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)

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

Angie Paola Abarca Moreno[1]
[1]Universidad CENFOTEC, San José, Costa Rica
email:aabarcam@ucenfotec.ac.cr

Resumen Ejecutivo. El Directorio Activo es el servicio central de gestión de identidades de la mayoría de las infraestructuras corporativas, convirtiéndose en el principal objetivo de los atacantes que buscan establecer persistencia y escalar privilegios. A pesar de su importancia crítica, muchas organizaciones carecen de una estrategia integral que combine hardening proactivo del entorno con mecanismos de detección continúa alineados con el comportamiento del adversario. Este artículo presenta el diseño y la validación empírica de un plan de hardening y monitoreo continuo para entornos de Directorio Activo on-premise, orientado a mitigar cinco técnicas de alto impacto basadas en las tácticas de Persistencia (TA0003) y Escalamiento de Privilegios (TA0004) del marco MITRE ATT&CK: T1078.002, T1484.002, T1134.002, T1547.002 y T1574001. La metodología adoptó un enfoque cualitativo, evaluativo y propositivo, fundamentado en la revisión sistemática de la 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 comprende 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 dashboard 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 capturadas 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.

I. INTRODUCCIÓN

El Directorio Activo (DA) se establece como el vector de ataque crítico por excelencia en los entornos corporativos modernos, dado su rol central en la gestión de identidades. En efecto posee las “llaves del reino”, ya que controla el acceso a los recursos críticos de toda la organización. Su compromiso concede a un adversario el control efectivo sobre la infraestructura de tecnología de información, lo que conduce inevitablemente a pérdidas económicas sustanciales, filtración de datos sensibles y daño reputacional severo. 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. El informe de inteligencia de CrowdStrike (2024) documentó 291 víctimas de filtración de datos y *ransomware* en América Latina, un aumento del 15% interanual, atribuido principalmente a la debilidad de las configuraciones por defecto del Directorio Activo y la ausencia de controles de *hardening* proactivo.

La raíz del problema reside en una combinación de factores: configuraciones permisivas heredadas, ausencia de monitoreo efectivo y la subestimación del Directorio Activo como superficie de ataque prioritaria. Investigaciones como la de Grillenmeire (2023) demuestran que una configuración robusta impacta directamente en la dificultad que encuentra un atacante durante las fases de reconocimiento, movimiento lateral y escalamiento de privilegios, técnicas catalogadas en la matriz MITRE ATT&CK. Sin embargo, la sola implementación de *hardening* resulta insuficiente sin un marco de monitoreo continuo que detecte y responda a actividades anómalas que intenten evadir los controles establecidos.

La revisión sistemática de la literatura confirmó que la mayoría de los estudios abordan el *hardening* y el monitoreo de forma independiente, pero no los integra de manera que los controles de endurecimiento(*hardening*) retroalimenten las capacidades de detección y viceversa. Esta desconexión deja a los entornos corporativos expuestos a brechas prolongadas y de alto impacto.

Ante esta brecha, la presente investigación tiene como objetivo general crear un plan de *hardening* y monitoreo continuo de Directorio Activo para mitigar técnicas de persistencia y escalamiento de privilegios. Los objetivos específicos son: (1) identificar técnicas de ataques comunes asociadas al Directorio Activo según MITTRE ATT&CK para reconocer amenazas relevantes; (2) comprender el estado de seguridad actual del Directorio Activo mediante la herramienta Purple Knight para interpretar hallazgos y debilidades en la configuración; (3) elaborar un plan de *hardening* basado en CIS Benchmark para fortalecer la seguridad del Directorio Activo; (4) clasificar reglas por medio de Wazuh para detectar comportamientos anómalos que puedan comprometer la integridad del Directorio Activo.

El trabajo se enmarca en el contexto de organizaciones con infraestructuras de Directorio Activo *on-premise*, sector donde la literatura aplicada es escaza y la necesidad de marcos de protección integrales y accionables es creciente.

II. MÉTODO

La investigación adoptó un enfoque cualitativo, evaluativo y propositivo, orientado a analizar una problemática existente, diagnosticar su estado actual y proponer un modelo estructurado de solución. El alcance es descriptivo y analítico, enfocado a caracterizar factores que incrementan la superficie de ataque del Directorio Activo y a establecer relaciones entre los controles de *hardening* y capacidades de detección.

