



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

TRABAJO DE GRADO

VERIFICACIÓN DEL GRADO DE INSEGURIDAD DE LAS INFRAESTRUCTURAS
WINDOWS DE DIRECTORIO ACTIVO Y CONSTRUCCION DE UNA GUIA DE
ASEGURAMIENTO QUE ELEVE EL NIVEL DE SEGURIDAD ENCONTRADO

CRISTIAN DAVID ARDILA FLOREZ
JUAN ALBERTO DAZA CASTRO

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

TRABAJO DE GRADO

VERIFICACIÓN DEL GRADO DE INSEGURIDAD DE LAS INFRAESTRUCTURAS
WINDOWS DE DIRECTORIO ACTIVO Y CONSTRUCCION DE UNA GUIA DE
ASEGURAMIENTO QUE ELEVE EL NIVEL DE SEGURIDAD ENCONTRADO

CRISTIAN DAVID ARDILA FLOREZ
JUAN ALBERTO DAZA CASTRO

Trabajo de grado para optar al título de Especialista en Seguridad de la
Información

Docente

HECTOR DARIO JAIMES PARADA
ESPECIALISTA EN SEGURIDAD DE REDES

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020



Atribución-NoComercial-CompartirIgual 2.5 Colombia (CC BY-NC-SA 2.5)

La presente obra está bajo una licencia:

Atribución-NoComercial-CompartirIgual 2.5 Colombia (CC BY-NC-SA 2.5)

Para leer el texto completo de la licencia, visita:

<http://creativecommons.org/licenses/by-nc-sa/2.5/co/>

Usted es libre de:



Compartir - copiar, distribuir, ejecutar y comunicar públicamente la obra
hacer obras derivadas

Bajo las condiciones siguientes:



Atribución — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciante (pero no de una manera que sugiera que tiene su apoyo o que apoyan el uso que hace de su obra).



No Comercial — No puede utilizar esta obra para fines comerciales.



Compartir bajo la Misma Licencia — Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

TABLA DE CONTENIDO

	Pág.
1. Introducción	3
2. Generalidades	5
2.1. Línea de Investigación	5
2.2. Planteamiento del Problema	5
2.2.1. Antecedentes del problema	6
2.2.2. Pregunta de investigación	8
2.2.3. Variables del problema	8
2.3. Justificación	8
2.4. Objetivos	9
2.4.1. Objetivo general	9
2.4.2. Objetivos específicos	10
3. Marcos de referencia	10
3.1. Marco conceptual	10
3.2. Marco teórico	10
3.3. Marco jurídico	11
3.4. Estado del arte	12
4. Metodología	13
4.1. Fases del trabajo de grado	13
4.2. Instrumentos o herramientas utilizadas	14
4.3. Alcances y limitaciones	15
5. Productos a entregar	16
6. Entrega De Resultados E Impactos	17
7. Estrategias de comunicación	18
8. Desarrollo del proyecto	19
8.1. Análisis de la encuesta	19
8.2. Implementación de Directorios Activos	22
8.3. Comparacion del nivel de aseguramiento en Directorios Activos	23
8.3.1. Resultados Pentest Directorios Activos	27
8.3.2. Ejecución de buenas practicas en Directorios Activos	35
8.4. Documentación de buenas y malas practicas	41
9. Conclusiones	44
10. Anexos	45

Anexo A	45
Anexo B	46
Anexo C	47
11. BIBLIOGRAFÍA	48

LISTA DE FIGURAS

Pág.

FIGURA 1. DELITOS INFORMÁTICOS EN COLOMBIA 2019	7
FIGURA 2. DELITOS INFORMÁTICOS DENUNCIADOS EN COLOMBIA	12
FIGURA 3 – VERSIÓN DE SISTEMA OPERATIVO DE DIRECTORIO ACTIVO.	19
FIGURA 4 – HARDENING APLICADOS A DIRECTORIO ACTIVO.	20
FIGURA 5 – CONSULTA DE ADMINISTRADORES DE GUÍAS DE ASEGURAMIENTO DE DIRECTORIO ACTIVO.....	20
FIGURA 6 - PERCEPCIÓN DE LOS ADMINISTRADORES EN COSTOS DE IMPLEMENTACIÓN. ..	21
FIGURA 7 – COMPARACIÓN DE VULNERABILIDADES NISSUS POR DIRECTORIO ACTIVO. ...	32
FIGURA 8 – SEVERIDAD DE VULNERABILIDADES EN DIRECTORIO ACTIVO INSEGURO.	32
FIGURA 9 – ANÁLISIS BLOODHOUND ESTRUCTURA DIRECTORIO ACTIVO INSEGURO.	33
FIGURA 10 - ANÁLISIS BLOODHOUND DIRECTORIO ACTIVO INSEGURO CUENTAS DE SERVICIO Y GENÉRICAS.	33
FIGURA 11 - ANÁLISIS BLOODHOUND ESTRUCTURA DIRECTORIO ACTIVO ASEGURADO. ...	34
FIGURA 12 - ANÁLISIS BLOODHOUND DIRECTORIO ACTIVO ASEGURADO CUENTAS DE SERVICIO Y GENÉRICAS.	35
FIGURA 13 – CUMPLIMIENTO DE BUENAS PRÁCTICAS DIRECTORIO ACTIVO INSEGURO. ...	40
FIGURA 14 – CUMPLIMIENTO DE BUENAS PRÁCTICAS DIRECTORIO ACTIVO ASEGURADO. ...	41

LISTA DE TABLAS

Pág.

TABLA 1 - INVERSIÓN EN MILLONES USD EN SEGURIDAD INFORMÁTICA A NIVEL MUNDIAL..	6
TABLA 2 - TIPOS DE ATAQUES EN COLOMBIA.....	7
TABLA 3 – FASES PENTEST WHITE BOX.....	23
TABLA 4 - HERRAMIENTAS PENTEST.....	24
TABLA 5 – RESULTADOS PENTEST DIRECTORIO ACTIVO INSEGURO.....	27
TABLA 6 – RESULTADOS PENTEST DIRECTORIO ACTIVO ASEGURADO.....	29
TABLA 7 – CUMPLIMIENTO DE BUENAS PRÁCTICAS DIRECTORIO ACTIVO INSEGURO.	35
TABLA 8 – CUMPLIMIENTO DE BUENAS PRÁCTICAS DIRECTORIO ACTIVO ASEGURADO.	37

1. INTRODUCCIÓN

Hoy día las empresas requieren recursos tecnológicos para la optimización de procesos, esto genera que se realice implementaciones de fácil manejo para centralizar la información y determinar perfiles de usuarios y equipos que acceden a estas soluciones.

Como solución a esta necesidad las empresas utilizan uno de los servicios más convencionales para su gestión, se trata del Directorio Activo (*Introducción a Active Directory Domain Services*, 2017), servicio incluido en los sistemas operativos de Windows Server en sus diversas versiones.

Este servicio puede ser implementado de forma On-Premise, Cloud Azure o de forma mixta (Microsoft, 2020d), dependiendo del tipo de implementación varía su administración y su aseguramiento ante posibles riesgos de seguridad de la información.

Atacantes aprovechan las implementaciones de Directorio Activo mal aseguradas, la firma de seguridad Rapid7 (*Under the Hoodie 2019*, 2019) realizó 180 pruebas de PenTesting de las cuales el 36% de los compromisos se centraron principalmente en evaluaciones de redes internas, de estas el 96% de vulnerabilidades potenciales se evidenciaron en Directorio Activo.

En el mercado existen entidades como el CIS (CIS Controls, 2020) y NIST (Franklin Smith, 2017) que generan guías de seguridad de parametrización de estándares de seguridad en Directorio Activo, algunas son publicadas de forma libre, pero información más detallada tiene costo.

El planteamiento de este proyecto consiste en la verificación del grado de inseguridad de las infraestructuras Windows Server de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado, en un modelo de Directorio Activo On-Premise es decir de forma local, esto debido a que nos reduce los costos de implementación, además de que todo el aseguramiento será propuesto por los autores del presente proyecto.

El proyecto se desarrollará en 4 fases con el fin de alcanzar los objetivos.

- Fase 1. Malas prácticas de implementación de Directorio Activo
- Fase 2. Análisis de Directorio Activo inseguro
- Fase 3. Implementación de Directorio Activo con aseguramiento
- Fase 4. Análisis de Directorio Activo asegurado

Este proyecto se apoya en la línea de investigación Software inteligente y convergencia tecnológica de la Universidad Católica (Universidad Católica, 2020)

donde tiene un alcance cuasiexperimental, en los cuales se manipulan las variables independientes.

Se determinaron diferentes riesgos y limitaciones que se pudieran presentar

- El periodo del licenciamiento de Windows Server implica varias instalaciones del sistema operativo Windows Server.
- La encuesta anónima no alcanzara una muestra de más de 35 administradores de plataforma tecnológica.
- La simulación consistirá en una prueba de concepto dentro de los recursos virtualizados en un computador personal.
- La reducción de riesgos se apoyará en los resultados de sistemas operativos virtualizados.
- La documentación se elaborará partiendo de los sistemas operativos simulados.
- Los análisis PenTest solo se ejecutarán las fases de reconocimiento, escaneo y enumeración, ya que hasta ese punto se puede demostrar el nivel de aseguramiento.

Teniendo en cuenta el conocimiento adquirido en la especialización seguridad de la información, se pretende desarrollar esta iniciativa de guía documentada de malas prácticas de implementación, correcta implementación, remediación y hardening. Para los administradores de Directorio Activo y las empresas que no cuentan con la experiencia en gestión de la seguridad de la información, encaminados en generar una cultura de protección de la información.

2. GENERALIDADES

2.1. LÍNEA DE INVESTIGACIÓN

Este proyecto se basa en la línea de investigación Software inteligente y convergencia tecnológica de la facultad de ingeniería de Universidad Católica de Colombia, para la Especialización de Seguridad de la Información.

2.2. PLANTEAMIENTO DEL PROBLEMA

Microsoft integra en sus sistemas operativos Windows Servers diversos servicios para gestión de equipos, usuarios, impresoras, entre otros, estos servicios se usan con el fin de una integración de recursos centralizados en una empresa.

Cuando se implementa un controlador de dominio, se levanta un servicio de Directorio Activo, el cual proporciona una infraestructura escalable y de fácil administración para gestión de usuario y equipos.

Actualmente existen formas de implementar este servicio ya sea On-Premise, Cloud Azure o de forma mixta, cada implementación se realiza en infraestructuras diferentes, estas implementaciones ofrecen beneficios en costos, a su vez cambia la forma de implementar los niveles de seguridad, sin embargo, ambas infraestructuras presentan debilidades.

Estas debilidades representan fallos muy críticos de seguridad, lo cual puede incurrir en comprometer la información de las empresas ocasionando pérdidas económicas, en 2019 Colombia reporto que los ataques a empresas generaron extorciones entre 32 millones y 160 millones de COP por ataque, esto conlleva a que el 60% de las empresas que sufren un ciberataque apenas se pueden sostener económicamente 6 meses (Ceballos Lopez et al., 2020), una débil implementación del Directorio Activo puede impactar a una empresa de forma negativa.

