del Directorio Activo que conectan uno o más árboles, de acuerdo con los elementos compartidos, ellos incluyen el esquema del Directorio Activo, la definición de catálogos globales y límites de seguridad. La comunicación entre los bosques se realiza mediante relaciones de confianza, lo que permite una independencia administrativa y protección de datos. (Simister, A, 2025).

2.2.1.2 Árbol

Un árbol se compone de uno o varios dominios que comparten esquema y configuración común, formando un espacio de nombres. (Microsoft,2025). Por ejemplo, si el dominio raíz es “seguridad.com”, un dominio hijo dentro del mismo árbol sería “consultoría.seguridad.com”, se establecen relaciones de confianza automáticas entre todos los dominios, basadas en protocolos de confianza. Los dominios del árbol pueden buscar en todos los dominios gracias al catálogo global que implementa consultas de dominio universales. (Simister, A, 2025).

2.2.1.3 Dominio

Es la unidad fundamental de la estructura lógica y el contenedor de seguridad del Directorio Activo. Funciona como una partición de seguridad activa que permite a los administradores gestionar los procedimientos de autenticación, autorización y replicación de bases de datos de forma centralizada. Además, contiene base de datos compartidas que todos sus controladores replican automáticamente y de forma eficiente para mantener la sincronización. (Simister, A, 2025).

2.2.1.4 Unidad Organizativa (OU)

Funcionan como contenedores que permiten agrupar lógicamente objetos como cuentas de usuario, de servicio o cuentas de equipo y grupos según agrupaciones lógicas. Por medio de esta agrupación los administradores pueden otorgar permisos a dominios específicos mediante OU y aplicar políticas de grupo a objetos seleccionados sin necesidad de afectar todo el dominio. (Simister, A, 2025).

2.2.1.5 Políticas de grupo (GPO)

Son reglas de configuración que se aplican a objetos del dominio y unidad organizativa (OU) con el fin de implementar medidas de seguridad, software y restricciones de control de usuarios. Las GPO se procesan jerárquicamente de acuerdo con el siguiente orden: sitio, dominio y luego unidad organizativa. (Microsoft,2025).

2.3 *Hardening*

El término *hardening*, que en español se puede traducir como bastionado o endurecimiento, su origen conceptual se encuentra en el ámbito militar. Según la Real Academia Española (RAE), un bastión hace referencia a una fortificación diseñada para defenderse de los ataques, estableciendo un lugar seguro desde donde resistir al enemigo. Esta descripción nos proporciona una analogía sobre por qué el bastionado es importante en el ámbito de ciberseguridad. En el pasado, las civilizaciones construían murallas, torres o puestos de vigilancia para protegerse de los invasores. De manera equivalente, en el ámbito digital, el *hadening* comprende un conjunto de acciones y procedimientos para fortalecer la seguridad de un sistema o una red empresarial. En términos prácticos, el endurecimiento de sistemas implica la reducción de la superficie de ataque mediante la eliminación de servicios innecesarios, aplicación de configuraciones seguras y el establecimiento de políticas restrictivas de acceso y controles técnicos que minimicen vulnerabilidades que pueden ser altamente explotadas convirtiéndose en una amenaza cibernética. (Lopez, 2024).

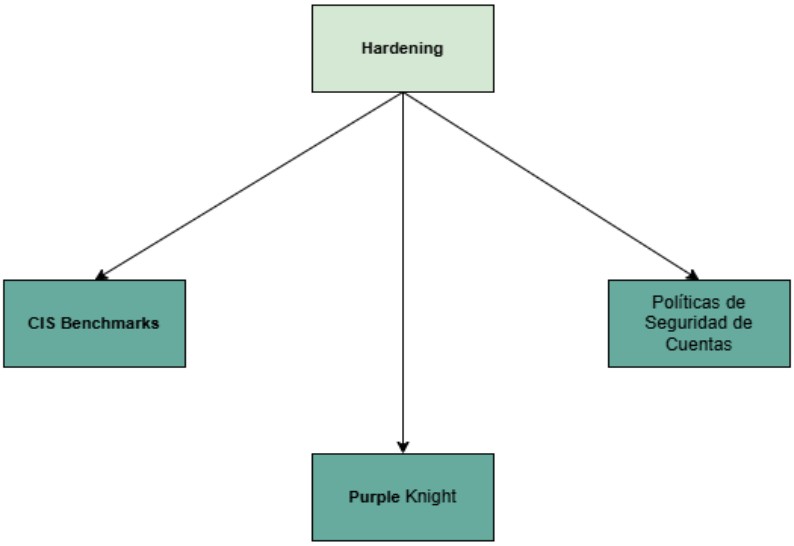

Ilustración 5 Diagrama de *Hardening* Fuente: Elaboración Propia utilizando el sitio web https://app.diagrams.net/

2.3.1 CIS Benchmarks

Son un conjunto de directrices técnicas orientadas a establecer configuraciones seguras en diversos componentes tecnológicos dentro de una infraestructura tecnológica empresarial. Estas guías representas un elemento fundamental en la estrategia defensiva como amenazas cibernéticas. (CIS,2022)

2.3.2 Purple Knight

Es una herramienta que realiza consultas al entorno del Directorio Activo de una empresa y ejecuta un conjunto exhaustivo de pruebas orientada a identificar los vectores de ataque más comunes y efectivos. Su objetivo principal es detectar riesgos y vulnerabilidades presentes en el Directorio Activo. Incluyes mapeo de indicadores de exposición según el marco de referencia MITRE ATT&CK, al correlacionar los hallazgos con este *framework*, facilita la comprensión del contexto de riesgos y prioriza las acciones remediales en funciones de la criticidad de cada vulnerabilidad detectada. (Semperis,2024)

2.3.3 Políticas de Seguridad de Cuentas

Establecen métricas que permiten identificar y evaluar vulnerabilidades presentes en cuentas de usuarios tanto individuales como integradas dentro del ecosistema del Directorio Activo. Estos indicadores son esenciales para detectar configuraciones inadecuadas, políticas de contraseñas débiles, permisos excesivos o comportamientos anómalos. Este indicador se encuentra en la herramienta Purple Knight.

2.4 MITRE ATT&CK

El marco MITRE ATT&CK, es una base de conocimiento integral que observa cómo se comportan los ciberataques en el mundo real. Es un recurso accesible a nivel mundial, que proporciona un lenguaje común para describir y compartir amenazas. (*Guía Completa de Tácticas de ATT&CK: El Marco MITRE*, s. f.)

MITRE ATT&CK considera que un ataque informático es una serie de pasos encadenados, no un solo evento. Esa cadena se divide en etapas cada una con sus propias señales y cada etapa representa una oportunidad para identificar y rechazar el asalto. (Beschokov, 2025).

Este *framework* tiene como objetivo describir las tres fases en función de tácticas, técnicas y conocimiento común que son los componentes claves. Las tácticas representan los objetivos generales, es el porqué de un ataque, cómo podemos obtener el acceso inicial o aumentar los privilegios. Por otro lado, las técnicas describen los métodos específicos además indican cómo el adversario logra estos objetivos. Finalmente, el conocimiento común abarca los casos documentados en los que los adversarios utilizan las tácticas y técnicas de forma espontánea. (*Guía Completa de Tácticas de ATT&CK: El Marco MITRE*, s. f.).

El marco MITRE ATT&CK permite comprender, clasificar y anticipar el comportamiento de los atacantes, brindando a las empresas una herramienta estructurada para fortalecer sus estrategias de detección, defensa y respuesta ante incidentes de seguridad.

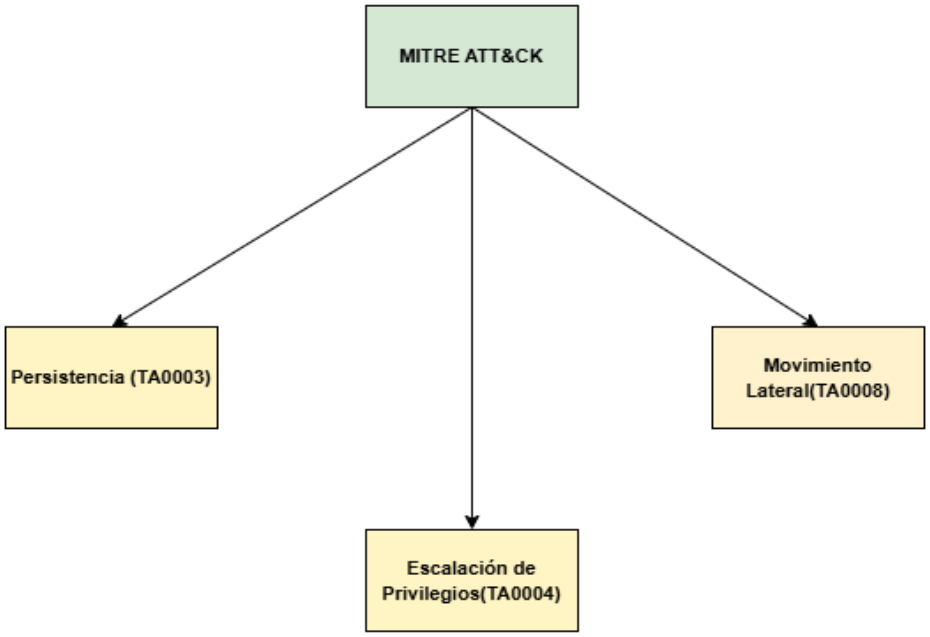

Ilustración 6 Diagrama de MITRE ATT&CK Fuente: Elaboración Propia utilizando el sitio web https://app.diagrams.net/

2.4.1 Persistencia (TA0003)

La persistencia hace referencia a diferentes técnicas que los atacantes utilizan para mantener el acceso a un sistema comprometido, incluso después de varios reinicios, actualizaciones o medidas de seguridad implementadas por los administradores. Esto busca que un atacante conserve su presencia dentro del entorno afectado durante el mayor tiempo posible. Por ejemplo, cuando se logra instalar un programa malicioso sin ser detectado por los filtros de seguridad a las rutinas de inicio del equipo o logra cambiar una configuración del sistema para activar automáticamente el programa malicioso. Con esto el atacante se asegura permanecer por un tiempo prolongado en el equipo, lo que aumenta las posibilidades de robar datos o lograr escalar en las redes. (Guía Completa de Tácticas de ATT&CK: El Marco MITRE, s. f.).

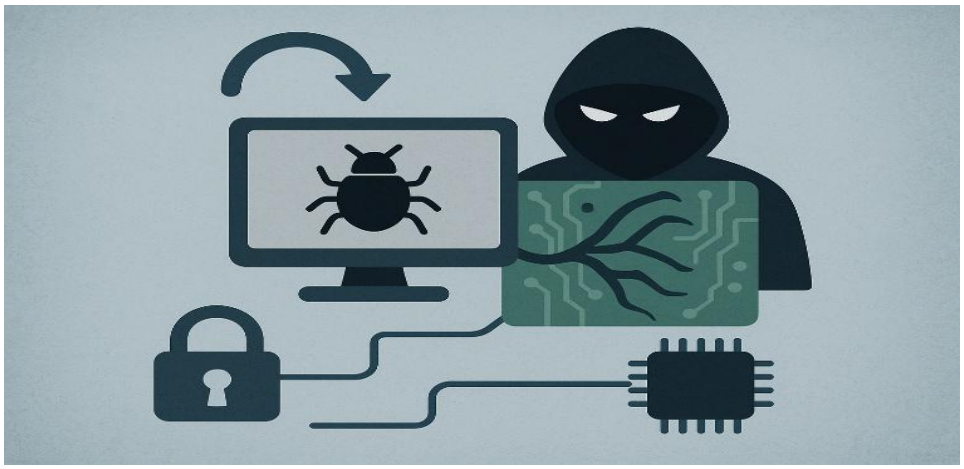

Ilustración 7 Táctica de Persistencia.

Fuente Elaboración Propia con IA

Las técnicas usadas para la persistencia incluyen cualquier acceso, acción o cambio de configuración que les permita mantener su punto de apoyo en los sistemas, como reemplazar o secuestrar código legítimo o añadir código que se ejecute al inicio. (*Persistence, Tactic TA0003 - Enterprise* | *MITRE ATT&CK*®, s. f.)

2.4.2 Escalación de privilegios (TA0004)

La escalación de privilegios se produce cuando un atacante con acceso básico intenta obtener permisos de nivel superior, como por ejemplo pasar de usuario normal a usuario administrador. Es decir, como si alguien que es invitado en una fiesta encontrara la llave maestra para ingresar al cuarto secreto de la casa del anfitrión. Con privilegios mejorados el atacante puede acceder a datos confidenciales o controlar sistemas críticos. (Guía Completa de Tácticas de ATT&CK: El Marco MITRE, s. f.).

Para los administradores de una infraestructura tecnológica la escalada de privilegios puede implicar una serie de acciones como explotar vulnerabilidades del *kernel*,

abuso de credenciales descargadas, configuraciones incorrectas, como no utilizar el principio de mínimo privilegio. Algunos ejemplos de acceso elevado incluyen:

- Nivel SYSTEM/root level
- Administrador local
- Cuenta de usuario con acceso similar al de un administrador
- Cuentas de usuario con acceso a un sistema específico o para desempeñar una función concreta

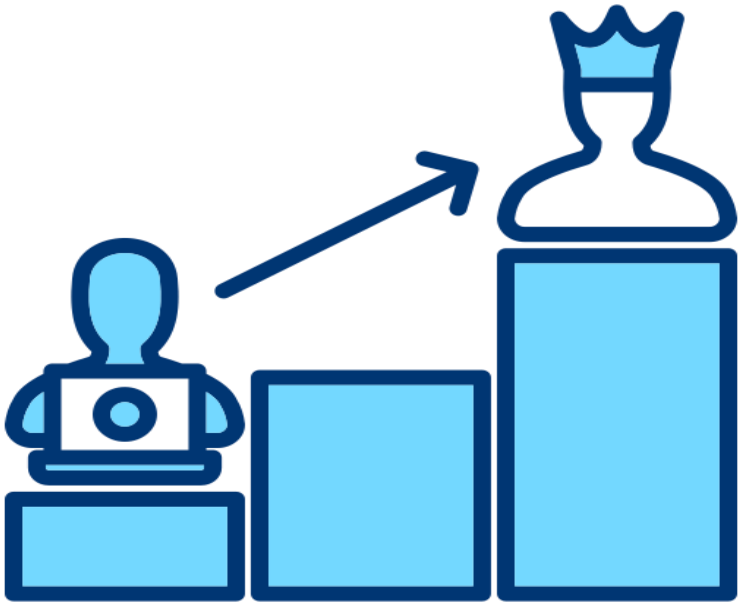

Ilustración 8 Estalación de Privilegios Fuente Marsiholo. (s. f.). Icono de escalada de privilegios [Icono]. Freepik. https://www.freepik.es/icono/escalada-privilegios_15163335

Estas técnicas a menudo se confunden con las técnicas de persistencia ya que las funcionalidades del sistema operativo que permiten a un adversario persistir pueden ejecutarse en un contexto elevado. (*Privilege Escalation, Tactic TA0004 - Enterprise | MITRE ATT&CK®*, s. f.)

2.4.3 Movimiento lateral (TA0008)

El movimiento lateral se produce cuando los atacantes se pueden mover de un sistema a otro dentro de la red con el fin de alcanzar su objetivo principal, esto puede ser en un servidor de base de datos, o un conjunto de archivos específicos. Los atacantes pueden utilizar credenciales robadas o aprovechar diferentes vulnerabilidades del software para saltar de una máquina a otra. La mayoría de los atacantes suelen aprovecharse de varios protocolos administrativos como SMB, WMI, RDP o SSH, además de los entornos de Kerberos donde métodos como el pase de moda o los billetes dorados permiten a los adversarios hacerse pasar por usuarios legítimos. Por eso es importante contar con segmentación a nivel de redes, aplicar el mínimo privilegio, combinar registros de XDR con eventos del Directorio Activo. (Guía Completa de Tácticas de ATT&CK: El Marco MITRE, s. f.).

Los adversarios pueden instalar sus propias herramientas de acceso remoto para llevar a cabo el movimiento lateral o utilizar credenciales legítimas junto con herramientas nativas de red y del sistema operativo, lo que puede hacer que sus acciones sean más sigilosas. (*Lateral Movement, Tactic TA0008 - Enterprise* | *MITRE ATT&CK®*, s. f.)

Ilustración 9 Movimiento lateral Fuente Elaboración Propia con IA

2.5 Monitoreo

Es una revisión continua, supervisión, observación crítica o determinación del estado con el fin de identificar cambios respecto al nivel de desempeño requerido o esperado.

Microsoft indica que un sistema sólido de monitoreo de registros de eventos es crucial para cualquier diseño seguro de Directo Activo. Muchas vulnerabilidades de seguridad informática se pueden detectar en una etapa temprana si los objetivos implementan un monitoreo y alerta adecuada de los registros de eventos. (Microsoft, s. f.)

Existen muchas herramientas disponibles para realizar monitoreos, pero la falta de efectividad en la configuración de monitoreo de eventos y el análisis de los registros continúa siendo un desafío importante. Si bien es posible detectar las brechas de seguridad, diversos estudios indican que en casos donde las organizaciones se han visto afectadas

contaban con la información necesaria en sus registros para identificar el incidente, pero les faltó realizar el análisis con mayor profundidad y atención.

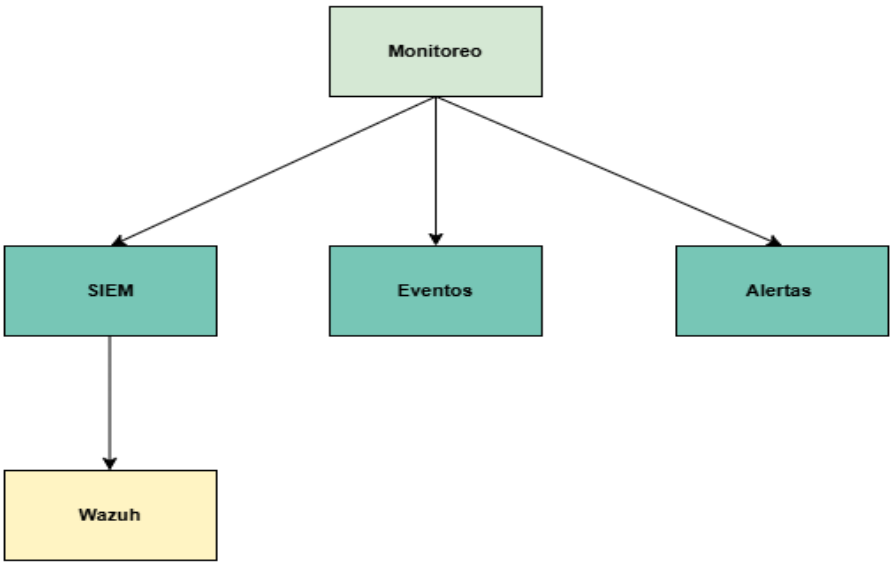

Ilustración 10 Diagrama de Monitoreo Fuente: Elaboración Propia utilizando el sitio web https://app.diagrams.net/

2.5.1 SIEM

La gestión de eventos e información de la seguridad, conocida por sus siglas en inglés como SIEM (*Security Information and Event Management*), constituye una solución integral de ciberseguridad en la cual su función principal es la recopilación, análisis y correlación de datos de seguridad provenientes de múltiples fuentes dentro de la infraestructura tecnológica de una empresa. (Trend Micro,2025)

Entre las soluciones de SIEM tanto comerciales como de código abierto, destaca Wazuh como una plataforma robusta y versátil que integra capacidades de monitoreo integral, detección de amenazas y cumplimiento normativo.

2.5.1.1 Wazuh

Es una plataforma de monitoreo que supervisa las configuraciones de sistemas, redes y aplicaciones para garantizar su complimiento con las políticas de seguridad, estándares y guías de endurecimiento (*hardening*) establecidas por la empresa. Los agentes de Wazuh están en constante ejecución con el fin de detectar configuraciones incorrectas o brechas de seguridad en los puntos finales (*endpoints*) que podrían ser aprovechadas por actores de amenazas. (Wazuh,2025)

2.5.2 Eventos

La ISO 27002:2023 define un evento como suceso que indica una posible violación de la seguridad de la información o un fallo de los controles.

2.5.3 Alertas

Una alerta de seguridad representa la correlación automatizada de eventos, procesos y actividades vinculados con un comportamiento anómalo o potencialmente malicioso detectado por el sistema de monitoreo**.** (IBM,2025)

Capítulo 3. Marco Metodológico

3.1Tipo de Investigación

El presente Trabajo Final de Graduación corresponde a una investigación evaluativa y aplicativa, ya que tiene como objetivo fundamental utilizar el conocimiento existente en el campo de la ciberseguridad para resolver una problemática concreta en entornos empresariales.

La investigación se centra en la "Creación de un plan de *hardening* y monitoreo continuo de Directorio Activo", constituyendo una meta práctica y orientada a la solución de desafíos de seguridad específicos en infraestructuras de directorio.

Para el desarrollo de este proyecto, se emplean como base marcos de conocimientos de acceso universal y continuamente actualizados, los cuales proporcionan un modelo consolidado para el análisis de técnicas adversarias. Estos marcos se complementan con metodologías de evaluación de seguridad y sistemas de correlación de eventos que permiten identificar vulnerabilidades y detectar actividades sospechosas en el entorno de Directorio Activo.

La finalidad del estudio es elaborar una propuesta técnica integral que sirva como guía para la mitigación de tácticas de persistencia y escalamiento de privilegios, elevando así el nivel de protección del Directorio Activo y fortaleciendo las capacidades de detección ante amenazas avanzadas persistentes.

3.2 Alcance Investigativo

El alcance de esta investigación es de tipo descriptivo y analítico, caracterizado por el análisis de los controles, tácticas y mecanismos de protección aplicables al Directorio Activo según los estándares de los marcos universales.

La investigación permitirá describir con precisión los factores que incrementan la superficie de ataque del Directorio Activo, entre los que se incluyen: configuraciones predeterminadas no seguras, gestión inadecuada de identidades privilegiadas, políticas de autenticación insuficientes y ausencia de sistemas de monitorización para eventos críticos.

La investigación analítica se refleja en la capacidad de establecer relaciones entre los distintos marcos universales, identificar equivalencias, vacíos o redundancias entre controles consolidando las mejores prácticas de *hardening* y monitoreo continuo.

A través del análisis descriptivo, la investigación definirá planes estructurados de *hardening* de seguridad y establecerá mecanismos de monitoreo continuo capaces de detectar comportamientos anómalos, correlacionar eventos de seguridad y generar alertas tempranas que permitan una respuesta oportuna ante potenciales incidentes.

3.3 Enfoque

El estudio adopta un enfoque de investigación cualitativo, ya que el objetivo principal es interpretar y contextualizar la información proveniente de fuentes documentales.

La investigación cualitativa está diseñada para abordar cuestiones de investigación que se centran en comprender el “por qué” y el “cómo” del comportamiento, en lugar de sólo el “qué” o el “cuántos” que suelen tratar los métodos de cuantitativos. (ATLAS.ti, s. f.)

Este enfoque permite interpretar y contextualizar la información proveniente de las fuentes documentales, priorizando la comprensión profunda del fenómeno sobre la cuantificación de variables.

3.4 Diseño

El diseño de esta investigación es de tipo evaluativo y propositivo, ya que su propósito es analizar la problemática de las configuraciones vulnerables y la falta de monitoreo continuo en entornos de Directorio Activo, identificando las brechas existentes en materia de seguridad frente a las tácticas de persistencia y escalamiento de privilegios.

A partir del diagnóstico documental, se busca proponer un modelo estructurado que integre controles de *hardening* y mecanismos de monitoreo continuo, alineados con los marcos universales, de modo que pueda ser aplicado en entornos corporativos reales.

3.5 Población y Muestreo

Con el fin de entender el concepto de población, se utiliza como referencia la definición provista por Fracica (1988, pág. 36), quien la define como el conjunto de todos los elementos a los cuales se refiere la investigación. Según Jany (1994), población es “la totalidad de elementos o individuos que tienen ciertas características similares y sobre las cuales se desea hacer inferencia” (p. 48).

Por otro lado, Bernal (2010, pág. 160) define muestra como la parte de la población que se selecciona, de la cual realmente se obtiene la información para el desarrollo del

estudio y sobre la cual se efectuarán la medición y observación de las variables objeto de estudio.

Tomando en consideración estas definiciones, para esta investigación no se trabaja con una población ni muestra en el sentido tradicional, dado que no se recolectan datos directamente de personas ni organizaciones reales mediante entrevistas, cuestionarios o instrumentos estadísticos. El estudio se sustenta en la revisión sistemática de marcos universales, y estudios técnicos relevantes sobre tácticas y técnicas de persistencia y escalamiento de privilegios en entornos de Directorio activo.

3.6 Instrumentos de Recolección de Datos

Bernal (2010, pág. 191) describe la recolección de información como un aspecto fundamental en el proceso de investigación, que guarda relación directa con la obtención de los datos necesarios, pues de ello dependen la confiabilidad y validez del estudio. Obtener información confiable y válida requiere cuidado y dedicación. Esta etapa, proporciona los datos mediante los cuales se responden las preguntas de investigación y se logran los objetivos del estudio originados del problema de la investigación.

3.6.1 Revisión documental

Se lleva a cabo un análisis exhaustivo de documentos técnicos, marcos de base de conocimientos universales y literatura científica, con el propósito de identificar las mejores prácticas, controles y mecanismos de monitoreo aplicables a entorno de Directorio Activo. Entre las fuentes analizadas se incluyen los marcos de MITRE ATT&CK, guía de CIS Benchmarks, además de artículos y publicados de organismos reconocidos como la IEEE, Semperis, Microsoft.

Este análisis se hace con el fin de alcanzar los siguientes objetivos específicos:

- Identificar técnicas de ataques comunes asociadas al Directorio Activo según MITRE-ATT&CK para reconocer amenazas relevantes.
- Elaborar un plan de *hardening* basado en CIS Benchmarck para fortalecer la seguridad del Directorio Activo.

3.7 Técnicas de Análisis de Información

Los datos recolectados en esta investigación se analizan mediante un enfoque cualitativo.

Análisis documental: La información obtenida mediante las fuentes documentales será clasificada y analizada, con el fin de categorizar temáticas como, por ejemplo, persistencia, escalamiento de privilegios.

Técnicas de Integración y Visualización: Para facilitar la interpretación y presentación de resultados, se emplearán las siguientes herramientas de visualización:

- **Mapas mentales y conceptuales:** Para representar las relaciones entre configuraciones de Directorio Activo y técnicas específicas de MITRE ATT&CK, facilitando la identificación de vectores de ataque críticos.

- **Diagramas de flujo y espinas de Ishikawa:** Para ilustrar las causas raíz de debilidades en *hardening* y los procesos involucrados en la explotación de vulnerabilidades.

Capítulo 4. Análisis del Diagnóstico

En este capítulo se presentan los resultados del análisis documental desarrollado según la metodología definida.