La recolección de datos se fundamentó en dos instrumentos principales. Primero, una revisión sistemática de la literatura con cadenas de búsqueda en repositorios como IEEE, ACM. EBSCO y MITRE.org, utilizando los términos "Active Directory" AND "MITRE ATT&CK", combinados con "persistence" OR "privilege escalation" y "hardening" OR "monitoring" OR "detection". Los criterios de inclusión exigieron que los estudios abordaran entornos de Directorio Activo *on-premise* y las tácticas TA0003 y TA0004 con propuestas técnicas aplicables. El proceso alcanzó una saturación teórica tras revisar 40 documentos. Segundo, una auditoría de seguridad mediante la herramienta Purple Knight 5.0 Cummunity Edition de Semperis, ejecutada sobre el entorno de Directorio Activo de una institución financiera costarricense con más de 25 años de operación, con 7 controladores de dominio sobre Windows Server 2016 o superior. Por razones de confidencialidad de la información, no se da a conocer el dominio donde se realizó el escaneo de la herramienta.

La propuesta se estructura en tres componentes interdependientes. El primero, diagnóstico de seguridad, se utilizó Purple Knight para evaluar más de 150 indicadores en cinco categorías: Kerberos Security, Group Policy Security, Account Security, AD Delegation y AD Infraestructure Security. El segundo, plan de *hardening*, comprende 25 controles técnicos organizados en cuatro secciones alineadas con técnicas de MITRE ATT&CK, fundamentados en CIS Benchmark para Windows Server y la plantilla de Microsoft. El tercero, monitoreo continuo, consiste en 34 reglas de detección personalizadas para Wazuh, complementadas con Sysmon como fuente de telemetría avanzada, organizadas por técnica y clasificadas por nivel de severidad según el esquema nativo de la plataforma.

El anexo A contiene la guía de *hardening* y el componente de monitoreo continuo de esta propuesta. A continuación, se describe el proceso recomendado para su implementación.

Prerrequisitos de infraestructura y conocimiento

El plan está diseñado para entornos con los siguientes requisitos: Windows Server 2016 o superior, PowerShell 5.1 o superior con el módulo de Directorio Activo instalado como parte de RSAT[1], y una cuenta con privilegios de Administrador de Dominio. Para el componente de monitoreo se requiere adicionalmente un servidor Wazuh 4.7 o superior con al menos 50 GB de espacio libre, Sysmon v15 o superior instalado en los controladores de dominio y la plantilla de configuración SwiftOnSecurity como base para la telemetría avanzada. Antes de ejecutar cualquier control, se recomienda realizar un *snapshot* o *backup* completo del controlador de dominio como media de contingencia.

En cuanto a conocimientos previos, el plan asume experiencia práctica en administración de Directorio Activo, manejo del editor de directivas de grupo, ejecución de *scripts* en PowerShell y comprensión de los conceptos fundamentales de autenticación en Windows como NTLM, Kerberos y *tokens* de acceso. Para el componente de

[1] RSAT (Remote Server Administration Tools) es un conjunto de herramientas gratuitas de Microsoft que permite a los administradores de TI gestionar funciones y características de Windows Server de forma remota desde estaciones de trabajo con Windows 10/11 (Pro/Enterprise)

monitoreo se requiere adicionalmente conocimiento en la plataforma de Wazuh, compresión del esquema de niveles de alerta que van del nivel 0 al 15, y la capacidad para interpretar eventos del registro de seguridad de Windows y del canal operativo de Sysmon.

El diagnóstico como punto de entrada

El primer paso antes de ejecutar cualquier control de la guía es establecer una línea base objetiva del estado de seguridad del entorno del Directorio Activo. Los controles que resultan más urgentes varían de una organización a otra; un entorno puede tener políticas de contraseñas correctamente configuradas, pero exposiciones críticas en delegación de permisos, mientras que otro puede presentar un patrón inverso. Aplicar todos los controles sin un diagnóstico previo es ineficiente y potencialmente disruptivo.

El instrumento de diagnóstico recomendado es Purple Knight 5.0 Community Edition de Semperis, disponible de forma gratuita con registro. La herramienta se ejecuta directamente desde el controlador de dominio como administrador, seleccionado el dominio objetivo y las cinco categorías *on-premise*: Kerberos Security, Group Policy Security, Account Security, AD Delegation y AD Infrastructure Security. El reporte final incluye el porcentaje global, un puntaje por categoría e indicadores de exposición (IoE) e indicadores de compromiso (IoC). El mismo es un mapa que orienta la priorización de los controles, por ejemplo: los indicadores con calificación más baja son los que se deben abordar primero, independientemente de la sección de la guía en que se encuentren.

