EVALUACIÓN DE SEGURIDAD A LA INFRAESTRUCTURA DE SERVIDORES CRÍTICOS DE LA EMPRESA ECODIESEL COLOMBIA S.A.

GABRIEL RICARDO PABON CASTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANCABERMEJA
2023

EVALUACIÓN DE SEGURIDAD A LA INFRAESTRUCTURA DE SERVIDORES CRÍTICOS DE LA EMPRESA ECODIESEL COLOMBIA S.A.

GABRIEL RICARDO PABON CASTILLO

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Ing. ALEXANDER LARRAHONDO NUÑEZ
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BARRANCABERMEJA
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

El presente trabajo de Grado se lo dedico a mis padres, los cuales siempre me han apoyado y guiado en todos los aspectos de mi vida; a mi amada esposa la cual es el faro que guía mi vida y el ancla que me hace aterrizar en los momentos cuando estoy más disperso, mi compañera de aventuras y amiga incondicional; y sobre todo a la razón por la cual me despierto cada día, a mi hijo, el motor que nos guía y por el cual todo tiene sentido en nuestra vida.

AGRADECIMIENTOS

Agradezco a todos los tutores que sin su guía y enseñanzas no habría sido posible la elaboración de este documento. A Ecodiesel Colombia S.A. por permitirme realizar este proyecto aplicado en la empresa y a las directivas de la Universidad Nacional Abierta y a Distancia UNAD por permitirme ser parte de su comunidad.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVOS: cualquier cosa que tiene valor para la organización[1] .

ACTIVOS DE INFORMACIÓN: en el entorno de la seguridad informática, activos de información se refiere a cualquier información o elemento relacionado con el tratamiento de esta que tenga valor para la entidad, por citar algunos ejemplos, las Bases de Datos, documentos, políticas, manuales, videos, entre otros.

ACTIVOS CRÍTICOS: son aquellos activos, servidores, aplicativos o dispositivos de red, los cuales son esenciales e imprescindibles para mantener y desarrollar el Core de la empresa, cuya afectación, perturbación o destrucción no permite soluciones alternativas inmediatas ocasionando perjuicios económicos, legales y reputacionales.

AMENAZA: Una amenaza en seguridad informática, es la posibilidad que un sistema o servicio, con una vulnerabilidad conocida, sea atacada y traiga consigo pérdidas materiales, económicas o reputacionales a la compañía.

APLICACIONES INFORMÁTICAS: Son piezas de software programadas para realizar una o múltiples tareas. En informática, son todos los programas que se pueden ejecutar en el sistema operativo, algunas básicas como la calculadora, Notepad, otras más complejas como AutoCAD, SAP, Office, etc. También entran en esta clasificación las aplicaciones web, las aplicaciones móviles, aplicaciones sin GUI (interfaz de usuario) como todos los comandos ejecutables desde cmd o el Shell de Linux, etc.

VULNERABILIDADES: Una vulnerabilidad es una falla en un sistema o servicio, el cual permitiría a un atacante usarla a su favor y acceder a dicho servicio o al sistema que lo contiene, ganar privilegios de administrador, indisponer el servicio de manera temporal o permanente. En la gran mayoría de los casos estas vulnerabilidades existen debido a errores en la configuración del servicio, malas prácticas en su implementación, deficiente plan de actualización, o como en el caso de los “Dia Cero “ (Zero Day), investigaciones por parte de analistas que encuentran fallos nuevos y no conocidos.

SEGURIDAD INFORMÁTICA: La seguridad informática es el área de la Informática que se encarga de velar por la seguridad de la infraestructura de sistemas computacionales y en todo lo que ésta se soporta. En esto último se incluye el Hardware (Servidores, discos duros, memorias, Switches, Router, AP, Canales de

[1] MINTIC. [Sitio Web]. Activo. [Consultado el 30 de Abril de 2023]. Disponible en: https://mintic.gov.co/portal/inicio/5444:Activo

comunicación, etc.) y software (sistemas operativos, aplicaciones, servicios) y los protocolos de comunicación como TCP/IP, UDP, SNMP, FTP, etc., dando énfasis en mantenerlos seguros de ataques o intrusos.

SISTEMA DE INFORMACIÓN: Un sistema de información es uno o un conjunto de elementos relacionados entre sí que tiene como finalidad tratar los datos de la empresa, para gestionarlos, almacenarlos y proveer información consolidada y precisa para la toma de decisiones y coordinación y control de esta. Un claro ejemplo de un sistema de información son los EDR (Sistema de planificación de Recursos Empresariales) como lo son SAP, Epicor, Oracle Net Suite, Microsoft Dynamics 365, entre otros.

SERVIDOR: Un servidor puede ser hardware o software. Si se habla de Hardware, es una máquina robusta, donde todas sus piezas físicas se ofrecen en redundancia (doble fuente de poder, doble controladora RAID, doble socket de procesador, canales de memoria RAM separada y dependiente del socket montado, dos o varias NIC de conexión de red, etc.) donde se instala y soportan aplicaciones de consumo masivo y en estos servidores físicos se montan (instalan) sistemas operativos para servidores (Windows Server, Debian, Fedora, CentOS, etc.) y software de tipo servidor para soportar las aplicaciones web (apache, JBoss, Tomcat, IIS, etc.) o de escritorio (SAP, Autodesk Vault, FTP, TrueNAS, etc.) y a los cuales los clientes se conectan para consumir estos servicios.

RESUMEN

Antes de la pandemia por COVID-19, en Ecodiesel Colombia S.A. las funciones de sus colaboradores se realizaban casi en su totalidad de manera presencial en sus dos sedes, ofreciendo la oportunidad de conexión por Escritorio Remoto de Microsoft Windows a unos cuantos colaboradores que así lo requerían. El Gobierno Nacional al decretar la cuarentena obligatoria en todo el territorio Colombiano conllevó no solo a que se aumentaran dichas conexiones de RDP en la compañía, también a que se expusieran más servicios, servidores, EndPoint, entre otros, a internet, aumentando considerablemente la superficie de ataque. A lo anterior se suma que la cantidad de ataques de Malware a nivel mundial ha tenido un crecimiento exponencial desde principios de 2020, coincidiendo con la declaración de pandemia y las cuarentenas en los países.

Al ser la seguridad de la información algo vital para Ecodiesel Colombia S.A., se propone en este proyecto aplicado, realizar un completo análisis de los servidores críticos de la compañía en busca de posibles vectores de ataques y vulnerabilidades en los servicios que tengan incorporados, usando para esto uno o varios de los métodos de intrusión existentes.

ABSTRACT

Before the COVID-19 pandemic, at Ecodiesel Colombia S.A. the functions of its collaborators were carried out almost entirely in person at its two locations, offering the opportunity to connect via Microsoft Windows Remote Desktop to a few collaborators who required it. The National Government, when decreeing the mandatory quarantine throughout the Colombian territory, led not only to the increase of said RDP connections in the company, but also to the exposure of more services, servers, EndPoint, among others, to the internet, considerably increasing the surface area. Of attack. In addition to the above, the number of Malware attacks worldwide has grown exponentially since the beginning of 2020, coinciding with the declaration of a pandemic and quarantines in the countries.

As information security is vital for Ecodiesel Colombia SA, it is proposed in this applied project, to carry out a complete analysis of the company's critical servers in search of possible vectors of attacks and vulnerabilities in the services they have incorporated, using to this one or more of the existing intrusion methods.

INTRODUCCIÓN

La información es el bien más valioso de toda compañía; el área de TI y todo su personal deben garantizar que se cumplan los 5 pilares de la Seguridad de la Información. Para esto es importante darle visibilidad a toda la infraestructura, analizarla, probar su seguridad y actuar en consecuencia.