4.1 Resultados de la revisión documental:

La fase preliminar de análisis permitió identificar y clasificar la información más relevante vinculada con la seguridad del Directorio Activo, las técnicas de persistencia y escalamiento de privilegios descritas en MITRE ATT&CK y las mejores prácticas de *hardening* y monitoreo continuo aplicables a entornos *on-premise*. La información recopilada sirvió como base para la construcción del marco teórico y orientó el diseño metodológico de este estudio.

4.1.1 Tendencias de investigación sobre tácticas de MITRE ATT&CK

Con el fin de contextualizar el uso del *framework* MITRE ATT&CK, se identificaron estudios que analizan la frecuencia con la que las distintas tácticas han sido objeto de investigación entre el 2019 y 2024. Este análisis permite reconocer en que fases del ciclo de vida del ataque se ha concentrado la atención académica y operativa.

En la tabla 1 se muestra un resumen de las tácticas de MITRE ATT&CK, únicamente se incluyen aquellas tácticas que fueron estudiadas explícitamente. Los valores presentados son el número de estudios en los que cada táctica fue analizada de forma central.

Nombre de Táctica (ID)	2019	2020	2021	2022	2023	2024	Total
Reconocimiento (TA0043)	0	0	2	9	23	16	50
Desarrollo de Recursos (TA0042)	0	0	2	6	12	12	32
Acceso Inicial (TA0001)	2	4	15	22	39	27	109
Ejecución (TA0002)	3	5	14	20	33	24	99
Persistencia (TA0003)	2	5	12	17	32	22	90
Escalada de Privilegios (TA0004)	2	4	10	18	29	21	81
Evasión de Defensa (TA0005)	1	5	13	16	28	21	84
Acceso a Credenciales (TA0006)	0	5	11	15	27	23	81
Descubrimiento (TA0007)	3	6	12	21	37	28	107
Movimiento Lateral (TA0008)	3	6	12	15	37	22	95
Recopilación (TA0009)	1	5	9	12	27	20	74
Comando y Control (TA0011)	2	3	9	16	33	21	84
Exfiltración (TA0010)	2	5	9	9	25	20	70
Afectar el Control de Procesos (TA0106)	0	0	1	2	9	3	15
Inhibir Función de Respuesta (TA0107)	0	0	0	2	7	3	12
Impacto (TA0040)	0	5	8	12	35	18	75

Tabla 1 Frecuencia de tácticas MITRE ATT&CK por año (2019-2024) (Jiang et al., 2025)

De acuerdo con estos datos se observa que tácticas como Acceso Inicial (TA0001), Ejecución (TA0002) y Descubrimiento (TA0007) reportan mayor frecuencia, acumulando en conjunto más del 30% del total de menciones. Lo que refleja un fuerte énfasis de investigación temprana de las campañas adversarias. (Jiang et al., 2025)

En el contexto del desarrollo de este trabajo, resulta especialmente relevante la evolución que presentan las tácticas de Persistencia (TA0003) y de Escalamiento de Privilegios (TA0004), esto debido a que ambas tácticas se encuentran directamente vinculadas con el compromiso del Directorio Activo. Es importante resaltar que estas

tácticas no son las más estudiadas en términos absolutos, su tendencia a la alza en los últimos años y el papel que desempeñan en el mantenimiento del control sobre el dominio justifican el enfoque de este trabajo en cinco técnicas específicas: T1078.002 (Valid Accounts – Domain Accounts), T1484.002 (Domain Policy Modification), T1134.002 (Token Impersonation/Theft), T1547.002 (Boot or Logon Autostart Execution) y T1574.001 (Hijack Execution Flow – DLL Side-Loading). Estas técnicas conforman una cadena de ataque lógico: las cuentas de dominio comprometidas (T078.002) proveen el punto de acceso inicial; la modificación de políticas de dominio (T1484.002) amplía el radio de acción sobre la infraestructura de la organización; la suplantación de tokens(T1134.002) eleva los privilegios sin necesidad de recurrir a credenciales adicionales; los mecanismos de autoarranque(T1547.002) garantizan persistencia encubierta ante reinicios; el secuestro del flujo de ejecución mediante DLL(T1574.001) permite evasión bajo procesos legítimos. Técnicas de alto impacto como T1158.001 (Golden Ticket) o T1003.006(DCSync) quedaron fuera del alcance no por carecer de relevancia, sino más bien porque su mitigación efectiva depende en gran medida de controles cubiertos por T1078.002 y T1484.002, evitando redundancia en el plan propuesto. Esta delimitación responde a criterios de viabilidad y profundidad, no de relevancia relativa entre técnicas del Directorio Activo.

4.1.2 Tácticas y técnicas de MITRE ATT&CK

A partir del análisis cualitativo centrado en las tácticas de Persistencia (TA0003) y Escalamiento de privilegios (TA0004), se seleccionaron cinco técnicas consideradas críticas en incidentes que afectan al Directorio Activo. A continuación, se presentan los principales hallazgos asociados a cada una.

4.1.2.1 Técnica T1078.002 – Valid Accounts (Domain Accounts)

La literatura coincide en que el abuso de cuentas válidas es uno de los métodos más frecuentes utilizados por adversarios para obtener acceso inicial, establecer persistencia o escalar privilegios en sistemas basados en Directorio Activo. Diversos estudios señalan que esta explotación se ve facilitada por configuraciones débiles de autenticación, ausencia de rotación de credenciales, superposición de permisos y falta de monitoreo adecuado.

Un caso ampliamente documentado se observó durante el ataque a la red eléctrica de Ucrania en 2015, donde el grupo Sandworm utilizó credenciales válidas para moverse lateralmente, escalar privilegios y mantener persistencia dentro de la red corporativa.

4.1.2.2 Técnica T1484.002: Domain Policy Modification.

Los estudios analizados evidencian que la manipulación de políticas de dominio y relaciones de confianza permite a un atacante ejecutar código arbitrario, escalar privilegios o evadir defensas mediante la alteración de configuraciones críticas. La modificación de *trusts* suele realizarse mediante herramientas como netdom, nltest o PowerShell, afectando atributos sensibles como *trustDirection*, *trustType* y *trustAttributes*. Este tipo de cambios suele pasar desapercibido cuando no existe auditoría avanzada.

4.1.2.3 Técnica T1134.002: Token Impersonation/Theft.

La revisión documental muestra que la manipulación o robo de *tokens* de acceso constituye un mecanismo ampliamente utilizado para suplantar identidades privilegiadas y ejecutar procesos elevados. Algunas campañas atribuidas a APT28 incluyen el aprovechamiento de vulnerabilidades del sistema, como CVE-2015-1701, para obtener el *token* SYSTEM y replicarlo en procesos controlados por el atacante.

4.1.2.4 Técnica T1547.002: Boot or Logon Autostart Execution.

La literatura describe que esta técnica se basa en manipular componentes de arranque o inicio de sesión con el fin de establecer persistencia a nivel de sistema. Se han documentado campañas en las que los atacantes crean o modifican claves de registro en rutas críticas de Active Setup o LSA para garantizar la ejecución automática de código malicioso sin levantar alertas.

4.1.2.5 Técnica T1574.001: Hijack Execution Flow – DLL Side-Loading.

El análisis evidencia que la alteración del flujo de ejecución mediante *DLL side-loading* constituye un método sigiloso y difícil de detectar. Se han documentado casos, como el incidente C0017 atribuido a APT41, en los que los atacantes lograron persistencia insertando DLL maliciosas mediante modificaciones en la Import Address Table (IAT) de ejecutables legítimos de Microsoft.

4.2 Relación del *hardening* en Directorio Activo

Los artículos analizados consideran al Directorio Activo como un componente importante para gestionar el acceso de alto nivel, quién obtiene qué permisos, y cómo diferentes equipos y usuarios se conectan al mismo. Los estudios resaltan que, cuando se logra escalar privilegios dentro del Directorio Activo, los atacantes adquieren la capacidad para moverse lateralmente y permanecer ocultos de las medidas de seguridad implementadas, especialmente si estas medidas son solo a nivel de equipos de red o dispositivos individuales.

Entre las debilidades reiterativas se encuentran:

1- Cuentas de usuarios con demasiados privilegios, generalmente heredados y sin revisión periódica.
2- Configuraciones débiles a nivel del grupo de políticas como, por ejemplo: políticas de contraseñas de tan solo 6 caracteres sin incluir caracteres especiales, desactivación de protocolos inseguros, o falta de restricciones a nivel de equipos como cierre de sesión inactiva o uso de puertos USB sin limitación.
3- Carencia de segmentación lógica entre cuentas de servicio, administrativas, y usuarios estándar.

4.2.1 Controles de *hardening* para Directorio Activo

Luego del análisis realizado a guías de buenas prácticas y estudios donde se han aplicado, se identifican medidas de seguridad que se alinean con las fuentes revisadas:

1- Segmentación de privilegios y administración de cuentas.
   - Separación de cuentas administrativas y usuario estándar.
   - Uso del mínimo privilegio para grupos de usuarios.
   - Revisión periódica de permisos a nivel de usuarios y grupos.

2- Fortalecimiento del grupo de políticas.
   - Utilización de plantillas de seguridad de CIS Benchmark combinadas con lineamientos de Microsoft.
   - Fortalecimiento de políticas de contraseñas, bloqueo de cuentas y autenticación.
   - Restricción de la administración remota solo a cuentas de servicio.

3- Protección de rutas críticas en el Directorio Activo
   - Control de delegaciones de controles y eliminación de permisos heredados.
   - *Hardening de* AdminSDHolder sobre unidades organizativas sensibles.

4- Reducción de la superficie de ataque en el Directorio Activo
   - Deshabilitación de protocolos inseguros u obsoletos.
   - Segmentación de redes con el fin de minimizar la exposición del controlador de dominio.

Estos controles se pueden reforzar con un análisis de auditoria realizado por la herramienta Purple Knight donde va a indicar el nivel de salud del Directorio Activo y los controles que se deben mejorar, con el fin de poder subir el porcentaje de seguridad en el entorno analizado.

4.3 Puntos débiles en el monitoreo continuo

Si bien existen herramientas que ayudan con el monitoreo del entorno empresarial, muchas veces están configuradas de forma general, lo que dificulta la visualización completa de lo que sucede a nivel del usuario y la interacción de los sistemas.

La falta de conocimiento al momento de implementar estas herramientas impide que se puedan detectar tácticas, técnicas y procedimientos más específicos.

4.3.1 Escasez en detección basada en comportamiento.

La configuración de un SIEM sin un enfoque se limita a registrar eventos como bloqueos o errores, dejando por fuera aquellos que si se completaron con éxito pero que pueden ser una señal de un ataque. Por ejemplo:

- Inicios de sesión con una cuenta de servicio con permisos de administrador a las 3 de la mañana, desde una ubicación inusual.

- Cambios exitosos en atributos de cuentas relacionadas con la técnica T1098, no generan alertas debido a que las reglas diseñadas para este tipo de actividad no se encuentran implementadas.

4.3.2 Cobertura Incompleta del *Framework* MITRE ATT&CK

La herramienta Wazuh se ha integrado con MITRE ATT&CK, lo cual demuestra un avance significativo en sistemas SIEM por el aporte que realiza, al revisar la documentación, algunas técnicas como la T1134 Token Impersontion/Theft y la 1574 Hijack Execution Flow – DLL Side-Loading no se logran detectar al menos que se configure Sysmon de forma avanzada y se definan las reglas de correlación específicas, algo que por defecto no viene activo.

4.3.3 *Hardening* y *monitoreo continuo coincidencia de enfoques*

La documentación permite relacionar una coincidencia de enfoques entre el *hardening* y el monitoreo continuo:

- La guía de CIS Benchmark propone controles concretos sobre cuentas, grupo de políticas, servicios y objetos de Directorio Activo para reducir la superficie de ataque.

El monitoreo continúo basado en MITRE ATT&CK utilizando Wazuh, se centra en convertir las técnicas adversarias en casos de uso de detección compatibles con eventos generados por el Directorio Activo.

4.4 Técnicas de integración y visualización.

Con el fin de representar visualmente los hallazgos del análisis documental se desarrollaron mapas mentales y conceptuales, diagramas de flujo y un diagrama de espina de Ishikawa.

En la ilustración 11 se presenta un mapa mental donde se visualizan las relaciones entre las configuraciones del Directorio Activo, las cinco técnicas escogidas a nivel de MITRE ATT&CK y los controles de *hardening y* monitoreo.

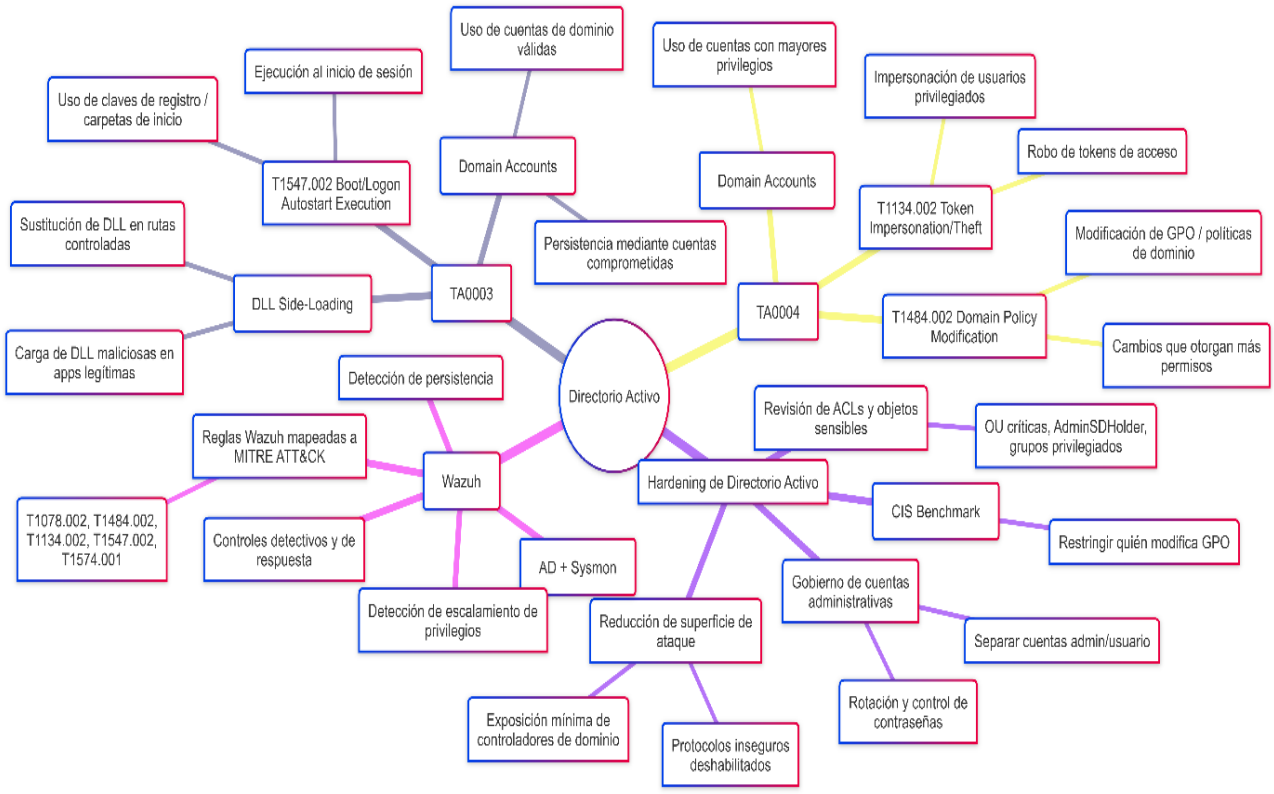

Ilustración 11 Mapa Mental controles en Directorio Activo con MITRE ATT&CK y Wazuh
Elaboración propia

La ilustración 12 muestra un mapa conceptual que vincula elementos del Directorio Activo con las tácticas y mecanismos de monitoreo basados en Wazuh

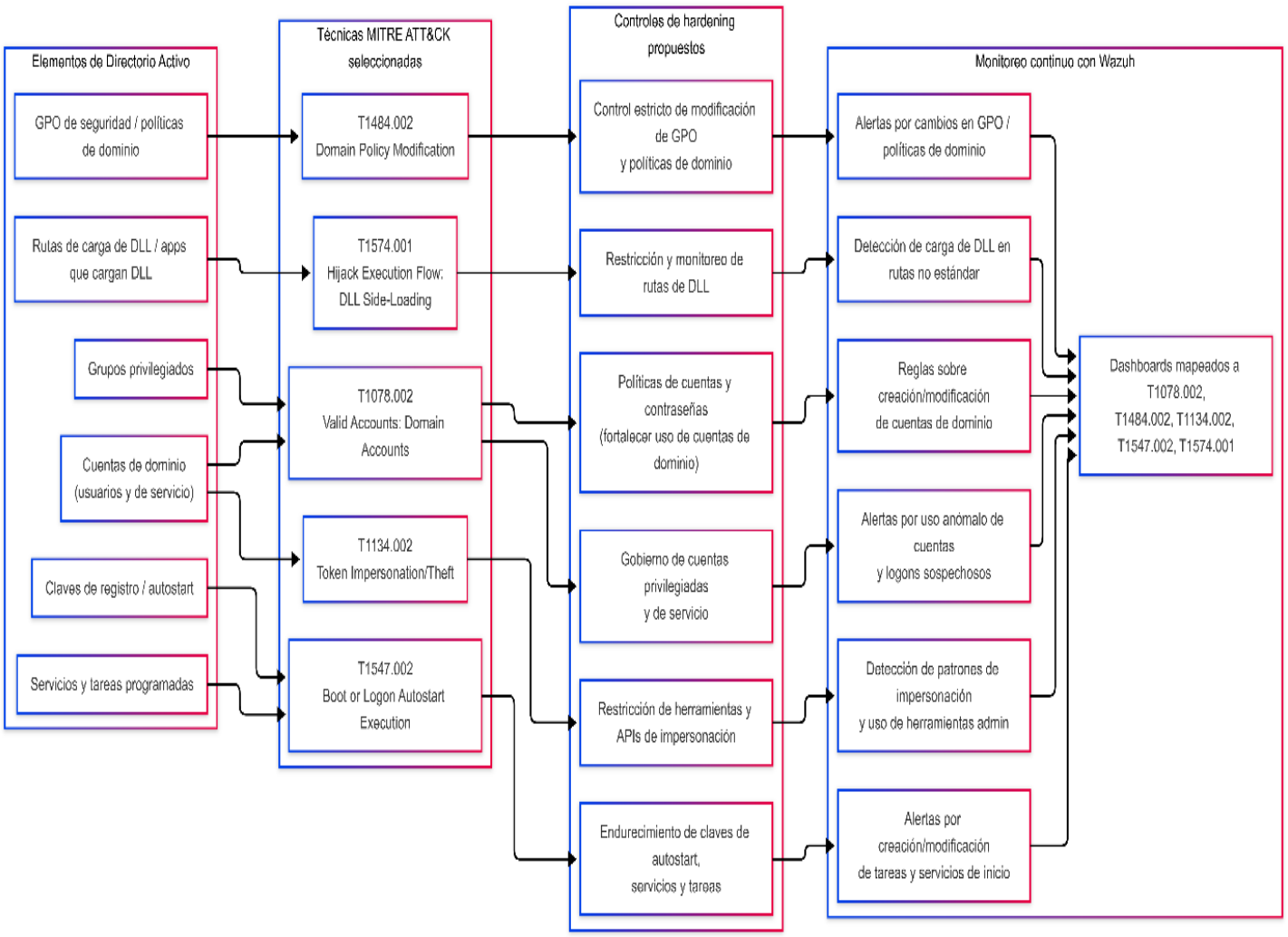

Ilustración 12 Mapa Conceptual de las relaciones entre configuraciones del Directorio Activo, técnicas de MITRE ATT&CK Y monitoreo continuo. Elaboración propia

En la ilustración 13 se visualiza un flujo del desarrollo de un ataque orientado al escalamiento de privilegios y persistencia, mientras que en la ilustración 14, por medio de un diagrama de Ishikawa, se pueden observar las causas raíz asociadas a un *hardening* deficiente y un monitorio continuo incompleto.

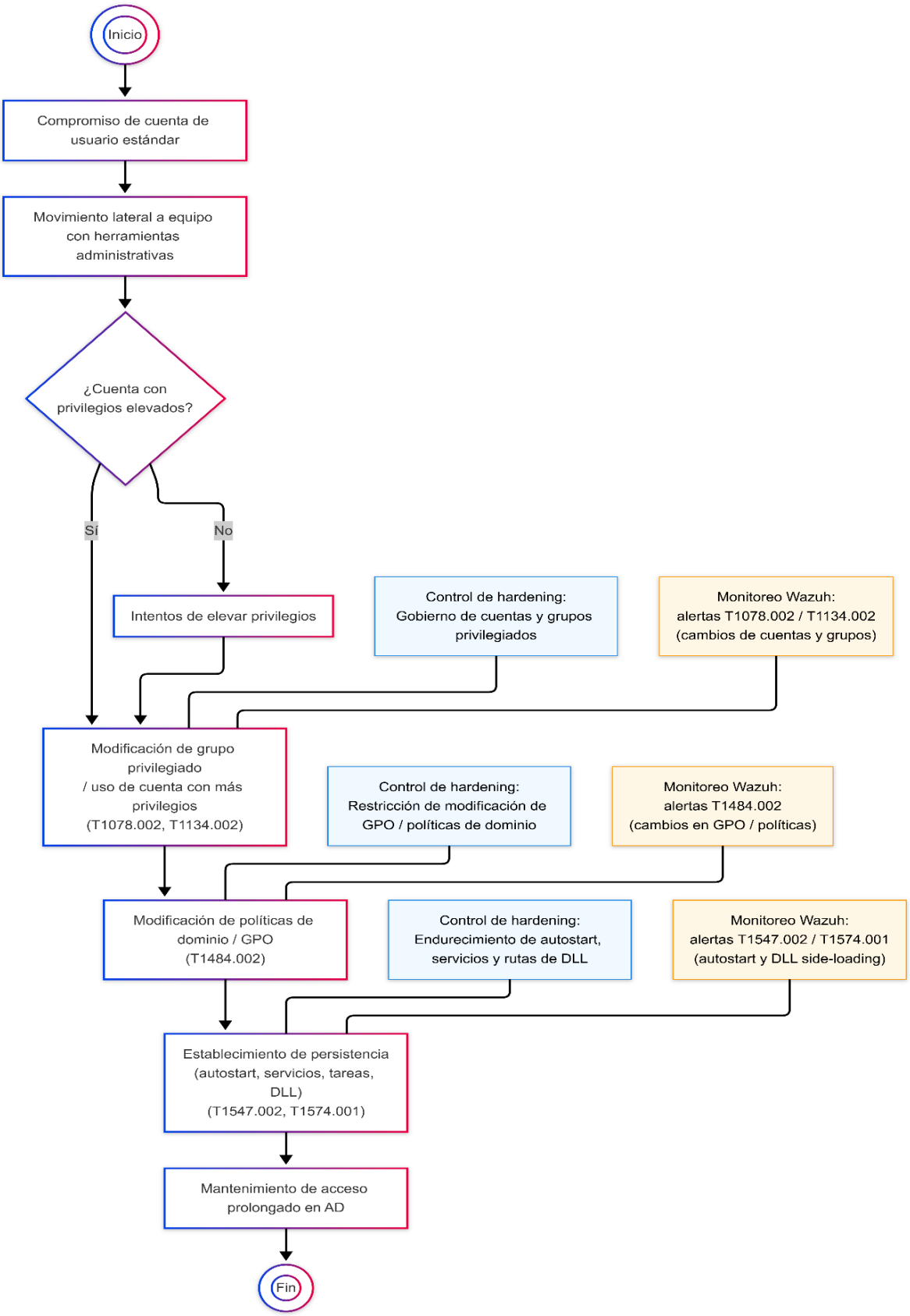

Ilustración 13 Diagrama de un escenario de compromiso. Elaboración propia

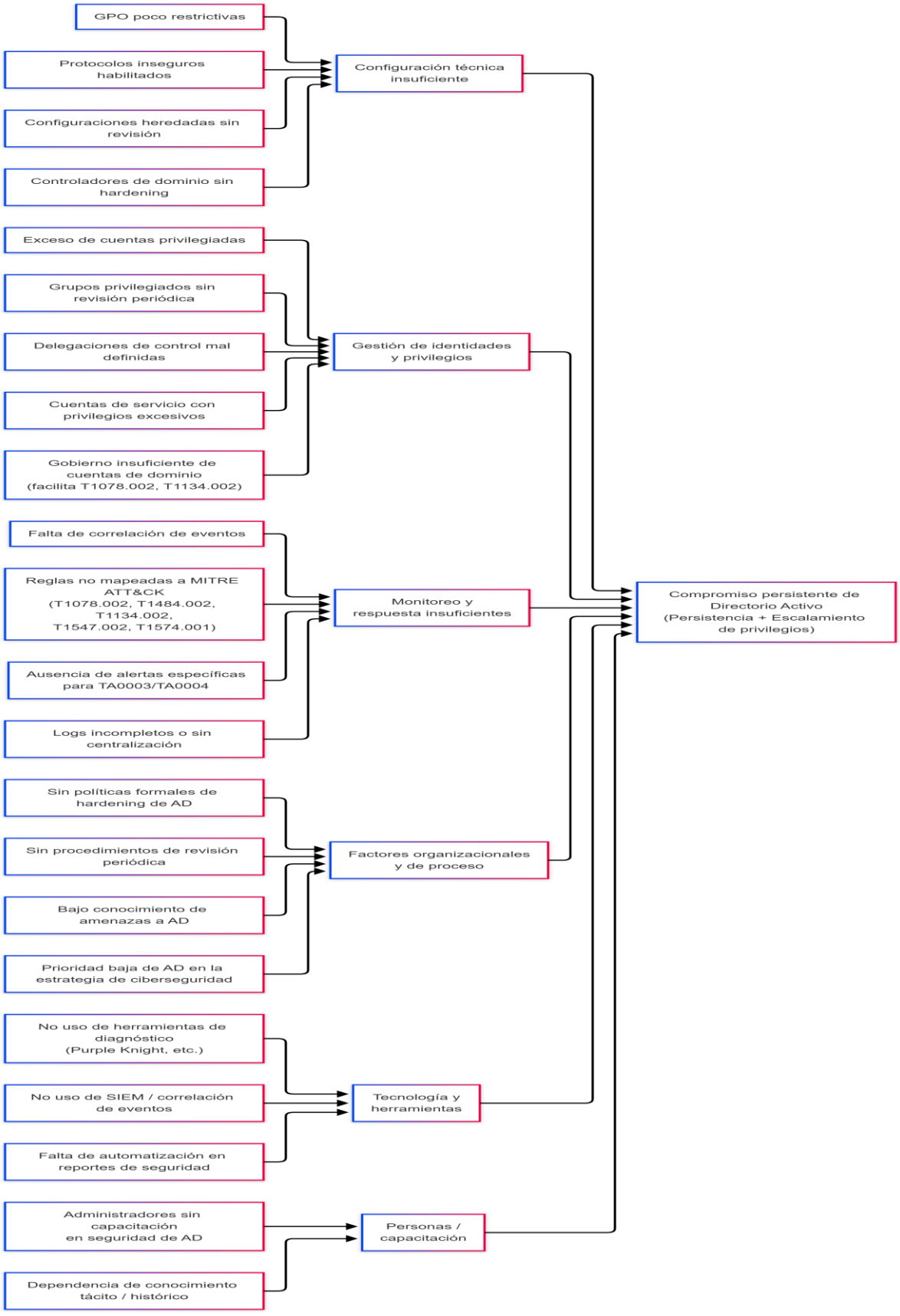

Ilustración 14 Diagrama de espiga de Ishawaka sobre causas raíz del compromiso persistente en el Directorio Activo. Elaboración propia

Capítulo 5. Propuesta de Solución

5.1 Descripción general de la propuesta

Basado en el diagnóstico realizado en el capítulo 4, donde se identificaron las debilidades más recurrentes en el entorno del Directorio Activo *on-premise* dentro de las cuales destaca la escasez en la detección basado en comportamiento, cobertura incompleta del marco MITRE ATT&CK en los sistemas de monitoreo y la desconexión entre el *hardening* y el monitoreo continuo, se plantea la presente propuesta de solución.