Un aspecto importante para considerar es el nivel de acceso de la cuenta utilizada para el escaneo. Con el fin de obtener una línea base completa, el diagnostico debe realizarse con una cuenta que tenga permisos de lectura sobre los contenedores relevantes del Directorio Activo, incluyendo el contenedor de Password Settings y las unidades organizativas de controladores de dominio. Un escaneo con acceso limitado evaluará menos indicadores, produciendo una línea base incompleta que puede llevar a subestimar la superficie de ataque real.

Sección 4.1 Controles de Gestión de Cuentas y Credenciales (T1078.002)

Esta sección es el inicio para la mayoría de las organizaciones, dado que T1078.002 es la técnica de mayor prevalencia en incidentes reales que involucran Directorio Activo. Sus cuatro controles actúan sobre el ciclo de vida de las credenciales del dominio, reduciendo la ventana de explotación de una credencial comprometida y eliminando la posibilidad de fabricar *Golden Tickets* a partir de un *hash* de KRBTGT antiguo.

El primer control es la política de contraseñas del dominio, configurada mediante la GPO Default Domain Policy con una longitud mínima de 15 caracteres, vigencia máxima de 60 días, historial de 24 contraseñas y complejidad habilitada. Estos valores representan un endurecimiento significativo respecto a los valores por defecto de Windows Server. El segundo control es la política de bloqueo de cuentas con umbral de 10 intentos fallidos, duración de bloqueo de 15 minutos y restablecimiento automático tras el mismo período. El tercer control es la Fine-Grained Password Policy para cuentas privilegiadas, que permite aplicar restricciones más estrictas al grupo de administradores de dominio sin afectar la política general. La guía recomienda crear un grupo dedicado como PSO-

Tier0-Admins con longitud mínima de 25 caracteres, historial de 24 contraseñas, vigencia máxima de 30 días y umbral de bloqueo de 3 intentos, implementado mediante PowerShell con privilegios de Domain Admin.

El cuarto control es la rotación periódica de la cuenta KRBTGT, cuya contraseña debe rotarse al menos cada 180 días y siempre después de un incidente de seguridad. La rotación debe ejecutarse dos veces con un intervalo mínimo de 10 horas entre ejecuciones para invalidar todos los *tickets* Kerberos activos en el dominio. Antes de ejecutarla es obligatorio validar el estado de la replicación entre controladores mediante repadmin /replsummary y dcdiag /test:replications. Este control requiere ventana de mantenimiento, plan de *rollback* documentado y aprobación formal del cambio.

Sección 4.2 Controles de Protección de Credenciales y Privilegios (T1078.002, T1134.002, T1547.002)

Esta sección agrupa los controles orientados a proteger las credenciales almacenadas en memoria y a restringir los derechos de usuario que permiten el escalamiento de privilegios. Son especialmente relevantes para mitigar el uso de herramientas como Mimikatz y técnicas de volcado de LSASS, dado que el proceso LSASS es el objetivo principal de los ataques de robo de credenciales en entornos Windows.

LSA Protection configura el proceso LSASS como Proceso Protegido Ligero mediante la clave de registro RunAsPPL, impidiendo que procesos no autorizados lean su memoria o inyecten código en él. Se configura mediante GPO en Configuración del equipo > Preferencias > Configuración de Windows > Registro. La deshabilitación de WDigest elimina el almacenamiento de contraseñas en texto plano en la memoria del proceso LSASS. Ambos controles pueden aplicarse sin ventana de mantenimiento, aunque se recomienda verificar su estado en cada controlador de dominio mediante PowerShell antes y después de aplicar la directiva.

La configuración de NTLMv2 con rechazo explícito de LM y NTLMv1 se realiza en Directivas locales > Opciones de seguridad. Antes de aplicar este control es indispensable auditar si existen sistemas heredados en el entorno que aún dependan de LM o NTLMv1, dado que su rechazo puede interrumpir la autenticación de esos sistemas. La restricción de derechos de usuario críticos como Crear un objeto *token*, Actuar como parte del sistema operativo y Depurar programas se configura en Directivas locales > Asignación de derechos de usuario y es directamente relevante para mitigar T1134.002.

La incorporación de cuentas privilegiadas al grupo Protected Users aplica automáticamente restricciones adicionales: no pueden autenticarse con NTLM, CredSSP ni Digest, sus *tickets* Kerberos no son renovables y no pueden utilizar delegación Kerberos no restringida. Antes de agregar cualquier cuenta al grupo es obligatorio auditar si alguna cuenta candidata es utilizada por servicios que dependan de estos mecanismos, dado que su incorporación puede causar interrupciones. El comando Get-ADUser -Filter {ServicePrincipalName -ne "$null"} -Properties ServicePrincipalName permite identificar las cuentas de servicio activas como punto de partida para esta verificación.