Cada día salen a la luz nuevas y más sofisticadas técnicas para saltarse la seguridad de un sistema o aplicativo, errores no conocidos en estos, o fallos producidos por errores de configuración o de desarrollo.

En este proyecto aplicado se caracterizan todos los servidores de la compañía Ecodiesel Colombia S.A., se evalúa su criticidad para el proceso con la metodología Magerit en su versión 3 y a los servidores con más alto puntaje se le realizaron una serie de pruebas y análisis para encontrar posibles vulnerabilidades a sus aplicaciones y sistemas operativos.

Al final se entregan no solamente los resultados de los análisis, también las recomendaciones para subsanar las más relevantes o de mayor impacto y reglas o configuraciones para aumentar su nivel de seguridad por medio de Hardening, mejorando así la seguridad y garantizando su información.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la última década los ataques de cibercriminales a empresas u organizaciones estatales o privadas ha venido en aumento[2]; la pandemia obligó a que muchas empresas migraran a un entorno remoto o híbrido[3], teniendo que exponer varios de sus servicios a internet para dar continuidad a su negocio; esto trajo consigo un aumento considerable en la superficie de ataques[4] que pueden llegar a ser explotadas por los mismos.

En caso de materializarse, la afectación a la que puede estar expuesta la compañía víctima es enorme, tanto en lo material como en lo reputacional; se ha documentado casos en los cuales las empresas no son capaces de recuperarse después de un ataque de Ransomware y lastimosamente van a la quiebra[5].

Los cibercriminales cuando logran su objetivo de vulnerar un sistema, estación de trabajo, IOT o controlador industrial, pueden usarlo a su favor de muchas maneras, por ejemplo: pueden utilizar el poder computacional de los servidores de la compañía para realizar minado de criptomonedas, puede secuestrar miles de equipos para usarlos como equipos Zombis para un ataque a un objetivo a gran escala (APT), realizar esa misma BotNet para realizar ataques de denegación de servicios distribuidos a otras víctimas, secuestrar, robar y posteriormente encriptar toda la información de la compañía para pedir un rescate por la misma, amenazar con publicar en internet o en la Dark Web información sensible para la victima; entre muchas otras cosas.

Para mitigar esta problemática, se debe tener muy claro cuáles son los servicios y servidores críticos para la compañía, realizando un análisis exhaustivo y metódico de los mismos para clasificarlos dependiendo de su criticidad en caso de fallo o

---

[2] INTERPOL. International Police [sitio web]. Ciberdelincuencia: Efectos de la COVID-19 [Consultado el 10 de Agosto de 2020]. Disponible en: https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

[3] ESET. WeLive Security By Eset. [sitio web]. El 42% de las empresas no estaba preparada para teletrabajar de forma segura [Consultado el 23 de Junio de 2020]. Disponible en: https://www.welivesecurity.com/la-es/2020/06/23/teletrabajo-seguro-empresas-no-estaban-preparadas/

[4] CSO COMPUTERWORLD [sitio web]. IDG, Crece la superficie de los ataques al Internet de las empresas [Consultado el 22 de Junio de 2020]. Disponible en: https://cso.computerworld.es/cibercrimen/crece-la-superficie-de-los-ataques-al-internet-de-las-empresas

[5] QUANTI [sitio web]. Compañía víctima de ransomware, quiebra y despide a sus 300 trabajadores. [Consultado el 22 de Junio de 2020]. Disponible en: https://quanti.com.mx/noticias/compania-victima-de-ransomware-quiebra-y-despide-a-sus-300-trabajadores/

vulneración. Partiendo de ese análisis, y usando una o varias de las metodologías de pruebas de intrusión existentes, se debe establecer el nivel de vulnerabilidad de cada uno de ellos y clasificar sus vectores dependiendo el impacto de cada uno si se llegan a materializar.

1.2 FORMULACIÓN DEL PROBLEMA

El resultado final del proyecto es ofrecer a la compañía Ecodiesel Colombia S.A., un completo análisis de lo anteriormente citado, y las recomendaciones de seguridad que se deben cumplir para subsanar cualquier vulnerabilidad encontrada o que su probabilidad sea alta.

¿Cómo se comprobaría la seguridad de la infraestructura de los servidores críticos de Ecodiesel Colombia S.A.?

2 JUSTIFICACIÓN

Tener todos los servidores, EndPoint y recursos compartidos dentro de un ecosistema cerrado de red y solo con salida a Internet desde un Firewall perimetral robusto, es el modelo de red idílico para cualquier administrador de red, siendo la realidad muy distinta, ciertos servidores y servicios deben ser publicados en Internet y los EndPoint se deben conectar a estos desde redes diferentes a la corporativa; es aquí donde proteger dichos servidores y servicios se vuelve algo crítico para cualquier organización.

Para lograr esto primero se debe tener claro cuáles son los servicios y servidores, su nivel de criticidad en caso de fallas o vulneraciones de seguridad y tener claro a que riesgos está o puede estar expuesto dichos recursos, para así aplicar los cambios respectivos para mitigarlos.

Debido a lo anterior, el desarrollo de este proyecto aplicado tiene como fin darle a la compañía Ecodiesel Colombia S.A. un panorama amplio de su infraestructura de red, de servidores y aplicaciones, los riesgos a los cuales pueden estar expuestos y un listado de recomendaciones para disminuir al mínimo posible dichos riesgos o, si lo compañía así lo decida, eliminar o dejar de publicar el servicio comprometido.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Evaluar la seguridad de la infraestructura de los servidores críticos de Ecodiesel Colombia S.A. mediante un enfoque metodológico con el fin de acoplar buenas prácticas de seguridad articuladas a estándares internacionales.

3.2 OBJETIVOS ESPECÍFICOS

- Argumentar la selección de los servidores críticos de Ecodiesel Colombia S.A. mediante una caracterización de cada uno de ellos con el fin de determinar los riesgos a los que están expuestos.

- Establecer la metodología para la evaluación de seguridad de la infraestructura de los servidores críticos mediante la clasificación y análisis de las más relevantes para seleccionar las más apropiada de acuerdo con la naturaleza de la organización.

- Examinar la infraestructura de los servidores críticos de Ecodiesel Colombia S.A. mediante la metodología seleccionada con el fin de identificar las vulnerabilidades.

- Proponer unas buenas prácticas articuladas con estándares internacionales con el fin de mitigar los riesgos y dar continuidad al negocio.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 **Framework COBIT e ITIL para mejorar la seguridad de la información.** COBIT e ITIL son Framework que se pueden aplicar para mejorar la seguridad de la información en cualquier organización. COBIT, abreviación de Objetivos de Control para las Tecnologías de la Información, nace como una guía de buenas prácticas que se muestra o presenta como Framework, pensado para el Gobierno de TI, inicialmente concebido para dar un enfoque de auditoría, dando objetivos de control y prácticas de control a los procesos. ITIL por su parte, es un Framework de administración de servicios de TI, ayudando a entender el cómo TI apoya a los procesos de la compañía siempre teniendo la tecnología como medio para lograrlo. La diferencia entre los dos es simple, COBIT le dice lo que debe hacer, mientras que ITIL le dice el Cómo debe hacerlo, ITIL se centra en los procesos, mientras que COBIT en control y métricas. La mezcla o combinación de estos dos Framework da un modelo muy fuerte en pro de la seguridad de la información y ante una auditoria de sistemas.

4.1.2 **Análisis de vulnerabilidades de los activos de una organización.** Como ya se mencionó anteriormente, se deben conocer cuáles son los activos catalogados como críticos en la organización, activos que si llegan a fallar supondrían una afectación parcial o completa al negocio o a la producción. En este sentido se deben catalogar y analizar a profundidad en busca de cualquier vector que se pueda usar para vulnerar el sistema. Este proceso se conoce como Pruebas de Penetración, Pentest o Hacking Ético. Para realizar dichos procesos se suelen utilizar diferentes software y técnicas avanzadas de intrusión y elevación de permisos. El entregable de este proceso es un documento donde se describen todos los pasos que se siguieron para lograr la intrusión y un apartado posterior donde se exponen las formas de intentar subsanarlo.