La cual consiste en un plan integral de *hardening* y monitoreo continuo para entornos de Directorio Activo *on-premise* sobre Windows Server 2016 o superior diseñado para mitigar cinco técnicas de alto impacto dentro del marco MITRE ATT&CK, específicamente en las categorías de Persistencia (TA0003) y Escalamiento de Privilegios (TA0004). Asimismo, se estructura en tres componentes interdependientes:

- **Componente 1: Diagnostico de seguridad**: evaluación del estado de seguridad del Directorio Activo mediate la herramienta Purple Knight de Semperis, con el fin de identificar los indicadores de explosión (IoE) e indicadores de compromiso (IoC) presentes en el entorno de Directorio Activo previo a la aplicación de controles.
- **Componente 2: Plan de *hardening* y monitoreo continuo***:*** conjunto estructurado de controles de seguridad basados en la guía de CIS Benchmark para Windows Server, y *template* de Microsoft, organizados por técnica MITRE ATT&CK y orientados a reducir la superficie de ataque del Directorio Activo.
- **Componente 3: Monitoreo continuo**: conjunto de reglas de detección implementadas en Wazuh, complementadas con Sysmon como fuente de telemetría avanzada,orientados a reducir la superficie de ataque del Directo Activo y fortalecer la identificación de técnicas, tácticas y procedimientos (TTPs) asociados a las cinco técnicas seleccionadas.

5.2 Componente 1: Diagnostico de seguridad

Purple Knight es una herramienta de evaluación de la seguridad del Directorio Activo desarrollada por Semperis, que ejecuta más de 150 indicadores de seguridad de exposición o compromiso organizados en categorías alineadas con el marco MITRE ATT&CK. Lo que nos ayuda a cuantificar objetivamente el estado de seguridad del Directorio Activo antes y después de aplicar los controles de *hardening*.

5.2.1 Rol de Purple Knight

Basado en el segundo objetivo específico de este trabajo: “Comprender el estado de seguridad actual del Directorio Activo mediante la herramienta Purple Knight para interpretar

hallazgos y debilidades en la configuración.” Purple Knight cumple dos roles dentro del *plan de hardening:*

- Línea base previa (pre-hardening): el escaneo inicial ayuda a identificar los indicadores críticos del entorno, lo cual orienta la priorización de los controles a implementar.
- Validación posterior (post-hardening): el escaneo final evidencia la reducción en el número de indicadores críticos y el incremento en el porcentaje de seguridad por categoría.

5.2.2 Procedimiento de ejecución

Para la ejecución de Purple Knight se deben seguir los siguientes pasos:

1. Descargar Purple Knight5.0 Community Edition desde https://www.semperis.com/es/purple-knight/ es necesario un registro gratuito.
2. Desde el controlador de dominio se ejecuta el PurpleKnight.exe como administrador y se selecciona el dominio objetivo.
3. Se seleccionan las cinco categorías *on-premises: Kerberos Security, Group Policy Security, Account Security,AD Delegation y AD Infraestructure Security.*

5.3 Componente 2: Plan de *hardening*

5.3.1 Prerrequisitos del entorno

Esta guía está diseñada para aplicarse en entornos de Directorio Activo *on-premise* sobre Windows Server 2016 o superior. Antes de realizar cualquier control o script, compruebe que el entorno cumple con los siguientes requisitos:

5.3.2 Prerrequisitos de Infraestructura

Requisito	Detalle
Sistema operativo del Directorio Activo	Windows Server 2016 en adelante (Standard o Datacenter)
Rol Instalado	Active Directory Domain Services (AD DS)
Nivel Funcional del dominio	Windows Server 2016 o superior (recomendado 2019)
Versión de PowerShell	5.1 o superior
.NET Framework	4.7.2 o superior
Módulo de PowerShell AD	Directorio Activo (parte de RSAT)
Acceso administrativo	Cuenta con privilegios de Domain Admin

Virtualización (para Credential Guard)	UEFI + Secure Boot + Hyper-V habilitado
Conectividad de red	LDAP (389/636), RPC entre DC y estación de admin
Espacio en disco (Wazuh)	Mínimo 50 GB libres en el servidor de Wazuh

Tabla 2 Prerrequisitos de Infraestructura

5.3.3 Prerrequisitos de Herramientas

Herramienta	Versión Recomendada	Cómo obtenerla
Purple Knight	5.0 Community Edition	https://www.semperis.com/purple-knight/ (registro gratuito)
Wazuh	4.7 o superior	https://wazuh.com/install/ (open source)
Sysmon	v15 o superior	https://learn.microsoft.com/sysinternals/downloads/sysmon
Sysmon config (base)	SwiftOnSecurity template	https://github.com/SwiftOnSecurity/sysmon-config
GPMC	Incluida en Windows Server 2019	Herramientas administrativas del servidor
RSAT (desde estación de admin)	Incluido en Windows 10/11	Configuración > Aplicaciones > Características opcionales

Tabla 3 Prerrequisitos de Herramientas

5.3.4 Prerrequisitos de Conocimiento

Esta guía asume que el lector posee conocimientos en las siguientes áreas. No es necesario ser experto, pero si tener experiencia práctica.

- **Administración de Directorio Activo:** creación y administración de usuarios, grupos, GPO´s y unidades organizativas.
- **PowerShell:** ejecución de scripts y cmdlets básicos.
- **Editor de directivas de grupo:** creación, vinculación y edición de GPO´s.
- **Conceptos básicos de seguridad:** manejo de términos como autenticación, privilegios, tokens y protocolos de red (NTLM, Kerberos).

Recomendación antes de comenzar: realice un *snapshot* o backup completo del controlador de dominio antes de aplicar cualquier control de esta guía. Aunque todos los cambios han sido diseñados para no interrumpir la operación, contar con un punto de restauración es una buena práctica.

5.3.5 Propósito

Esta guía define los controles técnicos de *hardening* y las estrategias de monitoreo continuo para entornos de Directorio Activo *on-premise* sobre Windows Server 2019 en adelante. Su objetivo es mitigar cinco técnicas de ataque de alto impacto catalogadas en el marco de MITRE ATT&CK, reduciendo la superficie de exposición y habilitando la detección temprana de actividad maliciosa.

5.3.6 Alcance

Dentro del alcance están incluidos: Entornos de Directorio Activo on-premise con Windows Server 2016 en adelante como controlador de dominio. Cinco técnicas de MITRE ATT&CK (ver Sección 2). Controles de seguridad basados en CIS Security y Template de Microsoft. Eventos de auditoría y detección asociados a cada técnica.

5.3.7 Técnicas de MITRE ATT&CK

Las siguientes cinco técnicas de MITRE ATT&CK en las que se fundamenta esta guía de *hardening* fueron seleccionadas debido a su alto impacto en entornos de Directorio Activo on-premise, su relevancia comprobada en campañas reales y la disponibilidad de controles de mitigación concretos y aplicables.

A continuación, se describen estas cinco técnicas, junto con sus vectores de explotación más comunes.

5.3.7.1 T1078.002 Valid Accounts: Domain Accounts

Atributo	Detalle
Táctica	Acceso Inicial / Persistencia / Escalada de Privilegios / Evasión de Defensas
Sub-tactica	T1078.002 – Domain Accounts
Plataforma	Windows – Directorio Activo
Técnica sombrilla	T1098 Account Manipulation
Impacto en Directorio Activo	Crítico

Tabla 4 T1078.002 Valid Accounts: Domain Accounts

Descripción

Los adversarios pueden obtener y abusar de las credenciales de una cuenta de dominio legítimas para evadir controles de seguridad y mantener la persistencia. A diferencia de crear nuevas cuentas, el uso de credenciales válidas evita crear alertas con la creación de objetos nuevos, los adversarios pueden comprometer las cuentas de dominio por diversos métodos como el volcado de credenciales del sistema o la reutilización de contraseñas. La técnica también cubre la manipulación de cuentas existentes(T1098): modificación de pertenencia a grupos privilegiados y cambio de atributos a cuentas como AdminSDHolder, SIDHistory, userAccountControl), y reinicio de contraseñas.

Vectores de explotación más comunes

- *Credential dumping* mediante Mimikatz sobre LSASS (Pass-the-Hash, Pass-the-ticket).
- Kerberoasting / AS-REP Roasting para extraer y cracker hashes de cuentas de servicio.
- *Phishing* con credenciales capturadas para inicio de sesión directo.
- Modificación de membresía en grupos privilegiados (Domain Admins, Schema Admins).
- Abuso de SIDHistory para escalar privilegios entre dominios.

5.3.7.2 T1484.002: Domain Policy Modification.

Atributo	Detalle
Táctica	Escalada de Privilegios / Evasión de Defensas
Sub-tactica	T1484.002 – Domain Trust Modification
Plataforma	Windows – Directorio Activo
Impacto en Directorio Activo	Crítico

Tabla 5 T1484.002: Domain Policy Modification

Descripción

Los adversarios modifican las políticas de dominio, principalmente las directivas de grupo y las relaciones de confianza entre dominios, para escalar privilegios o evadir controles de seguridad. Una GPO maliciosa puede afectar a todos los equipos y usuarios del dominio simultáneamente. El abuso de configuraciones de confianza entre dominios para obtener acceso no autorizado y control ampliado sobre recursos críticos.

Vectores de explotación más comunes

- Modificación de grupo de políticas para deshabilitar antivirus, habilitar RDP, agregar usuarios locales o ejecutar scripts maliciosos al inicio.
- Creación de confianzas de dominio no autorizados para persistencia entre bosques.

Abuso de permisos excesivos sobre SYSVOL y NETLOGON para inyectar scripts.

- Ataque de GPO *delegation*: explotación de permisos de escritura delegados en grupo de políticas específicas.

5.3.7.3 T1134.001: Token Impersonation/Theft.

Atributo	Detalle
Táctica	Escalada de Privilegios / Evasión de Defensas
Sub-tactica	T1134.001 – Token Impersonation/Thef
Plataforma	Windows
Impacto en Directorio Activo	Alto

Tabla 6 T1134.001: Token Impersonation/Theft

Descripción

Windows utiliza tokens de acceso para representar el contexto de seguridad de procesos e hilos. Los adversarios pueden duplicar y luego suplantar el token existente de otro usuario o proceso que corre bajo cuentas privilegiadas incluyendo SYSTEM o Domain Admin, usando funciones de la API de Windows como DuplicateToken o Duplicate TokenEx, una vez obtenido el toker puede utilizarse con ImpersonateLoggedOnUser o con SetThreadToken para asignar el token suplantado a un hilo cuando tiene un proceso especifico ya existente donde se desea asignar, y puede ser utilizado cuando el usuario objetivo tiene una sesión de inicio no relaciona con la red en el sistema.

Vectores de explotación más comunes

- Robo de *token* de proceso de SYSTEM mediante inyección de código en servicios del sistema.
- Incognito /*Meterpreter token impersonation*: listado y uso de *tokens* disponibles en memoria.
- Abuso de SeImpersonatePrivilege (privilegio de escalación mediante *Potato attacks*: JuicyPotate, SweetPotato).
- Impersonación de tokens de administradores de dominio en sesiones activas en el Directorio Activo.

5.3.7.4 T1547.002: Boot or Logon Autostart Execution.

Atributo	Detalle
Táctica	Persistencia / Escalada de Privilegios
Sub-tactica	T1547.002 – Authentication Package
Plataforma	Windows
Impacto en Directorio Activo	Alto

Tabla 7 Boot or Logon Autostart Execution

Descripción

Windows permite registrar paquetes de autenticación personalizados por medio de la clave de registro HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages. Cuando el sistema inicia, el subsistema LSASS carga automáticamente estas DLLs en su espacio de proceso, que corren con privilegios de SYSTEM. Un adversario puede modificar el registro para que Windows cargue una DLL maliciosa dentro del proceso LSA cada vez que el sistema arranca, lo que permite mantener acceso persistente y potencialmente con altos privilegios.

Vectores de explotación más comunes

- Registro de DLL maliciosa como *authentication package* para capturar credenciales al inicio de sesión.
- Modificación de Security Package list para inyectar código en LSASS al arranque.
- Combinación con T1574.001 para usar DLL *side-loading* como mecanismo de carga del paquete malicioso.

5.3.7.5 T1574.001: Hijack Execution Flow – DLL Side-Loading.

Atributo	Detalle
Táctica	Persistencia/ Escalada de Privilegios
Sub-tactica	T1574.001 – DLL Side-Loading
Plataforma	Windows
Impacto en Directorio Activo	Alto

Tabla 8 Hijack Execution Flow – DLL Side-Loading

Descripción

Los adversarios pueden abusar de los archivos de biblioteca de enlace dinámico (DLL), colocando una DLL maliciosa con el nombre de una legítima en un directorio de mayor prioridad. Cuando una aplicación carga una DLL sin especificar su ruta, Windows busca primero en el directorio del ejecutable, luego en System32, entre otros, permitiéndole ejecutar código malicioso disfrazado dentro de un proceso confiable.

Vectores de explotación más comunes

- Colocación de DLL maliciosa en el directorio de instalación de una aplicación firmada (por ejemplo, antivirus)
- Abuso de aplicaciones con manifiestos de activación COM que cargan DLLs sin ruta absoluta.

- Persistencia mediante colocación de DLL maliciosa que se carga con cada inicio de la aplicación objetivo. Evasión de EDR/AV: el código malicioso corre bajo el proceso padre legítimo, evitando firmas por bloqueo.

5.4 Recomendaciones de *Hardening*

Esta sección detalla la implementación de cada control de *hardening*, organizada por área técnica indicando para cada uno la técnica de MITRE ATT&CK que mitigan y la configuración recomendada. Esta guía se fundamenta en CIS Benchmark para Windows y en la plantilla de seguridad de Microsoft, el cual contiene 181 controles organizados en siete categorías de políticas.

5.4.1 Controles de Gestión de Cuentas y Credenciales

Técnica mitigada: T1078.002 – Valid Accounts: Domain Accounts (incluye aspectos de T1098)

5.4.1.1 Política de contraseñas

Las configuraciones de políticas de contraseñas y de bloqueo de cuentas se deben aplicar mediante la GPO Default Domain Policy para que tengan un efecto global en las cuentas de usuario de dominio como comportamiento predeterminado. (CIS,2023)

Se configura en: ***Configuración del equipo > Configuración de Windows> Configuración de seguridad > Directivas de cuenta > Directiva de contraseñas***.

Configuración	Valor requerido	Valor por defecto	Justificación
Almacenar contraseñas con cifrado reversible	Deshabilitado	Deshabilitado	Impide reutilización luego de que una cuenta fue comprometida
Exigir historial de contraseñas	24	1	Limita la ventana de uso de una credencial comprometida
La contraseña debe cumplir los requisitos de complejidad	Habilitado	Habilitado	Exige uso de mayúsculas, minúsculas, números y símbolos
Longitud mínima de la contraseña	15	1	Aumenta la resistencia de crackeo offline de hashes NTLM
Vigencia máxima de la contraseña	60 días	42 días	Limita la ventana de uso de credenciales comprometidas
Vigencia mínima de la contraseña	1 día	0	Impide evasión del historial cambiando contraseñas repetidamente.

Tabla 9 Política de contraseñas

5.4.1.2 Política de bloqueo de cuentas

Se configura en: ***Configuración del equipo > Configuración de Windows> Configuración de seguridad > Directivas de cuenta > Directiva de bloqueo de cuenta***.

Configuración	Valor requerido	Valor por defecto	Justificación
Duración del bloqueo de cuenta	15 minutos	15 minutos	Impide intentos continuos de ingreso de contraseña tras bloqueo automático.
Permitir bloqueo de cuenta de administrador	Habilitado	Habilitado	Reduce la probabilidad de un ataque de fuerza bruta sobre la cuenta de administrador integrada al dominio
Restablecer el bloqueo de cuenta después de	15 minutos	15 minutos	Reinicia el contador tras periodo de observación
Umbral de bloqueo de cuenta	10 intentos	10 intentos	Reduce la probabilidad de éxito de un ataque de fuerza bruta sobre cuentas del dominio

Tabla 10 Política de bloqueo de cuentas

5.4.1.3 Fine-Grained Password Policy para cuentas privilegiadas

La Fine-Grained Password Policies (FGPP) permiten aplicar políticas más estrictas a grupos específicos sin afectar la política general del dominio. Se configura una FGPP para el grupo Administradores del dominio**.**

Nota: Con el fin de no aplicar directamente la política sobre el grupo Administradores del dominio se recomienda crear un grupo especial para administradores protegidos como por ejemplo: PSO-Tier0-Admins.

```
# Crear FGPP para Domain Admins (ejecutar con privilegios de Domain Admin)
New-ADFineGrainedPasswordPolicy  -Name "PSO-Tier0-Admins"
-Precedence 1 # Prioridad entre políticas
-MinPasswordLength 25 # Longitud mínima de la contraseña
-PasswordHistoryCount 24 # Historial de la contraseña
-MaxPasswordAge (New-TimeSpan -Days 30) # Vigencia máxima de la contraseña
```

```
-MinPasswordAge (New-TimeSpan -Days 1) # Vigencia mínima de la contraseña

-ComplexityEnabled $true # La contraseña debe cumplir los requisitos de complejidad

-ReversibleEncryptionEnabled $false # Almacenar contraseñas con cifrado reversible

-LockoutThreshold 3 # Umbral de bloqueo de cuenta

-LockoutDuration (New-TimeSpan -Minutes 30) # Duración del bloqueo de cuenta

-LockoutObservationWindow (New-TimeSpan -Minutes 30) #Restablecer el bloqueo de cuenta después de 30 min


#Aplicar la política al grupo PSO-TIER0-Admins

Add-ADFineGrainedPasswordPolicySubject

-Identity "PSO-Tier0-Admins"

-Subjects "Domain Admins"

# Verificar

Get-ADFineGrainedPasswordPolicy -Identity 'PSO-Tier0-Admins'
```

5.4.1.4 Rotación periódica de la cuenta KRBTGT

La cuenta KRBTGT es utilizada por el servicio de Kerberos para generar Ticket Granting Tickets (TGT) en el dominio. Su compromiso permita la fabricación de Golden Tickets, garantizando al adversario acceso ilimitado al dominio.

Se recomienda lo siguiente:

- Rotar la contraseña al menos cada 180 días
- Siempre después de un incidente de seguridad
- La rotación debe ejecutarse dos veces con un intervalo mínimo de 10 horas para invalidar todos los *tickets* existentes

Nota: este procedimiento se debe realizar manualmente

```
# Verificar edad de contraseña KRBTGT

$krbtgt = Get-ADUser krbtgt -Properties PasswordLastSet

$dias = (New-TimeSpan -Start $krbtgt.PasswordLastSet -End (Get-Date)).Days

Write-Host "Dias desde ultima rotacion KRBTGT: $dias"


# RECOMENDACIÓN: Antes de rotar, valida replicación con repadmin/dcdiag (manual)
```

```
Write-Host "Recomendado antes de rotar: ejecutar 'repadmin /replsummary' y 'dcdiag /test:replications' en un DC." -ForegroundColor Yellow

Write-Host ""


# Rotar contraseña (ejecutar DOS VECES con intervalo de 10+ horas)

Set-ADAccountPassword -Identity krbtgt -Reset `

   -NewPassword (ConvertTo-SecureString -AsPlainText ([System.Web.Security.Membership]::GeneratePassword(32,8)) -Force)

Write-Host 'Primera rotacion completada. Repetir en 10-12 horas.'
```

5.4.2 Controles de Protección de Credenciales y Privilegios

Técnicas mitigadas: T1078.002, T1134.002, T1547.002

5.4.2.1 LSA Protection (RunAsPPL)

La Protección de LSA configura el proceso LSASS como un Proceso Protegido Ligero (Protected Process Light), este proceso es responsable de autenticación de usuarios, gestión de credenciales, manejo de tokens de acceso. Se recomienda la habilitación de este protocolo con el fin de impedir que herramientas como Mimikatz lean la memoria o inyecten código en él, además de fortalecer la protección de credenciales almacenadas en memoria.

Se configura en: ***Configuración del equipo > Preferencias> Configuración de windows> Registro***

Ruta del registro	Valor	Tipo	Valor requerido	Acción
HKLM\SYSTEM\CurrentControlSet\Control\Lsa	RunAsPPL	REG_DWORD	1	Actualización
HKLM\SYSTEM\CurrentControlSet\Control\Lsa	RunAsPPL	REG_DWORD	1	Actualización

Tabla 11 LSA Protection (RunAsPPL)

5.4.2.2 Deshabilitar WDigest

WDigest es un proveedor de autenticación obsoleto que almacena contraseñas en texto plano, lo que puede exponerla a riesgos de robo de credenciales, ya que el proceso Lsass.exe mantiene una copia de la contraseña del usuario. Evitar el almacenamiento de credenciales en texto plano en memoria ayuda a reducir la probabilidad de que un adversario pueda robar las credenciales de un usuario.

Se configura en: ***Configuración del equipo > Preferencias> Configuración de windows> Registro***

Ruta del registro	Valor	Tipo	Valor requerido	Acción
HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest	UseLogonCredential	REG_DWORD	0	Actualización

Tabla 12 Deshabilitar WDigest

5.4.2.3 Forzar NTLMv2 y deshabilitar protocolos obsoletos

Los protocolos de LM y NTLM presentan vulnerabilidades criptográficas conocidas y que pueden ser explotadas por adversarios para obtener o reutilizar credenciales de autenticación. Por eso la configuración de NTMLv2 fortalece el mecanismo de autenticación, ya que incorpora protocolos de mejoras de seguridad, pero si hay sistemas obsoletos se corre el riesgo que no puedan autenticar.

Se configura en: ***Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad:***

Configuración	Valor requerido
Seguridad de red: nivel de autenticación de LAN Manager	Enviar solo respuestas NTLMv2. Rechazar LM y NTLM
Seguridad de red: seguridad de sesión mínima para clientes NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2 Requerir cifrado de 128 bits
Seguridad de red: seguridad de sesión mínima para servidores NTLM basados en SSP (incluida RPC segura)	Requerir seguridad de sesión NTLMv2 Requerir cifrado de 128 bits
Seguridad de red: no almacenar valor de hash de LAN Manager en el próximo cambio de contraseña	Habilitada
Seguridad de red: permitir retroceso a sesión NULL de LocalSystem	Deshabilitada
Seguridad de red: restringir NTLM: tráfico NTLM saliente hacia servidores remotos	Denegar todo
Seguridad de red: restringir NTLM: autenticación NTLM en este dominio	Denegar servidores de dominio

Tabla 13 Forzar NTLMv2 y deshabilitar protocolos obsoletos

5.4.2.4 Derechos de usuario

Los siguientes derechos son críticos para mitigar T1134.002. Se configuran en ***Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Asignación de derechos de usuario:***

Derecho de usuario	Servidor Miembro	Controlador de Dominio	Explicación
Crear un objeto token	Ninguno	Ninguno	Asignar este derecho de usuario puede suponer un riesgo para la seguridad. No asigne este derecho a ningún usuario, grupo o proceso que no desee que tome posesión del sistema.
Actuar como parte del sistema operativo	Ninguno	Ninguno	Asignar este derecho de usuario puede constituir un riesgo para la seguridad. Asigne este derecho de usuario únicamente a usuarios de confianza.
Suplantar a un cliente tras la autenticación	Administradores, Local Service, Network Service, Service, IIS_IUSRS	Administradores, Local Service, Network Service, Service, IIS_IUSRS	Esta política permite que un usuario o programa actué con los permisos de un usuario que se conectó. Estos permisos deben ser exclusivamente de los valores agregados en la columna de Servidor Miembro y Controlador de Dominio.
Depurar programas	Solo Administradores	Solo Administradores	Este derecho de usuario determina qué usuarios pueden adjuntar un depurador a cualquier proceso o al kernel. Los programadores que depuran sus propias aplicaciones no necesitan que se les asigne este derecho de usuario.
Habilitar confianza con el equipo y las cuentas de	No asignado(vacío)	Solo administradores	Esta configuración de seguridad determina qué usuarios pueden establecer la

usuario para delegación			configuración Se confía para delegación en un objeto de equipo o usuario.
Bloquear páginas en la memoria	No asignado(vacío)	No asignado(vacío)	Esta configuración de seguridad determina qué cuentas puede usar un proceso para mantener datos en la memoria física, lo que impide al sistema paginar los datos en la memoria virtual del disco
Cargar y descargar controladores de dispositivo	Solo Administradores	Administradores, Opers. De Impresión	Este derecho de usuario determina qué usuarios pueden cargar y descargar dinámicamente controladores de dispositivo u otro código en modo kernel
Permitir el Inicio de sesión local	Administradores, Operadores de copia de seguridad	Administradores, Operadores de copia de seguridad	Determina los usuarios que pueden iniciar sesión en el equipo.
Permitir inicio de sesión a través de Servicios de Escritorio remoto	No configurado	Solo Administradores	Esta configuración de seguridad determina qué usuarios o grupos tienen permiso para iniciar sesión como un cliente de Servicios de Escritorio remoto.

Tabla 14 Derechos de usuario

5.4.2.5 Grupo de usuarios protegidos

El grupo de usuarios protegidos global a nivel de Directo Activo se utiliza para proteger contra ataques del robo de credenciales, aplicando automáticamente restricciones adicionales a sus miembros como: no autenticarse con NTLM, CreSSP ni Digest, sus tickets Kerberos no son renovables y no pueden utilizar delegación Kerberos no restringida.