Al consultar en Common Vulnerabilities and Exposures de Mitre (*CVE - Search Results*, 2020) reportan más de 500 vulnerabilidades asociadas a Directorio Activo, en solo lo que va del año en curso, por esta razón es muy importante aclarar la relevancia que tiene el Directorio Activo en las empresas ya que al ser un servicio centralizado su nivel de impacto es crítico, el Directorio Activo es un servicio de uso mundial, típicamente de uso interno en las empresas y con el fin de optimizar el acceso de los usuarios se integra a otras plataformas, como lo menciona Sean Metcalf fundador de Trimarc (Metcalf, 2020b), los atacantes les apetece vulnerar este servicio ya que no se trata solo de datos, se trata de controlar todo, un acceso a este servicio con privilegios de administrador puede ser el peor escenario para un administrador de esta plataforma, esto debido a que su transversalidad implica riesgos a toda la infraestructura tecnológica.

2.2.1. ANTECEDENTES DEL PROBLEMA

Es importante garantizar la seguridad de un Directorio Activo o de lo contrario puede comprometer los pilares de la seguridad de la información, CID (Icontec, 2020), esto implica pérdidas económicas para las empresas, según un estudio de Gartner (Moore, 2018), muestra que los gastos en inversión de seguridad informática a nivel mundial incrementan cada año en promedio en un 8,7%, esta inversión es significativa, pero necesaria si se quiere proteger la información.

Tabla 1 - Inversión en millones USD en Seguridad informática a nivel mundial.

Tipo de inversión	2017	2018	2019
Seguridad de la aplicación	2,434	2,742	3,003
Seguridad en la nube	185	304	459
Seguridad de datos	2,563	3,063	3,524
Gestión de acceso de identidad	8.823	9,768	10,578
Protección de infraestructura	12,583	14,106	15,337
Gestión Integrada de Riesgos	3.949	4,347	4.712
Equipo de seguridad de red	10,911	12,427	13,321
Otro software de seguridad de la información	1,832	2,079	2,285
Servicios de seguridad	52,315	58,92	64,237
Software de seguridad del consumidor	5,948	6.395	6.661
Total	101,544	114,152	124,116

Fuente (Moore, 2018)

Frente a tanta inversión en seguridad informática a nivel mundial, no es suficiente si no se cuenta con buenas prácticas de aseguramiento, por eso es de gran importancia proteger el Directorio Activo, tomar medidas preventivas en posibles escenarios de ataques pueden mitigar los riesgos para las empresas, consultando el sitio web de Common Vulnerabilities and Exposures de Mitre (*CVE - Search Results, 2020*) se evidencia que cuentan con más de 500 vulnerabilidades asociadas a Directorio Activo solo desde el 1 de enero de 2020 hasta la fecha de redacción de este documento.

Cuando tomamos una perspectiva nacional vemos que los ataques cibernéticos en Colombia van en aumento, informes como Tendencias Cibercrimen Colombia 2019 – 2020 (Ceballos Lopez et al., 2020), publicado por el observatorio de ciber crimen de la policía nacional (CAI Virtual, 2020), muestra que este país tiene el 30% de ataques Ransomware (Rodríguez Vallecilla & Mina Loango, 2019), a nivel Latinoamérica y el principal blanco fueron las Pymes con un total de 717 empresas vulneradas exitosamente, estos fueron los ataques realizados.

Tabla 2 - Tipos de ataques en Colombia.

Tipo de amenaza	Porcentaje
Phishing	42%
Suplantación de Identidad	28%
Ataque Malware	14%
Fraudes de pagos en línea	16%

Fuente (Ceballos Lopez et al., 2020)

En un análisis local, Bogotá fue la ciudad más afectada de Colombia se presentaron 5.308 denuncias en 2019, esto hace ver la necesidad de generar una cultura de buenas prácticas en materia de seguridad de la información, considerando que la incorrecta implementación y administración del Directorio Activo expone el 90% de las empresas a fallos de seguridad, en pruebas realizadas por Red Teams se evidencio que el 74% de las veces se obtienen las credenciales de administrador y esto se debe a malas prácticas por parte de los administradores Directorio Activo. (*Why Active Directory (AD) Protection Matters, 2020*)

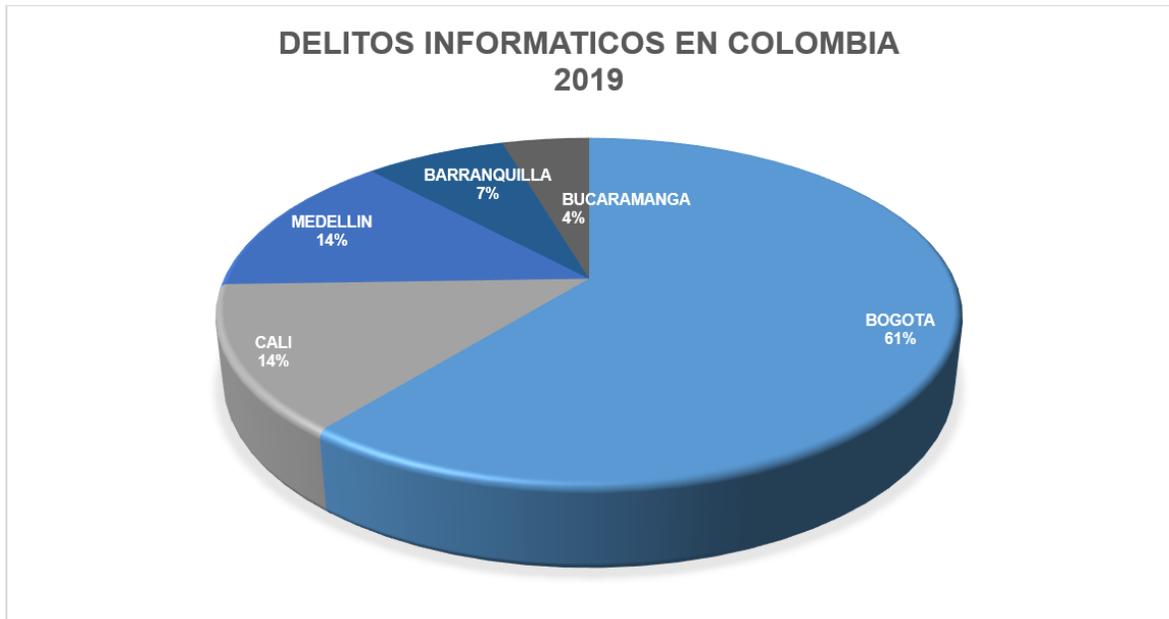


Figura 1. Delitos informáticos en Colombia 2019

Complementariamente las nuevas versiones de Ransomware (Moreno et al., 2020) de los últimos tres años son piezas lógicas de bastante complejidad, que bien pueden contaminar una maquina a través del típico click de un correo phishing o pueden buscar múltiples debilidades de servicios Windows expuestos directamente a internet, de igual forma cuanto la contaminación ocurre por un click en el correo el

malware es capaz de replicarse sin intervención humana a través de servicios Windows internos vulnerables, en contexto es claro que una infraestructura de Directorio Activo no asegurada aumenta la exposición y riesgo de contaminación por un Ransomware moderno.

2.2.2. PREGUNTA DE INVESTIGACIÓN

¿Cómo los administradores de tecnología pueden evitar impactos de seguridad y pérdidas económicas representativas para sus organizaciones si las prácticas generalizadas de configuración y administración de servidores de Directorio Activo presentan serios problemas de seguridad?

2.2.3. VARIABLES DEL PROBLEMA

Las variables asociadas al problema de esta investigación son las malas prácticas empresariales de aseguramiento del Directorio Activo, las variables que se determinan para la elaboración del proyecto son:

- Explotación de vulnerabilidades de Directorio Activo y servicios asociados.
- Auditoria de servicios, sistema operativo, usuarios y equipos.
- Controles de seguridad en gestión de usuarios y equipos.
- Aplicación de aseguramiento de Directorio Activo.
- Nivel de riesgo alto en violación de los pilares de la seguridad de la información CID (Confidencialidad, Integridad, Disponibilidad) (Icontec, 2020).

Estas variables hoy tiene valores preocupantes y son una evidencia clara del problema, nuestra propuesta incidirá drásticamente en una mejora del nivel de seguridad, una vulneración puede ser exitosa si no se cuenta con una adecuada línea base de implementación y administración durante el periodo de vida del servicio, por esta razón es importante mitigar los riesgos que puedan degradar o indisponer el servicio, para ello la mejor manera es administrar el Directorio Activo desde una postura enfocada en la seguridad de la información.

2.3. JUSTIFICACIÓN

El sistema operativo es fundamental para los servidores, estos requieren servicios que centralicen usuarios y equipos para llevar un control de ellos, actualmente

existen soluciones alternativas a Directorio Activo de Microsoft Windows como los son 389 Directory Server (389DS, 2017), Apache Directory Studio (Apache Directory Studio, 2018), sin embargo en la actualidad Microsoft Windows Server es el dominante del mercado por su uso en la infraestructura mundial de servidores, el cual tiene integrado la solución de Directorio Activo, según el informe de Statista (*Global Server Share by OS 2018-2019*, 2018) Windows Server domina con un 71.9% en 2018 y un 72.8% en 2019 del mercado mundial, teniendo en cuenta esta estadística se estima una cantidad importante de Directorios Activos en producción a nivel mundial.

El uso del Directorio Activo al ser un servicio indispensable de uso común y generalizado se convierte y un componente crítico a un nivel masivo donde el impacto al mismo puede causar repercusiones graves en una empresa, debido a esto la protección de este servicio debe salvaguardarse de la mejor manera y partiendo de ello surge la elaboración de este proyecto.

Este proyecto se basa en los conocimientos adquiridos en la especialización de Seguridad de la Información, se planteará la identificación de un entorno inseguro de infraestructura de Directorio Activo y construcción de una guía de aseguramiento para dicho escenario.

El elemento diferenciador de este proyecto es una propuesta de fácil entendimiento que generara una cultura de buenas prácticas en seguridad de la información e implementación y administración de Directorio Activo, a quienes adopten la guía que se pretende desarrollar.

Esta iniciativa permitirá incentivar la conciencia en los administradores de sistemas de las buenas prácticas en seguridad de la información por medio del desarrollo de las fases del proyecto, elaborando una guía documentada que permita mostrar cada fase en un entorno simulado donde se evidenciaran los riesgos, ataques, remediaciones y buenas prácticas.

2.4. OBJETIVOS

2.4.1. OBJETIVO GENERAL

Generar una guía de buenas prácticas para el aseguramiento del Directorio Activo de Windows Server por medio de unas pruebas de concepto con el cual se evalúa la seguridad del servicio de Directorio Activo en un entorno simulado.

2.4.2. OBJETIVOS ESPECÍFICOS

Determinar las buenas y malas prácticas en implementaciones de directorio activo.

Comparar la reducción de malas prácticas y vulnerabilidades al asegurar correctamente una infraestructura de Directorio Activo.

Proponer un modelo documentado para elevar el nivel de seguridad de Directorio Activo.

3. MARCOS DE REFERENCIA

3.1. MARCO CONCEPTUAL

El sistema operativo es el encargado de poner en funcionamiento una computadora, servidor, entre otros dispositivos electrónicos, como también es el encargado de gestionar el hardware para realizar diferentes operaciones, uno de los más comunes y usados a nivel empresarial y personal es el sistema operativo Windows en sus diferentes versiones, a nivel empresarial encontramos Windows server, el cual una de sus funcionalidades es el Directorio Activo, por el cual, se puede realizar la administración de recursos y de usuarios, por ser una solución comúnmente utilizada en las empresas es blanco de ataques por parte de los ciberdelincuentes, por lo que se hace necesario acudir a la seguridad de la información, y tomar medidas preventivas y reactivas como es la implementación de buenas prácticas, para mitigar los riesgos a los que están expuestos y no comprometer la confidencialidad, disponibilidad e integridad de su información.