4.1.3 **Metodologías de análisis de vulnerabilidades.** Las metodologías para el análisis de vulnerabilidades son aquellos procedimientos, guías o pasos a seguir en la búsqueda de vulnerabilidades a un sistema. Existen varias metodologías, como OSSTMM, NIST SP 800-115, ISSAF, PTES, OWASP, Cyber Kill Chain, entre otros; cada uno con sus ventajas, aplicabilidad y enfoque a sistemas específicos, como sistemas operativos, aplicaciones web o Desktop, etc.

4.2 MARCO CONCEPTUAL

4.2.1 **Activos Críticos.** Los activos críticos son todos aquellos equipos, infraestructura física o software, entre otros, en los cuales este soportado parte o todo el Core del negocio.

4.2.2 **Servidores Críticos.** Son aquellos servidores en los que está soportado el negocio, esto en forma de ERP (SAP, por ejemplo), servidor de correo (Exchange, POP), servidor de aplicaciones web (Apache, JBoss, NGinx), etc., y si éste llegase a fallar, tendría una afectación económica o reputacional muy alta para la compañía.

4.2.3 **Servicios.** Son todos aquellos roles o aplicaciones que estén ejecutándose en los equipos o servidores. Ejemplo de estos servicios tenemos, servidor FTP, rol de File Server con SMB, SQL Server, servidor SSH, VNC, Terminal Server RDP, entre otros.

4.2.4 **Vulnerabilidades.** Las vulnerabilidades son aquellos riesgos a los cuales están expuestos los servicios; por ejemplo, la vulnerabilidad CVE-2021-34527 también conocida como PrintNightmare el cual puede permitir la ejecución de código malicioso por medio de la cola de impresión en equipos Windows vulnerables; otra ejemplo es la vulnerabilidad CVE-2019-0708 también conocida como BlueKeep, en el cual, un atacante puede realizar una conexión por escritorio remoto a un equipo victima sin necesidad de conocer las credenciales del usuario.

4.2.5 **Vector de ataque.** Un vector de ataque es el medio, servicio, estación de trabajo, controladoras industriales, etc. por el cual un atacante podría ingresar a un sistema y así comprometerlo.

4.2.6 **Malware.** Un malware es todo aquel software malicioso que puede afectar a un equipo o sistema, secuestrándolo o pudiendo manipularlo de manera remota. Existen muchos tipos de Malware, como los virus, troyanos, RAT, ransomware, entre otros.

4.2.7 **Ransomware.** Es un tipo de Malware que, una vez ejecutado en el sistema, cifra toda la información del usuario o de la compañía, incluyendo todos los documentos, copias de seguridad, bases de datos, entre otros, para pedir un rescate por el mismo y/o la amenaza de publicar información sensible para la compañía.

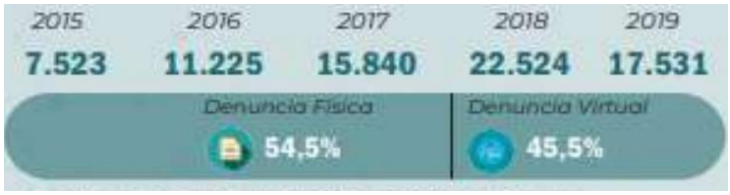
4.2.8 **Hacking Ético.** También conocido como Pentest, son una serie de pruebas de intrusión a sistemas, equipos, controladores industriales, IOT, etc., con el objetivo de obtener permisos de este y controlarlos parcial o completamente. A diferencia de los cibercriminales, los Hacker Éticos o de Sombrero Blanco, realizan dichos pentest en un entorno seguro, contratados por la misma compañía con el fin de poder encontrar todas las vulnerabilidades posibles y poder mitigarlas antes que se puedan materializar por los cibercriminales.

4.3 ANTECEDENTES O ESTADO ACTUAL

Todos los días aparecen nuevas y más novedosas formas o técnicas para comprometer un sistema, aplicación, protocolo o cualquier pieza de software/hardware; esto ha sido así prácticamente desde el inicio, muestra de ello es Jhon Nevil Maskelyne (1839 – 1917) quien fue un ilusionista e inventor de profesión del Reino Unido y es catalogado como el primer hacker de la historia, al interceptar una comunicación radial, entre el físico John Ambroise Fleming del Royal Institution de Londres y el ingeniero inventor Guglielmo Marconi (1903), demostrando así que era un sistema de comunicación vulnerable a interceptaciones.

Como lo certifican cada año las autoridades, se ve un incremento gradual en la detección de nuevas amenazas a nivel nacional, regional y mundial. En el siguiente gráfico de la Policía Nacional, se listan los Delitos informáticos reportados a esta entidad entre los años 2015 a 2019.

Figura 1. Delitos informáticos en Colombia



Fuente: Tendencias de Cibercrimen en Colombia 2019-2020. Policía Nacional. [PDF]. Recuperado de: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

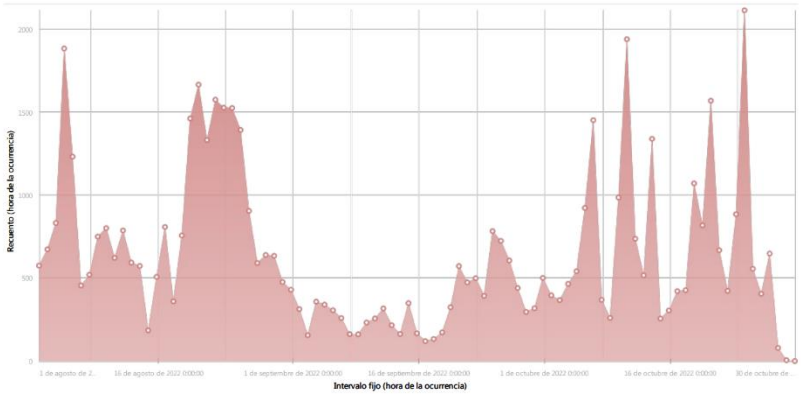
El confinamiento obligatorio derivado de la Pandemia de COVID-19 aumentó considerablemente la superficie de ataque, por lo que los ciberdelincuentes aprovecharon esa oportunidad y aumentaron considerablemente sus ataques a nivel mundial. En la siguiente gráfica se muestra con cifras, el considerable aumento de los ciberdelitos en 2020 con respecto al año 2019.

Figura 2. Comparación de ciberdelitos entre 2019 y 2020.

Fuente: En 2020 se profesionalizaron los delitos en la web y crecieron en un 84%. El espectador. [Sitio Web]. Recuperado de: https://www.elespectador.com/judicial/en-2020-se-profesionalizaron-los-delitos-en-la-web-y-crecieron-en-un-84-article/

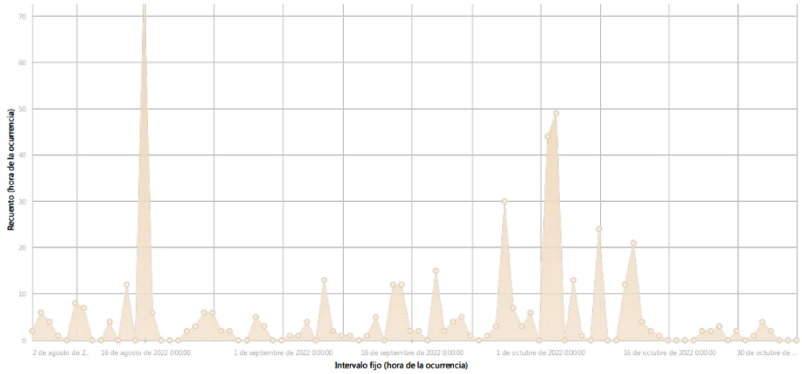
Este comportamiento es constante en todas las regiones y Ecodiesel Colombia S.A. no es ajena esto, en las siguientes gráficas se muestran los incidentes de seguridad de Firewall y de Antivirus proporcionadas por la consola centralizada de ESET; información recolectada de todos los EndPoint y Servidores de la compañía, en estas gráficas se muestran los meses de Agosto, Septiembre y Octubre de 2022.