Por medio de powershell podemos agregar todas las cuentas privilegiadas:

```
# Agregar cuentas privilegiadas al grupo Protected Users
Add-ADGroupMember -Identity 'Protected Users' -Members 'AdminDA1','AdminDA2'


# Verificar membresía
Get-ADGroupMember -Identity 'Protected Users' | Select-Object Name, SamAccountName
# ADVERTENCIA: Verificar compatibilidad de aplicaciones antes de agregar
```

cuentas de servicio, ya que no pueden usar NTLM ni delegacion Kerberos

O también buscamos el grupo en el Directorio Activo ***Contralos de dominio> Users> Protected Users > Miembros > Agregar***

Nota: antes de implementar es necesario auditar si alguna cuenta candidata a estar en el grupo de usuarios protegidos es utilizada por servicios que dependen de NTLM, CredSSP, delegación de Kerberos no restringida o autenticación Digest, dado que su incorporación al grupo puede causar interrupciones. Antes de agregar al grupo identificar las cuentas de servicios activos por medio del siguiente comando de powershell : Get-ADUser-Filter(ServicePrincipalName -ne “$null”) -Properties ServicePrincipalName

Opción de seguridad	Valor requerido	Explicación
Controlador de dominio: requisitos de firma de servidor LDAP	Requiere firma	Esta configuración de seguridad determina si el servidor LDAP requiere que la firma se negocie con clientes LDAP.
Controlador de dominio: requisitos del token de enlace de canal del servidor LDAP	Siempre	Esta configuración de seguridad determina si el servidor LDAP aplica la validación de los tokens de enlace de canal recibidos en las solicitudes de enlace LDAP que se envían a través de conexiones LDAPS.
Cliente de red de Microsoft: firma digital de comunicaciones (siempre)	Habilitada	Esta configuración de seguridad determina si el componente SMB de cliente debe solicitar la firma de paquetes. El protocolo Bloque de mensajes de servidor (SMB) te proporciona las bases para el uso compartido de archivos e impresoras, así como para otras operaciones de red como, por ejemplo, la administración remota de Windows.
Servidor de red de Microsoft: firma digital de comunicaciones (siempre)	Habilitada	Esta configuración de seguridad determina si la firma de paquetes es necesaria de acuerdo con el componente del servidor SMB. El protocolo Bloque de mensajes de servidor (SMB) te proporciona las bases para el uso compartido de archivos e impresoras, así como para otras operaciones de red como, por ejemplo, la

		administración remota de Windows.
Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en modo de protección con privilegios mejorados	Pedir credenciales en el escritorio segur	Esta configuración de seguridad controla el comportamiento de la petición de elevación para los administradores.
Control de cuentas de usuario: comportamiento de la petición de elevación para los administradores en modo de protección con privilegios mejorados	Habilitada	Esta configuración de directiva controla el comportamiento de la petición de elevación para los administradores que se ejecutan en el modo de protección con privilegios mejorados.
Control de cuentas de usuario: comportamiento de la petición de elevación para los usuarios estándar	Rechazar solicitudes de elevación automáticamente	Esta configuración de directiva controla el comportamiento de la petición de elevación para los usuarios estándar.
Acceso de red: evitar que los clientes con permiso realicen llamadas remotas a SAM	O:BAG:BAD:(A;;RC;;;BA)	Esta configuración de directiva te permite restringir conexiones remotas de RPC a SAM. Si no la seleccionas, se usará el descriptor de seguridad predeterminado.
Inicio de sesión interactivo: límite de inactividad de equipo.	900	Windows detecta inactividad en una sesión de inicio de sesión y, si el tiempo de inactividad excede el límite de inactividad, se ejecutará el protector de pantalla y se bloqueará la sesión.
Cuentas: limitar el uso de cuentas locales con contraseña en blanco solo para iniciar sesión en la consola	Habilitada	Esta configuración de seguridad determina si las cuentas locales que no están protegidas mediante contraseña pueden usarse para iniciar sesión desde ubicaciones distintas de la consola física del equipo. Si se habilita, las cuentas locales que no están protegidas mediante contraseña solo podrán iniciar sesión desde el teclado del equipo.
Miembro de dominio: cifrar o firmar digitalmente datos de un canal seguro (siempre)	Habilitada	Esta configuración determina si todo el tráfico de canal seguro que inicia el miembro de dominio cumple los

		requisitos de seguridad mínimos. Más concretamente, determina si todo el tráfico de canal seguro que inicia el miembro de dominio debe firmarse o cifrarse.
Acceso a redes: no permitir enumeraciones anónimas de cuentas SAM	Habilitado	Esta configuración de seguridad determina los permisos adicionales que se concederán para las conexiones anónimas al equipo.

Tabla 15 Opciones de seguridad críticas

5.4.3.2 Auditoría de permisos sobre GPOs y SYSVOL

Realizar una auditoría de permisos sobre GPOs y SYSVOL es importante con el fin de detectar GPO que puedan ser modificadas por usuarios no autorizados, esto nos ayuda a identificar posibles vectores de escalamiento de privilegios, ya que al modificar una GPO se puede permitir ejecutar código malicioso en múltiples equipos.

El siguiente script nos ayuda identificar si existen usuarios no autorizados con permiso para modificar GPOs.

```
# Listar GPOs con permisos de escritura a no administradores
Get-GPO -All | ForEach-Object {
    $gpo   = $_
    $perms = Get-GPPermission -Guid $gpo.Id -All
    $write = $perms | Where-Object {
        $_.Permission -in 'GpoEdit','GpoEditDeleteModifySecurity'
    }
    if ($write) {
        Write-Output "GPO: $($gpo.DisplayName)"
        $write | Select-Object Trustee, Permission | Format-Table
    }
}
```

5.4.4 Controles de Flujo de Ejecución y DLL

Técnica mitigada: T1574.001 – Hijack Execution Flow: DLL Side-Loading

5.4.4.1SafeDLLSearchMode

SafeDLLSearchMode busca primero en las carpetas especificas en la ruta del sistema priorizando el directorio SYSTEM32, y luego en la carpeta de la ruta actual, lo que reduce la efectividad de un ataque de DLL side-loading:

Antes de aplicar la configuración de la gpo, por medio de powershell podemos verificar si este habilitado el SafeDLLSearchMode:

```
# Verificar y habilitar SafeDllSearchMode

Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager' -
Name SafeDllSearchMode
```

Se configura en ***Configuración del equipo > Preferencias> Configuración de windows> Registro***

Ruta del registro	Valor	Tipo	Valor requerido	Acción
HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager	SafeDllSearchMode	REG_DWORD	1	Actualización

Tabla 16 SafeDLLSearchMode

5.4.4.2 AppLocker en Controlador de Dominio

Con AppLocker se pueden crear reglas para permitir o denegar la ejecución de archivos como scripts, instaladores de Windows Installer o bibliotecas de enlace dinámico (DLL). Al principio se debe habilitar en modo de Auditoria por cuatro semanas para identificar bloqueos en aplicaciones legítimas antes de activar el modo Enforce.

Antes de configurar AppLocker es necesario habilitar el servicio de Identificación de Aplicación:

Se configura en ***Configuración del equipo > Configuración de Windows> Configuración de Seguridad > Servicios del sistema:***

Configuración	Valor requerido
Identificación de aplicación	☑ Definir esta configuración de directiva: Automático

Tabla 17 AppLocker en Controlador de Dominio

Si el servicio de Identificación de aplicación no está habilitado, las reglas de AppLocker no se aplicarán. Luego se configura la gpo de Applocker

Se configura en *Configuración del equipo > Configuración de Windows> Configuración de Seguridad > Directiva de control de aplicaciones>AppLocker:*

Configuración	Valor requerido
Reglas de ejecutables	Solo Auditoría
Reglas de Windows Installer	Solo Auditoría

Reglas de scripts	Solo Auditoría
Reglas de aplicaciones empaquetadas	Solo Auditoría

Tabla 18 Directiva de control de aplicaciones

Durante el periodo de auditoría el en visor de eventos se registrarán los eventos, que permiten identificar las aplicaciones que serían bloqueadas.

Visualización: ***Visor de eventos > Registro de Aplicaciones y servicios > Microsoft > Windows > AppLocker***

Configuración de reglas: ***Configuración del equipo > Configuración de Windows> Configuración de Seguridad > Directiva de control de aplicaciones>AppLocker > Reglas ejecutables > Crear una nueva regla***

5.5 Componente 3: Monitoreo Continuo con Wazuh

Wazuh es una plataforma de monitoreo que integra capacidades de SIEM, detección de intrusos, y cumplimiento normativo en una plataforma de código abierto, con soporte nativo para el marco MITRE ATT&CK. Sysmon actúa como un colector de telemetría avanzada a nivel de *kernel*, los eventos se reenvían a Wazuh a través del agente instalado en cada controlador de dominio.

5.5.1 Arquitectura de Monitoreo

Componente	Función
Agente Wazuh	Recolección de eventos configuraciones y logs del sistema.
Sysmon	Telemetría avanzada de procesos, red, carga de módulos y registros.
Servidor Wazuh	Correlación de eventos, gestión de reglas y alertas.
Dashboard Wazuh	Visualización de alertas, matrices, MITRE ATT&CK, y métricas.

Tabla 19 Arquitectura de Monitoreo

5.5.2 Configuración de Sysmon

Sysmon debe configurarse utilizando la plantilla SwiftOnSecurity, la misma se puede descargar en el siguiente enlace https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml y agregar las siguientes reglas que permitan capturar eventos relevantes para las técnicas T1134.002, T1547.002 y T1574.001.

Estas reglas deben agregarse dentro de la sección ***<EventFiltering>*** del archivo de configuración de Sysmon.

5.5.2.1 Acceso a procesos sensibles (T1134.002)

Esta regla permite detectar procesos que intentan acceder a LSASS, lo cual puede indicar un intento de manipulación o extracción de token o credenciales.

```
<!-- T1134.002 - Acceso a LSASS -->
<RuleGroup name="T1134002-TokenManipulation" groupRelation="or">
  <ProcessAccess onmatch="include">
    <TargetImage condition="is">C:\Windows\System32\lsass.exe</TargetImage>
  </ProcessAccess>
</RuleGroup>
```

5.5.2.2 Creación de procesos con privilegios elevados (T1134.002)

Esta regla registra procesos creados con nivel de integridad SYSTEM, lo puede indicar un escalamiento de privilegios.

```
<!-- T1134.002 – Procesos con nivel SYSTEM -->
<RuleGroup name="T1134002-SystemProcess" groupRelation="or">
  <ProcessAccess onmatch="include">
    <IntegrityLevel condition="is">System</IntegrityLevel>
  </ProcessAccess>
</RuleGroup>
```

5.5.2.3 Authentication Packages en LSASS (T1547.002)

Esta regla permite identificar la carga de bibliotecas dinámicas en el proceso LSASS, lo cual puede indicar la instalación de paquetes de autenticación maliciosos.

```
<!-- T1547.002 – Monitoreo de DLL cargadas por LSASS-->
<RuleGroup name="T1547002-AuthPkg" groupRelation="or">
  <ImageLoad onmatch="include">
    <Image condition="is">C:\Windows\System32\lsass.exe</Image>
  </ImageLoad>
</RuleGroup>
```

Las siguientes claves de registro se utilizan para registrar *authentication packages* y *security packages*, las cuales pueden ser utilizadas para persistencia o robo de credenciales.

```
<!-- T1547.002 - Cambios en claves LSA -->
<RuleGroup name="LSA-Registry" groupRelation="or">
```

```
  <RegistryEvent onmatch="include">
    <TargetObject condition="contains">\Control\Lsa\Authentication
Packages</TargetObject>
  </RegistryEvent>
  <RegistryEvent onmatch="include">
    <TargetObject condition="contains">\Control\Lsa\Security Packages</TargetObject>
  </RegistryEvent>
  <RegistryEvent onmatch="include">
    <TargetObject condition="contains">\Control\Lsa\Notification Packages</TargetObject>
  </RegistryEvent>
</RuleGroup>
```

5.5.2.4 DLL potencialmente maliciosas (T1574.001)

Esta regla detecta la carga de DLL no firmadas, lo que puede indicar intentos de DLL search orden hijacking o sideloading.

```
<!-- T1574.001 – DLL no firmadas cargadas por procesos-->
<RuleGroup name="T1547001-DLLSideLoad" groupRelation="or">
  <ImageLoad onmatch="include">
    <Signed condition="is">false</Signed>
  </ImageLoad>
</RuleGroup>
```

5.5.3 Configuración del Agente de Wazuh para recolección de eventos

La configuración del agente de Wazuh se realiza en el archivo ossec.conf que se instala en el controlador de dominio.

Wazuh tiene niveles de alerta que clasifican la gravedad de los eventos que va del más bajo (0) al máximo (16), estos niveles son:

Nivel	Título	Descripción
0	Ignorado	Sin acción. Se usa para evitar falsos positivos. Estas reglas se analizan antes que todas las demás, incluyen eventos sin relevancia de seguridad y no aparecen en el panel de eventos de seguridad.

2	Notificación de baja prioridad del sistema	Mensajes de notificación o estado del sistema. No tienen relevancia de seguridad y no aparecen en el panel de eventos de seguridad.
3	Eventos exitosos / autorizados	Incluye intentos de inicio de sesión exitosos, eventos de permiso en el firewall, etc.
4	Error de baja prioridad del sistema	Errores relacionados con configuraciones incorrectas o dispositivos/aplicaciones no utilizadas. No tienen relevancia de seguridad y generalmente son causados por instalaciones predeterminadas o pruebas de software.
5	Error generado por el usuario	Incluye contraseñas incorrectas, acciones denegadas, etc. Por sí solos, no tienen relevancia de seguridad.
6	Ataque de baja relevancia	Indica un gusano o virus que no tiene efecto en el sistema (como Code Red para servidores Apache, etc.). También incluye eventos frecuentes de IDS y errores frecuentes.
7	Coincidencia de "palabras clave"	Incluye palabras como "bad", "error", etc. Estos eventos en su mayoría no están clasificados y pueden tener cierta relevancia de seguridad.
8	Visto por primera vez	Incluye eventos detectados por primera vez: la primera vez que se dispara un evento de IDS o que un usuario inicia sesión. También incluye acciones con relevancia de seguridad como la activación de un sniffer o actividades similares.
9	Error desde origen inválido	Incluye intentos de inicio de sesión con usuario desconocido o desde un origen inválido. Puede tener relevancia de seguridad (especialmente si se repite). También incluye errores relacionados con la cuenta de administrador (root).
10	Múltiples errores generados por el usuario	Incluye múltiples contraseñas incorrectas, múltiples inicios de sesión fallidos, etc. Puede indicar un ataque o simplemente que el usuario olvidó sus credenciales.
11	Advertencia de verificación de integridad	Incluye mensajes sobre modificación de binarios o presencia de *rootkits* (mediante Rootcheck). Puede indicar un ataque exitoso. También incluye eventos de IDS que serán ignorados por alta repetición.
12	Evento de alta importancia	Incluye mensajes de error o advertencia del sistema, kernel, etc. Puede indicar un ataque contra una aplicación específica.
13	Error inusual (alta importancia)	En la mayoría de los casos coincide con un patrón de ataque conocido.

14	Evento de seguridad de alta importancia	Se dispara generalmente mediante correlación e indica un ataque.
15	Ataque severo	Sin posibilidad de falsos positivos. Requiere atención inmediata.

Tabla 20 Wazuh. (s. f.). Rules classification - Rules · Wazuh documentation. https://documentation.wazuh.com/current/user-manual/ruleset/rules/rules-classification.html

5.5.3.1 T1078.002 – Valid Accounts: Domain Accounts

ID del Evento	Canal	Descripción	Indicador de comportamiento anómalo
4624	Seguridad	Inicio de sesión exitoso	Inicio de sesión tipo 3 *network* fuera de horario o desde IPs inusuales.
4625	Seguridad	Inicio de sesión fallido	Más de 5 intentos fallidos consecutivos para la misma cuenta en menos de 5 minutos.
4648	Seguridad	Inicio de sesión con credenciales explícitas	Utilización de runas o técnica de pass-the-hash desde cuentas no administradas.
4672	Seguridad	Privilegios especiales asignados al inicio de sesión	Cuenta estándar con privilegios sensibles.
4728	Seguridad	Miembro agregado a un grupo global de seguridad	Incorporación al grupo Administradores de dominio fuera de una ventana de mantenimiento.
4740	Seguridad	Cuenta de usuario bloqueada	Patrón de bloqueos repetitivos en múltiples cuentas.
4768	Seguridad	Solicitud de ticket Kerberos (TGT)	Solicitudes masivas desde un mismo origen.
4769	Seguridad	Solicitud de ticket de servicio Kerberos	Tipo de cifrado 0x17 (RC4)
4776	Seguridad	Validación de credenciales NTLM en Controlador de Dominio	Autenticación NTLM desde un controlador de Dominio hacia sí mismo.

Tabla 21 T1078.002 – Valid Accounts: Domain Accounts

5.5.3.1.1 Regla 100010 – Evento ID 4624: Inicio de Sesión tipo 3

Identifica los inicios de sesión exitosos de tipo Network 3.

```
<! -- Regla 100010: Evento 4624 - Inicio de sesión exitoso tipo 3 -->
<rule id="100010" level="7">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4624$</field>
```

```
  <field name="win.eventdata.logonType">^3$</field>
  <description>Evento 4624 - Inicio de sesion exitoso tipo 3 (Network) para
    $(win.eventdata.targetUserName) desde $(win.eventdata.ipAddress)</description>
  <group>authentication_success,windows,ad_hardening,</group>
</rule>
<! -- Regla 100010: Evento 4624 - Inicio de sesión exitoso tipo 3 -->
<rule id="100010" level="7">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4624$</field>
  <field name="win.eventdata.logonType">^3$</field>
```

5.5.3.1.2 Regla 100011 – Evento ID 4625: Posible Fuerza bruta

Detecta posibles ataques de fuerza bruta ejemplo 5 fallos de autenticación para la misma cuenta en menos de 2 minutos.

```
<! -- Regla 100011: Evento 4625 - Fuerza bruta: 5 fallos en 2 minutos para la misma cuenta -
->
<rule id="100011" level="10" frequency="5" timeframe="120" ignore="60">
  <if_matched_sid>60122</if_matched_sid>
  <same_field>win.eventdata.targetUserName</same_field>
  <description>Evento 4625 - Posible fuerza bruta contra $(win.eventdata.targetUserName)
    desde $(win.eventdata.ipAddress)</description>
  <mitre>
    <id>T1078.002</id>
  </mitre>
  <group>authentication_failed,bruteforce,windows,ad_hardening,</group>
</rule>
```

5.5.3.1.3 Regla 100012 – Evento ID 4648: Uso de credenciales explicitas

Identifica el uso de credenciales explicitas mediante un Runas.

```
<! -- Regla 100012: Evento 4648 - Uso de credenciales explicitas -->
<rule id="100012" level="8">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4648$</field>
```

```
  <description>Evento 4648 - Uso de credenciales explicitas por
$(win.eventdata.subjectUserName)
    hacia $(win.eventdata.targetUserName)</description>
  <group>explicit_credentials,windows,ad_hardening,</group>
</rule>
```

5.5.3.1.4 Regla 100013 – Evento ID 4672: Privilegios Especiales Asignados

Identifica la asignación de privilegios especiales al momento de inicio de sesión.

```
<! -- Regla 100013: Evento 4672 - Privilegios especiales asignados -->
<rule id="100013" level="9">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4672$</field>
  <description>Evento 4672 - Privilegios especiales asignados al inicio de sesion
    para $(win.eventdata.subjectUserName)</description>
  <group>privilege_assigned,windows,ad_hardening,</group>
</rule>
```

5.5.3.1.5 Regla 100014 – Evento ID 4728: Asignación a Grupo privilegiado

Detecta cuando un usuario estándar es agregado a grupos de alto nivel, por ejemplo: Administrador de dominio, Administrador Enterprise o Administradores.

```
<! -- Regla 100014: Evento 4728 - Usuario agregado a grupo global privilegiado -->
<rule id="100014" level="12">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4728$</field>
  <field name="win.eventdata.targetUserName" type="pcre2">
    (?i)domain admins|enterprise admins|administrators
  </field>
  <description>Evento 4728 - Usuario $(win.eventdata.memberName) agregado a grupo
    privilegiado $(win.eventdata.targetUserName) por
$(win.eventdata.subjectUserName)</description>
  <mitre>
    <id>T1484.002</id>
  </mitre>
  <group>group_modification,privilege_escalation,windows,ad_hardening,</group>
</rule>
```

5.5.3.1.6 Regla 100015 – Evento ID 4740: Cuenta Bloqueada

Identifica bloqueos de cuentas en usuarios estándar.

```
<! -- Regla 100015: Evento 4740 - Cuenta bloqueada -->
<rule id="100015" level="8">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4740$</field>
  <description>Evento 4740 - Cuenta $(win.eventdata.targetUserName) bloqueada.
    Origen: $(win.eventdata.callerComputerName)</description>
  <group>account_lockout,windows,ad_hardening,</group>
</rule>
```

5.5.3.1.7 Regla 100016 – Evento ID 4740: Bloqueos Multiples desde el mismo origen

Escala la severidad cuando se producen 3 o más bloqueos desde el mismo origen en 5 minutos.

```
<! -- Regla 100016: Evento 4740 - Bloqueos múltiples en poco tiempo -->
<rule id="100016" level="10" frequency="3" timeframe="300">
  <if_matched_sid>100015</if_matched_sid>
  <same_field>win.eventdata.callerComputerName</same_field>
  <description>Evento 4740 - Multiples bloqueos de cuenta desde el mismo origen
    $(win.eventdata.callerComputerName)</description>
  <group>account_lockout,bruteforce,windows,ad_hardening,</group>
</rule>
```

5.5.3.1.8 Regla 100017 – Evento ID 4768: Solicitudes de TGT Repetidas

Identifica el volumen inusual de solicitudes de TGT desde una misma IP en menos de 2 minutos.

```
<! -- Regla 100017: Evento 4768 - Solicitudes TGT repetidas -->
<rule id="100017" level="8" frequency="10" timeframe="120">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4768$</field>
  <same_field>win.eventdata.ipAddress</same_field>
  <description>Evento 4768 - Volumen inusual de solicitudes TGT
    desde $(win.eventdata.ipAddress)</description>
  <group>kerberos_tgt,windows,ad_hardening,</group>
```

```
</rule>
```

5.5.3.1.9 Regla 100018 – Evento ID 4769: Posible Kerberoasting por RC4

Identifica solicitudes de tickets del servicio Kerberos con cifrado RC4.

```
<! -- Regla 100018: Evento 4769 - Posible Kerberoasting por RC4 -->
<rule id="100018" level="12">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4769$</field>
  <field name="win.eventdata.ticketEncryptionType">^0x17$</field>
  <field name="win.eventdata.serviceName" negate="yes">\$$</field>
  <description>Evento 4769 - Posible Kerberoasting: ticket RC4 para
    $(win.eventdata.serviceName)</description>
  <mitre>
    <id>T1558.003</id>
  </mitre>
  <group>kerberoasting,windows,ad_hardening,</group>
</rule>
```

5.5.3.1.10 Regla 100019 – Evento ID 4776: Validación NTLM

Detecta validaciones de credenciales mediante NTLM.

```
<! -- Regla 100019: Evento 4776 - Validación NTLM -->
<rule id="100019" level="9">
  <if_group>windows</if_group>
  <field name="win.system.eventID">^4776$</field>
  <description>Evento 4776 - Validacion NTLM para $(win.eventdata.targetUserName)
    desde $(win.eventdata.workstation)</description>
  <group>ntlm_authentication,windows,ad_hardening,</group>
</rule>
```

5.5.4.2 T1484.002 -Domain Policy Modification

ID del Evento	Canal	Descripción	Indicador de comportamiento anómalo
5136	Seguridad	Objeto del directorio activo modificado.	Modificación de atributos a los objetos del directorio activo.

5137	Seguridad	Creación de objeto del directorio activo.	Creación de objetos en directorio activo fuera de una ventana de mantenimiento.
5141	Seguridad	Objeto de directorio activo eliminado.	Eliminación de un grupo de política de seguridad crítica.
4719	Seguridad	Políticas de auditoría del sistema modificada.	Intentos de des habilitación de auditoría de eventos.
4739	Seguridad	Política de dominio modificada.	Intentos de modificación de políticas de contraseña o bloqueo de cuentas.
4704	Seguridad	Asignación de derecho de usuarios.	Asignación de privilegios elevados a cuentas no autorizadas.