Sección 4.3 Controles de Políticas de Dominio y Opciones de Seguridad (T1484.002)

Esta sección protege la integridad de la infraestructura de directivas del dominio, que es el vector que un adversario con acceso al dominio utilizaría para propagar cambios maliciosos a todos los equipos miembros de forma simultánea. Sus controles se distribuyen entre opciones de seguridad críticas y la auditoría de permisos sobre GPOs y SYSVOL.

Las opciones de seguridad críticas se configuran mediante GPO en Directivas locales > Opciones de seguridad. El control de mayor criticidad de esta sección es la firma LDAP, que debe configurarse en modo "Requiere firma" para impedir ataques de intermediario sobre el tráfico de directorio, implementándose de forma escalonada iniciando en modo "Negociar firma" para identificar clientes que no soporten la firma antes de activar el modo requerido. La guía documenta adicionalmente once opciones de seguridad que incluyen la firma SMB para cliente y servidor, las restricciones de UAC, la restricción de llamadas RPC anónimas a SAM, el límite de inactividad de equipo en 900 segundos y la prohibición de enumeraciones anónimas de cuentas SAM.

La auditoría de permisos sobre GPOs y SYSVOL se realiza mediante el *script* de PowerShell documentado en la sección 4.3.2 de la guía, que lista todas las GPOs del dominio e identifica aquellas sobre las que usuarios no administradores tienen permisos de escritura. Este *script* debe ejecutarse como parte del diagnóstico inicial y repetirse periódicamente. La detección de permisos de escritura no autorizados sobre una GPO es un hallazgo de alta criticidad que debe remediarse de inmediato, dado que su explotación permite al adversario propagar código malicioso a todos los equipos del dominio afectados por esa directiva.

Sección 4.4 Controles de Flujo de Ejecución y DLL (T1574.001)

Esta sección mitiga la técnica de DLL *side-loading*, mediante la cual un adversario coloca una DLL maliciosa con el nombre de una legítima en un directorio de mayor prioridad en el orden de búsqueda de Windows. Sus dos controles actúan sobre el mecanismo de carga de DLL del sistema operativo y sobre la política de ejecución de aplicaciones en los controladores de dominio.

SafeDLLSearchMode modifica el orden de búsqueda de DLL del sistema operativo, priorizando el directorio SYSTEM32 sobre el directorio de trabajo actual. Se verifica y configura mediante GPO en Configuración del equipo > Preferencias > Configuración de Windows > Registro, estableciendo el valor SafeDllSearchMode en 1. La guía incluye el comando de verificación correspondiente para confirmar el estado del control antes y después de aplicar la directiva.

AppLocker permite crear reglas para permitir o denegar la ejecución de archivos, *scripts*, instaladores de Windows y DLLs en los controladores de dominio. Su implementación sigue un proceso en dos etapas: primero debe habilitarse el servicio de Identificación de Aplicación como requisito previo; segundo, AppLocker debe configurarse en modo Solo Auditoría durante un período mínimo de cuatro semanas, revisando los eventos registrados en Visor de Eventos > Microsoft > Windows > AppLocker para identificar aplicaciones legítimas que serían bloqueadas antes de activar el modo Enforce. La transición al modo Enforce es el control de mayor impacto operativo potencial de toda la

guía y requiere ventana de mantenimiento, revisión exhaustiva de los eventos de auditoría y aprobación formal del cambio.

Sección 5 Implementación del componente de monitoreo continuo con Wazuh

El componente de monitoreo continuo puede implementarse en paralelo con cualquiera de las secciones de *hardening* de la guía, dado que no tiene dependencias directas sobre los controles de configuración. La arquitectura del componente, documentada en la sección 5.1 de la guía, integra cuatro elementos: el agente de Wazuh instalado en cada controlador de dominio para recolección de eventos, configuraciones y *logs*; Sysmon para telemetría avanzada a nivel de *kernel* sobre procesos, red, carga de módulos y registros; el servidor Wazuh para correlación de eventos, gestión de reglas y generación de alertas; y el *dashboard* de Wazuh para visualización de alertas, matrices MITRE ATT&CK y métricas de autenticación del Directorio Activo.