Figura 3. Incidentes de Firewall para ESET en meses 8, 9 y 10 de 2022.



Fuente: Generación Propia

Figura 4. Incidentes de Antivirus para ESET en meses 8, 9 y 10 de 2022



Fuente: Generación Propia

4.4 MARCO LEGAL

El Congreso y la Presidencia de la República de Colombia han realizado muchos esfuerzos para legislar a favor o en Pro de proteger tanto a las entidades públicas como a las privadas y a los ciudadanos de a pie ante ataques cibernéticos o usando las TIC para realizar cualquier actividad ilegal.

En un documento realizado por la Revista Criminalidad de la Policía Nacional de Colombia, denominado “Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia”[6] realizan un compendio de todas las

[6] OSPINA DÍAZ, MILTON RICARDO y SANABRIA RANGEL, PEDRO EMILIO. [en línea]. Revista Criminalidad. Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. [Consultado el 15 de Diciembre de 2021]. Disponible en: https://www.policia.gov.co/file/263913/download?token=7WrMYa4a

normativas sobre ciberseguridad en Colombia, en este se engloba todo este esfuerzo realizado por el Congreso y la Presidencia de la República.

Tabla 1. Marco normativo sobre ciberseguridad en Colombia.

Normatividad	Descripción
Ley 527	Acceso y uso de mensajes de datos, comercio electrónico y firmas digitales, y determinación de entes certificadores (Congreso de la República de Colombia, 1999).
Ley 594	Seguridad de archivos (Congreso de la República de Colombia, 2000a)
Ley 599	Violación ilícita de comunicaciones, derechos de autor y algunos delitos informáticos en el código Penal (Congreso de la República de Colombia, 2000b).
Ley 679	Prevención y ataque contra la explotación, la pornografía y el turismo sexual con menores (Congreso de la República de Colombia, 2001).
Ley 962	Reducción de trámites y procedimientos administrativos de entidades públicas o privadas con funciones públicas o de servicios públicos (Congreso de la República de Colombia, 2005).
Ley 1266	Habeas data y manejo de información de bases de datos personales (Congreso de la República de Colombia, 2008)
Ley 1273	Modificación del código Penal para acoger la protección de la información y la preservación integral de los sistemas de usan TIC (Congreso de la República de Colombia, 2009a).
Ley 1341	Principios y conceptos sobre la sociedad de la información y la organización de las TIC y creación de la Agencia Nacional del Espectro (Congreso de la República de Colombia, 2009b).
Ley 1437	Pruebas electrónicas para tipificar los delitos en el Código de Procedimiento Administrativo y de los Contencioso Administrativo (Congreso de la República de Colombia, 2011a).
Ley 1480	Protección al consumidor por medios electrónicos y seguridad en transacciones electrónicas en el Estatuto del Consumidor (Congreso de la República de Colombia, 2011b).
Decreto -Ley 019	Reducción de trámites en el estado a través de medios electrónicos y establecimiento de criterios de seguridad (Presidencia de la República de Colombia, 2012a).
Decreto 2693	Estrategia de gobierno electrónico (Presidencia de la República de Colombia, 2012b).
Decreto 2364	Posibilidad de la firma electrónica (Presidencia de la República de Colombia, 2012c).
Decreto 2609	Posibilidad del expediente electrónico en el esquema de gestión documental estatal (Presidencia de la República de Colombia,2012d).
Ley 1581	Regulación de la protección de datos personales de los individuos (Congreso, 2012).

Ley Estatutaria 1621	Normatividad para las labores de Inteligencia y contrainteligencia y criterios de seguridad para este rol (Congreso de la República de Colombia, 2013).
Decreto 1377	Reglamentación de la protección de datos personales de los individuos (Presidencia de la República de Colombia, 2013a).
Decreto 1510	Contratación y compra pública por medios electrónicos (Presidencia de la República de Colombia, 2013b).
Ley 1712	Criterio de transparencia en el acceso a la información pública (Congreso de la República de Colombia, 2014).
Decreto 333	Determinación de las entidades de certificación digital (Presidencia de la República de Colombia, 2014).
Ley 1978	Modernización del sector de las tecnologías de la información y las comunicaciones (Congreso de la República de Colombia, 2019).
Decreto 620	Lineamientos generales en el uso y operación de los servicios ciudadanos digitales (Presidencia de la República de Colombia, 2020).
Conpes 3975	Política Nacional para la transformación Digital e Inteligencia Artificial (DNP, 2019).

Fuente: Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista Criminalidad.

Aunque se han realizado todos estos esfuerzos, en la actualidad ha quedado patente que no son suficientes, los ataques cibernéticos van cada año en aumento, disparados, entre otras cosas, por la pandemia de COVID-19, los cambios de paradigmas de seguridad, el aumento en la superficie de ataque al tener que publicar servicios en internet que antes estaban bajo la red privada de las empresas, el trabajo en casa y que las empresas no estén preparadas para esto entre otros factores.

A pesar de todo lo anterior, se nota un enfoque por parte del gobierno a darle mayor importancia a los temas referentes a la ciberseguridad y establecer normas y criterios para protegerse a sí mismo como Gobierno y a las entidades privadas y ciudadanía en General; aún existen falencias y vulnerabilidades antes amenazas cibernéticas, pero son pasos gigantes los dados.

4.4.1 **Ley 1273 del 2009, Ley de Delitos Informáticos.** En Colombia no se tenía una ley que amparara a las empresas o al ciudadano si estos fueran víctimas de un incidente de seguridad, existía este Limbo Jurídico. Por esto, el 5 de Enero de 2009, el congreso de la república publica la ley 1273, la cual denominaron “De la Protección de la Información y de los Datos”, el cual es un bien jurídico tutelado.

Esta ley se divide en dos capítulos, el primero “De los atentados contra la confidencialidad, la integridad y la Disponibilidad de los datos y de los sistemas Informáticos” y un segundo capítulo llamado “De los atentados informáticos y otras infracciones”.

En esta Ley se tipifican como delitos:

- Las Obstaculizaciones a un sistema informático, como lo puede ser un ataque de Denegación de Servicios Distribuidos o DDoS.
- La interceptación de datos informáticos de una empresa o ciudadano haciendo alusión a intrusiones o interceptación de datos “Man-In-The-Middle”.
- El daño informático haciendo alusión a eliminación total o parcial de información sin la previa autorización del dueño.
- El uso de software malicioso como malware tanto para los creadores de este tipo de software como para los tenedores de este.
- Suplantación de sitios web para capturar datos personales, hace referencia a ataques de tipo Phishing, Vishing, Smishing, entre otros, los cuales se basan en Ingeniería Social para intentar engañar a sus víctimas para que ingresen a una URL maliciosa y entregue sus credenciales.
- Violación de datos personales, hace referencia que, habiendo conseguido el acceso a datos sensibles de la víctima, ésta se venda, distribuya o entregue buscando algún beneficio económico. Incluyen a los que sustraen la información, como a quienes la distribuyan y obtengan.

Las penas por los casos anteriores son variables, pero van desde los 36 meses hasta los 96 meses de prisión, y una multa entre los 100 y los 1000 salarios mínimos legales mensuales vigentes.