Tabla 22 T1484.002 -Domain Policy Modification

5.5.4.2.1 Regla 100020 – Modificación de directivas de grupo o relación de confianza

Identifica cambios en objetos de tipo *groupPolicyContainer* o *trustDamain* en Directorio Activo. Incluyendo cambios a directivas de grupo (GPO), relación de confianza, políticas de auditoría y asignación de derechos de usuario.

```
<group name="windows,ad_hardening,policy_change">
<! -- Regla 100020: Modificación de GPO o relación de confianza -->
  <rule id="100020" level="12">
    <if_group>windows</if_group>
    <field name="win.system.eventID">^(5136|5137|5141)$</field>
    <field name="win.eventdata.objectClass">^(groupPolicyContainer|trustDomain)$</field>
    <description>T1484.002 - Modificacion de GPO o relacion de confianza
      detectada por $(win.eventdata.subjectUserName)</description>
    <mitre>
      <id>T1484.002</id>
    </mitre>
    <group>policy_change,ad_hardening,</group>
  </rule>
```

5.5.4.2.2 Regla 100021 – Modificación de Política de Auditoría

Detecta cambios en la política de auditoría del sistema relacionada con el evento ID 4719.

```
<! -- Regla 100021: Modificación de política de auditoría -->
  <rule id="100021" level="14">
    <if_group>windows</if_group>
    <field name="win.system.eventID">^4719$</field>
    <description>T1484.002 - Modificacion de politica de auditoria
```

```
    por $(win.eventdata.subjectUserName)</description>
   <mitre>
    <id>T1484.002</id>
   </mitre>
   <group>policy_change,ad_hardening,</group>
  </rule>
```

5.5.4.2.3 Regla 100022 – Modificación de Política de Dominio

Identifica cambios en la política de dominio como cambios a la política de contraseñas, bloqueo de cuentas o política de Kerberos.

```
  <! -- Regla 100022: Política de dominio modificada -->
  <rule id="100022" level="13">
   <if_group>windows</if_group>
   <field name="win.system.eventID">^4739$</field>
   <description>T1484.002 - Politica de dominio modificada
    por $(win.eventdata.subjectUserName)</description>
   <mitre>
    <id>T1484.002</id>
   </mitre>
   <group>policy_change,ad_hardening,</group>
  </rule>
```

5.5.4.2.4 Regla 100023 – Asignación de derechos de usuario

Detecta cuando se asigna un derecho de usuario a una cuenta estándar convirtiéndola en privilegiada

```
<! -- Regla 100023: Asignación de derechos de usuario -->
  <rule id="100023" level="13">
   <if_group>windows</if_group>
   <field name="win.system.eventID">^4704$</field>
   <description>T1484.002 - Asignacion de derecho de usuario
    por $(win.eventdata.subjectUserName)</description>
   <mitre>
    <id>T1484.002</id>
   </mitre>
   <group>policy_change,ad_hardening,</group>
  </rule>
```

```
</group>
```

5.5.5.3 T1134.002 – Token Impersonation/Theft

ID del Evento	Canal	Descripción	Indicador de comportamiento anómalo
4672	Seguridad	Privilegios asignados al nuevo inicio de sesión	SeImpersonatePrivilege o SeDebugPrivilege en cuentas no administrativas.
4673	Seguridad	Llamada a un servicio privilegiado	Uso de SeAssignPrimaryTokenPrivilege o SeCreateTokenPrivilege
4688	Seguridad	Creación de un nuevo proceso	Procesos en modo incognito.exe, tokenvator.exe o técnicas de Potato attacks
Sysmon 1	Microsoft-Windows-Sysmon/Operational	Creación de proceso	Proceso con IntegrityLevel = System creado por proceso de un usuario estándar
Sysmon 10	Microsoft-Windows-Sysmon/Operational	Acceso a un proceso	Acceso a memoria LSASS por procesos no autorizados

Tabla 23 T1134.002 – Token Impersonation/Theft

5.5.5.3.1 Regla 100024 – Sysmon10: Acceso a LSASS (Base)

Identificación de cualquier acceso a la memoria de LSASS por procesos fuera de la *whitelist* Nivel 10 como alerta base.

```
<! -- Regla base: acceso a LSASS por proceso no whitelisted -->
<rule id="100024" level="10">
  <if_group>windows</if_group>
  <field name="win.system.channel">Microsoft-Windows-Sysmon/Operational</field>
  <field name="win.system.eventID">^10$</field>
  <field name="win.eventdata.targetImage" type="pcre2">(?i)lsass\.exe</field>
  <!-- Whitelist: procesos legítimos que acceden a LSASS -->
  <field name="win.eventdata.sourceImage" negate="yes" type="pcre2">
    (?i)(MsMpEng|svchost|csrss|wininit|lsm|services|
        taskmgr|wmiprvse|perfmon|msiexec|
        SentinelAgent|CSFalconService|CylanceSvc|
        ArcticWolfAgent|Cortex)\\b
  </field>
  <description>T1134.002 - Acceso a LSASS por proceso no whitelisted:
```

```
    $(win.eventdata.sourceImage)</description>
  <mitre>
    <id>T1134.002</id>
  </mitre>
  <group>credential_access,windows,lsass_access</group> </rule>
```

5.5.5.3.2 Regla 100025 – Sysmon 10: Volcado de Memoria

Escala la severidad cuando el campo grantedAccess indica que permisos típicos de herramientas de volcado como Mimikatz.

```
<! -- Escala a crítico si grantedAccess indica volcado de memoria -->
<rule id="100025" level="15">
  <if_sid>100025</if_sid>
  <field name="win.eventdata.grantedAccess" type="pcre2">
    (?i)(0x1010|0x1410|0x1438|0x143a|0x1418|0x1fffff)
  </field>
  <description>T1134.002 CRITICO - Acceso a LSASS con permisos de volcado:
    $(win.eventdata.sourceImage)
    [Access: $(win.eventdata.grantedAccess)]</description>
  <mitre>
    <id>T1134.002</id>
  </mitre>
  <group>credential_access,windows,critical,ad_hardening</group>
</rule>
```

5.5.5.3.3 Regla 100026 – Sysmon 10: Correlación Temporal

Detecta cuando el mismo proceso accede a LSASS n cantidad de veces en un intervalo corto, secuencia recurrente de herramientas que realizan múltiples lecturas de memoria.

```
<! -- Correlación: mismo proceso accede a LSASS múltiples veces -->
<rule id="100026" level="15" timeframe="120" frequency="2">
  <if_matched_sid>100026</if_matched_sid>
  <same_field>win.eventdata.sourceProcessId</same_field>
  <description>T1134.002 - Patron de token theft: accesos múltiples a LSASS
    por $(win.eventdata.sourceImage) en 2 minutos</description>
  <mitre>
    <id>T1134.002</id>
  </mitre>
```

```
  <group>credential_access,windows,critical,ad_hardening</group>
</rule>
```

5.5.5.3.4 Regla 100027 -Evento ID 4672: Privilegios Especiales

Identifica la asignación de *SeImpersonatePrivilege* o *SeDebugPrivilege* a cuentas que no son administrativas por ejemplo cuentas de usuario estándar.

```
<! -- Evento 4672: SeImpersonate o SeDebug en cuenta no administrativa -->
<rule id="100027" level="10">
  <if_group>windows</if_group>
  <field name="win.system.channel">Security</field>
  <field name="win.system.eventID">^4672$</field>
  <field name="win.eventdata.privilegeList" type="pcre2">
    (?i)(SeImpersonatePrivilege|SeDebugPrivilege)
  </field>
  <! -- Excluir cuentas de sistema y administrativas -->
  <field name="win.eventdata.subjectUserName" negate="yes" type="pcre2">
    (?i)(SYSTEM|Administrator|.*\\$$|LOCAL SERVICE|NETWORK SERVICE)
  </field>
  <description>T1134.002 - SeImpersonate o SeDebug en cuenta no administrativa:
    $(win.eventdata.subjectUserName)</description>
  <mitre>
    <id>T1134.002</id>
  </mitre>
  <group>credential_access,windows,ad_hardening,privilege_escalation</group>
</rule>
```

5.5.5.3.5 Regla 100028 – Evento ID 4673: Token Privilegiado

Detecta el uso de *SeCreateTokenPrivilege* y *SeAssignPrimaryTokenPrivilege*. Si se detecta un *SeCreateTokenPrivilege* es extremadamente raro en una operación normal.

```
<! -- Evento 4673: Uso de privilegio de creación/asignación de token -->
<rule id="100028" level="12">
  <if_group>windows</if_group>
  <field name="win.system.channel">Security</field>
  <field name="win.system.eventID">^4673$</field>
  <field name="win.eventdata.privileges" type="pcre2">
    (?i)(SeAssignPrimaryTokenPrivilege|SeCreateTokenPrivilege)
```

```
  </field>
  <description>T1134.002 - Uso de privilegio de manipulacion de token:
    $(win.eventdata.privileges) por $(win.eventdata.subjectUserName)</description>
  <mitre>
    <id>T1134.002</id>
  </mitre>
  <group>credential_access,windows,ad_hardening,privilege_escalation</group>
</rule>
```

5.5.5.3.6 Regla 100029 – Evento ID 4688: Herramientas de Token Theft

Identifica la ejecución de herramientas conocidas de robo de *tokens* y ataques por ejemplo tipo Potato.

```
<!-- Evento 4688: Ejecución de herramienta conocida de token theft -->
<rule id="100029" level="15">
  <if_group>windows</if_group>
  <field name="win.system.channel">Security</field>
  <field name="win.system.eventID">^4688$</field>
  <field name="win.eventdata.newProcessName" type="pcre2">
    (?i)(incognito|tokenvator|juicypotato|rottenpotato|
        sweetpotato|roguepotato|genericpotato|multipotato)(\.exe)?
  </field>
  <description>T1134.002 - Herramienta de token theft detectada:
    $(win.eventdata.newProcessName)</description>
  <mitre>
    <id>T1134.002</id>
  </mitre>
  <group>credential_access,windows,ad_hardening,critical</group>
</rule>
```

5.5.5.3.7 Regla 100030 – Sysmon 1: Proceso SYSTEM desde usuario estándar

Detecta cuando un proceso con *IntegrityLevelSystem* es creado por un usuario estándar, lo cual indica una escala de privilegios exitosa.

```
<! -- Sysmon 1: IntegrityLevel System desde proceso no privilegiado -->
<rule id="100030" level="13">
  <if_group>windows</if_group>
  <field name="win.system.channel">Microsoft-Windows-Sysmon/Operational</field>
```

```
  <field name="win.system.eventID">^1$</field>
  <field name="win.eventdata.integrityLevel" type="pcre2">
    (?i)^System$
  </field>
  <! -- Excluir procesos que legítimamente crean hijos con nivel System -->
  <field name="win.eventdata.parentImage" negate="yes" type="pcre2">
    (?i)(services|wininit|smss|csrss|lsass|winlogon)(\.exe)?
  </field>
  <description>T1134.002 - Proceso con IntegrityLevel System creado por
    proceso no privilegiado: $(win.eventdata.image)
    hijo de $(win.eventdata.parentImage)</description>
  <mitre>
    <id>T1134.002</id>
  </mitre>
  <group>credential_access,windows,ad_hardening,privilege_escalation</group>
</rule>
```

5.5.6.4 T1547.002 – Boot or Logon Autostart: Authentication Packages

ID del Evento	Canal	Descripción	Indicador de comportamiento anómalo
4657	Seguridad	Valor de registro modificado	Escritura en HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Control\Lsa\ Authentication Packages
4697	Seguridad	Servicio instalado en el sistema	Instalación de un sistema o servicio con privilegios de SYSTEM fuera de horario o ventana de mantenimiento
Sysmon 13	Sysmon/ Operational	Escritura en clave de registro	Escritura de claves LSA: Authentication Packages
Sysmon 7	Sysmon/ Operational	Imagen de módulo cargada	DLL sin firma digital cargada por LSASS fuera de System32

Tabla 24 T1547.002 – Boot or Logon Autostart: Authentication Packages

5.5.6.4.1 Regla100031 – Sysmon 13: Escritura en Claves LSA

Identifica cualquier escritura en las claves de registro de *Authentication Packages*, *SecurityPackages o Notification Packages.*

```
<! -- Regla 100031: Escritura en claves LSA de authentication packages -->
<rule id="100031" level="15">
  <if_group>windows</if_group>
  <field name="win.system.channel">Microsoft-Windows-Sysmon/Operational</field>
```

```
  <field name="win.system.eventID">^13$</field>
  <field name="win.eventdata.targetObject" type="pcre2">
    (?i)\\Control\\Lsa\\(Authentication|Security|Notification) Packages
  </field>
  <description>T1547.002 - Modificacion de Authentication Packages en LSA:
    $(win.eventdata.targetObject)</description>
  <mitre>
    <id>T1547.002</id>
  </mitre>
  <group>persistence,windows,ad_hardening,critical</group>
</rule>
```

5.5.6.4.2 Regla 100032 – Sysmon 7: DLL no firmada cargada por LSASS

Detecta cuando una LSASS carga una DLL que no tiene firma digital válida. Las DLLs legitimas del sistema y de software de seguridad siempre están firmadas.

```
<! -- Regla 100031: DLL sin firma cargada por LSASS -->
<rule id="100032" level="14">
  <if_group>windows</if_group>
  <field name="win.system.channel">Microsoft-Windows-Sysmon/Operational</field>
  <field name="win.system.eventID">^7$</field>
  <field name="win.eventdata.image" type="pcre2">(?i)lsass\.exe</field>
  <field name="win.eventdata.signed">false</field>
  <description>T1547.002 - DLL no firmada cargada por LSASS:
    $(win.eventdata.imageLoaded)</description>
  <mitre>
    <id>T1547.002</id>
  </mitre>
  <group>persistence,windows,ad_hardening,critical</group>
</rule>
```

5.5.6.4.3 Regla 100033 – Evento ID 4657: Modificación del valor de registro LSA

Identifica cuando un valor de registro LSA ha sido modificado a nivel de la ruta HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages, *SecurityPackages o Notification Packages.*

```
<!-- Regla 100033: Evento 4657 - Modificación de valor de registro LSA -->
```

```
<rule id="100033" level="13">
  <if_group>windows</if_group>
  <field name="win.system.channel">Security</field>
  <field name="win.system.eventID">^4657$</field>
  <field name="win.eventdata.objectName" type="pcre2">
    (?i)\\Control\\Lsa\\(Authentication|Security|Notification) Packages
  </field>
  <description>T1547.002 - Modificacion de registro LSA via Event 4657:
    $(win.eventdata.objectName) por $(win.eventdata.subjectUserName)</description>
  <mitre>
    <id>T1547.002</id>
  </mitre>
  <group>persistence,windows,ad_hardening</group>
</rule>
```

5.5.6.4.4 Regla 100034 – Evento ID 4697: Servicio de instalación con privilegios de SYSTEM

Detecta cuando se instaló un nuevo servicio en Windows para correr como SYSTEM

```
<! -- Regla 100034: Event 4697 - Servicio instalado con privilegios SYSTEM -->
<rule id="100034" level="13">
  <if_group>windows</if_group>
  <field name="win.system.channel">Security</field>
  <field name="win.system.eventID">^4697$</field>
  <field name="win.eventdata.serviceAccount" type="pcre2">
    (?i)(LocalSystem|SYSTEM)
  </field>
  <description>T1547.002 - Servicio instalado con cuenta SYSTEM:
    $(win.eventdata.serviceName) por $(win.eventdata.subjectUserName)</description>
  <mitre>
    <id>T1547.002</id>
  </mitre>
  <group>persistence,windows,ad_hardening</group>
</rule>
```

5.5.7.5 T1574.001 – Hijack Execution Flow: DLL Side-Loading

ID del Evento	Canal	Descripción	Indicador de comportamiento anómalo
4688	Seguridad	Creación de proceso	Proceso firmado desde una DLL cargada desde AppData, temp o directorios de usuarios.
7034	Sistema	Servicio Cerrado inesperadamente	Sistema se cerró forzosamente luego de una carga DLL maliciosa.
Sysmon 1	Sysmon/ Operational	Creación de proceso	Procesos firmados con DLLs cargadas desde Appdata, temp o directorio de usuario.
Sysmon 7	Sysmon/ Operational	Imagen de modulo cargada	DLL sin firma cargada por proceso firmado desde una ruta no estándar ejemplo Appdata, temp y usuario.

Tabla 25 T1574.001 – Hijack Execution Flow: DLL Side-Loading

5.5.7.5.1 Regla 100040 – Sysmon 7: DLL Sin Firma Cargada por Proceso Firmado

Identifica el patrón central de *DLL side-loading* un proceso con firma digital valida carga una DLL sin firma desde una ruta no estándar.

```
<! -- Regla 100040: DLL sin firma cargada por proceso firmado - side-loading -->
<rule id="100040" level="12">
  <if_group>windows</if_group>
  <field name="win.system.channel">Microsoft-Windows-Sysmon/Operational</field>
  <field name="win.system.eventID">^7$</field>
  <!-- DLL sin firma -->
  <field name="win.eventdata.signed">false</field>
  <!-- Proceso origen debe estar firmado (patrón de side-loading) -->
  <field name="win.eventdata.signatureStatus">Valid</field>
  <!-- DLL cargada desde ruta no estándar -->
  <field name="win.eventdata.imageLoaded" type="pcre2">
    (?i)(AppData|Temp|Users|Downloads|Desktop)
  </field>
  <description>T1574.001 - Posible DLL Side-Loading:
    $(win.eventdata.imageLoaded) cargada por $(win.eventdata.image)</description>
  <mitre>
    <id>T1574.001</id>
  </mitre>
```

```
  <group>hijack_execution,windows,ad_hardening</group>
</rule>
```

5.5.7.5.2 Regla 100041 – Sysmon 1: Proceso Firmado Ejecutado desde una ruta Inusual

Detecta procesos con firma digital que se ejecutan desde directorios de usuario como AppData o Temp

```
<! -- Regla 100041: Proceso firmado ejecutándose desde ruta inusual -->
<rule id="100041" level="11">
  <if_group>windows</if_group>
  <field name="win.system.channel">Microsoft-Windows-Sysmon/Operational</field>
  <field name="win.system.eventID">^1$</field>
  <! -- Proceso con firma válida -->
  <field name="win.eventdata.signed">true</field>
  <! -- Ejecutado desde directorio inusual -->
  <field name="win.eventdata.currentDirectory" type="pcre2">
    (?i)(AppData|Temp|Downloads|Desktop)
  </field>
  <description>T1574.001 - Proceso firmado ejecutado desde ruta inusual:
    $(win.eventdata.image) en $(win.eventdata.currentDirectory)</description>
  <mitre>
    <id>T1574.001</id>
  </mitre>
  <group>hijack_execution,windows,ad_hardening</group>
</rule>
```

5.5.7.5.3 Regla 100042 – Evento ID 4688: Proceso desde Ruta Inusual

Es un complemento para la regla 100041 usando el canal de seguridad, identifica que procesos fueron creados desde rutas no estándar.

```
<! -- Regla 100042: Proceso creado desde ruta inusual vía Evento 4688 -->
<rule id="100042" level="10">
  <if_group>windows</if_group>
  <field name="win.system.channel">Security</field>
  <field name="win.system.eventID">^4688$</field>
  <field name="win.eventdata.newProcessName" type="pcre2">
    (?i)(AppData|Temp|Downloads|Desktop)
  </field>
```

```
  <description>T1574.001 - Proceso ejecutado desde ruta inusual:
    $(win.eventdata.newProcessName)</description>
  <mitre>
    <id>T1574.001</id>
  </mitre>
  <group>hijack_execution,windows,ad_hardening</group>
</rule>
```

5.5.7.5.4 Regla 100043 – Evento ID 7034: Servicio termino inesperadamente

Identifica fallos de servicios de Windows, que pueden ocurrir cuando una DLL maliciosa es cargada por *side loading* causando una excepción no controlada en el proceso del servicio.

```
<! -- Regla 100043: Servicio terminó inesperadamente - posible crash por DLL maliciosa -->
<rule id="100043" level="10">
  <if_group>windows</if_group>
  <field name="win.system.channel">System</field>
  <field name="win.system.eventID">^7034$</field>
  <description>T1574.001 - Servicio termino inesperadamente (posible DLL maliciosa):
    $(win.eventdata.serviceName)</description>
  <mitre>
    <id>T1574.001</id>
  </mitre>
  <group>hijack_execution,windows,ad_hardening</group>
</rule>
```

5.6 Implementación de la propuesta

A continuación, se documentan los resultados obtenidos durante la implementación de los dos componentes de la propuesta en el entorno de Directorio Activo evaluado, por razones de confidencialidad de la información, no se da a conocer el dominio donde se implementó la propuesta.

La implementación se realizado en una financiera con más de 25 años de presencia en el país, ayudando a mejorar la postura de seguridad en su entorno de Directorio Activo.

Esta parte de la ejecución de *Purple Knight* como diagnóstico inicial, comparando los hallazgos con los controles definidos en la guía de *hardening* sección 5.3, y documenta el estado de avance sobre cada control, reconociendo que el entorno analizado es un

ambiente de producción activo, lo que impone una serie de restricciones legítimas sobre la velocidad y el alcance de la remediación.

5.6.1 Diagnóstico inicial: resultados del escaneo con Purple Knight

Se realiza el primer escaneo de Purple Knight sobre el entorno de Directorio Activo *on-premise* con el propósito de medir las variaciones en la postura de seguridad del entorno. El escaneo evaluó 109 indicadores en 17 minuto y 58 segundos, abarcando las cinco categorías relevantes para entornos *on-premise*.

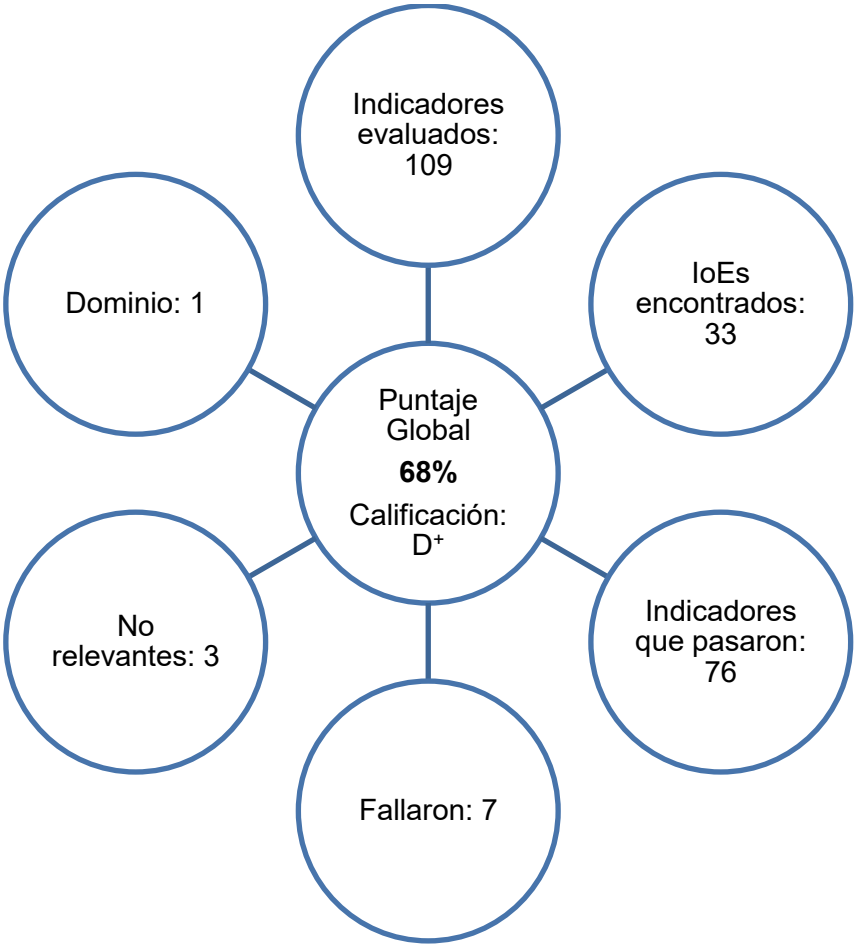

Ilustración 15 Resultados del escaneo con Purple Knight

Durante el análisis del informe brindado por Purple Knight del diagnóstico sobre el entorno no presento ningún indicador crítico activo de los 109 evaluados. Asimismo, se identificaron 25 IoEs de severidad advertencia e informativos, y 4 indicadores críticos que no pudieron ejecutarse porque el controlador de dominio número 3 se encuentra apagado, lo que representa una exposición a un riesgo que se debe atender. Seguidamente se presenta el análisis detallado de los hallazgos.

5.6.1.1 Análisis de resultados: Seguridad del Directorio Activo

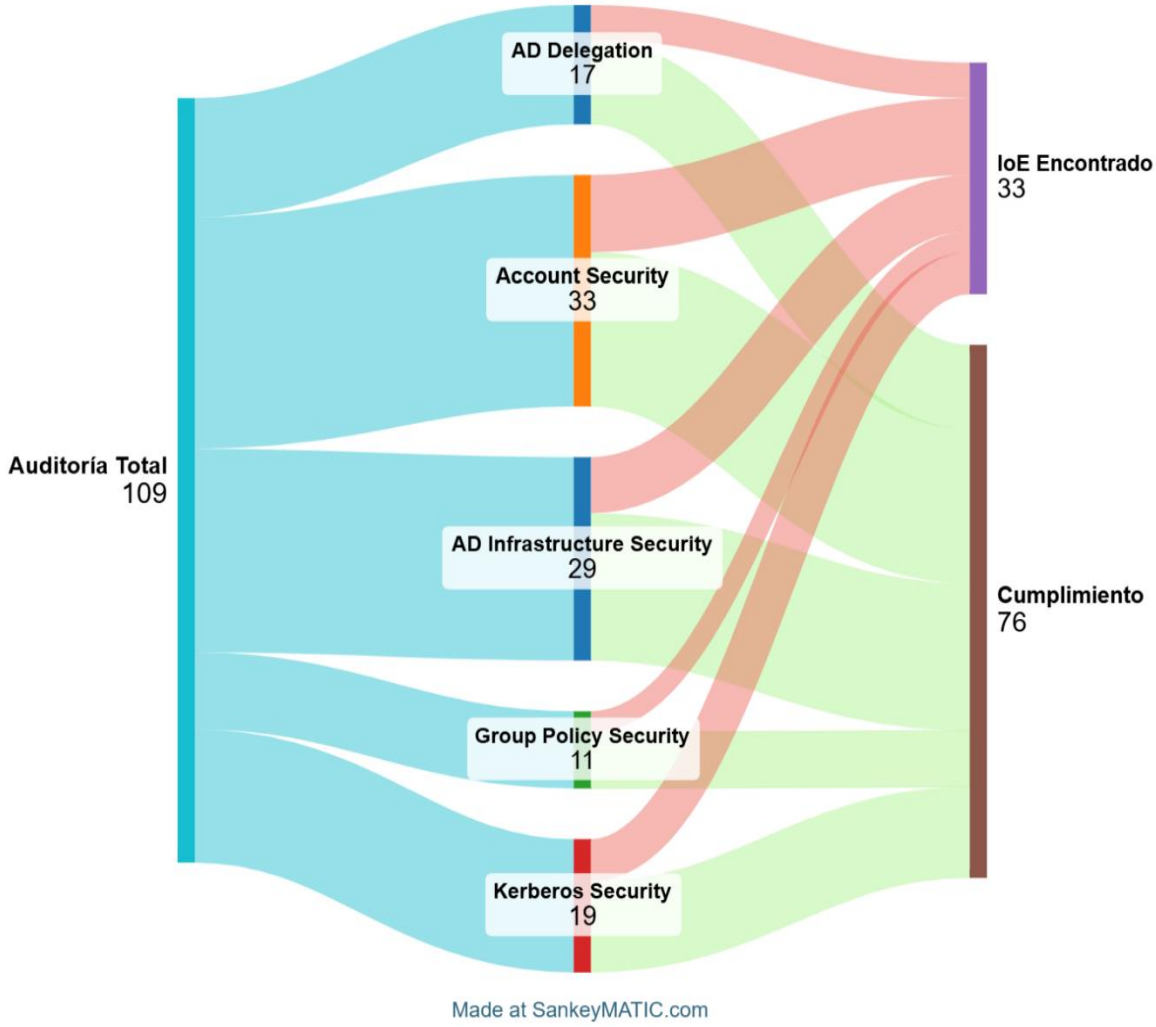

Ilustración 16 Resultados de Seguridad del Directorio Activo Elaboración Propia

La visualización mediante la Ilustración 15 que hace referencia al diagrama de Sankey permite un análisis tridimensional de la seguridad del entorno: volumen de evaluación, segmentación crítica y densidad de hallazgos.

El flujo inicial demuestra que el análisis se centró predominantemente en las categorías de *Account Security* y *AD Infraestructure Security* con 33 y 29 indicadores respectivamente. Esta distribución es metodológicamente intencional, ya que estas categorías representan la mayor superficie de ataque en entornos de controladores de dominio.

Asimismo, se observa una relación directa entre la complejidad de la categoría y las vulnerabilidades, aunque *Account Security* presenta 11 IoEs, su porcentaje es de 92% indicando que los controles base están presentes, pero existen excepciones detectadas que son críticas.

Se observa que AD *Delegation* y *AD Infraestructure Security*, a pesar de tener un porcentaje menor en los indicadores que *Account Security*, presenta porcentajes de 88% y

89% respectivamente, esto indica que la higiene de la seguridad en la delegación de permisos y configuración de servidores es proporcionalmente más débil, lo que podría facilitar movimientos laterales o escalada de privilegios.

Sin embargo, la categoría de Group Policy Security destaca como la más robusta con un 95% de cumplimiento, donde solo se encontraron 3 hallazgos de los 11 evaluados.

El análisis cuantitativo de la herramienta Purple Knight refleja que el entorno de Directorio Activo tiene una postura de seguridad de 68% $D^{+,}$ lo cual es inferior al promedio reportado por Semperis (2024) para organizaciones en su primer escaneo, lo cual indica que la postura de seguridad puede fortalecerse de manera significativamente. Cabe mencionar que este puntaje refleja el estado actual del entorno del dominio previo a la aplicación sistemática de los controles de la guía de *hardening*.