El primer paso de implementación es la configuración de Sysmon, documentada en la sección 5.2 de la guía. Sysmon debe instalarse utilizando la plantilla SwiftOnSecurity como configuración base y agregar cuatro grupos de reglas específicos dentro de la sección EventFiltering del archivo de configuración: acceso a procesos sensibles para T1134.002, creación de procesos con privilegios elevados para T1134.002, *authentication packages* en LSASS para T1547.002, y DLL potencialmente maliciosas para T1574.001. Estas cuatro extensiones son indispensables porque las técnicas T1134.002 y T1574.001 no son capturables de forma confiable únicamente mediante el registro nativo de eventos de Windows.

El segundo paso es la configuración del agente de Wazuh en el archivo ossec.conf de cada controlador de dominio, habilitando la recolección de tres canales de eventos: el canal Security para autenticación y modificación de directivas, el canal System para eventos de servicio, y el canal Microsoft-Windows-Sysmon/Operational para la telemetría avanzada de Sysmon. El tercer paso es la incorporación de las 34 reglas personalizadas al servidor Wazuh, documentadas en la sección 5.3 de la guía y organizadas en cinco grupos según la técnica que cubren: 10 reglas para T1078.002, 4 para T1484.002, 7 para T1134.002, 4 para T1547.002 y 4 para T1574.001. Los niveles de severidad van del 0 al 15 según el esquema nativo de Wazuh, donde los niveles más altos corresponden a detecciones sin posibilidad de falso positivo que requieren atención inmediata.

Guía de *hardening* de Directorio Activo como proceso continuo y no como lista de verificación

El tratamiento correcto de la guía no termina con la implementación de todos sus controles ni con la incorporación de las 34 reglas de Wazuh. La seguridad del Directorio Activo es dinámica: cada cambio de infraestructura, incorporación de nuevos controladores de dominio, migración de servicios o modificación de la estructura organizativa puede introducir nuevas exposiciones o revertir controles previamente aplicados. Por esta razón, el ciclo de diagnóstico con Purple Knight, implementación de controles y validación mediante un segundo escaneo debe formalizarse como proceso periódico con frecuencia mínima de 90 días, o ejecutarse inmediatamente

después de cualquier cambio relevante en la infraestructura del dominio. Las reglas de Wazuh deben revisarse y actualizarse al menos dos veces al año tomando como referencia las actualizaciones publicadas por el marco MITRE ATT&CK.

La integración entre *hardening* y monitoreo es el principio que da coherencia a toda la propuesta: mientras los controles de la guía reducen la superficie de ataque, las reglas de detección aseguran que cualquier intento de explotar las configuraciones residuales genere una alerta trazable y clasificada por técnica de MITRE ATT&CK. Este ciclo de retroalimentación convierte la seguridad del Directorio Activo en un proceso dinámico, medible y sostenible, que no depende de una intervención única sino de una práctica continúa orientada por evidencia y validada en cada etapa del proceso de mejora.

III. Resultados

Los resultados que se presentan siguen la estructura de los tres componentes de la propuesta: hallazgo del diagnóstico inicial, estado de implementación del plan de *hardening* y comparación entre escaneos, y validación del monitoreo continuo.

Técnicas de MITRE ATT&CK seleccionadas

La revisión sistemática permitió identificar y caracterizar las cinco técnicas que estructuran el plan de *hardening*. La tabla 1 estructura cada técnica, su táctica principal y el nivel de impacto en entornos de Directorio Activo.

ID de Técnica	Nombre	Táctica Principal	Impacto en Directorio Activo
T1078.002	Valid Accounts – Domain Accounts	Persistencia / Escalamiento	Crítico
T1484.002	Domain Policy Modification	Escalamiento / Evasión	Crítico
T1134.002	Token Impersonation/Theft	Escalamiento / Evasión	Alto
T1547.002	Boot or Logon Autostart Execution	Persistencia / Escalamiento	Alto
T1574.001	Hijack Execution Flow – DLL Side-Loading	Persistencia / Escalamiento	Alto

Tabla 1 Técnicas de MITRE ATT&CK seleccionadas y su impacto en el Directorio Activo

Las técnicas seleccionadas forman una cadena de ataque: T1078.002 provee el acceso inicial; T1484.002 amplía el radio de acción; T1134.002 eleva privilegios sin credenciales adicionales; T1574.002 garantiza persistencia ante reinicios; T1574.001 permite evasión bajo procesos legítimos.