3.2. MARCO TEÓRICO

El Directorio Activo de Windows Server, es una las herramientas de administración de equipos y usuarios más usadas en el mercado, por lo que existen ataques constantes a esta solución, pero, así como se cuentan con atacantes también se cuenta con expertos en seguridad protegiendo las organizaciones.

Sean Metcalf fundador de Trimarc (Metcalf, 2020b) y conferencista es uno de los más grandes investigadores sobre la seguridad del Directorio Activo, en su trabajo se ha encargado de evidenciar las vulnerabilidades detectadas y prácticas realizadas en la explotación del Directorio Activo, cuenta con publicaciones para plataformas de Directorio Activo On-Premise, Cloud Azure y Office 365 (Microsoft, 2020a), en su sitio ADSecurity (Metcalf, 2020a), adicional a este trabajo de investigación encontramos tesis relevantes para la protección del Directorio Activo.

Sandra Patricia Beltran, en su trabajo de grado presentado en la Universidad Católica de Colombia; Explotación Avanzada del Directorio Activo: 2019 (Beltran, 2019), mostrando las posibles vulnerabilidades que se pueden presentar en el Directorio Activo en un ambiente simulado. Presenta un informe ejecutivo, el cual se toma como base para este proyecto dándole un enfoque más técnico y profundo.

Es importante tener en cuenta que el intervenir un Directorio Activo con fines mal intencionados de una organización trae repercusiones legales.

3.3. MARCO JURÍDICO

El afectar servicios como lo son el Directorio Activo a empresas puede incurrir en delitos tipificados por la ley colombiana entre estos se encuentran.

Ley estatutaria 1266 de 2008: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Normativa Nacional, Ley 1266 de 2008, 2008)

Ley estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. (Normativa Nacional, Ley 1581 de 2012, 2012)

ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. (Normativa Nacional, Ley 1273 de 2009, 2009)

Ley 256 de 1996 Artículo 9: Actos de desorganización, Artículo 16: Divulgación de secretos. (Ley 256 de 1996, 1996)

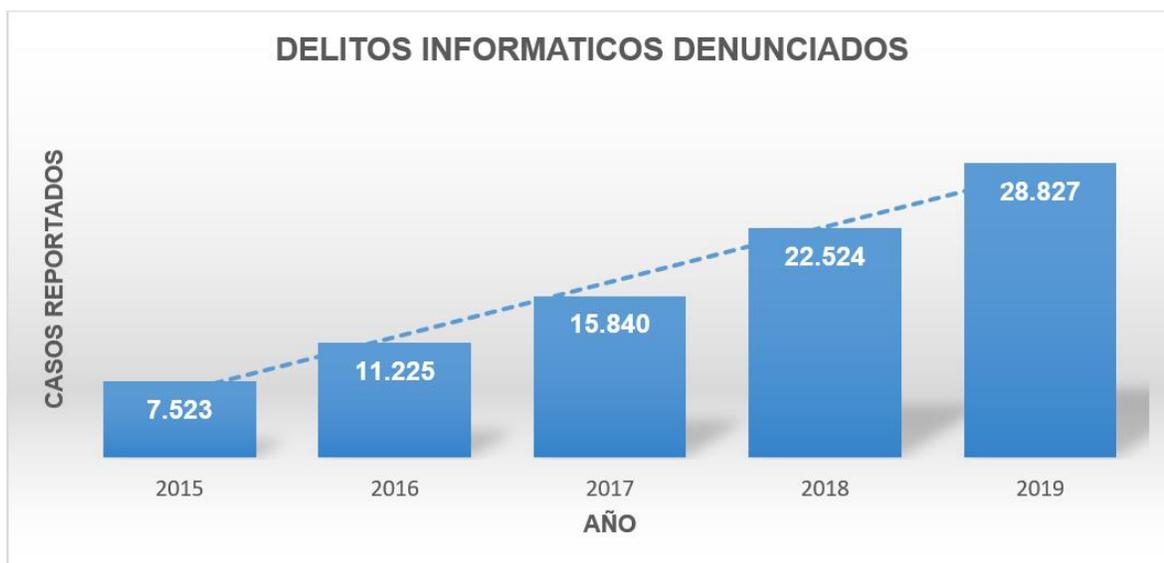


Figura 2. Delitos informáticos denunciados en Colombia

La tasa de delitos informáticos crece año tras año y estas leyes son parte fundamental para protegernos de posibles ataques informáticos, por ello es importante llevar un correcto manejo de las infraestructuras tecnológicas y mantener una postura preventiva antes de llegar a los marcos jurídicos, por ello se cuentan con estudios que anteceden este tema, los cuales se usan como base de investigación para la elaboración de este proyecto.

3.4. ESTADO DEL ARTE

Esta investigación permite visualizar un análisis realizado internacionalmente a las vulnerabilidades en Directorio Activo por falta de buenas prácticas.

Under the Hoodie 2019, es un estudio estadístico sobre el arte de las pruebas de penetración para encontrar hallazgos de vulnerabilidades, se realizó 180 trabajos de pruebas de penetración durante 9 meses, entre mediados de septiembre y finales de mayo de 2019. En los compromisos involucrados se encontraron vulnerabilidades expuestas a los atacantes, las contraseñas fueron uno de los factores donde más compromisos se encontró ya que el 60% de las contraseñas eran fáciles de adivinar.

En las evaluaciones internas, se centraron en Directorio Activo de Windows, teniendo como resultado que el 96% evidencio vulnerabilidad, como estándares de cifrados débiles, políticas de contraseñas débiles, software desactualizado y parches faltantes entre otros. (*Under the Hoodie 2019*, 2019).

4. METODOLOGÍA

4.1. FASES DEL TRABAJO DE GRADO

La elaboración de la guía de aseguramiento para Directorio Activo se plantea con base a la ejecución de tres fases de PenTesting White Box (Poston, 2020), reconocimiento, escaneo y enumeración, que son las necesarias para alinear los objetivos de este proyecto, este PenTest tipo White Box implica que la evaluación de la seguridad y las pruebas son con conocimiento completo de la infraestructura, por parte del PenTester, para ello se llevaron a cabo estas etapas, las cuales se pueden consultar en el Anexo B.

- **Análisis de la muestra**
 - Elaboración de encuesta
 - Publicación de encuesta
 - Análisis de resultados de encuestas

- **Fase 1. Malas prácticas de implementación de Directorio Activo**
 - Implementación de servidor con ajustes predeterminados
 - Instalación de Directorio Activo inseguro
 - Creación de cuentas de usuario y equipos
 - Creación de GPO
 - Cuentas de servicio o genéricas
 - Creación de grupos de seguridad

- **Fase 2. Análisis de Directorio Activo inseguro**
 - Fase de reconocimiento
 - Fase de escaneo
 - Fase de enumeración

- **Fase 3. Implementación de Directorio Activo con aseguramiento**
 - Implementación de Servidor con ajustes asegurados
 - Instalación de Directorio Activo asegurado

- **Fase 4. Análisis de Directorio Activo asegurado**
 - Fase de reconocimiento
 - Fase de escaneo
 - Fase de enumeración

- **Conclusión y Recomendaciones**
 - Resultado de buenas practicas
 - Resultado PenTest

4.2. INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Para la elaboración de las fases del proyecto se usará el software para la virtualización de sistemas operativos Windows Server y partiendo de ello se creará la guía de aseguramiento, para quienes accedan obtengan una experiencia más cercana a la puesta en práctica, el resultado de este material se puede encontrar en los anexos del proyecto.

Para desarrollar este proyecto se requiere el uso de software de Microsoft, GNU (*GNU Sistema Operativo*, 2020) y encuestas web.

- **VirtualBox.** (Oracle, 2020) Este software permitirá realizar la virtualización del sistema operativos Windows Server y desarrollar los laboratorios de cada fase del proyecto.
- **Kali Linux** (OffSec Services, 2020a) es la base para la ejecución de la herramienta Nessus.
- **Nessus** (Tenable, 2020), este permitirá realizar los análisis de vulnerabilidades a los servidores y con esto determinar su método de explotación.
- **Google Forms** (GSuite, 2020), software incluido en el paquete GSuite institucional, se aplicará una encuesta a la población tomada del total de estudiantes de pregrado y posgrado la facultad de ingeniería de la universidad Católica de Colombia, se tomará una muestra de 35 estudiantes que desempeñan cargos como administradores de plataforma tecnológica con un nivel de confianza del 90% y un margen de error del 14%.
- **NMAP** (Lyon, 2020) una potente herramienta de escaneo de redes incluida en Kali Linux (con esta herramienta se realizará el escaneo y auditoria de puertos al Directorio Activo, se ejecuta un reconocimiento como el fin de evidenciar información relevante que puede ser aprovechada por un atacante.
- **BloodHound** (Robbins, 2016/2020) es una aplicación web Javascript, con una base de datos Neo4j (Neo4j, 2020) alimentada por un recolector de datos C #, utiliza la teoría de gráficos para revelar las relaciones ocultas y a menudo, no deseadas dentro de un entorno de Directorio Activo.
- **SharpHound** (Vazarkar, 2017/2020) Recolector de datos de JSON (json.org, 2020) de Directorio Activo, es el necesario para extraer la información que será importada a BloodHound.
- **LDAPDomainDump** (Dirk-jan, 2016/2020) herramienta en base Python desarrollada por permite recuperar información desde cualquier usuario o equipo autenticado en el Directorio Activo, esto a través de LDAP.

4.3. ALCANCES Y LIMITACIONES

Alcance

Verificación del grado de seguridad de las infraestructuras Windows Server de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado se apoya de la entrega de este documento, de la guía de aseguramiento la cual permitirá proporcionar una guía de fácil entendimiento para los administradores de Directorio Activo.

Este proyecto está en la capacidad de:

- Construir una guía de aseguramiento de Directorio Activo con las mejores prácticas de seguridad informática.
- Encuesta para evidenciar las malas prácticas de implementación de Directorio Activo.
- Comparar el estado de aseguramiento de los entornos inseguro y asegurado de Directorio Activo.

Limitaciones

- El periodo del licenciamiento de Windows Server implica varias instalaciones del sistema operativo Windows Server.
- La encuesta anónima no alcanzara una muestra de más de 35 administradores de plataforma tecnológica.
- La simulación consistirá en una prueba de concepto dentro de los recursos virtualizados en un computador personal.
- La reducción de riesgos se apoyará en los resultados de sistemas operativos virtualizados.
- La documentación se elaborará partiendo de los sistemas operativos virtualizados.
- Los análisis PenTest solo se ejecutarán las fases de reconocimiento, escaneo y enumeración, ya que hasta ese punto se puede demostrar el nivel de aseguramiento.

5. PRODUCTOS A ENTREGAR

Como resultado de la investigación y elaboración de las fases del proyecto se obtienen como entregables los siguientes documentos, en entre los cuales se incluye la guía de aseguramiento:

- Artículo IEEE verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado en el ambiente simulado.
- Documento de proyecto de grado verificación del grado de inseguridad de las infraestructuras Windows de directorio activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado.
- Guía de Aseguramiento de Directorio Activo, documento de análisis previo y posterior al aseguramiento del Directorio Activo de Windows Server 2016.