5.6.1.2 Análisis del reporte contra la guía de *hardening*

El análisis comparativo entre el reporte de Purple Knight y los controles definidos en la guía de *hardening*, se organiza siguiendo la misma estructura de la guía: la sesión 5.2 con sus cuatro subsecciones de controles. Asimismo, para cada indicador reportado por la herramienta se identifica el control correspondiente en la guía, se describe el hallazgo real en el entorno y se estable el estado de implementación, tomando en cuenta que varios controles presentan restricciones operativas por tratarse de un ambiente de producción activo.

5.6.1.2.1 Sección 5.4.1 Controles de Gestión de Cuentas y Credenciales

La sección 5.4.1 establece los controles base para la gestión de cuentas y credenciales en el dominio, organizado en cuatro controles: política de contraseñas (5.4.1.1), política de bloqueo de cuentas (5.4.1.2), Fine-Grained Password Policy para cuentas privilegiadas (5.4.1.3) y rotación periódica de la cuenta KRBTGT (5.4.1.4). Estos controles mitigan la técnica T1078.002 – Valid Accounts: Domain Accounts, lo cual permite al adversario abusar de las credenciales legitimas para evadir controles de seguridad y mantener acceso persistente en el entorno.

5.6.1.2.1.1 Política de contraseñas y bloqueo de cuentas

El indicador *Privileged Users with Weak Password Policy* obtuvo un resultado aprobado con un porcentaje de 100%, lo que evidencia que la política de contraseñas del dominio cumple con los valores requeridos por la sección 5.4.1.1 de la guía y los criterios del framework ANSSI. Asimismo, el indicador Abnormal Password Refresh paso satisfactoriamente, confirmando que no existen cambios de contraseña sin replicación correspondiente. Por otro lado, no se detectaron valores negativos relacionados con la política de bloqueo de cuentas, lo que indica que los valores de 10 intentos, la duración de 15 minutos y el restablecimiento automático definidos en la sección 5.4.1.2 están correctamente configurados en el entorno del dominio.

5.6.1.2.1.2 Fine-Grained Password Policy (FGPP)

En cambio, el indicador de *FGPP not applied to Global group* falló al ejecutarse, debido a que la cuenta utilizada no tenía permisos suficientes para leer el contenedor de

Password Settings Container, lo cual impidió verificar si la *Fine-Grained Password Policy* está definida. Se realiza una verificación manual lo cual indica que la política no está definida. Esta situación implica que todas las cuentas privilegiadas quedan sujetas únicamente a la política de contraseñas general del dominio, sin el endurecimiento adicional que exige la sección 5.4.1.3, representando un riesgo de exposición de credenciales en cuentas de alto valor.

5.6.1.2.1.3 Rotación de la cuenta KRBTGT

Se detectó un hallazgo de mayor urgencia el cual está en la sección *Kerberos KRBTGT account with old password*, con un porcentaje de 94% con calificación B y con una severidad media. El reporte determino que la contraseña de la cuenta KRBTGT no ha sido cambiada desde el 06 de febrero del 2013, acumulando alrededor de más de 4700 días sin actualización. Si bien el porcentaje es B refleja que únicamente una cuenta está afectada, la criticidad operativa de este hallazgo supera su calificación numérica, esto debido a que la cuenta KRBTG es la base criptográfica del servicio de Kerberos, su *hash* es utilizado para firmar y cifrar todos los *tickets* del dominio. La sección 5.4.1.4 se establece que esta cuenta debe rotarse al meno cada 180 días, siempre en dos etapas con un intervalo de 10 horas entre cada cambio para garantizar la replicación completa en todos los controladores de dominio. El incumplimiento de este control mantiene el riesgo de fabricación de *Golden Tickets*, esto debido a que un adversario puede comprometer el hash de KRBTGT generando *tickets* de Kerberos falsos con acceso ilimitado al dominio.

5.6.1.2.1.4 Cuentas privilegiadas con contraseñas que no caduca

Por otra parte, el indicador *Privileged accounts with a password never expires* obtuvo el porcentaje más bajo de esta sección con un 15% F con severidad alta. Se identificaron 7 cuentas privilegiadas con el atributo de contraseña no caduca habilitado, algunas de ella tienen hasta 3864 días sin rotación. La sección 5.4.1.1 establece una vigencia máxima de 60 días para el cambio de contraseñas. En las cuentas administrativas este control se puede aplicar de forma directa; sin embargo, las cuentas de servicio requieren una coordinación previa con las áreas propietarias de cata sistema para evitar interrupciones operativas al forzar la caducidad de la contraseña.

Control	Indicador	Hallazgo	Estado
Política de contraseñas (longitud ≥15, historial 24, vigencia máx. 60 días)	Privileged Users with Weak Password Policy	Porcentaje 100% La política del dominio cumple los criterios ANSSI	Aplicado
Vigencia máxima 60 días (cuentas privilegiadas)	Privileged accounts with password that never expires	Porcentaje 15% (F) 7 cuentas privilegiadas sin expiración (hasta 3,864 días sin rotar)	No aplicado
Política de bloqueo (10 intentos, 15 min)	No reportado como IoE negativo	No hay indicador de política débil en el reporte	Aplicado

FGPP para Domain Admins	FGPP not applied to Global group	Falló al ejecutar cuenta de auditoría sin permisos para leer el contenedor de FGPP	No aplicado
Rotación KRBTGT (cada 180 días, dos veces)	Kerberos KRBTGT account with old password	Porcentaje 94% (B) Última rotación: 06/02/2013. Más de 4,700 días sin rotar	No aplicado

Tabla 26 Estado de Implementación - Controles de la sección 5.4.1 de la guía de *hardening*

5.6.1.2.2 Sección 5.4.2 Controles de Protección de Credenciales y Privilegios

En la sección 5.4.2 se definen cinco controles orientados a proteger las credenciales almacenadas en el proceso LSASS y a restringir la asignación de privilegios elevados. Con estos controles se mitigan las técnicas 1078.002, t1134.002 y T1547.002. El reporte de Purple Knight en esta sección refleja una mayor concentración de hallazgos de severidad alta reflejando las exposiciones de mayor riesgo del entorno.

5.6.1.2.2.1 Controladores de protocoles de autenticación

Solo tres de los indicadores del reporte confirmaron que los controles de protocolos de autenticación están correctamente configurados, los cuales son: *GPO Weak LM Hash storage enabled, User Accounts that use DES encryption y Users with Kerberos pre-authentication disabled* pasaron con un porcentaje del 100%, esto indica que el hash de *LAN Manager* esta deshabilitado, además que ninguna cuenta tiene habilitado el cifrado DES y por último el entorno no es vulnerable a ataques *ASREP*-Roasting lo cual va en línea con el forzado de NTLMv2 y autenticación fuerte configurada en el dominio. Para los controles LSA Protection y WDigest no son evaluados directamente por la herramienta, por lo que su estado requiere de una verificación manual en cada controlador de dominio.

5.6.1.2.2.3 Derechos de usuario peligrosos asignados por GPO

El indicador *Dangerous user rights granted by GPO* obtuvo un porcentaje de 47% D- con una severidad alta, este indicador está directamente relacionado con la sección 5.4.2.4 de la guía sobre los derechos de usuario. El reporte identifico que una cuenta tiene asignado el privilegio SeTcbPrivilege actuar como parte del sistema operativo asignado en la GPO {33E1067C-CA68-4BBB-82BE-B40D76DB2D5B}. En la sección 5.4.2.4 se estable que este derecho debe ser igual a Ninguno tanto en servidores miembro como en controladores de dominio, ya que su asignación puede constituir un riesgo de seguridad al permitir que un proceso actúe con permisos del sistema operativo, creando un vector de escalamiento de privilegios local.

5.6.1.2.2.4 Shadow Credentials y delegación RBCD sobre controladores de Dominio

Los indicadores *Shadows Credentials on privileged objects* y *Write access to RBCD on DC* obtuvieron un porcentaje de 15% F con severidad alta. El primero identifico que una cuenta tiene permisos de escritura sobre el siguiente atributo *msDS- KeyCredentialLink en* los siete controladores de dominio. El segundo detecto que esa misma cuenta tiene permisos de GenericAll sobre el atributo *msDS-AllowedToActOnBehalfOfOtherIdentity* habilitando ataques de inyectar credenciales alternativas y delegación restringida basada en recursos sobre los controladores de dominio. Un atacante con escritura *msDS-*

KeyCredentialLink puede inyectar credenciales alternativas (Shadow Credential) en la cuenta de la víctima y autenticarse como ella sin necesidad de conocer su contraseña, explotando el mecanismo PKINIT de Kerberos, esto está directamente relacionado con la técnica T1134.002 – Access Token Manipulation: Create Process with Token. Por otro lado, la escritura sobre RBCD permite a un adversario configurar un servicio bajo su control actuando en nombre de cualquier cuenta sobre los controladores de dominio, abriendo un camino directo hacia la escalada de privilegios a nivel de dominio. Ambos hallazgos están relacionados con la sección 5.4.2 de la guía sobre restricción de permisos excesivos sobre objetos privilegiados.

5.6.1.2.2.5 Grupo Protected Users

Se hallaron 12 cuentas privilegiadas que no son miembro del grupo Protected Users. El indicador Protected Users group not in use obtuvo un porcentaje de 88% C+. En la sección 5.4.2.5 se estable la incorporación de todas las cuentas privilegiadas a este grupo, el cual aplica automáticamente restricciones como la deshabilitación de autenticación NTLM, la prohibición de delegación de Kerberos no restringida y la limitación de la renovación de *tickets*. Sin embargo, este control debe aplicarse con precaución, ya que la deshabilitación de NTLM puede interrumpir servicios que dependan de este protocolo.

Control	Indicador	Hallazgo	Estado
LSA Protection (RunAsPPL = 1)	No evaluado por Purple Knight	No hay indicador directo. Verificar manualmente en cada controlador de dominio.	Verificar
Deshabilitar WDigest (UseLogonCredential = 0)	No evaluado por Purple Knight	No hay indicador directo. Verificar manualmente en cada controlador de dominio.	Verificar
Deshabilitar LM Hash	GPO Weak LM Hash storage enabled	Porcentaje 100% Hash LM correctamente deshabilitado	Aplicado
Deshabilitar DES	User accounts that use DES encryption	Porcentaje 100% Ninguna cuenta usa DES	Aplicado
NTLMv2 / pre-autenticación Kerberos	Users with Kerberos pre-authentication disabled	Porcentaje 100%Pre-autenticación habilitada en todas las cuentas	Aplicado
Derechos de usuario (SeTcbPrivilege = Ninguno)	Dangerous user rights granted by GPO	Porcentaje 47% (D) tiene SeTcbPrivilege en GPO {33E1067C..}	No aplicado
Permisos sobre objetos privilegiados	Shadow Credentials on privileged objects	Porcentaje 15% (F) con escritura en msDS-KeyCredentialLink en 7 DCs	No aplicado

Permisos sobre objetos privilegiados	Write access to RBCD on DC	Porcentaje 15% (F) con GenericAll sobre RBCD en 7 DCs	No aplicado
Grupo Protected Users	Protected Users group not in use	Porcentaje 88% (C+)12 cuentas privilegiadas fuera del grupo	No aplicado

Tabla 27 Estado de Implementación - Controles de la sección 5.4.2 de la guía de *hardening*

5.6.1.2.3 Sección 5.4.3 Controles de Políticas de Dominio y Opciones de seguridad

La sección 5.4.3 cubre las opciones de seguridad crítica del dominio y la auditoría de permisos sobre el grupo de políticas y SYSVOL, orientadas a mitigar la técnica T1484.002 – Domain Policy Modification, la cual busca que un adversario modifique las políticas del dominio para escalar privilegios o establecer persistencia. Los hallazgos se organizan en dos subsecciones: la evaluación de opciones de seguridad críticas del dominio y la auditoría de permisos sobre objetos de directiva de grupo y SYSVOL.

5.6.1.2.3.1 Firma LDAP en controladores de dominio

El indicador LDAP signing is not required on Domain Controllers obtuvo el porcentaje más bajo de la sección 5.4.3, con un resultado de 0% y una calificación F de severidad alta. Durante el análisis se determinó que cinco de los 7 controladores de dominio no exigen firma digital en las solicitudes LDAP entrantes. Dos de los controladores no eran accesibles desde el equipo donde se ejecutó el Purple Knight al momento del escaneo, por lo que su estado no pudo ser determinado.

La guía establece en su sección 5.4.3.1 que cada controlador de dominio debe configurarse con el valor Requiere firma en la opción Controlador de dominio: requisitos de firma de servidor LDAP. La ausencia de esta configuración expone un canal de comunicación a ataques de intermediario (*man in the middle*), mediante el cual un adversario puede interceptar, modificar o redirigir el tráfico LDAP sin autenticación. Este control se clasifica como restricción de producción y requiere un proceso escalonado en tres fases: configurar la negociación de firma en los clientes, habilitar el requisito de firma en los controladores de dominio y forzar la firma en los clientes.

5.6.1.2.3.2 Soporte de cifrado RC4 y DES en Kerberos

RC4 or DES encryption type are supported by Domain Controller obtuvo un porcentaje de 15% F con una severidad alta. De los siete controladores de dominio soportan el tipo de cifrado RC4_HMAC_MD5 de forma simultánea con AES-128 y AES-256. La coexistencia de RC4 junto a tipos de cifrados modernos no ofrece una protección equivalente a la de un entorno exclusivamente con AES, un adversario puede forzar la negociación de *tickets* Kerberos con cifrado RC4 mediante ataques de degradación, facilitando técnicas como Kerberoasting y Pass the Ticket.

5.6.1.2.3.3 Firma SMB y protocolo SMBv1 en controladores de dominio

En dos de los controladores de domino no se pudieron evaluar los indicadores SMB Signing is no required on Domain Controllers y SMBv1 is enabled on Domain Controllers,

debido a que se encontraban fuera del alcance del equipo de análisis. La guía establece en su sección 5.4.3.1 que la firma digital de comunicaciones SMB debe habilitarse tanto en el cliente como en el servidor de red, a fin de prevenir ataques de retransmisión NTLM y accesos no autorizados a SYSVOL. La imposibilidad de evaluar estos indicadores constituye una exposición potencial que debe atenderse mediante una verificación directa en esos servidores.

5.6.1.2.3.4 Auditoría de permisos sobre GPOs y SYSVOL

El indicador Changes to Default Domain Policy or Default Domain Controllers Policy in the last 7 days aprobó con un porcentaje del 100%, confirmando que no se registraron modificaciones no autorizadas sobre las políticas de dominio predeterminadas durante el período evaluado.

Sin embargo, el indicado GPO linking delegation at the domain controller OU level consiguio un porcentaje de 64% D. Se identificaron que dos cuentas poseen permisos sobre GenericAll sobre la unidad organizativa que contiene los controladores de dominio, lo que permite vincular GPOs arbitrarias sobre los activos más críticos del dominio.

Asimismo, el indicador GPO linking delegation at the domain level alcanzó un porcentaje de 82% C, se identificó una cuenta que posee permisos GenericAll sobre naming context raíz, lo que permite vincular GPOs de forma global sobre toda la estructura del dominio. Cabe destacar que esta cuenta aparece comprometida en ambos indicadores de la subsección 5.4.2, lo que sugiere una delegación excesiva que debe corregirse como hallazgo unificado, reduciendo el nivel de acceso al mínimo necesario conforme al principio de privilegio mínimo.

Control	Indicador	Hallazgo	Estado
Firma LDAP	LDAP signing is not required on DCs	Porcentaje 0% F: 5 de 7 controladores de dominio sin firma LDAP requerida	No aplicado
Firma SMB	SMB Signing is not required on DCs	No evaluados dos controladores de dominio no accesibles.	Verificar
Deshabilitar SMBv1	SMBv1 is enabled on DCs	No evaluado dos controladores de dominio no accesibles.	Verificar
Kerberos solo AES-128 y AES-256	RC4 or DES encryption type are supported by DCs	Porcentaje 15% F: Los 7 controladores de dominio soportan RC4_HMAC_MD5 junto a AES-128 y AES-256.	No aplicado
UAC configurado correctamente	No reportado como indicador negativo	Sin indicador negativo de UAC en el reporte.	Aplicado

Auditoria de cambios en Default Domain Policy	Changes to Default Domain Policy (últimos 7 días)	Porcentaje 100%: Sin cambios no autorizados durante el período evaluado.	Aplicado
Permisos GPO sobre OU DCs	GPO linking delegation at DC OU level	Porcentaje 64% D: dos cuentas con GenericAll sobre la OU del controlador de dominio.	No aplicado
Permisos GPO sobre naming context	GPO linking delegation at domain level	Porcentaje 82% C: una cuenta con GenericAll	No aplicado

Tabla 28 Controlades de la sección 5.4.3 de la guía de *hardening*. Elaboración Propia

5.6.1.2.4 Sección 5.4.4 Controles de Flujo de Ejecución y DLL

La sección de la guía 5.4.4 define dos controles para mitigar la técnica T1574.001 -Hijack Execution Flow: DLL Side-Loading: SafeDLLSearchModel y AppLocker en modo auditoría. Purple Knight tiene una cobertura limitada sobre esta técnica, ya que opera principalmente en tiempo de ejecución y no genera exposiciones estáticas en el Directorio Activo. Por este motivo, ambos controles requieren de una verificación directa en cada uno de los controladores de dominio.

Ambos controles se clasifican como no aplicados en el entorno actual y no cuentan con cobertura de indicadores por parte de Purple Knight, por lo cual su remediación depende exclusivamente de la ejecución manual de los pasos descritos en la siguiente tabla:

Control	Estado	Pasos para remediación
SafeDLLSearchMode = 1	Verificar	Ejecutar: Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager' -Name SafeDLLSearchMode. Si el valor no es 1, configurar mediante GPO conforme a la sección 5.4.4.1
Habilitar servicio AppIDSvc (prerrequisito de AppLocker)	No aplicado	Configurar en GPO: Configuración del equipo > Seguridad > Servicios del sistema > Identificación de aplicación = Automático.
AppLocker en modo Solo Auditoría (4 semanas)	No aplicado	Configurar reglas en modo Solo Auditoría para ejecutables, Windows Installer, scripts y aplicaciones empaquetadas. Revisar el Visor de Eventos > AppLocker semanalmente durante 4 semanas antes de activar el modo Enforce.

Tabla 29 Controles de la sección 5.4.4 de la guía de *hardening*. Elaboración Propia

5.6.2 Estado consolidado e impacto proyectado

El análisis comparativo entre los hallazgos de Purple Knight y los controles de la guía de *hardening* permite establecer un estado consolidado de implementación. De los 25 controles analizados en las cuatro secciones de la guía, 7 se encuentran correctamente aplicados, 5 requieren una verificación manuela directa por no ser evaluados por la herramienta, y el 13 no han sido implementados aún. Esta distribución refleja que el entorno de Directorio Activo cuenta con una base de configuración sólida en políticas de

contraseñas y autenticación básica, pero presenta exposiciones significativas en la gestión de privilegios, configuraciones de protocolos de red y control de flujo de ejecución.

El hallazgo más significativo es la concentración de permisos en una cuenta que aparece comprometida de forma simultánea en cuatro indicadores de distintas secciones de la guía: permisos GenericAll sobre el naming context dol dominio, habilitando un ataque de DCSync, permisos de escritura sobre msDS-KeyCredentialLink en los siente controladores de dominio, autorizando Shadow Credentials mediante PKINIT, permisos GenericAll SOBRE msDS-AllowedToActOnBehalfOfOtherIdentity, facultando la delegación de RBCD, y permisos GenerecAll sobre la OU de controlador de dominio, permitiendo la vinculación de GPOs arbitrarias. La materialización de cualquiera de estos vectores comprometería en su totalidad del dominio, por lo que su corrección debe tratarse como acción prioritaria independientemente de las restricciones operativas.

Estado	Descripción	Controles	Porcentaje
Aplicado	Control implementado y confirmado por la herramienta Purple Knight.	**7**	**28%**
No aplicado	Control identificado, pero no implementado.	**13**	**52%**
Verificar	Controles no evaluados requieren comprobación manual.	**5**	**20%**
Total	25 controles de *hardening* evaluados		**100%**

Tabla 30 Distribución del estado de implementación de controles de *hardening*. Elaboración Propia

Desglose por sección de la guía de *hardening*

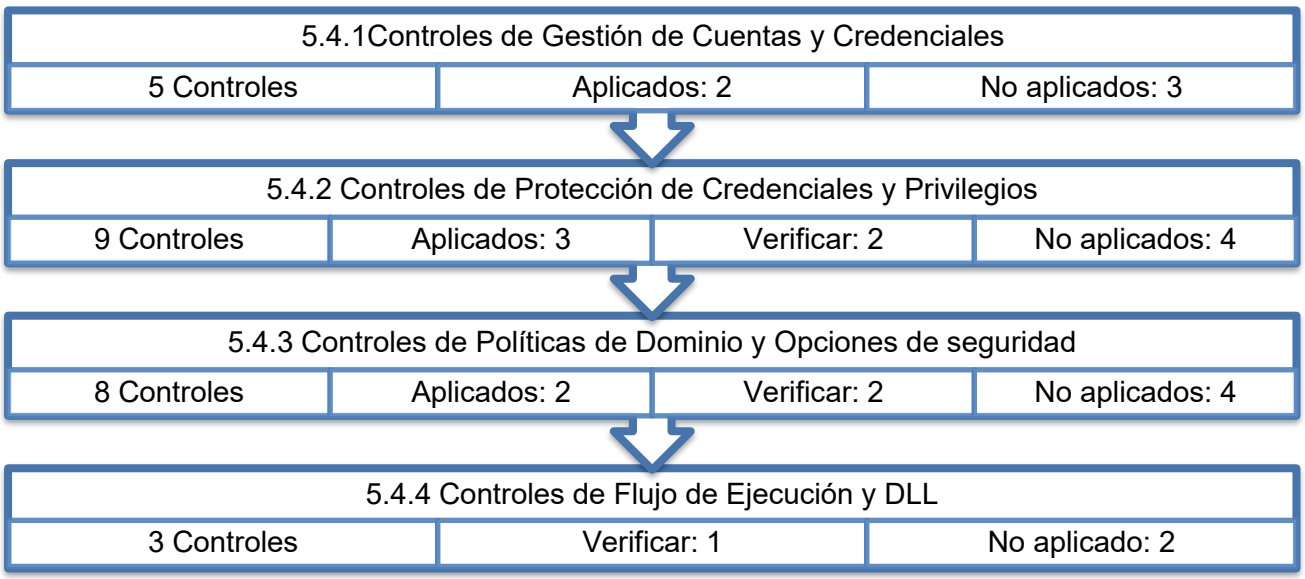

Ilustración 17 Desglose por sección de la guía de hardening. Elaboración Propia

5.6.3 Plan de implementación por fases

Con base a los resultados del primer escaneo de Purple Knight, se crea un plan de implementación de tres fases. Esto permite diferenciar las acciones según su impacto a nivel operativo en el ambiente de producción. Las fases del plan se ordenan por urgencia y viabilidad de ejecución inmediata. Después de cumplir con cada una de las fases del plan, se realizará otro escaneo de la herramienta con el fin de ver el avance del porcentaje a nivel de salud o seguridad del Directorio Activo.

5.6.3.1 Primera Fase – Aplicación sin impacto en producción

Estos controles se pueden implementar sin riesgos de interrupción para los servicios del controlador de dominio. Esto incluye:

- Limpieza de permisos excesivos sobre objetos privilegiados: eliminar los atributos msDS-KeyCredentialLink, msDS-AllowedToActOnBehalfOfOtherIdentity y los accesos GenericAll sobre la unidad organizativa de Domain Controllers y el naming context raíz de cualquier cuenta no autorizada.
- Eliminación del privilegio SeTcbPrivilege de la GPO.
- Creación de la FGPP para Administradores del Dominio.
- Incorporación al grupo de Protected Users de cuentas administrativas excluyendo inicialmente cuentas de servicio para evitar interrupciones por deshabilitación de NTLM.
- Validación manual de LSA Protection, WDigest y SafeDLLSearchMode de las secciones 5.4.2.1,5.4.2.2 y 5.4.4.1 esto debe verificarse directamente en cada controlador de dominio.
- Deshabilitación de cuentas inactivas: previa validación de dependencias de servicio.

5.6.3.2 Segunda Fase – Ventana de mantenimiento planificada

Los controles de esta fase requieren pruebas de compatibilidad previos coordinación con equipos de propietarios de servicio:

- Habilitación de LDAP Signing se debe seguir un proceso de tres pasos establecido en la sección 5.4.3.1: negociar firma en clientes, luego requerir firma en controladores de dominio, y por último fimar en clientes.
- Rotación de la contraseña KRBTGT según procedimiento se debe esperar un mínimo de 10 horas para garantizar la replicación completa en todos los controladores de dominio.
- Eliminación de la bandera de contraseña no caduca en las cuentas de servicio, debe estar presente los equipos propietarios ante cualquier evento.

5.6.3.3 Tercera Fase – Implementación a mediano plazo

Los controles de esta fase requieren un trabajo de preparación más extenso o depende de la finalización de fases anteriores:

- Deshabilitación de RC4 en Kerberos requiere identificación previa mediante el ID del evento 4769 que aplicaciones solicitan tickets con cifrado RC4 y migrar esas cuentas a AES.
- Activación de AppLocker en modo Enforce solo puede ejecutarse luego de completar las cuatro semanas de autoría, luego de confirmar que ninguna aplicación legítima vaya a ser bloqueada.