Esta ley contempla unos agravantes de las penas anteriores, si estos son cometidos por funcionarios públicos, si la víctima del ataque es una entidad pública, con fines terroristas, usando un tercero de buena fe, si el que realiza el ataque es el encargado de salvaguardar los sistemas, entre otros. SI lo anterior se cumple, las penas aumentaran entre de la mitad a las tres cuartas partes de la condena original.

Esta ley se puede consultar completa en el siguiente enlace: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

4.4.2 **Ley 1581 del 2012, Ley de Protección de datos Personales.** Se entiende como datos personales a toda aquella información que individualice o logre identificar a una persona y empresa, como ejemplo su edad. Dato sensible se define como aquella información personal que afecte la intimidad del titular, y que con el uso indebido de esta se pueda llegar a discriminarlo por ejemplo su raza, su vida sexual, datos biométricos, su orientación religiosa o política etc.

El 17 de Octubre de 2012, el congreso de la república publica la ley 1581, la cual se conoce como “Ley de Habeas Data” o “Ley de protección de Datos Personales”, en ella se constituye un marco general de la protección de los datos personales en el territorio Colombiano. En esta ley se faculta el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que hayan sido recogidas de ellas en bases de datos o archivos.

En esta ley se relacionan los principios rectores para el tratamiento de datos personales, los cuales son:

- Principio de Legalidad en materia de tratamiento de Datos
- Principio de Finalidad
- Principio de Libertad
- Principio de veracidad o Calidad
- Principio de Transparencia
- Principio de Acceso y Circulación Restringida
- Principio de Seguridad
- Principio de Confidencialidad.

Se estipula en esta Ley la prohibición del tratamiento de datos sensibles, exceptuando ciertos casos, por ejemplo, si el titular de los datos ha dado autorización explicita para ello, si la información se usa para salvaguardar el interés vital del titular y si este último no está facultado física o jurídicamente, cuando la información se refiera a datos que sean necesarios para el reconocimiento , ejercicio o defensa de un derecho en un proceso judicial, si el tratamiento de estos datos tengan una finalidad estadística o científica[7] .

La ley se puede encontrar completa en el siguiente enlace: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

4.4.3 **Decreto 1377 del 2013, Decreto que impulsó la Ley de Protección de Datos personales[8].** Este decreto complementa la Ley de Habeas Data y la reglamente parcialmente, en este decreto se eximen las bases de datos que se mantengan en un ámbito personal o doméstico.

---

[7] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. [Sitio Web]. Protección de Datos Personales, preguntas frecuentes. [Consultado el 10 de Diciembre de 2021]. Disponible en: https://www.sic.gov.co/preguntas-frecuentes-pdp#:~:text=La%20Ley%201581%20de%202012%20proh%C3%ADbe%20la%20transferencia%20de%20datos,adecuados%20de%20protecci%C3%B3n%20de%20datos.&text=Transferencias%20legalmente%20exigidas%20para%20la,derecho%20en%20un%20proceso%20judicial.

[8] SUIN JURISCOL. [Sitio Web]. Sistema Único de Información Normativa. Decreto 1377 De 2013. [Consultado el 14 de Diciembre de 2021]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081

Se definen algunos conceptos que quedaron un poco ambiguos en la Ley 1581 de 2012, los cuales son:

- Aviso de privacidad
- Dato Público
- Datos Sensible
- Transferencia
- Transmisión

En este decreto se obliga a los responsables a entregar a la Superintendencia de Industria y Comercio una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso. Y no se podrá en ningún caso utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales.
Los responsables deben solicitar autorización explícita al titular de la información en el momento de la recolección de los datos, así como explicar todas las finalidades específicas para las cuales se solicita el consentimiento. Además, se debe informar al titular si dichas finalidades cambiaron y solicitarle una nueva autorización para su tratamiento.

Se expresa tajantemente que ninguna actividad podrá condicionarse a que el titular entregue o suministre datos personales sensibles.

Se define los modos de obtención de la autorización por parte del titular, los cuales son por escrito, de forma oral, mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio se podrá considerar una conducta inequívoca.

Los responsables deberán salvaguardar las pruebas de la obtención de la autorización por parte de los titulares.
Los titulares podrán ejercer en cualquier momento su derecho a solicitar la eliminación de la información personal contenida en cualquier base de datos o revocar el permiso para su tratamiento. Para esto los responsables deben ofrecer mecanismos gratuitos y prácticos para que los titulares puedan realizar dicha solicitud.

Se obliga a que los responsables desarrollen una política de protección de datos personales, y obliguen a los responsables de su tratamiento a que las cumplan a cabalidad. Dicha política debe ser pública y ser puesta en conocimiento de los titulares.

El decreto consta de varios otros artículos, se puede visualizar el Decreto completo desde la siguiente dirección: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081

5 DESARROLLO DE LOS OBJETIVOS

5.1 ARGUMENTAR LA SELECCIÓN DE LOS SERVIDORES CRÍTICOS DE ECODIESEL COLOMBIA S.A. MEDIANTE UNA CARACTERIZACIÓN DE CADA UNO DE ELLOS CON EL FIN DE DETERMINAR LOS RIESGOS A LOS QUE ESTÁN EXPUESTOS.

5.1.1 **Detalle de infraestructura tecnológica.** ECODIESEL COLOMBIA S.A., por medio de los servicios del área de Gestión TIC cuenta con los servicios de un Centro de Datos Principal donde se concentran los canales de acceso de terceros, junto con el Core principal de la red LAN, para atender la operación normal del negocio. Este centro de datos principal está ubicado en la ciudad de Bucaramanga, un centro de cómputo en la ciudad de Barrancabermeja.

El detalle de esta infraestructura tecnológica se presenta en los siguientes numerales para el Centro de Datos Principal y los servicios tecnológicos que tiene en la actualidad ECODIESEL COLOMBIA S.A.

5.1.1.1 **Telecomunicaciones, Servidores Y Almacenamiento.** ECODIESEL COLOMBIA S.A. cuenta con una infraestructura de red altamente disponible conformada por los siguientes canales de comunicaciones:

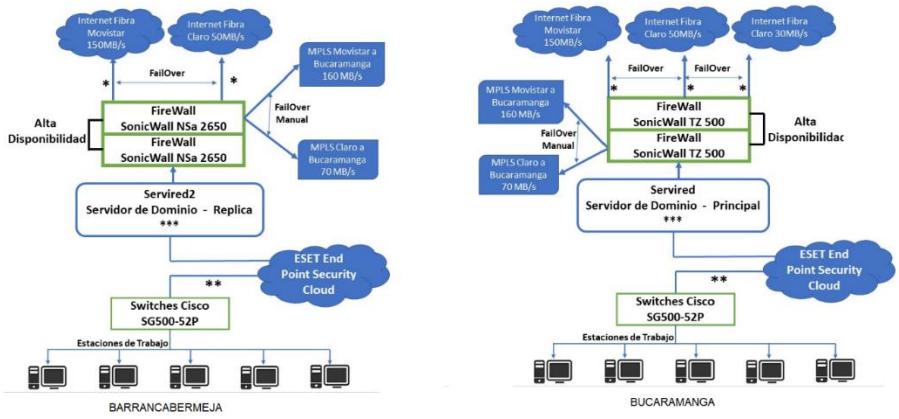
Tabla 2. Conectividad

Servicio	Proveedor	Velocidad (MB/S)	Ciudad
Internet Fibra	Movistar	150	Barrancabermeja
Internet Fibra	Claro	100	Barrancabermeja
Internet Fibra	Movistar	150	Bucaramanga
Internet Fibra	Claro	100	Bucaramanga
Internet Fibra	Claro	100	Bucaramanga
MPLS Datos	Claro	100	Bucaramanga/Barrancabermeja
MPLS Datos	Movistar	160	Bucaramanga/Barrancabermeja

Fuente: Elaboración Propia.