6. ENTREGA DE RESULTADOS E IMPACTOS

Visualizar la problemática que existe en el entorno simulado al existir una implementación laxa o débil en buenas prácticas de aseguramiento de Directorio Activo.

Confirmar o descartar que las malas prácticas de aseguramiento generan un entorno inseguro en el Directorio Activo.

Generar una guía de recomendaciones que robustezcan las prácticas de aseguramiento de Directorio Activo.

Futuros profesionales y especialistas de ingeniería puedan tomar como referencia esta guía de aseguramiento desde repositorio de la Universidad Católica de Colombia y aplicarla a entornos de Directorio Activo.

7. ESTRATEGIAS DE COMUNICACIÓN

La publicación del documento de grado, la guía de aseguramiento y el artículo IEE de la verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado, serán publicados en el repositorio de la universidad católica de Colombia.

8. DESARROLLO DEL PROYECTO

8.1. ANÁLISIS DE LA ENCUESTA

Se aplicó una encuesta por medio de Google Forms (GSuite, 2020) de 13 preguntas a una muestra de no más de 35 administradores de plataforma de Directorio Activo, donde se obtuvieron unos resultados que permitieron determinar ajustes para la elaboración de la guía de aseguramiento.

Los resultados determinados se enfocan en la aplicación de la guía de aseguramiento, estos resultados pueden ser consultados en el Anexo C.

Partiendo de los resultados se pudo determinar que el 60% de los encuestados usan Windows Server 2016 para la implementación de Directorio Activo, esto permitió determinar cuál sistema operativo implementar para en la guía de aseguramiento.

¿Sobre que versión de Windows Server se encuentra implementado su Directorio Activo?
35 responses

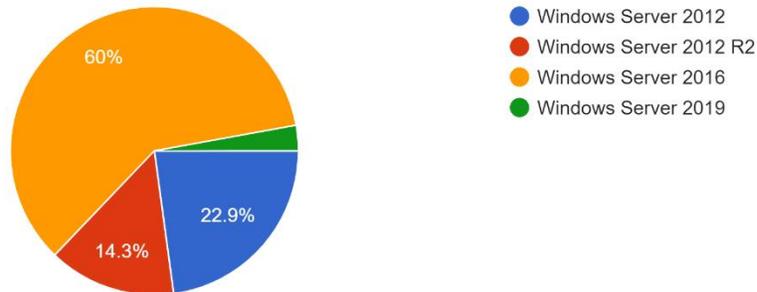


Figura 3 – Versión de sistema operativo de Directorio Activo.

Se pudo comprobar que el 54.3% de los encuestados no cuentan con un BaseLine de aseguramiento lo cual puede comprometer las Confidencialidad, integridad y disponibilidad de la plataforma, esto permite que se pueda elaborar una guía de aseguramiento que pueda ser usada por los administradores de plataforma para la implementación de buenas prácticas en Directorio Activo.

¿Cuenta con un BaseLine de aseguramiento (Hardening) en su Directorio Activo?

35 responses

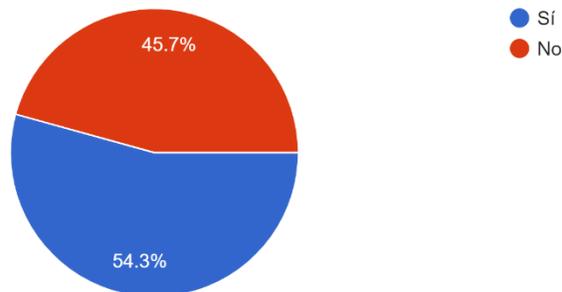


Figura 4 – Hardening aplicados a Directorio Activo.

El 40% de los encuestados no ha consultado un manual de buenas prácticas, es un porcentaje significativo y por medio de la elaboración de la guía de aseguramiento se puede reducir este porcentaje y brindar un modelo de buenas prácticas.

¿Alguna vez ha consultado un manual o guía de buenas prácticas sobre Directorio Activo?

35 responses

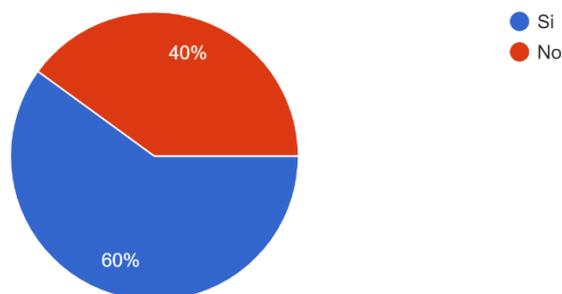


Figura 5 – Consulta de administradores de guías de aseguramiento de Directorio Activo.

En el sondeo realizado se evidencia que el 60% de los encuestados tienen una percepción de que se debe realizar una inversión económica, para el aseguramiento de Directorio Activo, por medio de la guía se demuestra que no es necesario incurrir en gastos adicionales.

¿Considera que es posible contar con un Directorio Activo correctamente asegurado sin incurrir en gastos?

35 responses

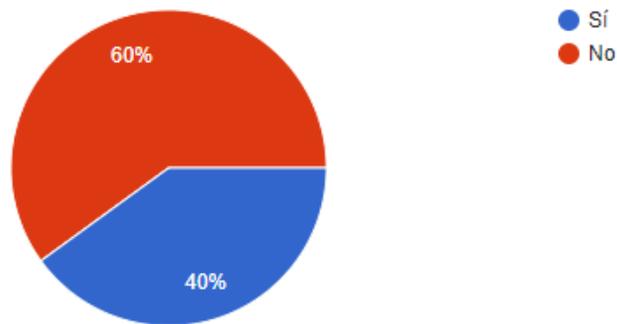


Figura 6 - Percepción de los administradores en costos de implementación.

Partiendo de estos antecedentes se evidencia la importancia del plantear una guía de aseguramiento de Directorio Activo sobre Windows Server 2016, que permita demostrar la diferencia entre el nivel de aseguramiento en un entorno inseguro y otro asegurado, se demuestra cómo proteger dicha plataforma tanto de malas prácticas como de posibles vulnerabilidades que permitan el acceso no autorizado por los atacantes, esta guía de aseguramiento corresponde al Anexo B.

8.2. IMPLEMENTACIÓN DE DIRECTORIOS ACTIVOS

La implementación de los directorios activos se realizó en un ambiente virtualizado utilizando la plataforma VirtualBox (Oracle, 2020), realizando la instalación de Windows Server 2016 (Microsoft, 2020c), simulando dos entornos, el primero aplicando malas prácticas (inseguro) y el segundo entorno aplicando buenas prácticas (asegurado).

Para el entorno inseguro se realizó una instalación de sistema operativo Windows Server 2016 (Microsoft, 2020c) con ajustes predeterminados sin ningún tipo de configuración de redundancia para servicios y sin tener en cuenta ninguna buena práctica, el rol de AD DS (Active Directory Directory Services) (Foulds, 2018) se promovió sobre este servidor inseguro, en cual se creó el dominio CATOLICA.CO.

Se realizó la creación de las Organizational Unit (OU) con una jerarquía basada en objetos y organización, se ajustaron GPO predeterminadas y se limitaron los permisos de medios removibles, para la gestión de cuentas de usuarios y equipos se establecieron políticas básicas, se crearon cuentas de servicios y genéricas haciéndolas miembro de grupos operadores, se deshabilitaron herencias de GPO y se concedieron permisos de acceso remoto a grupos de seguridad, para más detalle de este entorno consultar el capítulo 2 del Anexo B.

Para el entorno asegurado se implementaron dos servidores Windows Server 2016 (Microsoft, 2020c), aplicando buenas prácticas desde su implementación, puesta en producción y gestión, para ello se aprovisionaron dos tarjetas de red en cada uno, en este entorno se realizaron actividades de parchado, remediación de vulnerabilidades, NIC Teaming (Delprato, 2020), antes de promover el AD DS (Active Directory Directory Services), para este Directorio Activo se promovió el dominio CATOLICA.SI y se modificaron las rutas predeterminadas para SYSVOL y NTDS, se usaron los dos servidores con el fin de contar con dos controladores de dominio con capacidad de Catalogo Global y tener redundancia de servicios, además de realizar la destrucción de roles FSMO (Deland-Han, 2020a).

Para este entorno se implementaron Organizational Unit (OU) con jerarquía híbrida (ADR Formacion, 2020), GPO BaseLine con Security Compliance Toolkit (SCT) (Montemayor, 2020), almacenamiento de eventos para SIEM apoyada en el numeral A12.4.1 de ISO 27002 (MinTIC, 2018), limitación de cuentas genéricas y de servicio, configuración de relojes apoyada en el numeral A12.4.4 de ISO 27002 (MinTIC, 2018), por parte de los autores del proyecto y desde su experiencia se propone estas buenas prácticas, proceso de depuración de cuentas de equipos y usuarios, GPO BaseLine personalizadas, respaldo de GPO, creación masiva de usuarios, cronograma de parchado y ajuste de nomenclatura de equipos, para mayor detalle consultar el capítulo 4 del Anexo B.

8.3. COMPARACION DEL NIVEL DE ASEGURAMIENTO EN DIRECTORIOS ACTIVOS

Por medio de la ejecución de tres etapas de PenTest tipo White Box, se logró determinar el grado de aseguramiento de los entornos de Directorio Activo tanto el inseguro CATOLICA.CO y el asegurado CATOLICA.SI, estas etapas de PenTest fueron determinantes para reflejar la importancia de buenas prácticas desde la implementación, configuración y gestión del Directorio Activo.

Solo se aplicaron tres etapas del PenTest ya que con ello se pudo demostrar el grado de aseguramiento de los dos entornos.

Tabla 3 – Fases PenTest White Box

FASES PENTEST WHITE BOX	
FASES	DESCRIPCION
Reconocimiento	Esta fase es la que más tiempo insume dentro de la planificación. Lo que se busca en primera instancia es definir al objetivo y, a partir de ello, obtener la mayor cantidad de información sobre él. En el ámbito corporativo, además se buscarán direcciones IP, resolución de nombres DNS, etcétera.
Escaneo	En esta fase utilizaremos la información previa con el objetivo de detectar vectores de ataque en la infraestructura de la organización. En primer lugar, comenzaremos con el escaneo de puertos y servicios del objetivo. Determinamos qué puertos se encuentran abiertos y luego, en reglas generales, asociamos el puerto a un servicio dado. Una vez que hemos finalizado con esto, llega el turno del escaneo de vulnerabilidades. Éste nos permitirá encontrar vulnerabilidades en él o los equipos objetivo, tanto del sistema operativo como de las aplicaciones.
Enumeración	El objetivo de esta fase es obtener información relativa a los usuarios, nombres de equipos, recursos y servicios de red. Para esto, se generan conexiones activas con los sistemas y se realizan consultas directas para obtener esa información. Es decir, a diferencia del caso anterior, las consultas siempre se hacen al equipo objetivo y en forma activa, lo que trae aparejado que las conexiones puedan ser detectadas y registradas.

Acceso	Una vez detectadas las vulnerabilidades, el gran paso es el ingreso al sistema definido como objetivo, aquí se utilizan los recursos y conocimientos de manera condensada. Una vez encontrada una vulnerabilidad, el atacante buscará un exploits que le permita explotarla.
Mantenimiento de acceso	Una vez obtenido el acceso, lo que realmente se busca es mantener al equipo comprometido entre las filas del atacante. Para esto, hay que buscar la manera de que el acceso ganado sea perdurable en el tiempo. En la mayoría de los casos, esto se logra a partir de la instalación y ejecución de diversos tipos de software malicioso.