5.6.3.4 Plan de implementación de controles Directorio Activo

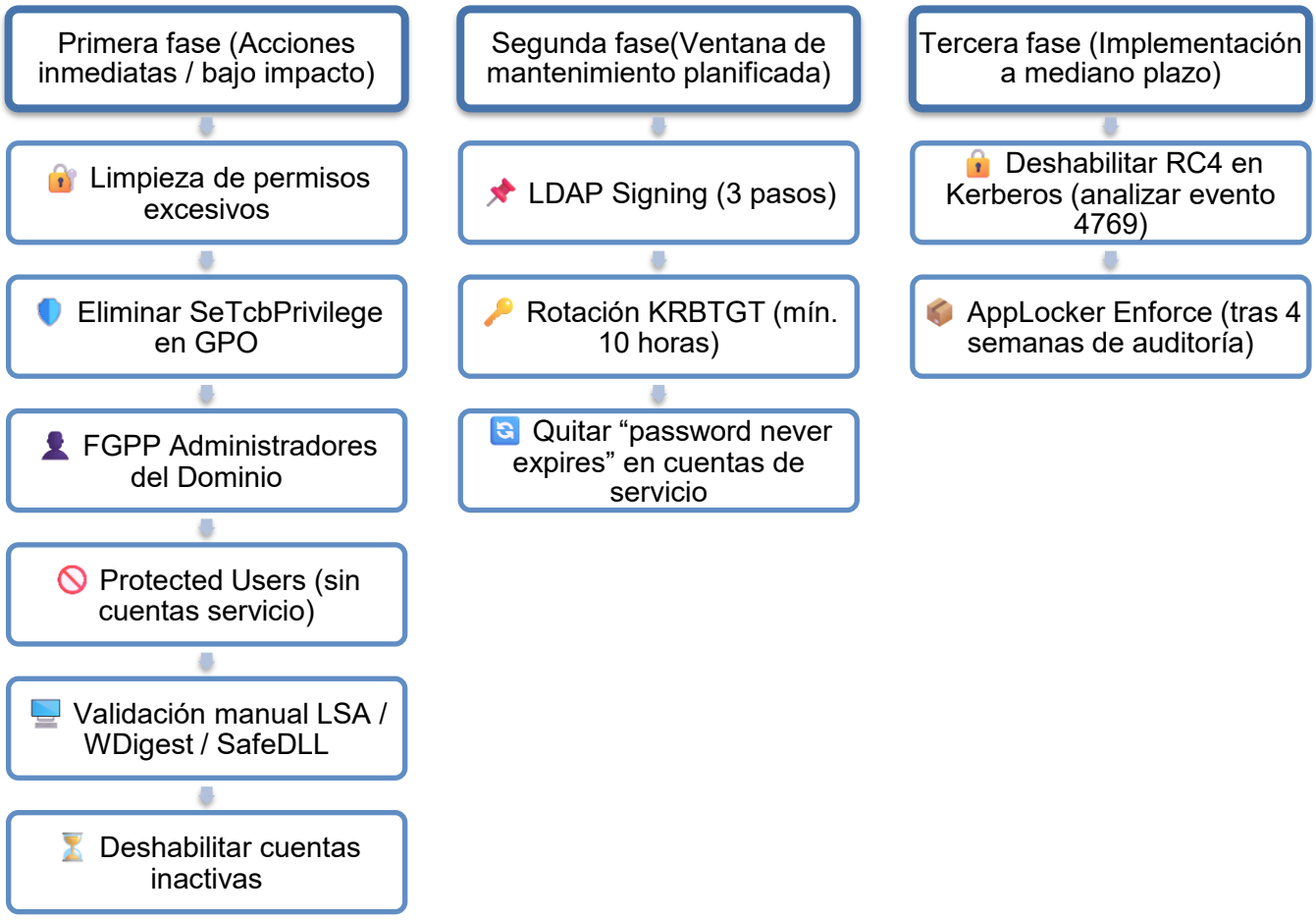

Ilustración 18 Plan de implementación de controles Directorio Activo Elaboración propia

5.7 Evaluación del Impacto de los Controles Aplicados en Directorio Activo: Escaneo 1 vs. Escaneo 2

Con el fin de validar el impacto de las primeras acciones de *hardening* implementadas, se realizó un segundo escaneo con la herramienta Purple Knight el 20 de abril del 2026. Esto sirvió como validación empírica de la fase 1 del plan de implementación

definido en la sección 5.6.3. Las acciones realizadas fueron controles clasificados en la fase 1. Se trató de una limpieza de permisos excesivos sobre objetos privilegiados. Esta fase no requería ventana de mantenimiento ni coordinación con propietarios de servicios. Los dos escaneos delimitan el estado antes y después de la intervención deliberada y documentada, Esto permite atribuir las variaciones observadas a las acciones realizadas y no a cambios operativos externos.

5.7.1 Alineación entre el plan de implementación y las acciones ejecutadas

Las acciones de remediación realizadas el 20 de abril del 2026 corresponden a la fase 1 del plan de implementación por fases, según lo establecido en la sección 5.6.3. Estas acciones se enfocaron en la eliminación de permisos excesivos sobre objetos privilegiados del Directorio Activo, ya que no requerían una ventana de mantenimiento.

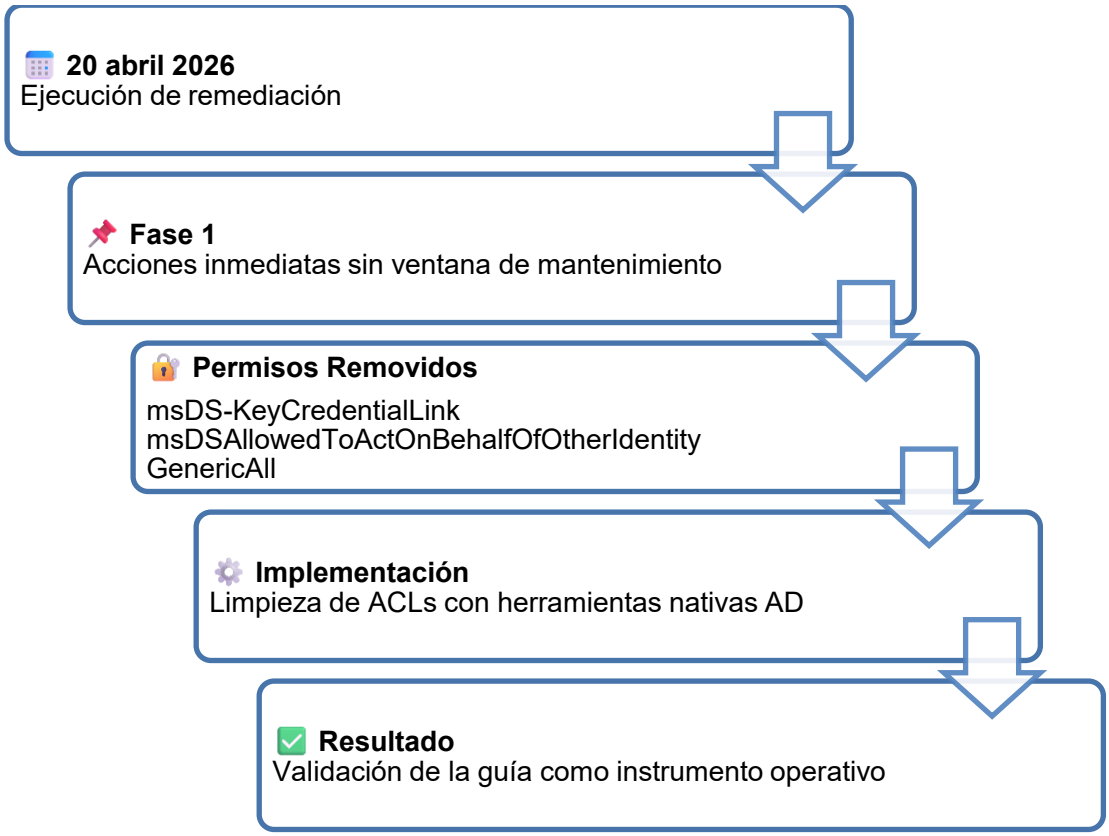

Ilustración 19 Correspondencia entre el Plan de Implementación y su Ejecución

Elaboración Propia

Los resultados que se presentan confirman que las acciones llevadas a cabo responden directamente a los controles que se priorizaron durante la fase 1. Esto le da mayor solidez a la comparación entre escaneos, ya que existe una línea clara entro lo que se planificó técnicamente y lo que finalmente se aplicó en el entorno operativo.

5.7.2 Mejora del porcentaje global

El porcentaje general del entorno mejoró del 68% D+ en el primer escaneo al 82 %C en el segundo escaneo, lo que representa un avance de 14 puntos porcentuales que se

puede atribuir directamente a las acciones ejecutadas en la fase 1 del plan de implementación. Este resultado es relevante porque supera el umbral de C que Semperis (2024) establece como mínimo aceptable de seguridad para entornos de Directorio Activo en entornos productivos, tomando como base datos recopilados de organizaciones evaluadas con la herramienta Purple Knight a nivel global.

Es cierto que ese punto de referencia no está segmentado por sector ni región geográfica, pero su uso sigue siendo válido desde el punto de vista metodológico, ya que tanto la herramienta como el modelo de puntuación se aplican de manera consistente en todas las evaluaciones.

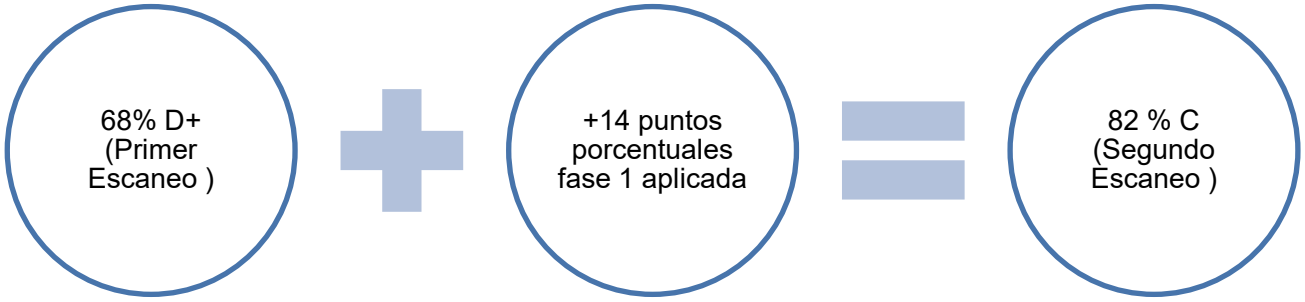

Ilustración 20 Mejora del porcentaje global de seguridad del Directorio Activo Elaboración Propia

5.7.3 Controles resueltos con impacto crítico

Como resultado de la fase1, cinco de los indicadores de máxima criticidad llegaron a una calificación perfecta de 100% A+. Entre ellos se encuentran controles relacionados con Shadow Credentials, delegación restringida basada en recursos (RBCD), privilegios peligrosos asignados mediante GPO, delegaciones de vinculación de políticas en niveles críticos del dominio.

Indicador	Antes	Después
Shadow Credentials	15% F	100% A+
Write access to RBCD on DC	15% F	100% A+
Dangerous user rights	47% D	100% A+
GPO linking at DC OU	64% D	100% A+
GPO linking at domain	82% C	100% A+

Tabla 31 Indicadores Resueltos tras Ejecución de la Fase 1 Elaboración Propia

La mejora simultánea de estos indicadores confirma que las acciones aplicadas atendieron directamente los hallazgos priorizados en el diagnóstico inicial, y demuestra que hubo una coherencia en todo el proceso: desde la guía de *hardening* y la planificación por fases, hasta la intervención ejecutada y los resultados obtenidos en el segundo escaneo.

5.7.4 Hallazgos pendientes y variaciones interpretativas

Algunos indicadores siguen pendientes de remediación, lo cual responden directamente a la priorización definida en el plan de implementación. La firma LDAP en los controladores de dominio se mantiene en 0% F, resultado esperado dado que su atención está programada para la fase 2, y de igual manera la contraseña de KRBTGT, se encuentra en 94% B, si bien fue identificada como una acción prioritaria, estos hallazgos dependen de una ventana de mantenimiento, por lo cual su ejecución no se había completado al momento del segundo escaneo.

En cuanto al indicador de soporte de cifrado RC4 o DES, este pasó del 15% al 27% sin que se haya aplicado ninguna remediación. El aumento se debe a un cambio en el universo evaluado: al desconectarse de forma permanente uno de los controladores de dominio, el total paso de siete a seis. Con menos controladores en el denominador, el hallazgo RC4 sigue activo, la herramienta recalculó el porcentaje y el valor subió aritméticamente. Esto no refleja ninguna mejora real; los controladores restantes siguen soportando RC4_HMAC_MD5 y riesgo asociado permanece vigente.

5.7.5 Nuevos hallazgos detectados en el segundo escaneo

El segundo escaneo reveló tres indicadores de exposición que no habían aparecido en la evaluación inicial. Esto se explica de forma sencilla, la cuenta utilizada en esta ocasión cuenta con mayores privilegios de auditoría, lo que permitió a la herramienta de Purple Kinght ver más de lo que pudo ver la primera vez.

Los nuevos hallazgos encontrados fueron los siguientes:

- **Dangerous GPO logon script path**: existe la posibilidad de que scripts alojados en SYSVOL sean modificados sin autorización,
- **Non-privileged users with access to gMSA passwords**: usuarios sin privilegios tienen acceso a credenciales que no deberían estar a su alcance.
- **Unexpected accounts in Cert Publishers Group**: hay cuentas que no deberían estar en este grupo sensible y que representan una exposición innecesaria.

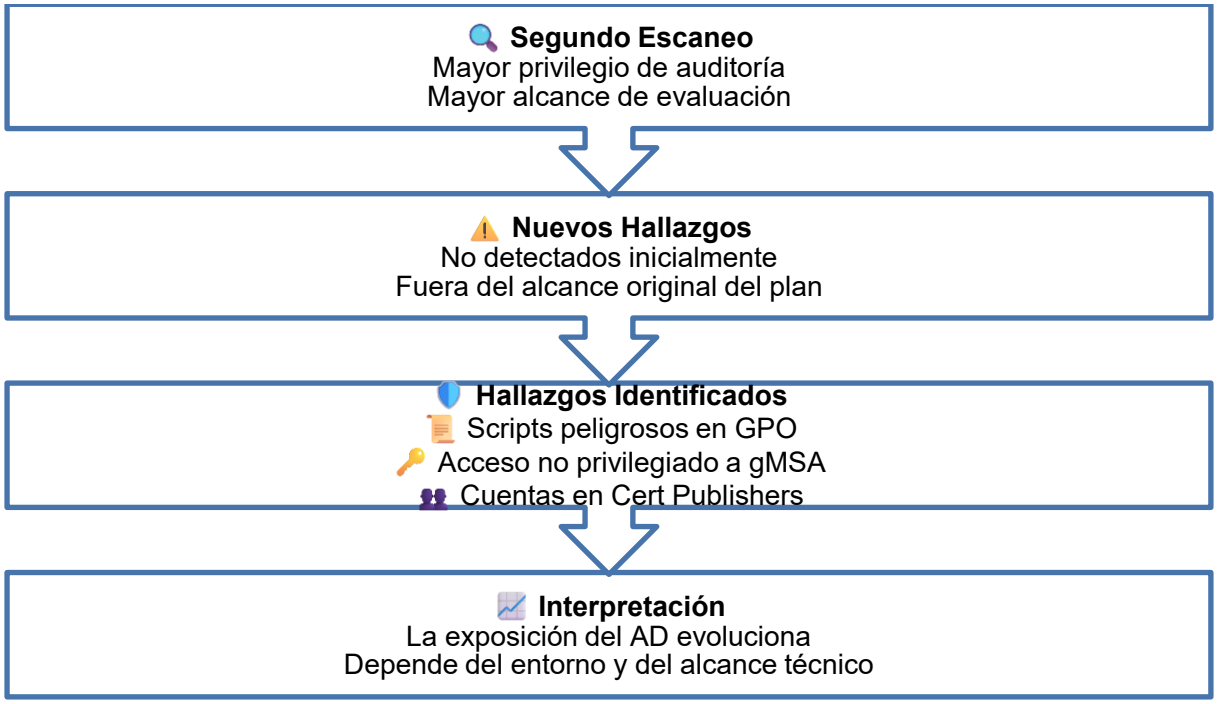

Ilustración 21 Nuevos Hallazgos Detectados Elaboración Propia

Estos hallazgos dejan claro algo importante, la superficie de exposición de un entorno de Directorio Activo no es fija. Lo que se detecta dependen tanto del estado real de la infraestructura y el nivel de acceso con el que se hace la evaluación. Por eso, las nuevas vulnerabilidades deben incorporarse al plan de implementación y atenderse lo más pronto posible, siempre que no requieran una ventana de mantenimiento para realizar la corrección.

Indicador	Escaneo 1	Escaneo 2	Cambio	Estado
Protocolos de red				
LDAP signing not required on DCs	0% F	0% F		Sin cambio
SMB signing not required on DCs	N/A	N/A		Inaccesible
SMBv1 enabled on DCs	N/A	N/A		Inaccesible
RC4 or DES encryption on DCs	15% F	27% F	+12 pp	Aritmético
Políticas y GPO				
UAC configurado correctamente	100% A+	100% A+		Mantenido
Changes to Default Domain Policy (7 días)	100% A+	100% A+		Mantenido

GPO linking delegation — DC OU level	64% D	100% A+	+36 pp	Resuelto
GPO linking delegation — domain level	82% C	100% A+	+18 pp	Resuelto
Dangerous GPO logon script path	-	82% C		Nuevo hallazgo
Cuentas y credenciales				
Privileged accounts — password never expires	15% F	15% F		Sin cambio
FGPP not applied to Global group	N/A	N/A		Sin permisos
KRBTGT account with old password	94% B	94% B		Sin cambio
Shadow credentials on privileged objects	15% F	100% A+	+85 pp	Resuelto
Write access to RBCD on DC	15% F	100% A+	+85 pp	Resuelto
Dangerous user rights — SeTcbPrivilege	47% D	100% A+	+53 pp	Resuelto
Protected Users group not in use	88% C+	89% C+	+1 pp	Mantenido
Non-privileged users with access to gMSA passwords	-	63% D	-	Nuevo hallazgo
Unexpected accounts in Cert Publishers Group	-	88% C+	-	Nuevo hallazgo

Tabla 32 Comparación de indicadores de seguridad entre escaneo 1 y escaneo 2 - Purple Knight

5.8 Componente de Monitoreo Continuo

Con el fin de complementar la propuesta técnica con evidencia del funcionamiento del componente de monitoreo, se presenta a continuación una seria de capturas del dashboard de Wazuh correspondientes al período de observación, posterior a la implementación de las reglas documentadas en la sección 5.5, Estas visualizaciones permiten corroborar que las reglas de detección se encuentran activas, generando alertas clasificadas por táctica y técnica de MITRE ATT&CK, las métricas de autenticación del Directorio Activo son capturadas y correlacionadas de forma continua sobre el agente instalado en los controladores de dominio de la organización.

5.8.1 Dashboard de alertas MITRE ATT&CK

La ilustración 20 muestra el dashboard de seguridad de Wazuh con filtros activos sobre las tácticas de Persistencia y Escalamiento de Privilegios, pertinente a las técnicas documentadas en este trabajo. Se evidencia la evolución temporal de las alertas, las distribuciones por técnica (Domain Accounts, Pass the Hash, Remote Desktop Protocol) y la cobertura por agente. La visualización de alertas bajo las tácticas TA0003 y TA0004 confirman que las reglas personalizadas diseñadas en la sección 5.5 están operando de forma correcta y produciendo telemetría para su respectiva revisión en caso de algún incidente.

Ilustración 22 Dashboard de alertas MITRE ATT&CK en Wazuh tácticas de Persistencia y Escalamiento de Privilegios. Elaboración propia, captura del entorno de producción, abril 2026.

5.8.2 Dashboard de métricas de autenticación del Directorio Activo

En la ilustración 21 se presentan las métricas de autenticación capturadas en una ventana de 24 horas sobre el controlador de dominio. Se registraron 2.682 inicios de sesión exitosos y 470 inicios de sesión fallidos, con su respectiva línea de tiempo en intervalos de 30 minutos. Este dashboard corresponde a las reglas asociadas a la técnica T1078.002(Valid Accounts – Domain Accounts), cuyo propósito es detectar patrones de autenticación anómala como aumento de intentos fallidos, autenticaciones fuera de horario habitual o accesos desde cuentas inactivas. La visibilidad continua sobre estas métricas permite identificar desviaciones respecto al comportamiento de referencia y escalar según los umbrales de severidad definidos en la sección 5.5.2.

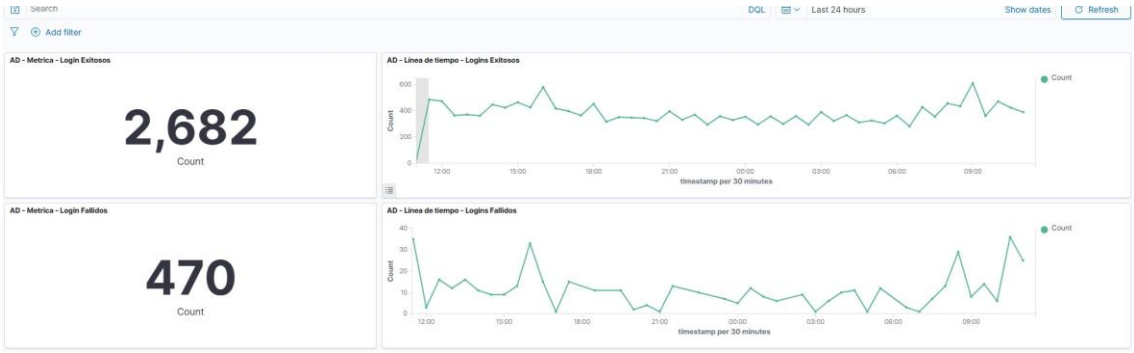

Ilustración 23 Dashboard de métricas de autenticación del Directorio Activo inicios de sesión exitosos (2.682) y fallidos (470) en ventana de 24 horas. Elaboración propia, captura del entorno de producción, abril 2026.

Ambas ilustraciones muestran el valor operativo de la integración entre el plan de *hardening* y el componente de monitoreo continuo: los controles de *hardening* reducen la superficie de ataque, mientras que las reglas de detección en Wazuh aseguran que cualquier intento de explotar las configuraciones residuales genera una alerta trazable y clasificada por las técnicas de MITRE ATT&CK.

Capítulo 6. Conclusiones y Recomendaciones

6.1 Conclusiones

Las conclusiones presentadas a continuación siguen el orden de los objetivos específicos, culminando con una evaluación del objetivo principal.

6.1.1 Conclusión sobre el objetivo específico 1: Identificar técnicas de ataques comunes asociadas al Directorio Activo según MITTRE ATT&CK para reconocer amenazas relevantes. El objetivo específico fue alcanzado y se concluye que:

La revisión sistemática de la literatura y el análisis del marco MITRE ATT&CK permitieron identificar y definir con precisión cinco técnicas de ataque de alto impacto que afectan directamente a los entornos de Directorio Activo *on-premise*. Las técnicas seleccionadas fueron: T1078.002 (Valid Accounts – Domain Accounts), T1484.002 (Domain Policy Modification), T1134.002 (Token Impersonation/Theft), T1547.002(Boot or Logon Autstart Execution) y T1574.001(Hijack Execution Flow – DLL Side-Loading). La selección se basó en tres criterios: prevalencia de incidentes reales, impacto sobre la infraestructura de identidad y disponibilidad de controles de mitigación concretos.

Las cinco técnicas no operan por separado: forman una cadena. Las cuentas comprometidas dan acceso inicial y abren la puerta a las demás técnicas. La manipulación de políticas expande el control sobre toda la infraestructura, la suplantación de *tokens* eleva privilegios sin necesitar credenciales adicionales. Asimismo, los mecanismos de autoarranque y el secuestro del flujo de ejecución mantienen la persistencia incluso tras reinicios y actualizaciones.

6.1.2 Conclusión sobre el objetivo específico 2: Comprender el estado de seguridad actual del Directorio Activo mediante la herramienta Purple Knight para interpretar hallazgos y debilidades en la configuración. El objetivo específico fue alcanzado y se concluye que:

La ejecución de la herramienta Purple Knight sobre el entorno de Directorio Activo produjo un diagnóstico cuantificable del estado de seguridad antes de aplicar controles. El puntaje inicial fue de 68% D+ confirmando una postura por debajo del promedio reportado por Semperis (2024), con una superficie de ataque considerable en gestión de cuentas, delegación y configuración de infraestructura. Los hallazgos más críticos fueron:

- La cuenta KRBTGT sin rotación por más de 4.700 días.
- Permisos GenericAll sobre naming context del dominio.
- Escritura sobre msDS-KeyCredentialLink en los siente controladores de dominio.
- Ausencia de firma LDAP en cinco de ellos.

Tras ejecutar la primera fase, el segundo escaneo registro una mejora de 14 puesto, llegado a un porcentaje de 82% C, por encima del umbral mínimo del fabricante. La

herramienta cumplió un doble rol: línea base para priorizar controles y mecanismo de validación del progreso.

6.1.3 Conclusión sobre el objetivo específico 3: Elaborar un plan de *hardening* basado en CIS Benchmark para fortalecer la seguridad del Directorio Activo. El objetivo específico fue alcanzado y se concluye que:

El plan de *hardening* consta de 25 controles organizados en cuatro secciones. Integra las directrices de CIS Benchmark para Windows Server y la plantilla de seguridad de Microsoft, además vincula cada control con la técnica de MITRE ATT&CK que mitiga. Asimismo, este plan fue implementado en un entorno de producción real. La primera fase estuvo enfocada a eliminar permisos excesivos sobre objetos privilegiados, resolviendo cinco indicadores que pasaron de F y D a 100% A+.

La división en tres fases según el nivel de impacto operativo es útil para organizaciones que necesitan mejorar su seguridad sin interrumpir a la operación. El plan generado es tanto replicable como trazable.

6.1.4 Conclusión sobre el objetivo específico 4: Clasificar reglas por medio de Wazuh para detectar comportamientos anómalos que puedan comprometer la integridad del Directorio Activo. El objetivo específico fue alcanzado y se concluye que:

La literatura sobre *hardening* de Directorio Activo rara vez aborda la detección de comportamientos anómalos. Este trabajo cierra esa brecha con 34 reglas de correlación personalizadas para Wazuh, organizadas por las técnicas de MITRE ATT&CK y clasificadas por severidad. Las reglas cubren patrones de autenticación anómala, fuerza bruta, escrituras en claves de registro críticas de LSA, acceso a memoria de LSASS y carga de DLL no firmadas desde rutas no estándar. La integración con Sysmon amplía la cobertura para las técnicas que el registro nativo de Windows no captura de forma confiable.

La validación está documentada en la sesión 5.8 con ilustraciones del dashboard de Wazuh en producción. Las reglas están activas y generan alertas bajo las tácticas TA0003 y TA0004. En una ventana de 24 horas se registraron 2.682 inicios de sesión exitosos y 470 fallidos, lo que confirma que la telemetría se correlaciona de forma continua y que la técnica T10078.002 produce visibilidad operativa real.

El resultado no es un catálogo de reglas, más bien es una capacidad de detección probada en un ambiente productivo.

6.1.5 Conclusión objetivo general: Crear un plan de hardening y monitoreo continuo de Directorio Activo para mitigar técnicas de persistencia y escalamiento de privilegios.

El objetivo fue alcanzado. La propuesta desarrollada integra de forma consecuente y complementaria tres componentes:

1. Diagnostico con la herramienta Purple Knight.

2. El plan de *hardening basado* en CIS Benchmark y alineado con MITRE ATT&CK.
3. Reglas de detección en Wazun con telemetría extendida mediante Sysmon.

La implementación en un ambiente de producción real valida empíricamente que el plan creado no es únicamente un ejercicio teórico, sino una propuesta técnica con impacto comprobado en ambos componentes: aplicación del *hardening* en el Directorio Activo evidenciando una mejora del puntaje global de Purple Knight que subió de 68% a 82 %, donde se resolvieron cinco indicadores críticos. Las ilustraciones del dashboard de Wazuh muestran alertas activas bajo las tácticas TA0003 y TA0004, y métricas de autenticación del Directorio Activo en el ambiente de producción capturadas de forma continua.