Como se observa en la figura a continuación esta arquitectura permite el FailOver automático para conectividad a internet de cualquiera de las sedes y FailOver manual para la interconexión entre sede Bucaramanga y Barrancabermeja.

Figura 5. Esquema telecomunicaciones



Fuente: Propia

A nivel de servidores y almacenamientos ECODIESEL COLOMBIA S.A., cuenta con los siguientes equipos:

Tabla 3. Listado de Servidores Físicos y Virtuales[9]

HOSTNAME	Marca	Referencia	RAM	CORES	HDD	FUNCIÓN PRINCIPAL
SERVER1	DELL	PowerEdge R740	64	48	1800	Hyper-V Manager
TS	-	-	32	10	80	TERMINAL SERVER
SERVER2	-	-	4	4	100	HELPDESK
SERVER3	-	-	4	8	40	TELEFONÍA IP
SERVER4	-	-	2	1	8	HELPDESK

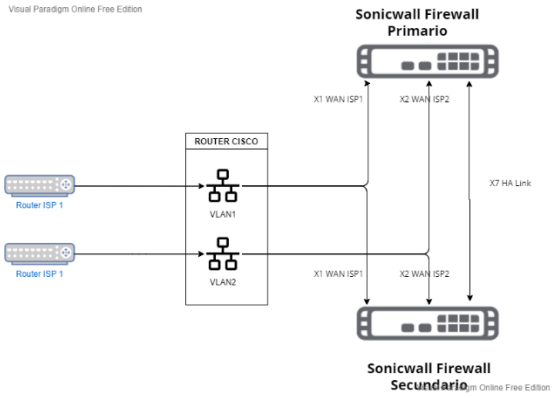
[9] Los nombres de los servidores se han modificado para dar cumplimiento al acuerdo de confidencialidad firmado con la empresa.

SERVER5	-	-	1	1	9	GESTION DOCUMENTAL PRUEBAS
SERVER6	-	-	3	1	20	UNIFI SERVER
SERVER7	-	-	4	1	30	BACKUP
SERVER8	HP	ProLiant DL360e Gen8	16	4	1000	AZURE AD
SERVER9	HP	ProLiant DL360e Gen8	16	4	1000	File Server, Duplicati, Veam Backup, Grabadora a Cintas.
SERVER10	DELL	PowerEdge R530	24	24	400	Hyper-V Manager
TS2	-	-	16	1	80	TERMINAL SERVER
SERVER11	HP	ProLiant DL380e Gen8	16	4	1000	BASE DE DATOS NOMINA
AD	HP	ProLiant DL360e Gen8	16	4	1000	Ad, Dns, Dhcp. Heinsohn Nómina. Soo Agent Sonicwall. File Server
SAP	DELL	PowerEdge R620	24	24	1000	SAP BO, SQL Server 2012 R2, SGI Addons

Fuente: Elaboración Propia.

5.1.1.2 **Seguridad.** A nivel de seguridad perimetral ECODIESEL COLOMBIA S.A cuenta con una topología liderada por equipos de seguridad perimetral Sonicwall configurados en alta disponibilidad tal como se observa a continuación.

Figura 6. Esquema conexión SonicWall High Availability



Fuente: Propia.

Para lo cual se tiene un par de equipos Sonicwall NSa2650 para la sede de Barrancabermeja y un par TZ500 para la sede de Bucaramanga la cual garantiza un esquema de alta disponibilidad en modo activo-pasivo ante una falla de hardware de alguno de los dispositivos de seguridad perimetral.

Se utilizaron para las VLAN Switch Cisco Catalyst 2960 ya que ofrecen una gran estabilidad, seguridad, poseen doble fuente de alimentación (redundante) y son fácilmente administrable.

El esquema de HA es prácticamente idéntico para ambas sedes, lo único que varia es que en la sede Bucaramanga se tiene un tercer canal de Internet, por lo tanto, son tres (3) las VLAN creadas en un Switch Cisco.

5.1.1.3 **Aplicaciones.** Los servicios de tecnología identificados como críticos son los siguientes:

- Aplicaciones SAP Business One y Servidor Base de datos SQL SERVER.
- Aplicaciones SAP Terminal Server.
- Directorio Activo

Los cuales son los mínimos necesarios para garantizar la operación del sistema SAP Business One.

5.1.1.4 **Aplicaciones SAP Business One y Servidor Base de datos SQL SERVER.** ECODIESEL COLOMBIA S.A. tiene soportada la información de sus aplicativos en bases de datos. En la siguiente tabla se presentan las bases de datos empleadas de acuerdo con la respectiva aplicación:

Tabla 4. Aplicaciones y Motores de Bases de Datos[10]

APLICACIÓN	BASE DE DATOS	BASE DE DATOS
SAP BUSINESS ONE	MS SQL SERVER	BD1
HEINSOHN NÓMINA	MS SQL SERVER	BD2
INFOMANTE	MS SQL SERVER	BD3
ZKACCESS	MS SQL SERVER	BD4

Fuente: Elaboración Propia.

Se identifican los servidores críticos de la organización, aquellos que son esenciales para la supervivencia de la organización, que son imprescindibles para que supere una situación crítica o que sustentan las actividades legales y financieras de la empresa y se les aplicara un método sistemático de análisis de riesgos para conocer las vulnerabilidades y amenazas a los que están expuestos. El resultado de este análisis arrojara aquellos servidores que requieren medidas oportunas y eficaces para mantener los riesgos bajo control. Para esto se usará la metodología MAGERIT

5.1.2 **MAGERIT.** La metodología MAGERIT fue elaborada por el Consejo Superior de Administración Electrónica del Gobierno de España como respuesta al creciente uso de las tecnologías de la información. Esta metodología tiene como objetivo analizar y gestionar los riesgos a los que se pueden ver expuestas las organizaciones en cuanto a la seguridad informática.

5.1.3 **Implementación Metodología Magerit.**

1. Paso 1: Determinar los activos relevantes de la organización en este caso los servidores utilizados para el correcto funcionamiento de la actividad económica de la compañía soportados en ERP SAP B1. De igual forma se calibran tres dimensiones;

[10] Los nombres de las Bases de Datos se han modificado para dar cumplimiento al acuerdo de confidencialidad firmado con la empresa.

Tabla 5. Valoración Cuantitativa

Valoración Cuantitativa		
Confidencialidad (C): es cuando la información no se coloca a disposición ni se revela a individuos, entidades o procesos no autorizados. **Ejemplo** ¿qué daño causaría que lo conociera quien no debe?	**Integridad (I):** es el mantenimiento de la exactitud y estado completo de la información y sus métodos de proceso. **Ejemplo** ¿qué perjuicio causaría que estuviera dañado o corrupto?	**Disponibilidad (D):** es el acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran. **Ejemplo** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
Así mismo cada valor dentro de la escala representa un criterio de niveles de daño ocasionado por la ausencia de confidencialidad, disponibilidad e integridad como se ve en la siguiente tabla:		

Fuente: Elaboración Propia.

Tabla 6. Valor – Criterio

VALOR		CRITERIO	
10	Muy Alto	MA	Daño muy grave
7-9	Alto	A	Daño grave
4-6	Medio	M	Daño importante
1-3	Bajo	B	Daño menor

Fuente: Elaboración Propia.

La suma de la valoración de las tres variables sobre el activo determina el valor total del activo en el proceso. El valor máximo de un activo es 30 y mínimo es 0. La valoración total del activo será clasificada con la siguiente escala de colores:

Tabla 7. Valor – Clasificación

VALOR	CLASIFICACIÓN
0-10	BAJO
10 - 20	MEDIO
20 - 30	ALTO

Fuente: Elaboración Propia.