Fuente: (Seguridad Informática, 2019)

Una vez que se definió el alcance del PenTest se determinaron las herramientas usadas para la detección de malas prácticas y vulnerabilidades en los entornos de Directorios Activos.

Tabla 4 - Herramientas PenTest.

HERRAMIENTAS PENTEST		
FASES	HERRAMIENTA	DESCRIPCION
Fase de reconocimiento	RSOP	RSOP.msc, (Deland-Han, 2020b) este comando trae un informe de todas las configuraciones de las GPO aplicadas para usuarios y equipos dentro de Directorio Activo,
	Gpresult	Alternativa en caso de contar con permisos suficientes para la ejecución de RSOP se puede ejecutar un gpresult (Ross, 2020), con el cual se puede obtener el mismo resultado.
	POLENUM	Polenum (OffSec Services, 2020b), es un script en Python incluido en Kali Linux (OffSec Services, 2020a), utiliza la biblioteca Impacket de CORE Security Technologies para extraer la información de la política de contraseñas de una máquina con Windows. Esto permite a un usuario que

		no es de Windows consultar la política de contraseñas de un Windows remoto.
	Net group	Se pueden realizar las consultas de los usuarios asociados a grupos del Directorio Activo, las consultas se realizan con un usuario de dominio con mínimos privilegios, se puede consultar la asignación de usuarios a grupos, este tipo de información es muy relevante para los atacantes ya que permite la detección de cuentas de servicio, para ello ejecutamos la sintaxis la cual varia si se ejecuta desde Windows net group (Microsoft, 2020b).
	Net rpc group members	Alternativa en caso de contar con permisos suficientes para la ejecución de net group (Tridgell, 2020) se puede ejecutar un net rpc group members desde Kali Linux (OffSec Services, 2020a).
	LDAPDomainDump	La herramienta LDAPDomainDump, en base Python desarrollada por Dirkjanm (Dirk-jan, 2016/2020) permite recuperar información desde cualquier usuario o equipo autenticado en el Directorio Activo, esto a través de LDAP. Esto hace que LDAP sea un protocolo interesante para recopilar información en la fase de reconocimiento de un pentest de una red interna.
Fase de escaneo	NMAP	NMap (Network Mapper) (Lyon, 2020), una potente herramienta de escaneo de redes incluida en Kali Linux (OffSec Services, 2020a) con esta herramienta se realizará el escaneo y auditoria de puertos al Directorio Activo.

	VulScan	NMap (Lyon, 2020) tiene múltiples funciones entre ellos integrar los scripts de vulscan.nse, esta herramienta desarrollada por Marcruet (Ruef, 2017/2020), es un módulo que mejora NMap y que lo convierte en un escáner de vulnerabilidades, habilita la detección de versiones por servicio, lo que permite determinar fallas potenciales según el producto identificado, compara sus scripts contra bases de datos de vulnerabilidades como CVE de Mitre (CVE - Search Results, 2020), OpenVas (OpenVAS, 2020), XForce (IBM Security, 2020), SecurityFocus (SecurityFocus, 2020).
	Nessus	Nessus 8.11.1 (Tenable, 2020) sobre Kali Linux (OffSec Services, 2020a), esta herramienta de la empresa Tenable una de las más precisas del mercado, con los índices más bajos de falsos positivos y con mayor cantidad de módulos, lo cual permite la detección de vulnerabilidades de diversos servicios.
Fase de enumeración	SharpHound	SharpHound herramienta desarrollada Rvazarkar (Vazarkar, 2017/2020), esta herramienta es un recolector JSON de datos de Directorio Activo.
	BloodHound	BloodHound (Robbins, 2016/2020), es una aplicación web Javascript, con una base de datos Neo4j (Neo4j, 2020), alimentada por un recolector de datos C #, utiliza la teoría de gráficos para revelar las relaciones ocultas y a menudo, no deseadas dentro de un entorno de Directorio Activo. los atacantes pueden usar BloodHound (Robbins, 2016/2020) para identificar fácilmente rutas de ataque altamente complejas que de otro modo serían imposibles de identificar rápidamente. Los defensores pueden usar BloodHound (Robbins, 2016/2020) para identificar y eliminar esas mismas rutas

		de ataque. Tanto los Blue Teams como los Red Teams pueden usar BloodHound para obtener fácilmente una comprensión más profunda de las relaciones de privilegios en un entorno de Directorio Activo.
Fase de acceso	Ninguna	No se cuentan con herramientas, ya que esta fase no hace parte del alcance de la guía de aseguramiento.
Fase de mantenimiento de acceso	Ninguna	No se cuentan con herramientas, ya que esta fase no hace parte del alcance de la guía de aseguramiento.

Fuente: Recurso propio

8.3.1. RESULTADOS PENTEST DIRECTORIOS ACTIVOS

Estos análisis definieron la vulnerabilidad del Directorio Activo inseguro en comparación contra el Directorio Activo asegurado, demostrando el grado de aseguramiento de ambas plataformas, para esta guía se ejecutaron tres etapas de PenTest tipo White Box, esto debido a que se alinea con el alcance y los objetivos del proyecto de Verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado, se puede consultar mayor detalle de las fases de PenTest en los capítulos 3 y 5 del Anexo B.

Para el primer entorno de Directorio Activo inseguro correspondiente al dominio CATOLICA.CO se obtuvieron estos resultados tras la ejecución del PenTest.

Tabla 5 – Resultados PenTest Directorio Activo inseguro.

EJECUCION PENTEST DIRECTORIO ACTIVO INSEGURO			
FASES	HERRAMIENTA	RESULTADO	CONCLUSION
Fase de reconocimiento	RSOP	POSITIVO	Reconocimiento pasivo, se obtiene la aplicación de políticas sobre el usuario.
	Gpresult	POSITIVO	Reconocimiento pasivo, se obtiene la aplicación

			de políticas sobre el usuario.
	POLENUM	POSITIVO	Reconocimiento activo, se usa una herramienta intrusiva ajena al dominio la cual puede ser detectada, se obtienen las políticas de contraseña.
	Net group	POSITIVO	Reconocimiento pasivo, Se obtiene información de los usuarios asociados a grupos.
	Net rpc group members	POSITIVO	Reconocimiento pasivo, Se usa una herramienta ajena al dominio, Se obtiene información de los usuarios asociados a grupos.
	LDAPDomainDump	POSITIVO	Reconocimiento activo, se usa una herramienta intrusiva ajena al dominio, se obtiene nombres de grupos, usuarios y equipos, detalles de políticas de contraseña y usuarios sin caducidad de contraseña.
Fase de escaneo	NMAP	POSITIVO	Escaneo de puertos, se detectan puertos asociados a servicios.
	VulScan	POSITIVO	Escaneo de puertos, se detectan puertos asociados a vulnerabilidades.
	Nessus	POSITIVO	Escaneo de Vulnerabilidades, se ejecuta el análisis de vulnerabilidades se evidencias vulnerabilidades explotables.

Fase de enumeración	SharpHound	POSITIVO	Extracción de información, se logra extraer información de la estructura del Directorio Activo.
	BloodHound	POSITIVO	Se grafica la información obtenida y se evidencias las rutas más cortas para ejecutar el acceso al Directorio Activo.
Fase de acceso	Ninguna	SIN RESULTADO	No es parte del alcance de la guía de aseguramiento.
Fase de mantenimiento de acceso	Ninguna	SIN RESULTADO	No es parte del alcance de la guía de aseguramiento.

Fuente: Recurso propio

Para el segundo entorno de Directorio Activo asegurado correspondiente al dominio CATOLICA.SI se obtuvieron estos resultados tras la ejecución del PenTest.

Tabla 6 – Resultados PenTest Directorio Activo asegurado.

EJECUCION PENTEST DIRECTORIO ACTIVO ASEGURADO			
FASES	HERRAMIENTA	RESULTADO	CONCLUSION
Fase de reconocimiento	RSOP	NEGATIVO	Reconocimiento pasivo, no se logra ejecutar la sintaxis, gracias a la aplicación de políticas restrictivas para los usuarios.
	Gpresult	NEGATIVO	Reconocimiento pasivo, no se logra ejecutar la sintaxis, gracias a la aplicación de políticas restrictivas para los usuarios.

	POLENUM	POSITIVO	Reconocimiento activo, se usa una herramienta intrusiva ajena al dominio la cual puede ser detectada, se obtienen las políticas de contraseña.
	Net group	NEGATIVO	Reconocimiento pasivo, no se logra ejecutar la sintaxis, gracias a la aplicación de políticas restrictivas para los usuarios.
	Net rpc group members	POSITIVO	Reconocimiento pasivo, Se usa una herramienta ajena al dominio, Se obtiene información de los usuarios asociados a grupos.
	LDAPDomainDump	NEGATIVO	Reconocimiento activo, se usa una herramienta intrusiva ajena al dominio, no se logra obtener información gracias al aseguramiento del puerto LDAP SSL por medio de GPO SCT.
Fase de escaneo	NMAP	POSITIVO	Escaneo de puertos, se detectan puertos asociados a servicios, aunque no logra determinar la versión del sistema operativo.

	VulScan	NEGATIVO	Escaneo de puertos, no se detectan puertos asociados a vulnerabilidades.
	Nessus	NEGATIVO	Escaneo de Vulnerabilidades, se ejecuta el análisis de vulnerabilidades, no se evidencias vulnerabilidades explotables.
Fase de enumeración	SharpHound	NEGATIVO	Extracción de información, no se logra extraer información de la estructura del Directorio Activo, esto debido la protección de Windows Defender.
	BloodHound	NEGATIVO	No es posible graficar la información debido a que no se obtiene con SharpHound.
Fase de acceso	Ninguna	SIN RESULTADO	No es parte del alcance de la guía de aseguramiento.
Fase de mantenimiento de acceso	Ninguna	SIN RESULTADO	No es parte del alcance de la guía de aseguramiento.

Fuente: Recurso propio

Sobre los análisis de vulnerabilidades se obtuvieron estos resultados, donde se comprueba que la realización de parchado y la remediación de vulnerabilidades antes de la puesta en producción, reducen en un 100% las exposiciones posibles explotaciones en el Directorio Activo, se pueden consultar los resultados de los análisis de vulnerabilidades en el capítulo 7 Anexo B.

ANALISIS DE VULNERABILIDADES NESSUS - DIRECTORIOS ACTIVOS

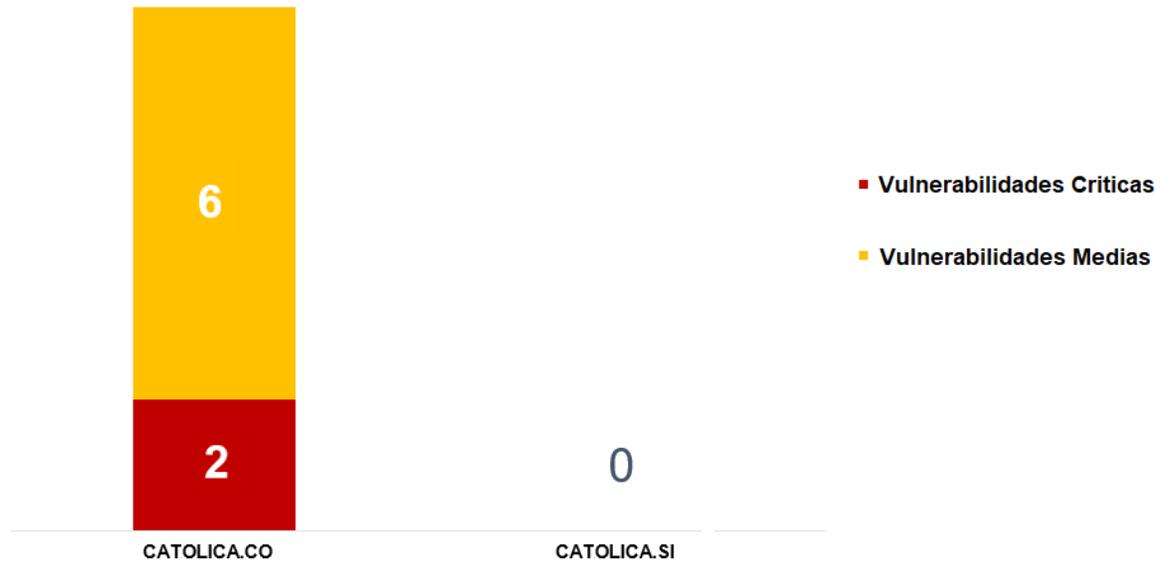


Figura 7 – Comparación de vulnerabilidades Nessus por Directorio Activo.