Diagnóstico inicial con Purple Knight

El escaneo inicial evaluó 109 indicadores en 17 minutos y 58 segundos. El entorno obtuvo un porcentaje global de 69% con una calificación D+, inferior al promedio reportado por Semperis (2024) para organizaciones durante su primer escaneo, el umbral mínimo aceptado es de calificación C. Se identificaron 33 indicadores de exposición (IoEs), de los cuales ninguno resultó crítico activo, aunque 4 no pudieron ejecutarse por encontrarse un controlador de dominio apagado. A continuación, la tabla 2 presenta el estado de seguridad por categoría.

Categoría	Porcentaje	IoEs encontrados	Estado
Account Security	92%	11	Controles base presentes con excepciones críticas
AD Delegation	88%	Múltiples	Higiene de delegación débil
AD Infrastructure Security	89%	Múltiples	Configuración de servidores con posibilidades de mejora
Group Policy Security	95%	3	Categoría más robusta
Kerberos Security	94%	1 (KRBTGT)	Riesgo por antigüedad de contraseña

Tabla 2 Resultados del diagnóstico inicial por categoría (Purple Knight, primer escaneo)

Los hallazgos con mayor criticidad fueron: contraseña de la cuenta KRBTGT sin rotar desde el 6 de febrero del 2013 con más de 4.700 días; una cuenta con permisos GenericAll sobre *naming context* en la raíz del dominio, habilitando ataques DCSync; escritura sobre msDSKeyCredentialLink en los 7 controladores de dominio, permitiendo Shadow Credentials, permisos GenericAll sobre msDS-AllowedToActOnBehalfOfOtherIdentity, habilitando delegación RBCD; ausencia de firma LDAP en 5 de 7 controladores; soporte activo de cifrado RC4_HMAC_MD5 en Kerberos; y 12 cuentas privilegiadas fuera del grupo Protected Users.

Plan de *hardening*: estructura y estado de implementación

El plan de *hardening* comprende 25 controles organizados en cuatro sesiones. La tabla 3 presenta el estado de implementación consolidado tras el diagnóstico inicial.

Sección	Técnica	Controles	Aplicados	No aplicados	Verificar
5.4.1Controles de Gestión de Cuentas y Credenciales	T1078.002	5	2	3	0

5.4.2 Controles de Protección de Credenciales y Privilegios	T1078.002, T1134.002, T1547.002	9	3	4	2
5.4.3 Controles de Políticas de Dominio y Opciones de seguridad	T1484.002	8	2	4	2
5.4.4 Controles de Flujo de Ejecución y DLL	T1574.001	3	0	2	1
Total		25	7 (28%)	13 (52%)	5 (20%)

Tabla 3 Desglose por sección de la guía de hardening

Los controles que indican verificar corresponden a configuraciones no evaluadas por Purple Knight, lo cual requieren una comprobación manual en cada controlador de dominio.

Monitoreo continuo arquitectura y reglas de detección

El componente de monitoreo continuo integra Wazuh como plataforma SIEM y Sysmon como fuente de telemetría avanzada a nivel de *kernel*. Se diseñaron 34 reglas de correlación personalizadas, distribuidas por técnica de MITRE ATT&CK. En la tabla 4 se detalla la distribución de las reglas por técnica y los canales de eventos cubiertos.

Técnica	Reglas	Canales cubiertos	Rango de severidad en Wazuh
T1078.002	10	Security (4624, 4625, 4648, 4672, 4728, 4740, 4768, 4769, 4776)	Nivel 7–12
T1484.002	4	Security (5136, 5137, 5141, 4719, 4739, 4704)	Nivel 12–14
T1134.002	7	Security + Sysmon/Op (EventID 1, 10)	Nivel 10–15
T1547.002	4	Security + Sysmon/Op (EventID 7, 13)	Nivel 13–15

T1574.001	4	Security + System + Sysmon/Op (EventID 1, 7)	Nivel 10–12

Tabla 4 Distribución de reglas de detección en Wazuh por técnica de MITRE ATT&CK

Validación empírica: comparación entre escaneos

El 20 de abril de 2026 se ejecutó un segundo escaneo con Purple Knight, posterior a la implementación de los controles de la primera fase (eliminación de permisos excesivos sobre objetos privilegiados, sin requerir ventana de mantenimiento). La Tabla 5 presenta los indicadores con cambios significativos.

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

El incremento aritmético del indicador RC4 (de 15% a 27%) se debe a la desconexión permanente de un controlador de dominio, que redujo el universo evaluado de 7 a 6 unidades, sin que se haya aplicado ninguna remediación sobre cifrado.