Tabla 8. Servidores Puntaje

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	CONFIDEN-CIALIDAD	DISPONI-BILIDAD	INTEGRI-DAD	RESUL-TADO
EQUIPOS INFORMÁTICOS (SERVIDORES)	SERVER1	10	9	9	**28**
	TS	6	6	8	**20**
	SERVER2	6	5	6	**17**
	SERVER3	5	8	7	**20**
	SERVER4	6	5	6	**17**
	SERVER5	4	5	7	**16**
	SERVER6	4	6	5	**15**
	SERVER7	8	7	7	**22**
	SERVER8	4	5	5	**14**
	SERVER9	4	6	5	**15**
	SERVER10	6	7	6	**19**
	TS2	6	7	6	**19**
	SERVER11	9	10	10	**29**
	AD	9	9	10	**28**
	SAP	10	8	10	**28**

Fuente: Elaboración Propia.

2. Paso 2: Determinar las amenazas a las que están expuestos estos activos.

Estas amenazas pueden ser:

- Desastres Naturales
- De Origen Industrial
- Errores y fallos no intencionados
- Ataques Intencionados

Para este paso se tendrán en cuenta dos ítems

- Degradación o Impacto: Que tan perjudicado resultaría el activo
- Frecuencia: Cada cuanto se materializa la amenaza

Tabla 9. Paso 2 - Primera Parte

Frecuencia (Tasa Anual de Ocurrencia)	Descripción	Degradación o Impacto	Descripción 2
5	Muy Frecuente (A Diario)	5	Muy Alta (o)
4	Frecuente (Mensual)	4	Alta (o)
3	Normal (Una vez al Año)	3	Media (o)
2	Poco Frecuente (Cada Varios Años)	2	Baja (o)
1	Nunca Ocurre	1	Sin Degradación o Impacto

Fuente: Elaboración Propia.

Tabla 10. Paso 2 - Segunda Parte

TIPO DE ACTIVO	NOMBRE DEL ACTIVO	AMENAZAS	FRECU-ENCIA	DEGRA-DACIÓN O IMPACTO
EQUIPOS INFORMÁTICOS (SERVIDORES)	SERVER1, TS,SERVER2,SERVER3,SERVER4,SERVER5,SERVER6,SERVER7,SERVER8,SERVER9,SERVER10,TS2,SERVER11, AD,SAP	Daños por agua	2	3
		Condiciones inadecuadas de temperatura o humedad	4	4
		Corte del suministro eléctrico	2	4
		Fuego	2	4
		Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3
		Errores de Configuración	2	3
		Desastres naturales	1	3
		Fuga de Información	2	4
		Fallo de servicios de comunicaciones	4	4
		Interrupción de otros servicios y suministros esenciales	4	3
		Degradación de los soportes de almacenamiento de la información	2	4
		Alteración de la Información	1	4
		Destrucción de la información	1	4
		Caída del sistema por sobrecarga	4	3

		abusos de privilegios de acceso	1	4
		Caída del sistema por agotamiento de recursos	3	4
		Difusión de software dañino	1	5
		Denegación de Servicio	3	4
		Errores de mantenimiento / Actualización de programas	3	4
		Acceso no autorizado	1	5
		Errores del administrador	2	3
		Indisponibilidad del personal	1	4
		Ingeniería Social	1	4
		Suplantación de identidad del usuario	1	4
		Interceptación de información (escucha)	1	4

Fuente: Elaboración Propia.

3. Paso 3: Determinación del riesgo

La siguiente fórmula matemática permite determinar el valor del riesgo que tiene un activo de información.

Tabla 11. Ecuación Valor del Riesgo

Vr. Total de Activo x Vr. Frecuencia de Amenaza x Vr. Degradación o Impacto = Vr. Riesgo

Fuente: Elaboración Propia.

Conociendo el valor total del riesgo y el nivel que representa; en la siguiente tabla se define a que riesgos se les debe hacer un proceso de tratamiento de riesgos.

Tabla 12. Valor del Riesgo - Nivel – Tratamiento

VR. RIESGO	NIVEL	TRATAMIENTO
0 - 149	Bajo / Aceptable	Aceptar el riesgo, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre asumir el riesgo o compartirlo.
150 - 299	Medio / Importante	Reducir, Compartir o transferir el riesgo. La organización debe diseñar planes de contingencia, para protegerse en caso de que se materialicen riesgos de este nivel.

300 - 750	Alto / Inaceptable	Evitar, Reducir, Compartir o transferir el riesgo. Es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la probabilidad del riesgo, de protección para disminuir el Impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

Fuente: Elaboración Propia.

Tabla 13. Resultados Evaluación de Riesgos[11]

NOMBRE DEL ACTIVO	VR TOTAL ACTIVO	AMENAZAS	FRECU-ENCIA	DEGRADA-CIÓN O IMPACTO	VALOR RIESGO
SERVER1	28	Daños por agua	2	3	168
	28	Condiciones inadecuadas de temperatura o humedad	4	4	448
	28	Corte del suministro eléctrico	2	4	224
	28	Fuego	2	4	224
	28	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	168
	28	Errores de Configuración	2	3	168
	28	Desastres naturales	1	3	84
	28	Fuga de Información	2	4	224
	28	Fallo de servicios de comunicaciones	4	4	448
	28	Interrupción de otros servicios y suministros esenciales	4	3	336

[11] Los valores reflejados en la "Tabla 13. Resultados Evaluación de Riesgos" fueron calculados con base al historial de mantenimientos de los equipos, la periodicidad de los daños en el sistema de enfriamiento del Data Center, los daños en Hardware que han presentado, como en los Coolers de los servidores, discos duros, Board, controladora RAID y demás.

	28	Degradación de los soportes de almacenamiento de la información	2	4	224
	28	Alteración de la Información	1	4	112
	28	Destrucción de la información	1	4	112
	28	Caída del sistema por sobrecarga	4	3	336
	28	abusos de privilegios de acceso	1	4	112
	28	Caída del sistema por agotamiento de recursos	0	0	0
	28	Difusión de software dañino	1	5	140
	28	Denegación de Servicio	3	4	336
	28	Errores de mantenimiento / Actualización de programas	3	4	336
	28	Acceso no autorizado	1	5	140
	28	Errores del administrador	2	3	168
	28	Indisponibilidad del personal	1	4	112
	28	Ingeniería Social	1	4	112
	28	Suplantación de identidad del usuario	1	4	112
	28	Interceptación de información (escucha)	1	4	112
TS	20	Daños por agua	2	3	120
	20	Condiciones inadecuadas de temperatura o humedad	4	4	320
	20	Corte del suministro eléctrico	2	4	160
	20	Fuego	2	4	160

	20	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	120
	20	Errores de Configuración	2	3	120
	20	Desastres naturales	1	3	60
	20	Fuga de Información	2	4	160
	20	Fallo de servicios de comunicaciones	4	4	320
	20	Interrupción de otros servicios y suministros esenciales	4	3	240
	20	Degradación de los soportes de almacenamiento de la información	2	4	160
	20	Alteración de la Información	1	4	80
	20	Destrucción de la información	1	4	80
	20	Caída del sistema por sobrecarga	4	3	240
	20	abusos de privilegios de acceso	1	4	80
	20	Caída del sistema por agotamiento de recursos	0	0	0
	20	Difusión de software dañino	1	5	100
	20	Denegación de Servicio	3	4	240
	20	Errores de mantenimiento / Actualización de programas	3	4	240
	20	Acceso no autorizado	1	5	100
	20	Errores del administrador	2	3	120
	20	Indisponibilidad del personal	1	4	80