ANALISIS DE VULNERABILIDADES NESSUS - CATOLICA.CO

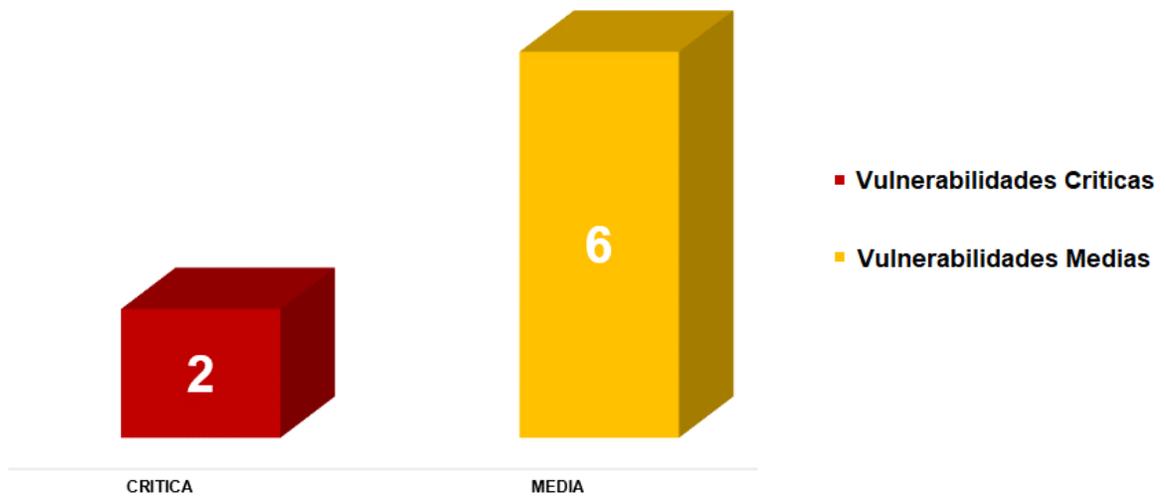


Figura 8 – Severidad de vulnerabilidades en Directorio Activo inseguro.

El análisis BloodHound (Robbins, 2016/2020), correspondiente a la fase de enumeración realiza la consulta de las rutas más cortas para escalar privilegios a grupos como Admins. del Dominio, en la ejecución de la herramienta sobre el

Directorio Activo inseguro se evidencia ausencia de GPO, mala distribución de OU y malas prácticas en ajustes de usuarios, grupos, múltiples brechas para que una atacante pueda acceder al Directorio Activo, estos análisis se pueden consultar en el Anexo B.

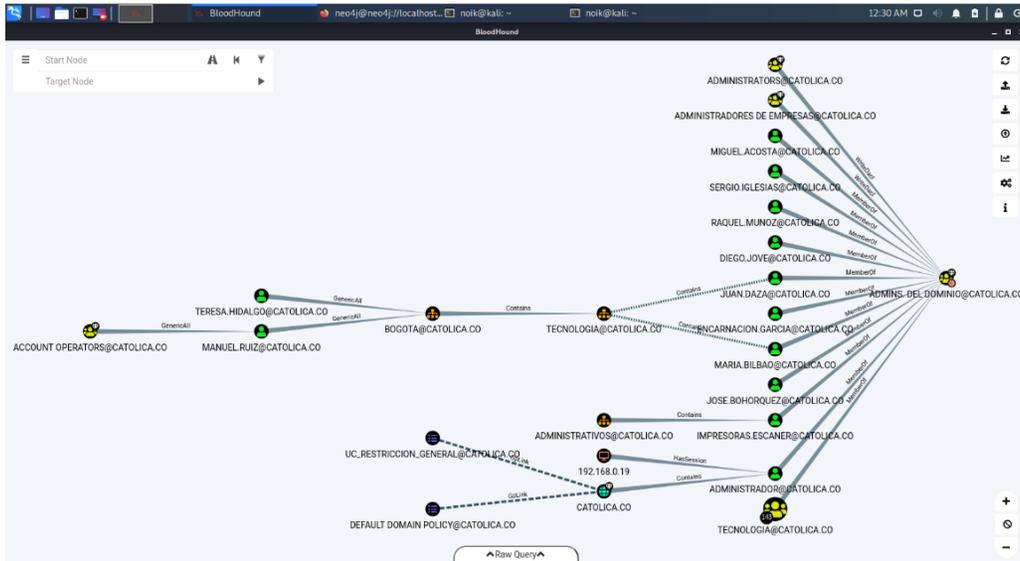


Figura 9 – Análisis BloodHound estructura Directorio Activo inseguro.

Se evidencia cuentas de servicio o genéricas asociadas a grupos de operadores lo cual ocasiona que puedan escalar privilegios.

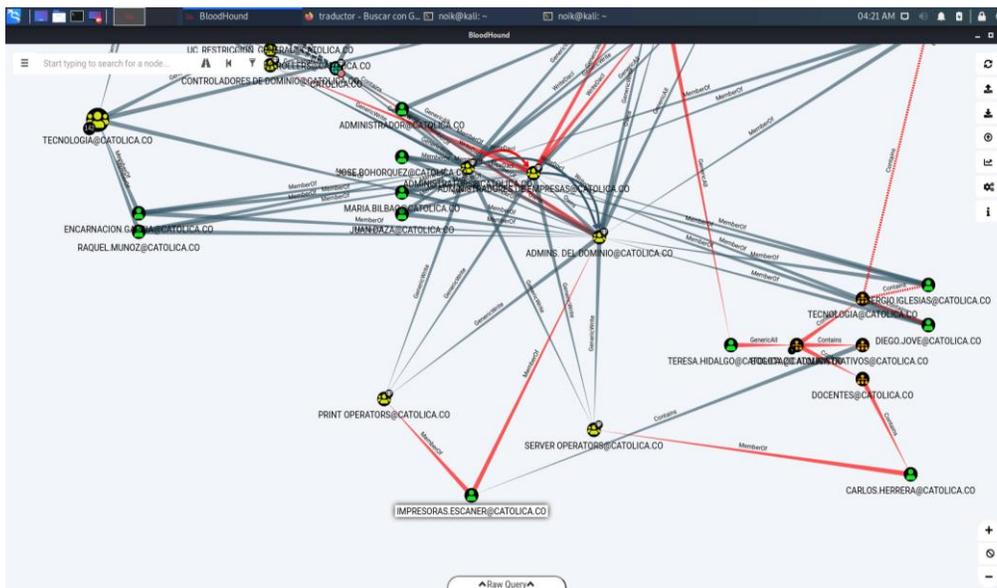


Figura 10 - Análisis BloodHound Directorio Activo inseguro cuentas de servicio y genéricas.

El análisis de enumeración sobre el Directorio Activo asegurado no se puede realizar debido a la aplicación las GPO SCT, para este caso solo se realiza la consulta con consentimiento de los autores del proyecto con el fin de mostrar el estado de del Directorio Activo.

Se consulta la ruta más corta para llegar a los Admins. Del Dominio, en este caso se evidencias las diferentes GPO y UO en las cuales se debe estar ubicado para lograr escalar privilegios, se comprueba que dos usuarios cuentan con privilegios de administrador y el usuario local se encuentra desactivado.



Figura 11 - Análisis BloodHound estructura Directorio Activo asegurado.

No se evidencian brechas que se puedan usar para escalar privilegios con usuarios genéricos o de servicios.

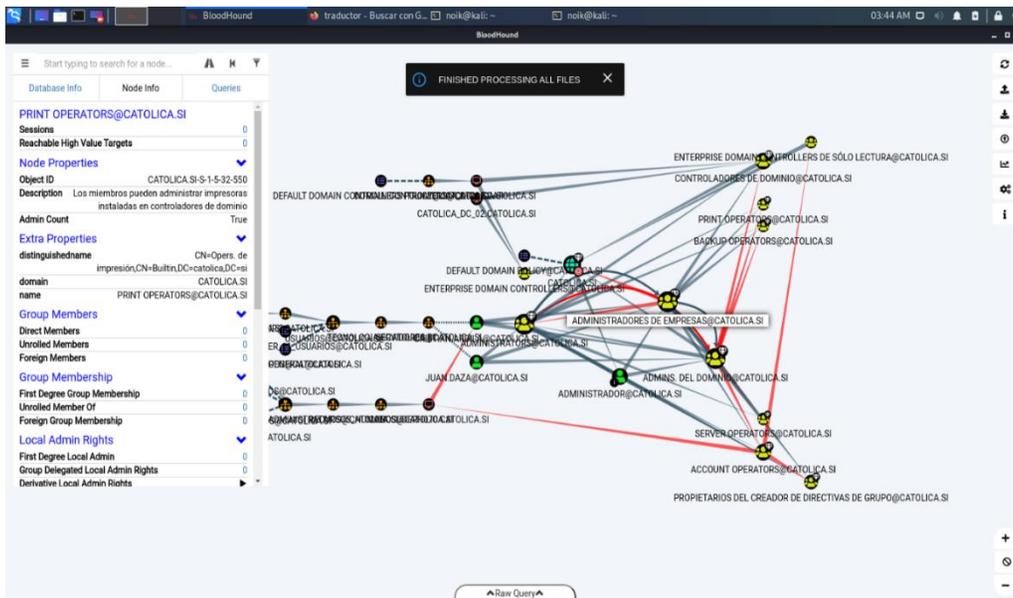


Figura 12 - Análisis BloodHound Directorio Activo asegurado cuentas de servicio y genéricas.

8.3.2. EJECUCIÓN DE BUENAS PRACTICAS EN DIRECTORIOS ACTIVOS

En la implementación y gestión del Directorio Activo inseguro se plantea una bitácora de cumplimiento de buenas prácticas, sobre esta implementación se evidencia descuido del administrador, se puede permitir la obtención de información valiosa ya sea para la ejecución de exploits o el uso de ingeniería social.

Tabla 7 – Cumplimiento de buenas prácticas Directorio Activo inseguro.

BUENAS PRACTICAS DIRECTORIO INSEGURO		
BUENA PRACTICAS	CUMPLE	ESTADO DIRECTORIO ACTIVO INSEGURO
Infraestructura con redundancia en sistema operativo y servicios.	NO	Esta implementación de Directorio Activo no cuenta con un respaldo en caso de fallo, para los roles AD DS y DNS.
Infraestructura con redundancia en conexiones red.	NO	El servidor implementado no cuenta con un respaldo de conexión de red en caso de fallo propio o ajeno.
Parchado de sistema operativo.	NO	No se realizó el parchado del sistema operativo tras su implementación.
Establecer cronogramas de parchado.	NO	No se cuenta con ningún ajuste para esta actividad.