El segundo escaneo también reveló tres nuevos indicadores de exposición no visibles en el primer escaneo: Dangerous GPO logon script path, Non-privileged users with access to gMSA passwords y Unexpected accounts in Cert Publishers Group. Esto se explica por el mayor nivel de privilegios de la cuenta utilizada en el segundo escaneo, que permitió a la herramienta evaluar contenedores previamente inaccesibles. Este hallazgo confirma que la superficie de ataque de un entorno de Directorio Activo no es estática y que el nivel de acceso con el que se realiza la auditoría influye directamente en la completitud del diagnóstico.

Validación del componente de monitoreo

Con el fin de complementar la propuesta técnica con evidencia del funcionamiento del componente de monitoreo, se presenta a continuación una serie de capturas del *dashboard* de Wazuh correspondientes al período de observación, posterior a la implementación de las reglas documentadas. 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.

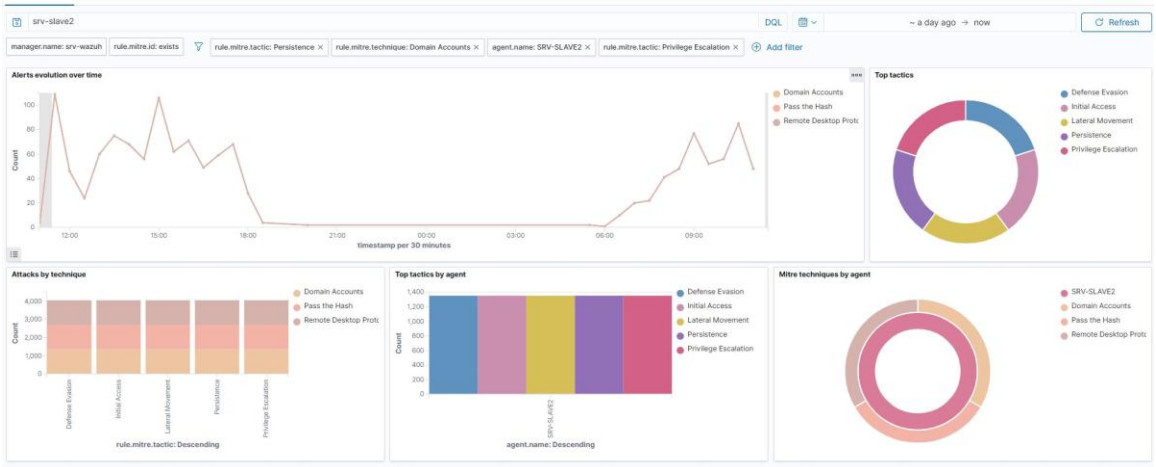

Ilustración 1Dashboard de alertas MITRE ATT&CK en Wazuh tácticas de Persistencia y Escalamiento de Privilegios.

La ilustración 1 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, están operando de forma correcta y produciendo telemetría para su respectiva revisión en caso de algún incidente.

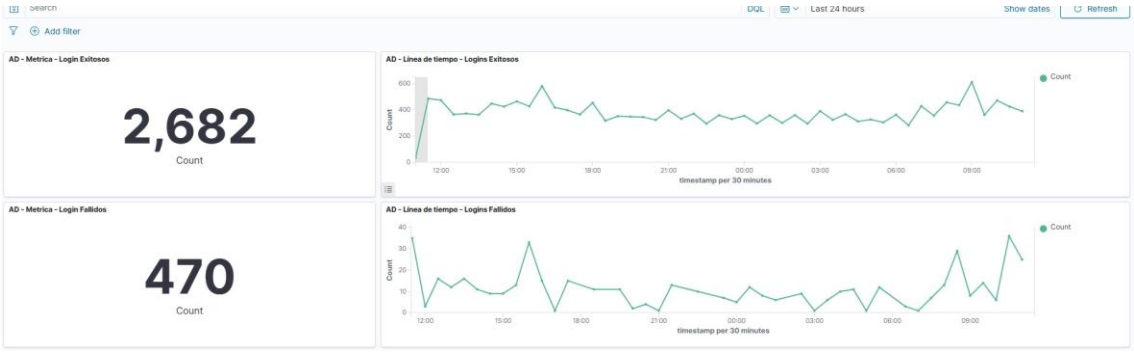

Ilustración 2 Dashboard de métricas de autenticación del Directorio Activo inicios de sesión exitosos (2.682) y fallidos (470) en ventana de 24 horas.

En la ilustración 2 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.

IV. Discusión

Los resultados obtenidos permiten realizar tres observaciones de fondo sobre el problema de seguridad del Directorio Activo en entornos corporativos.