En definitiva, la revisión de la literatura demostró que la mayoría de los estudios y herramientas existentes abordan el *hardening* y monitoreo de forma independiente, pero no los integran de manera que los controles de endurecimiento(*hardening*) retroalimenten las capacidades de detección y viceversa.

Esta propuesta cierra esa brecha con evidencia empírica: no como un marco teórico más, sino como un plan ejecutado, medido y validado en un entorno de producción corporativo. Donde se muestra que el *hardening* a nivel de Directorio Activo y el monitoreo continuo no son procesos separados, sino una parte de un ciclo continuo. Donde aplicar controles de endurecimiento(*hardening*) ayuda a reducir la superficie de ataque mientras que las reglas de detección asegurar una visibilidad sobre cualquier intento de explotar configuraciones residuales, convirtiendo la seguridad del Directorio Activo en un proceso dinámico, medible y sostenible cuyos resultados son repetibles y atribuibles a acciones concretas.

6.2 Recomendaciones

A través de la experiencia obtenida durante el desarrollo de esta investigación, se presentan las siguientes recomendaciones. Las cuales buscan fortalecer futuros trabajos relacionados con la evaluación, endurecimiento y monitoreo continuo de entornos de Directorio Activo, así como optimizar el proceso metodológico en términos de precisión, diagnostico, profundidad analítica y viabilidad operativa de los resultados en escenarios organizacionales reales.

- Ejecutar Purple Knight con una cuenta de dominio con privilegios de administrador o auditoría completos: la comparación entre escaneos demostró que el nivel de acceso influye directamente en la cantidad de indicadores evaluados. Por lo tanto, el escaneo inicial debe realizarse siempre con permisos suficientes sobre todos los contenedores relevantes, incluido el contenedor de *Password Settings*, con el fin de

obtener una línea base más completa y representativa del estado de seguridad del entorno del Directorio Activo.

- Replicar el proceso en un entorno de laboratorio previo a la implementación en producción, si bien la propuesta fue validada directamente en un entorno productivo, se recomienda realizar una ejecución completa en un ambiente controlado, incluyendo una simulación de técnicas de ataque, antes de aplicarla dentro de una organización que no cuente con un equipo técnicamente especializado en Directorio Activo.
- Ampliar el análisis a técnicas adicionales de TA0003 y TA0004, en futuras investigaciones se puede extender la cobertura hacia otras técnicas como T1558.001 – Golden Ticket, T1003.006 – DCSync o T1098.001 – Additional Cloud Credentials, incorporando controles de *hardening* y reglas de detección que permitan ampliar el alcance preventivo y de monitoreo continuo del plan propuesto.
- Considerar la extensión del plan a entorno híbridos: el alcance de esta investigación se limitó únicamente a entornos *on-premise*. Se recomienda explorar en trabajos futuros cómo los controles y reglas propuestas se adaptan en escenarios de identidad híbrida como Azure Entra ID Connect.
- Formalizar el uso del plan como un insumo para auditorías de cumplimiento, la estructura del plan y la correspondencia entre controles, técnicas de MITRE ATT&CK y hallazgos de Purple Knight facilita su adaptación como lista de verificación bajo marcos como ISO 27001, NIST CSF o CIS Controls.

Glosario

A

AdminSDHolder Objeto especial del Directorio Activo que actúa como plantilla de permisos para cuentas privilegiadas. El proceso SDProp aplica periódicamente sus permisos a los objetos protegidos, evitando modificaciones no autorizadas en sus listas de control de acceso.

Fuente: *Microsoft. (2025). AdminSDHolder, Protected Groups and SDPROP. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information. Agencia francesa de seguridad de sistemas de información cuyas guías de configuración segura del Directorio Activo son referencia internacional en hardening. Sus criterios son utilizados por Purple Knight para evaluar la robustez de las políticas de contraseñas.

Fuente: *ANSSI. (2023). Active Directory Security. Agence Nationale de la Sécurité des Systèmes d'Information.* https://www.cert.ssi.gouv.fr/uploads/ad_en.html

AppLocker Función de control de aplicaciones de Windows que permite definir listas blancas de ejecutables, scripts, instaladores y DLL que pueden ejecutarse en un sistema, reduciendo la superficie de ataque asociada a técnicas de secuestro del flujo de ejecución.

Fuente: *Microsoft. (2025). AppLocker overview. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

AS-REP Roasting Técnica de ataque contra Kerberos que aprovecha cuentas configuradas sin preautenticación obligatoria. El atacante solicita un ticket AS-REP cifrado con el hash de la contraseña del usuario y lo descifra fuera de línea para obtener la credencial en texto claro.

Fuente: *MITRE. (2024). Steal or Forge Kerberos Tickets: AS-REP Roasting (T1558.004). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1558/004/

C

Credential dumping Proceso mediante el cual un atacante extrae credenciales almacenadas en memoria o en disco de un sistema comprometido. Herramientas como Mimikatz realizan volcados del proceso LSASS para obtener hashes NTLM y tickets Kerberos de usuarios autenticados.

Fuente: *MITRE. (2024). OS Credential Dumping (T1003). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1003/

D

DCSync Técnica de ataque (T1003.006) que simula el comportamiento de un controlador de dominio para solicitar la replicación de hashes de contraseñas mediante el protocolo MS-DRSR, sin necesidad de ejecutar código directamente en el controlador de dominio.

Fuente: *MITRE. (2024). OS Credential Dumping: DCSync (T1003.006). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1003/006/

DLL (Dynamic Link Library) Biblioteca de enlace dinámico. Archivo que contiene código y datos reutilizables por múltiples programas simultáneamente en Windows. Su mecanismo de carga puede ser abusado mediante técnicas de DLL side-loading o DLL search order hijacking para ejecutar código malicioso bajo el contexto de un proceso legítimo.

Fuente: *Microsoft. (2025). Dynamic-Link Libraries. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-libraries

E

EDR (Endpoint Detection and Response) Solución de seguridad de endpoints que monitorea y analiza de forma continua la actividad de los dispositivos para detectar, investigar y responder a amenazas avanzadas, incluyendo técnicas de evasión como el DLL side-loading.

Fuente: *Trend Micro. (2025). What is Endpoint Detection and Response (EDR)?* https://www.trendmicro.com/en_us/what-is/endpoint-security/endpoint-detection-response.html

F

Fine-Grained Password Policy (FGPP) Mecanismo del Directorio Activo que permite aplicar políticas de contraseñas y bloqueo de cuentas diferenciadas a grupos o usuarios específicos sin afectar la política general del dominio. Se configura mediante objetos PSO almacenados en el contenedor Password Settings Container.

Fuente: *Microsoft. (2025). Fine-Grained Password Policies. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-

G

GenericAll Permiso de control de acceso en el Directorio Activo que otorga control total sobre un objeto, incluyendo la capacidad de leer y modificar todos sus atributos, cambiar su propietario y modificar sus permisos. Su asignación indebida a cuentas no privilegiadas representa un vector crítico de escalamiento de privilegios.

Fuente: *Microsoft. (2025). Active Directory Access Control. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/win32/adschema/r-generic-all

gMSA (Group Managed Service Account) Tipo de cuenta de servicio administrada del Directorio Activo cuya contraseña es gestionada automáticamente por el dominio y puede ser utilizada por múltiples servidores. El acceso no autorizado a sus credenciales por parte de usuarios sin privilegios representa un riesgo de seguridad relevante.

Fuente: *Microsoft. (2025). Group Managed Service Accounts overview. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

Golden Ticket Ticket Kerberos forjado usando el hash de la cuenta KRBTGT que otorga al atacante acceso irrestricto y persistente a todos los recursos del dominio. Su creación es posible cuando el hash de KRBTGT ha sido comprometido y no ha sido rotado.

Fuente: *MITRE. (2024). Steal or Forge Kerberos Tickets: Golden Ticket (T1558.001). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1558/001/

I

IAT (Import Address Table) Tabla de importaciones de un ejecutable de Windows que contiene las referencias a las funciones de las DLL que utiliza. Es el objetivo principal en los ataques de DLL side-loading, ya que su manipulación redirige llamadas legítimas hacia código malicioso.

Fuente: *Microsoft. (2025). PE Format. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/win32/debug/pe-format

IoC (Indicador de Compromiso) Evidencia forense observable en una red o sistema que indica con alta probabilidad que ha ocurrido una intrusión activa. Puede incluir hashes de archivos maliciosos, conexiones a dominios de comando y control, o modificaciones en objetos críticos del Directorio Activo.

Fuente: *CISA. (s.f.). Indicators of Compromise. Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/topics/cyber-threats-and-advisories/indicators-of-compromise

IoE (Indicador de Exposición) Condición de configuración identificada en un entorno que representa una debilidad potencialmente explotable, sin que implique necesariamente un compromiso activo. Purple Knight evalúa indicadores de este tipo para cuantificar la postura de seguridad del Directorio Activo.

Fuente: *Semperis. (2025). Purple Knight User Guide.* https://www.semperis.com/purple-knight/

K

Kerberoasting Técnica de ataque (T1558.003) que solicita tickets de servicio Kerberos cifrados con el hash de la contraseña de cuentas con SPN registrado. El atacante descifra los tickets fuera de línea para obtener las credenciales en texto claro.

Fuente: *MITRE. (2024). Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1558/003/

L

LSA Protection (RunAsPPL) Configuración de seguridad de Windows que eleva el proceso LSASS a la categoría de Proceso Protegido Ligero, impidiendo que herramientas como Mimikatz lean su memoria o inyecten código. Se habilita mediante la clave de registro RunAsPPL en HKLM\SYSTEM\CurrentControlSet\Control\Lsa.

Fuente: *Microsoft. (2025). Configuring Additional LSA Protection. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

LSASS (Local Security Authority Subsystem Service) Proceso crítico de Windows responsable de la autenticación de usuarios, la gestión de credenciales y el manejo de tokens de acceso. Es el objetivo principal de técnicas de extracción de credenciales, ya que almacena hashes NTLM y tickets Kerberos en memoria.

Fuente: *Microsoft. (2025). Configuring Additional LSA Protection. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

M

Man-in-the-middle (MITM) Tipo de ataque en el que el adversario intercepta y potencialmente altera las comunicaciones entre dos partes sin que ninguna lo detecte. En el contexto del Directorio Activo, la ausencia de firma LDAP expone el tráfico de directorio a este tipo de ataque.

Fuente: *MITRE. (2024). Adversary-in-the-Middle (T1557). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1557/

Mimikatz Herramienta de post-explotación ampliamente utilizada para extraer credenciales en texto claro,

hashes NTLM y tickets Kerberos desde la memoria del proceso LSASS. Su uso está asociado a múltiples técnicas de MITRE ATT&CK como T1003 y T1134.

Fuente: *MITRE. (2024). Software: Mimikatz (S0002). MITRE ATT&CK.* https://attack.mitre.org/software/S0002/

MS-DRSR (Directory Replication Service Remote Protocol) Protocolo de Microsoft utilizado para la replicación de datos entre controladores de dominio. Es abusado en la técnica DCSync, donde el atacante simula ser un controlador de dominio y solicita la replicación de hashes de contraseñas.

Fuente: *Microsoft. (2025). [MS-DRSR]: Directory Replication Service (DRS) Remote Protocol. Microsoft Learn.* https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-drsr

msDS-KeyCredentialLink Atributo del Directorio Activo utilizado por el mecanismo PKINIT de Kerberos para la autenticación sin contraseña. La escritura no autorizada sobre este atributo permite inyectar credenciales alternativas (Shadow Credentials) en la cuenta víctima.

Fuente: *Microsoft. (2025). MS-DS-Key-Credential-Link attribute. Microsoft Learn.* https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/aa0dc7d5-4b5e-4e55-8e8c-dcc2f5e5d4a8

P

Pass-the-Hash (PtH) Técnica de ataque (T1550.002) que permite al adversario autenticarse ante servicios de red usando el hash NTLM de una contraseña en lugar de la contraseña en texto claro, sin necesidad de descifrarla.

Fuente: *MITRE. (2024). Use Alternate Authentication Material: Pass the Hash (T1550.002). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1550/002/

Pass-the-Ticket (PtT) Técnica de ataque (T1550.003) en la que el adversario roba un ticket Kerberos válido desde la memoria de un sistema comprometido y lo utiliza para autenticarse ante otros servicios de la red sin necesidad de conocer la contraseña del usuario.

Fuente: *MITRE. (2024). Use Alternate Authentication Material: Pass the Ticket (T1550.003). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1550/003/

PKINIT Extensión del protocolo Kerberos que permite la autenticación mediante certificados de clave pública en lugar de contraseñas. Es el mecanismo que hace posible los ataques de Shadow Credentials, donde una clave pública maliciosa se inyecta en el atributo msDS-KeyCredentialLink.

Fuente: *Microsoft. (2025). Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). Microsoft Learn.* https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-pkca

Potato attacks (JuicyPotato, SweetPotato) Familia de técnicas de escalamiento de privilegios local en Windows que abusan del privilegio SeImpersonatePrivilege para suplantar el token de una cuenta privilegiada (usualmente SYSTEM), capturando autenticaciones NTLM o COM mediante

servidores locales bajo control del atacante.

Fuente: *MITRE. (2024). Access Token Manipulation: Token Impersonation/Theft (T1134.001). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1134/001/

PSO (Password Settings Object) Objeto del Directorio Activo que contiene una Fine-Grained Password Policy. Se almacena en el contenedor Password Settings Container y se vincula a usuarios o grupos para aplicarles configuraciones de contraseñas más restrictivas que la política general del dominio.

Fuente: *Microsoft. (2025). Fine-Grained Password and Account Lockout Policy. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100-

R

RBCD (Resource-Based Constrained Delegation) Tipo de delegación de Kerberos controlada desde el recurso de destino mediante el atributo msDS-AllowedToActOnBehalfOfOtherIdentity. Su configuración maliciosa permite a un atacante con permisos de escritura sobre dicho atributo configurar servicios bajo su control para actuar en nombre de cualquier usuario ante los controladores de dominio.

Fuente: *Microsoft. (2025). Resource-Based Constrained Delegation. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-constrained-delegation-overview

RC4-HMAC-MD5 Tipo de cifrado utilizado históricamente por el protocolo Kerberos en Windows. Considerado criptográficamente débil, su coexistencia con AES permite ataques de degradación en los que el adversario fuerza la emisión de tickets con este cifrado para facilitar técnicas como Kerberoasting.

Fuente: *Microsoft. (2025). Kerberos Encryption Types. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/security/kerberos/preventing-kerberos-change-password-that-uses-rc4-secret-keys

RDP (Remote Desktop Protocol) Protocolo propietario de Microsoft que permite el acceso remoto a escritorios de Windows. Es frecuentemente abusado por atacantes para el movimiento lateral dentro de entornos corporativos una vez obtenidas credenciales válidas.

Fuente: *MITRE. (2024). Remote Services: Remote Desktop Protocol (T1021.001). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1021/001/

S

SafeDLLSearchMode Configuración del registro de Windows que modifica el orden de búsqueda de DLL, priorizando las rutas del sistema (System32) sobre el directorio de trabajo actual, reduciendo la efectividad de ataques de DLL search order hijacking. Se habilita mediante la clave SafeDllSearchMode en HKLM\SYSTEM\CurrentControlSet\Control\Session Manager.

Fuente: *Microsoft. (2025). Dynamic-Link Library Search Order. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-search-order

SAM (Security Account Manager) Base de datos local de Windows que almacena las credenciales de cuentas locales en forma de hashes NTLM. Restringir el acceso remoto a SAM mediante RPC es una medida de hardening para prevenir ataques de enumeración y extracción de credenciales.

Fuente: *Microsoft. (2025). Network access: Restrict clients allowed to make remote calls to SAM. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

SDProp (Security Descriptor Propagator) Proceso del Directorio Activo que se ejecuta cada 60 minutos y aplica los permisos del objeto AdminSDHolder a todas las cuentas y grupos protegidos, revirtiendo cualquier modificación no autorizada en sus listas de control de acceso.

Fuente: *Microsoft. (2025). AdminSDHolder, Protected Groups and SDProp. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory

SeImpersonatePrivilege Privilegio de Windows que permite a un proceso suplantar el token de seguridad de otro usuario o proceso. Su asignación a cuentas no administrativas representa un vector crítico para técnicas de escalamiento de privilegios como los Potato attacks.

Fuente: *Microsoft. (2025). Impersonate a client after authentication. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/impersonate-a-client-after-authentication

SeTcbPrivilege Privilegio de Windows denominado "Actuar como parte del sistema operativo". Su asignación permite a un proceso actuar con los permisos del sistema operativo, representando un riesgo crítico de escalamiento de privilegios. CIS Benchmark establece que debe asignarse únicamente a la cuenta de sistema.

Fuente: *Microsoft. (2025). Act as part of the operating system. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/act-as-part-of-the-operating-system

Shadow Credentials Técnica de ataque que consiste en inyectar una clave pública maliciosa en el atributo msDS-KeyCredentialLink de una cuenta del Directorio Activo. Permite al atacante autenticarse como esa cuenta mediante PKINIT sin conocer su contraseña.

Fuente: *MITRE. (2024). Account Manipulation: Additional Cloud Credentials (T1098.001). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1098/001/

SIDHistory Atributo del Directorio Activo que almacena los identificadores de seguridad anteriores de una cuenta, utilizados durante migraciones de dominio. Su abuso permite a un atacante agregar SIDs de grupos privilegiados a su cuenta, obteniendo acceso a recursos sin pertenecer formalmente a esos grupos.

Fuente: *MITRE. (2024). Access Token Manipulation: SID-History Injection (T1134.005). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1134/005/

SMB (Server Message Block) Protocolo de red de Microsoft para compartir archivos, impresoras y recursos entre sistemas. La ausencia de firma digital en SMB expone las comunicaciones a ataques de retransmisión NTLM (NTLM relay), que pueden usarse para autenticarse ante otros servicios sin conocer las credenciales.

Fuente: *Microsoft. (2025). Overview of file sharing using the SMB 3 protocol. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/storage/file-server/file-server-smb-overview

SMBv1 Primera versión del protocolo SMB, considerada obsoleta e insegura. Fue explotada masivamente por el ransomware WannaCry mediante la vulnerabilidad EternalBlue. Su deshabilitación es una medida de hardening básica recomendada por CIS Benchmark.

Fuente: *Microsoft. (2024). How to detect, enable and disable SMBv1, SMBv2, and SMBv3. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

SPN (Service Principal Name) Identificador único de una instancia de servicio en el Directorio Activo, utilizado por Kerberos para asociar un servicio con una cuenta de inicio de sesión. Las cuentas con SPN registrados son susceptibles a ataques de Kerberoasting.

Fuente: *Microsoft. (2025). Service Principal Names. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names

SYSVOL Carpeta compartida replicada entre controladores de dominio que contiene scripts de inicio de sesión, plantillas de directivas de grupo y archivos de configuración del dominio. Su exposición a permisos de escritura excesivos representa un vector de ataque para inyección de scripts maliciosos.

Fuente: *Microsoft. (2025). SYSVOL and NETLOGON shares. Microsoft Learn.* https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/sysvol-netlogon-shares-not-present-after-upgrade

T

TGT (Ticket Granting Ticket) Ticket emitido por el KDC de Kerberos tras la autenticación inicial del usuario. Permite solicitar tickets de servicio sin necesidad de volver a autenticarse. Su compromiso, como en el caso del Golden Ticket, otorga al atacante acceso persistente a todos los recursos del dominio.

Fuente: *Microsoft. (2025). Kerberos Authentication Overview. Microsoft Learn.* https://learn.microsoft.com/en-us/windows-

server/security/kerberos/kerberos-authentication-overview

Token de acceso (Access Token) Objeto de seguridad de Windows que describe el contexto de seguridad de un proceso o subproceso, incluyendo la identidad del usuario, sus grupos y privilegios. Las técnicas T1134.001 y T1134.002 abusan de los mecanismos DuplicateToken e ImpersonateLoggedOnUser para manipular estos tokens y ejecutar acciones con privilegios elevados.

Fuente: *Microsoft. (2025). Access Tokens. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/win32/secauthz/access-tokens

U

UAC (User Account Control) Mecanismo de seguridad de Windows que solicita confirmación o credenciales de administrador antes de permitir cambios que afecten al sistema, reduciendo el impacto de software malicioso que se ejecuta con privilegios de usuario estándar.

Fuente: *Microsoft. (2025). How User Account Control works. Microsoft Learn.* https://learn.microsoft.com/en-us/windows/security/application-security/application-control/user-account-control/how-it-works

W

WMI (Windows Management Instrumentation) Infraestructura de gestión de Windows que proporciona una interfaz unificada para la administración de sistemas. Es frecuentemente utilizada por atacantes para el movimiento lateral y la ejecución remota de comandos, ya que está presente de forma nativa en todos los sistemas Windows.

Fuente: *MITRE. (2024). Windows Management Instrumentation (T1047). MITRE ATT&CK.* https://attack.mitre.org/techniques/T1047/

X

XDR (Extended Detection and Response) Evolución del EDR que unifica la detección y respuesta a amenazas a través de múltiples capas de seguridad (endpoints, red, identidad y nube) en una sola plataforma. Wazuh se clasifica como una solución SIEM/XDR de código abierto.

Fuente: *Wazuh. (2025). What is XDR? Wazuh Documentation.* https://documentation.wazuh.com/current/getting-started/use-cases/xdr.html

Referencias

Active Directory Domain Services overview. (n.d.). Microsoft.com. Retrieved May 3, 2026, from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Active Directory security assessment. (2022, May 25). Purple Knight. https://www.semperis.com/purple-knight/

CIS benchmarks®. (s/f). CIS; Center for Internet Security. Recuperado el 3 de mayo de 2026, de https://www.cisecurity.org/cis-benchmarks

CIS Center for Internet Security. (s. f.). CIS. https://www.cisecurity.org/

Dieterich, A., Schopp, M., Stiemert, L., Steininger, C., & Pöhn, D. (2023). Evaluation of persistence methods used by malware on Microsoft windows systems. Proceedings of the 9th International Conference on Information Systems Security and Privacy, 552–559.

Getting to Know the CIS Benchmarks. (2022, 14 abril). CIS. https://www.cisecurity.org/insights/blog/getting-to-know-the-cis-benchmarks

Goel, D., Ward, M., Neumann, A., Neumann, F., Nguyen, H., & Guo, M. (2024). Hardening Active Directory Graphs via Evolutionary Diversity Optimization-based Policies. ACM Transactions On Evolutionary Learning And Optimization, 5(3), 1-36. https://doi.org/10.1145/3688401

Grillenmeier, G. (2023). Improving your Active Directory security posture: AdminSDHolder to the rescue. Cyber Security: A Peer-Reviewed Journal, 6(3), 242. https://doi.org/10.69554/yeek7400

Guía completa de tácticas de ATT&CK: el marco MITRE. (s. f.). https://www.startupdefense.io/es-us/blog/guia-completa-de-tacticas-de-att-ck-el-marco-mitre

Holdsworth, J., & Kosinski, M. (2025, noviembre 27). ¿Qué es la seguridad de la información? Ibm.com. https://www.ibm.com/es-es/think/topics/information-security

IBM security QRadar EDR. (2026, enero 29). Ibm.com. https://www.ibm.com/docs/en/security-qradar-edr/3.12?topic=endpoints-reviewing-alerts

International Organization for Standardization. (2012). ISO/IEC 27005:2012: Information technology — Security techniques — Information security risk management. ISO.

International Organization for Standardization. (2023). ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection — Information security controls. ISO.

Jiang, Y., Meng, Q., Shang, F., Oo, N., Minh, L. T. H., Lim, H. W., & Sikdar, B. (2025). MITRE ATT&CK applications in cybersecurity and the way forward. En arXiv [cs.CR]. https://doi.org/10.48550/arXiv.2502.10825

Lateral Movement. (n.d.). Mitre.org. Retrieved May 3, 2026, from https://attack.mitre.org/tactics/TA0008/

Lopez, V. (2024, 13 marzo). Bastionado de redes y sistemas: qué es y para qué sirve | S2GRUPO. S2GRUPO. https://s2grupo.es/bastionado-de-redes-y-sistemas-que-es-y-para-que-sirve/

Markruss. (s. f.). *Sysmon - sysinternals*. Microsoft Learn. https://learn.microsoft.com/sysinternals/downloads/sysmon

Marsiholo. (s. f.). Icono de escalada de privilegios [Icono]. Freepik. https://www.freepik.es/icono/escalada-privilegios_15163335

Monitoring Active Directory for signs of compromise. (n.d.). Microsoft.com. Retrieved May 3, 2026, from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

Officedocspr. (s. f.). *Security baselines guide*. Microsoft Learn. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

Orin-Thomas. (n.d.). Group Policy overview for Windows Server. Microsoft.com. Retrieved May 3, 2026, from https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview

Persistence. (n.d.). Mitre.org. Retrieved May 3, 2026, from https://attack.mitre.org/tactics/TA0003/

Privilege Escalation. (n.d.). Mitre.org. Retrieved May 3, 2026, from https://attack.mitre.org/tactics/TA0004/

¿Qué es la investigación cualitativa? (2025, February 11). ATLAS.ti. https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/investigacion-cualitativa

¿Qué es la seguridad de la información (InfoSec)? | Seguridad de Microsoft. (s. f.). https://www.microsoft.com/es-es/security/business/security-101/what-is-information-security-infosec

Rahman, M. R., & Williams, L. (2022). An investigation of security controls and MITRE ATT&CK techniques. En arXiv [cs.CR]. https://doi.org/10.48550/arXiv.2211.06500

Sharma, S. (2025, 19 julio). Applying MITRE ATT&CK framework to your Active Directory. Fidelis Security. https://fidelissecurity.com/threatgeek/active-directory-security/applying-mitre-attck-framework-to-active-directory/

Simister, A., & Simister, A. (2025, 26 noviembre). What is Active Directory and How It Works? | Lepide Blog. Lepide Blog: A Guide To IT Security, Compliance And IT Operations. https://www.lepide.com/blog/what-is-active-directory/

SwiftOnSecurity. (s. f.). *GitHub - SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing*. GitHub. https://github.com/SwiftOnSecurity/sysmon-config

Tactics - Enterprise. (n.d.). Mitre.org. Retrieved May 3, 2026, from https://attack.mitre.org/tactics/

Villalón-Huerta, A., Marco-Gisbert, H., & Ripoll-Ripoll, I. (2022). A taxonomy for threat actors' persistence techniques. Computers & Security, 121(102855), 102855. https://doi.org/10.1016/j.cose.2022.102855

Wazuh. (2023, August 18). Security configuration assessment. Wazuh. https://wazuh.com/resources/use-cases/security-configuration-assessment/

Wazuh. (s. f.). *Rules classification - Rules · Wazuh documentation*. https://documentation.wazuh.com/current/user-manual/ruleset/rules/rules-classification.html

What is Information Security (InfoSEC)? | Microsoft Security. (s. f.). https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec

What is security information and event management (SIEM)? (n.d.). Trend Micro. Retrieved May 3, 2026, from https://www.trendmicro.com/en/what-is/security-operations/security-information-and-event-management.html