Limitar segmentos de red.	NO	Tanto el Directorio Activo como los equipos cliente se encuentran en la misma VLAN.
Evitar rutas predeterminadas para las ubicaciones de SYSVOL y NTDS.	NO	Estas bases de datos se almacenan en las rutas predeterminada.
Contar con OU jerárquicas.	NO	Faltas la OU basadas en función.
Proteger OU contra eliminación accidental.	SI	Todas las unidades cuentan con protección accidental es un ajuste predeterminado.
Solicitar cambios de contraseña cada 60 días.	SI	La GPO Default Domain Policy cuenta con una solicitud de cambio cada 60 días.
Contar con una contraseña segura de 14 caracteres y requisitos de complejidad. (mayúsculas, minúsculas, caracteres especiales y números).	NO	No se cuenta con esta configuración, ya que se dejan los ajustes predeterminados del Default Domain Policy.
Solicitar cambio de contraseña tras crear usuarios.	NO	Al realizar la creación de los usuarios no se configura ningún parámetro para que solicite cambio de contraseña.
En creaciones masivas de usuarios se deben asignar contraseñas diferentes.	NO	Se asigna la misma contraseña a todos los usuarios tras su creación.
Limitar perfiles de usuario por medio de GPO.	NO	No se limitan los perfiles de usuario solo se asignan GPO para bloqueo de medios extraíbles.
Sincronización de relojes, configuración NTP.	NO	Se realiza el ajuste de relojes contra la SIC. (Superintendencia de Industria y Comercio)
Asegurar con GPO OU sin herencia.	NO	Solo se deshabilitan la herencia de forma general.
Limitar el acceso de cuentas de servicio o genéricas en equipos o servidores.	NO	No se limitan estas cuentas solo se ubican sobre las OU que usan las cuentas.
Limitar la asignación de cuentas de servicio o genéricas a grupos de seguridad.	NO	Se asignan cuentas de servicio como el de impresoras.escaner al grupo Operadores de Impresión.

Limitar los usuarios Admins. del Dominio.	NO	Se asignan todos los miembros del grupo de seguridad de tecnología.
Deshabilitar usuario Administrador.	NO	El usuario se deja activo.
Limitar el acceso RDP o deshabilitar de ser necesario.	NO	Se habilita el acceso RDP a todos los usuarios miembros del grupo de seguridad Tecnología.
Contar con un plan de depuración de cuentas de equipos y usuarios.	NO	No se cuenta con ningún ajuste para esta actividad.
Realizar Backups de periódicos de GPO.	NO	No se cuenta con ningún ajuste para esta actividad.
Restringir que los usuarios modifiquen ajustes de Antivirus y Firewall.	NO	No se cuenta con restricción.

Fuente: Recurso propio

En la implementación y gestión del Directorio Activo asegurado evidencia un resultado muy positivo en cuanto al nivel de aseguramiento, gracias a actividades de parchado, remediación de vulnerabilidades y aplicación de SCT (Montemayor, 2020) sobre las GPO y ajuste de buenas prácticas, se alcanzó un nivel de seguridad óptimo, se logró el bloqueo y detección de la mayoría de reconocimiento y enumeración del PenTest, lo cual limitó la obtención de acceso a la plataforma.

Tabla 8 – Cumplimiento de buenas prácticas Directorio Activo asegurado.

EJECUCION DE BUENAS PRACTICAS		
BUENA PRACTICAS	CUMPLE	ESTADO DIRECTORIO ACTIVO ASEGURADO
Infraestructura con redundancia en sistema operativo y servicios.	SI	Se cuenta con 2 Controladores de Dominio para respaldar como medida de respaldo en caso de falla, puede mejorar si se implementa un tercer controlador de solo lectura.
Infraestructura con redundancia en conexiones red.	SI	Se configura NIC Teaming con 2 tarjetas de red por cada Controlador de Dominio esto para garantizar mayor redundancia de red.

Parchado de sistema operativo.	SI	Se realiza el parchado de los dos Controladores de Dominio a nivel de Windows Update, es recomendable plantear la implementación de una herramienta de gestión como WSUS o una de terceros.
Establecer cronogramas de parchado.	SI	Se establece un cronograma de parchado mensual documentando, KB, periodos de prueba y periodos de despliegue.
Limitar segmentos de red.	SI	Para este entorno se realizó la creación de dos segmentos de red, con el fin de independizar red de operación y red de Controladores de Dominio.
Evitar rutas predeterminadas para las ubicaciones de SYSVOL y NTDS.	SI	Se redistribuyen las bases de datos en diferentes unidades de red.
Contar con OU jerárquicas.	SI	Se implementan las OU en jerarquías híbridas tanto para equipos como usuarios.
Proteger OU contra eliminación accidental.	SI	Todas las unidades cuentan con protección accidental es un ajuste predeterminado.
Solicitar cambios de contraseña cada 60 días.	SI	La GPO Default Domain Policy con SCT solicita el cambio de credenciales cada 40 días.
Contar con una contraseña segura de 14 caracteres y requisitos de complejidad. (mayúsculas, minúsculas, caracteres especiales y números).	SI	La GPO Default Domain Controller Policy con SCT, esta ajustada para ajustar las contraseñas con estos parámetros.
Solicitar cambio de contraseña tras crear usuarios.	SI	Al realizar la creación de usuarios se asigna el argumento -ChangePasswordAtLogon el cual solicita el cambio en el primer inicio de sesión.
En creaciones masivas de usuarios se deben asignar contraseñas diferentes.	SI	Se generan contraseñas de forma aleatoria y se asigna una contraseña diferente a cada usuario.

Limitar perfiles de usuario por medio de GPO.	SI	Se realiza la creación de UC_Usuarios_General, la cual se usa como BaseLine para todos los usuarios.
Sincronización de relojes, configuración NTP.	SI	Se realiza el ajuste de relojes contra la SIC. (Superintendencia de Industria y Comercio)
Contar auditoria de eventos.	SI	La GPO Default Domain Controller Policy con SCT, cuenta con eventos de seguridad avanzada activados.
Asegurar con GPO OU sin herencia.	SI	Al deshabilitar la herencia para OU como Servidores se aplican directamente GPO Default Domain Policy, UC_Internet_Explorer_11_Usuarios.
Limitar el acceso de cuentas de servicio o genéricas en equipos o servidores.	SI	Se limitan las cuentas de servicio y genéricas, estas solo pueden ser usadas en horarios de lunes a viernes 08:00 – 18:00, en equipos específicos.
Limitar la asignación de cuentas de servicio o genéricas a grupos de seguridad.	SI	No se asignan las cuentas de servicio o genéricas a ningún grupo de seguridad con privilegios.
Limitar los usuarios Admins. del Dominio.	SI	Solo se asignan estos privilegios a los usuarios administradores de plataforma.
Deshabilitar usuario Administrador.	SI	Se deshabilita el usuario Administrador.
Limitar el acceso RDP o deshabilitar de ser necesario.	SI	Se deshabilita el acceso RDP, para este entorno no se requiere este acceso ya que el este entorno virtual se puede usar el HyperVisor, y la gestión de roles se puede realizar desde RSAT.
Contar con un plan de depuración de cuentas de equipos y usuarios.	SI	Se elabora un script para eliminación de cuentas de equipos y usuarios. (Deshabilitar usuarios con 8 días de inactividad), (Deshabilitar equipos con 1 mes de inactividad), (Eliminar usuarios con 1 mes de inactividad) (Eliminar equipos con 2 meses de inactividad.)

Realizar backups de periódicos de GPO.	SI	Para este entorno se plantea un script de backups automáticos de GPO.
Restringir que los usuarios modifiquen ajustes de Antivirus y Firewall.	SI	Se cuentan con este ajuste y se restringe por medio de GPO para que los usuarios pueden deshabilitarlos o hacer excepciones.

Fuente: Recurso propio

CUMPLIMIENTO DE BUENAS PRACTICAS EN DIRECTORIO ACTIVO INSEGURO

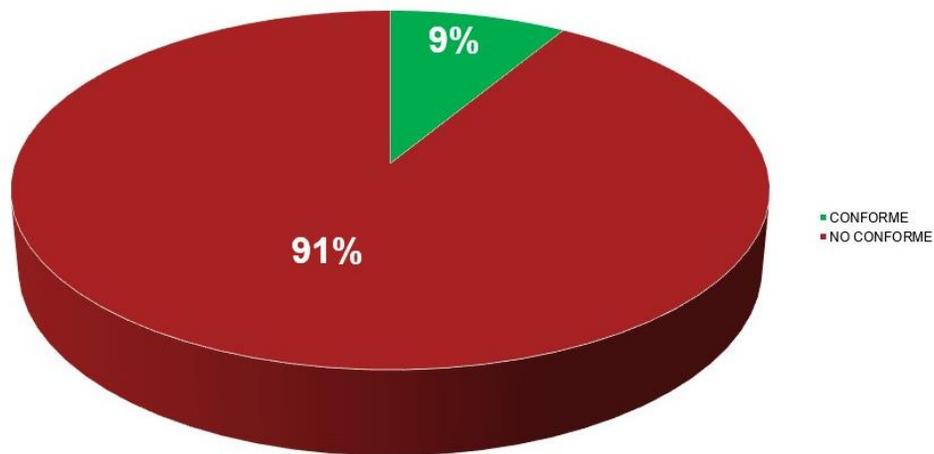


Figura 13 – Cumplimiento de buenas prácticas Directorio Activo inseguro.

CUMPLIMIENTO DE BUENAS PRACTICAS EN DIRECTORIO ACTIVO ASEGURADO



Figura 14 – Cumplimiento de buenas prácticas Directorio Activo asegurado.

8.4. DOCUMENTACIÓN DE BUENAS Y MALAS PRACTICAS

Se documentan las buenas y malas prácticas sobre el Directorio Activo, planteando la guía de aseguramiento donde se comparan dos entornos con prácticas de seguridad opuestas, en la guía de aseguramiento se hacen comentarios sobre malas prácticas en el Directorio Activo inseguro, estos comentarios se realizan a lo largo de su implementación y configuración, estas son algunas malas prácticas para este entorno, para mayor detalle consultar Anexo B.

- En la asignación de los recursos solo se contempla un servidor, el cual cuenta con una sola tarjeta de red, esto afecta la disponibilidad del servicio en caso de falla.
- No se realiza el parchado tras la instalación del sistema operativo, aunque la versión es relativamente reciente, esto no indica que pueda estar libre de vulnerabilidades.
- Realizar la instalación de un solo Controlador de Dominio afecta la disponibilidad del servicio en caso de falla.