En primer lugar, los hallazgos del diagnóstico inicial confirman la hipótesis planteada en la revisión de literatura: los entornos de Directorio Activo presentan exposiciones significativas no por ausencia de herramientas de seguridad, sino por ausencia de una estrategia integral que incorpore *hardening* y monitoreo. El entorno analizado contaba con políticas de contraseñas y autenticación básica correctamente configuradas (Account Security al 92%), pero presentaba exposiciones críticas en delegación de permisos y configuración de protocolos de red. Esta combinación es característica de entornos donde la seguridad se ha gestionado de forma reactiva y fragmentada, fortaleciendo componentes visibles sin atender vectores menos evidentes como los permisos sobre atributos de objetos privilegiados.

En segundo lugar, la validación empírica demuestra que los controles, que no requieren ventanas de mantenimiento ni coordinación con propietarios de cuentas de servicio o servicios, pueden producir mejoras sustanciales y medibles en la postura de seguridad. La implementación de la primera fase, limitada exclusivamente a la limpieza de permisos excesivos, elevó el puntaje global 14 puntos porcentuales y resolvió cinco indicadores que previamente habilitaban vectores de ataque de alta criticidad, incluyendo Shadow Credentials, delegación RBCD y vinculación arbitraria de GPOs sobre los controladores de dominio. Este resultado tiene implicaciones prácticas importantes para organizaciones que perciben el *hardening* como un proceso de alto riesgo operativo: existe un conjunto significativo de controles aplicables sin impacto en la continuidad del servicio.

En tercer lugar, el hallazgo más significativo del diagnóstico fue la concentración de permisos excesivos en una única cuenta que aparecía comprometida de forma simultánea en cuatro indicadores de distintas secciones del plan. Esta cuenta tenía permisos GenericAll sobre el *naming context* raíz del dominio, escritura sobre msDS-KeyCredentialLink en los 7 controladores, GenericAll sobre msDS-AllowedToActOnBehalfOfOtherIdentity y GenericAll sobre la unidad organizativa de controladores de dominio. La materialización de cualquiera de estos vectores comprometería la totalidad del dominio. Este patrón ilustra un riesgo sistemático frecuente en entornos con administración descentralizada y sin revisión periódica de delegaciones.

Respecto al componente de monitoreo, la investigación confirma que la cobertura de técnicas como T1134.002 y T1574.001 no es viable exclusivamente mediante el registro nativo de eventos de Windows. La integración de Sysmon como fuente de telemetría avanzada es una condición necesaria para detectar accesos a la memoria de LSASS con permisos de volcado y la carga de DLL no firmadas desde rutas no estándar, dos patrones que herramientas como Mimikatz y técnicas de DLL *side-loading* explotan de forma sistemática. Esta dependencia de Sysmon no es una limitación del plan sino una decisión de diseño informada por la naturaleza de las técnicas abordadas.

V. Conclusiones

Este trabajo demuestra que la integración coherente de *hardening* y monitoreo continuo en entornos de Directorio Activo, donde cada control de endurecimiento optimiza las capacidades de detección y viceversa, constituye un modelo más efectivo que abordar ambas disciplinas de forma independiente. Los resultados empíricos obtenidos en un entorno de producción real del sector financiero costarricense validan que el plan propuesto no es únicamente un ejercicio teórico, sino una propuesta técnica con impacto comprobado.

La mejora de 14 puntos porcentuales en la postura de seguridad global, obtenida exclusivamente con los controles de la primera fase que no requirieron ventana de mantenimiento, confirma que existe un conjunto de acciones de alto impacto y bajo riesgo operativo que muchas organizaciones no han ejecutado, no por falta de herramientas, sino por ausencia de una guía estructurada que las priorice y las vincule a técnicas adversarias reales.

Las 34 reglas de detección en Wazuh y la integración con Sysmon cierran la brecha identificada en la literatura: la desconexión entre los controles de configuración segura y la capacidad de detectar su evasión. Esta integración permite que las organizaciones no solo endurezcan el entorno del Directorio Activo, sino que también monitoreen de

forma específica los patrones de comportamiento que indicarían que un adversario está intentando explotar las configuraciones residuales.

Al no quedarnos únicamente con la confección del plan sino llevarlo a una prueba de concepto en un entorno real, se demuestra que este plan es viable para implementar en organizaciones que utilicen Directorio Activo y que los beneficios que pueden obtener son muy prometedores.

APPENDIX

Guía de Hardening
Directorio Activo

BIBLIOGRAFÍA

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