- Si se almacenan los archivos de registro NTDS y la base de datos SYSVOL en las rutas predeterminadas sobre un solo Controlador de Domino en la partición C, se puede comprometer el Directorio Activo de tres formas, fallo en la unidad C: afecta la disponibilidad del servicio, las rutas predeterminadas son un objetivo de los atacantes, puede degradarse el acceso a NTDS y SYSVOL si se afecta el bloque de almacenamiento.
- Las GPO aplicadas tienen configuraciones escasas, no se ajustaron políticas para los equipos y no se ajustaron políticas de auditoría, para el almacenamiento de eventos, lo cual no permite realizar una trazabilidad a los eventos en el Controlador de Dominio.
- Deshabilitar la herencia sin vincular GPO con mayor jerarquía, puede otorgar permisos indirectos a los usuarios.
- Asignar a cuentas genéricas a grupos de operaciones es una mala práctica que puede ocasionar la escalación de privilegios, en caso de usar cuentas genéricas o de servicios se deben ajustar controles.
- Hacer miembros de “Admins. Del Dominio” a otros grupos, permite que cualquier usuario miembro de ese grupo sea un administrador con permisos totales sobre el Directorio Activo, los atacantes pueden hacerse miembros de estos grupos y tener control total.
- Asignar permisos RDP a grupos de seguridad a este servicio, ocasionaría que cualquier usuario miembro de este grupo acceda al servidor de forma remota, un atacante puede marcar como objetivo grupos con estos permisos.
- Asignar la misma contraseña a todos los usuarios, sin solicitar el cambio de esta, puede ocasionar que un atacante use cualquier usuario.

Para el caso del entorno de Directorio Activo asegurado se considera la aplicación de buenas prácticas en todo su proceso de implementación y configuración.

- Configuración de dos Controladores de Dominio para garantizar su disponibilidad en caso de fallo.
- Instalación de parches y remediación de vulnerabilidades antes de la promoción de Controladores de Dominio, adicional se sugiere una bitácora de parchado.
- Ajustes de redundantes de configuración de red.

- Redistribución de archivos de registro NTDS y la base de datos SYSVOL para optimizar su funcionamiento y garantizar su disponibilidad.
- Redistribución de roles FSMO entre Controladores de Dominio.
- Creación de UO con jerarquías híbridas.
- Asignación de nomenclatura para cuentas de equipos.
- Ajuste BaseLine para GPO, fortalecimiento de políticas para equipos, usuarios y Controladores de Dominio.
- Backups de GPO
- Proceso de depuración de cuentas de usuarios y equipos.
- Ajuste de relojes.
- Limitación de cuentas genéricas y de servicio.

9. CONCLUSIONES

Definimos conclusiones de cada fase de la elaboración del proyecto tomando como referencia el objetivo general y los objetivos específicos.

Los resultados de la encuesta permitieron determinar el grado de aseguramiento de Directorios Activos reales y en producción, esta información se usa como apoyo para a la elaboración de la guía de aseguramiento.

Con el resultado de los entornos simulados se evidencio lo vulnerable que puede ser un Directorio Activo ante una configuración predeterminada de sistema operativo y de roles en Windows Server 2016.

Se puede contrastar el grado de exposición en los dos entornos de Directorio Activo de la guía de aseguramiento, donde se comprueba que la aplicación de buenas prácticas permite reducir las vulnerabilidades y grado de exposición ante atacantes.

Las herramientas de PenTest permiten obtener información relevante a pesar de ser intrusivas, las ausencias de buenas prácticas permiten su ejecución sin ser detectadas.

Un Directorio Activo asegurado demanda un mayor tiempo del administrador de plataforma durante su implementación, configuración y gestión, esto debido a que se deben realizar más configuraciones en un entorno asegurado, con el fin de brindar apoyo y reducir tiempos, se proponen los scripts de automatización en la guía, esto optimiza tareas de rutina como por ejemplo la depuración de usuarios y la creación de Backups de GPO.

Es recomendable someter un Directorio Activo asegurado a análisis de PenTest periódicos, con el fin de fortalecer las configuraciones ya aplicadas.

Esta guía de aseguramiento de Directorio Activo deja abierta la posibilidad a futuras investigaciones con diferentes entornos de Directorio Activo y pruebas PenTest.

10. ANEXOS

ANEXO A

Articulo IEEE verificación del grado de inseguridad de las infraestructuras Windows de Directorio Activo y construcción de una guía de aseguramiento que eleve el nivel de seguridad encontrado en el ambiente simulado.

ANEXO B

Guía de Aseguramiento de Directorio Activo, documento de análisis previo y posterior al aseguramiento del Directorio Activo de Windows Server 2016.

ANEXO C

Resultados de encuesta de Aseguramiento de Directorio Activo, para la elaboración de la guía de aseguramiento de Directorio Activo.

11. BIBLIOGRAFÍA

389DS. (2017). 389 Directory Server. 389 Directory Server. <https://directory.fedoraproject.org/>

ADR Formacion. (2020). *Definición de unidades organizativas en un servidor*. https://www.adrformacion.com/knowledge/administracion-de-sistemas/definicion_de_unidades_organizativas_en_un_servidor.html

Apache Directory Studio. (2018). *Apache Directory Studio*. Apache Directory Studio. <https://directory.apache.org/studio/>

Beltran, S. (2019). *Explotación avanzada del directorio activo*. <https://repository.ucatolica.edu.co/handle/10983/24059>

Ceballos Lopez, A., Bautista Garcia, F., Mesa Guzman, L., & Arguez Quintero, C. (2020). *Tendencias Cibercrimen Colombia 2019—2020*. Policia Nacional. https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

CIS Controls. (2020). *Cybersecurity Best Practices*. <https://www.cisecurity.org/cybersecurity-best-practices/>

CVE - Search Results. (2020). CVE. <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ldap>

Deland-Han. (2020a). *Active Directory FSMO*. <https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/fsmo-roles>

Deland-Han. (2020b). *Usar RSoP. msc para recopilar la Directiva de equipo—Windows Server*. <https://docs.microsoft.com/es-es/troubleshoot/windows-server/group-policy/use-resultant-set-of-policy-logging>

Delprato, G. (2020). *Windows Server 2012: Equipos de NIC (NIC Teaming)*. *WindowServer*. <https://windowserver.wordpress.com/2012/09/16/windows-server-2012-equipos-de-nic-nic-teaming/>

Dirk-jan. (2020). *Ldapdomaindump* [Python]. <https://github.com/dirkjanm/ldapdomaindump> (Original work published 2016)

Foulds, I. (2018). *DNS y AD DS*. <https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/dns-and-ad-ds>

Franklin Smith, R. (2017). *NIST Cybersecurity Framework for Active Directory Security*. <https://www.quest.com/whitepaper/nist-cybersecurity-framework-for->

active-directory-security8132489/
Global server share by OS 2018-2019. (2018). Statista.
<https://www.statista.com/statistics/915085/global-server-share-by-os/>

GNU Sistema Operativo. (2020). Free Software Foundation.
<https://www.gnu.org/home.es.html>

GSuite. (2020). *Google Form.* <https://gsuite.google.com/intl/es-419/products/forms/>
IBM Security. (2020). *IBM X-Force Exchange.*
<https://exchange.xforce.ibmcloud.com/search/%23vulnerability>

Icontec. (2020). *Sistemas de Gestión de seguridad de la información. Icontec.*
https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion/

Introducción a Active Directory Domain Services. (2017).
<https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

json.org. (2020). *JSON.* <https://www.json.org/json-es.html>

Lyon, G. (2020). *Nmap: The Network Mapper—Free Security Scanner.*
<https://nmap.org/>

Metcalf, S. (2020a). *ADSecurity.* ADSecurity. <https://adsecurity.org/>

Metcalf, S. (2020b). *TRIMARC Securing the Enterprise.* Trimarc.
<https://www.trimarcsecurity.com/research>

Microsoft. (2020a). *Microsoft 365.* <https://www.microsoft.com/es-es/microsoft-365>

Microsoft. (2020b). *Net group.* [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc754051\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc754051(v=ws.11))

Microsoft. (2020c). *Prueba Windows Server 2016 en Microsoft Evaluation Software [Windows Server].* Microsoft. <https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2016/>

Microsoft. (2020d). *Prueba Windows Server on-premises o en el cloud.* Microsoft Cloud-Platform - ES (Español). <https://www.microsoft.com/es-es/cloud-platform/windows-server-trial>

MinTIC. (2018). *Modelo de Seguridad.* <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

Montemayor, D. (2020). *Microsoft Security Compliance Toolkit 1.0—Windows security*. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10>

Moore, S. (2018). *Gartner Forecasts Worldwide Information Security Spending to Exceed \$124 Billion in 2019*. <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

Moreno, J., Rodríguez, C., & Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. *I+D Tecnológico*, 16(1), 39-45. <https://doi.org/10.33412/idt.v16.1.2438>

Neo4j. (2020). *Neo4j Graph Platform*. Neo4j Graph Database Platform. <https://neo4j.com/>

OffSec Services. (2020a). *Kali*. <https://www.kali.org/>

OffSec Services. (2020b). *Polenum*. <https://tools.kali.org/password-attacks/polenum>

OpenVAS. (2020). *OpenVAS - Open Vulnerability Assessment Scanner*. <https://www.openvas.org/>

Oracle. (2020). *Oracle VM VirtualBox [Java]*. <https://www.virtualbox.org/>

Ley 256 de 1996, (1996). http://www.secretariassenado.gov.co/senado/basedoc/ley_0256_1996.html

Poston, H. (2020). *What are Black Box, Grey Box, and White Box Penetration Testing?* Infosec Resources. <https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/>

Rapid7. (2019). *Under the Hoodie 2019* [Research, stories, and findings from Rapid7 penetration tests]. <https://www.rapid7.com/research/under-the-hoodie/>

Robbins, A. (2020). *BloodHoundAD/BloodHound [PowerShell]*. BloodHoundAD. <https://github.com/BloodHoundAD/BloodHound> (Original work published 2016)

Rodríguez Vallecilla, A., & Mina Loango, J. E. (2019). Descripción del funcionamiento de ataque del Malware ransomware (WannaCry) en sus procesos de infección, encriptación y propagación en el sistema operativo Windows [Thesis, Universidad Santiago de Cali]. En *Repositorio Institucional USC*. <https://repository.usc.edu.co/handle/20.500.12421/137>

Ross, E. (2020). *Gpresult*. <https://docs.microsoft.com/en-us/windows-50>

server/administration/windows-commands/gpresult

Ruef, M. (2020). *Scipag/vulscan* [Lua]. scip ag. <https://github.com/scipag/vulscan> (Original work published 2017)

SecurityFocus. (2020). *SecurityFocus*. <https://www.securityfocus.com/>
Seguridad Informatica. (2019). *Penetration Testing*. 20.

Tenable. (2020). *Nessus*.
<https://www.tenable.com/downloads/nessus?loginAttempted=true>

Tridgell, A. (2020). *net—Tool for administration of Samba and remote CIFS servers*.
<https://www.samba.org/samba/docs/current/man-html/net.8.html>

Normativa Nacional, Ley 1266 de 2008, (2008).
<https://ucatolica.codigosleyex.info/LyxNormas/view/15709/htm>

Normativa Nacional, Ley 1273 de 2009, (2009).
<https://ucatolica.codigosleyex.info/LyxNormas/view/9282/htm>

Normativa Nacional, Ley 1581 de 2012, (2012).
<https://ucatolica.codigosleyex.info/LyxNormas/view/21817/htm>

Universidad Católica. (2020). *UCatolica*. Universidad Católica De Colombia.
<https://www.ucatolica.edu.co/portal/>

Vazarkar, R. (2020). *BloodHoundAD/SharpHound* [C#]. BloodHoundAD.
<https://github.com/BloodHoundAD/SharpHound> (Original work published 2017)

Why Active Directory (AD) Protection Matters. (2020).
<https://www.bankinfosecurity.com/whitepapers/active-directory-ad-protection-matters-w-5783>