	20	Ingeniería Social	1	4	80
	20	Suplantación de identidad del usuario	1	4	80
	20	Interceptación de información (escucha)	1	4	80
SERVER2	17	Daños por agua	2	3	102
	17	Condiciones inadecuadas de temperatura o humedad	4	4	272
	17	Corte del suministro eléctrico	2	4	136
	17	Fuego	2	4	136
	17	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	102
	17	Errores de Configuración	2	3	102
	17	Desastres naturales	1	3	51
	17	Fuga de Información	2	4	136
	17	Fallo de servicios de comunicaciones	4	4	272
	17	Interrupción de otros servicios y suministros esenciales	4	3	204
	17	Degradación de los soportes de almacenamiento de la información	2	4	136
	17	Alteración de la Información	1	4	68
	17	Destrucción de la información	1	4	68
	17	Caída del sistema por sobrecarga	4	3	204
	17	abusos de privilegios de acceso	1	4	68
	17	Caída del sistema por agotamiento de recursos	0	0	0

	17	Difusión de software dañino	1	5	85
	17	Denegación de Servicio	3	4	204
	17	Errores de mantenimiento / Actualización de programas	3	4	204
	17	Acceso no autorizado	1	5	85
	17	Errores del administrador	2	3	102
	17	Indisponibilidad del personal	1	4	68
	17	Ingeniería Social	1	4	68
	17	Suplantación de identidad del usuario	1	4	68
	17	Interceptación de información (escucha)	1	4	68
SERVER3	20	Daños por agua	2	3	120
	20	Condiciones inadecuadas de temperatura o humedad	4	4	320
	20	Corte del suministro eléctrico	2	4	160
	20	Fuego	2	4	160
	20	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	120
	20	Errores de Configuración	2	3	120
	20	Desastres naturales	1	3	60
	20	Fuga de Información	2	4	160
	20	Fallo de servicios de comunicaciones	4	4	320
	20	Interrupción de otros servicios y suministros esenciales	4	3	240

	20	Degradación de los soportes de almacenamiento de la información	2	4	160
	20	Alteración de la Información	1	4	80
	20	Destrucción de la información	1	4	80
	20	Caída del sistema por sobrecarga	4	3	240
	20	abusos de privilegios de acceso	1	4	80
	20	Caída del sistema por agotamiento de recursos	0	0	0
	20	Difusión de software dañino	1	5	100
	20	Denegación de Servicio	3	4	240
	20	Errores de mantenimiento / Actualización de programas	3	4	240
	20	Acceso no autorizado	1	5	100
	20	Errores del administrador	2	3	120
	20	Indisponibilidad del personal	1	4	80
	20	Ingeniería Social	1	4	80
	20	Suplantación de identidad del usuario	1	4	80
	20	Interceptación de información (escucha)	1	4	80
SERVER4	17	Daños por agua	2	3	102
	17	Condiciones inadecuadas de temperatura o humedad	4	4	272
	17	Corte del suministro eléctrico	2	4	136
	17	Fuego	2	4	136

	17	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	102
	17	Errores de Configuración	2	3	102
	17	Desastres naturales	1	3	51
	17	Fuga de Información	2	4	136
	17	Fallo de servicios de comunicaciones	4	4	272
	17	Interrupción de otros servicios y suministros esenciales	4	3	204
	17	Degradación de los soportes de almacenamiento de la información	2	4	136
	17	Alteración de la Información	1	4	68
	17	Destrucción de la información	1	4	68
	17	Caída del sistema por sobrecarga	4	3	204
	17	abusos de privilegios de acceso	1	4	68
	17	Caída del sistema por agotamiento de recursos	0	0	0
	17	Difusión de software dañino	1	5	85
	17	Denegación de Servicio	3	4	204
	17	Errores de mantenimiento / Actualización de programas	3	4	204
	17	Acceso no autorizado	1	5	85
	17	Errores del administrador	2	3	102
	17	Indisponibilidad del personal	1	4	68

	17	Ingeniería Social	1	4	68
	17	Suplantación de identidad del usuario	1	4	68
	17	Interceptación de información (escucha)	1	4	68
SERVER5	16	Daños por agua	2	3	96
	16	Condiciones inadecuadas de temperatura o humedad	4	4	256
	16	Corte del suministro eléctrico	2	4	128
	16	Fuego	2	4	128
	16	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	96
	16	Errores de Configuración	2	3	96
	16	Desastres naturales	1	3	48
	16	Fuga de Información	2	4	128
	16	Fallo de servicios de comunicaciones	4	4	256
	16	Interrupción de otros servicios y suministros esenciales	4	3	192
	16	Degradación de los soportes de almacenamiento de la información	2	4	128
	16	Alteración de la Información	1	4	64
	16	Destrucción de la información	1	4	64
	16	Caída del sistema por sobrecarga	4	3	192
	16	abusos de privilegios de acceso	1	4	64
	16	Caída del sistema por agotamiento de recursos	0	0	0

	16	Difusión de software dañino	1	5	80
	16	Denegación de Servicio	3	4	192
	16	Errores de mantenimiento / Actualización de programas	3	4	192
	16	Acceso no autorizado	1	5	80
	16	Errores del administrador	2	3	96
	16	Indisponibilidad del personal	1	4	64
	16	Ingeniería Social	1	4	64
	16	Suplantación de identidad del usuario	1	4	64
	16	Interceptación de información (escucha)	1	4	64
SERVER6	15	Daños por agua	2	3	90
	15	Condiciones inadecuadas de temperatura o humedad	4	4	240
	15	Corte del suministro eléctrico	2	4	120
	15	Fuego	2	4	120
	15	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	90
	15	Errores de Configuración	2	3	90
	15	Desastres naturales	1	3	45
	15	Fuga de Información	2	4	120
	15	Fallo de servicios de comunicaciones	4	4	240
	15	Interrupción de otros servicios y suministros esenciales	4	3	180

	15	Degradación de los soportes de almacenamiento de la información	2	4	120
	15	Alteración de la Información	1	4	60
	15	Destrucción de la información	1	4	60
	15	Caída del sistema por sobrecarga	4	3	180
	15	abusos de privilegios de acceso	1	4	60
	15	Caída del sistema por agotamiento de recursos	0	0	0
	15	Difusión de software dañino	1	5	75
	15	Denegación de Servicio	3	4	180
	15	Errores de mantenimiento / Actualización de programas	3	4	180
	15	Acceso no autorizado	1	5	75
	15	Errores del administrador	2	3	90
	15	Indisponibilidad del personal	1	4	60
	15	Ingeniería Social	1	4	60
	15	Suplantación de identidad del usuario	1	4	60
	15	Interceptación de información (escucha)	1	4	60
SERVER7	22	Daños por agua	2	3	132
	22	Condiciones inadecuadas de temperatura o humedad	4	4	352
	22	Corte del suministro eléctrico	2	4	176
	22	Fuego	2	4	176

	22	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	132
	22	Errores de Configuración	2	3	132
	22	Desastres naturales	1	3	66
	22	Fuga de Información	2	4	176
	22	Fallo de servicios de comunicaciones	4	4	352
	22	Interrupción de otros servicios y suministros esenciales	4	3	264
	22	Degradación de los soportes de almacenamiento de la información	2	4	176
	22	Alteración de la Información	1	4	88
	22	Destrucción de la información	1	4	88
	22	Caída del sistema por sobrecarga	4	3	264
	22	abusos de privilegios de acceso	1	4	88
	22	Caída del sistema por agotamiento de recursos	0	0	0
	22	Difusión de software dañino	1	5	110
	22	Denegación de Servicio	3	4	264
	22	Errores de mantenimiento / Actualización de programas	3	4	264
	22	Acceso no autorizado	1	5	110
	22	Errores del administrador	2	3	132
	22	Indisponibilidad del personal	1	4	88

	22	Ingeniería Social	1	4	88
	22	Suplantación de identidad del usuario	1	4	88
	22	Interceptación de información (escucha)	1	4	88
SERVER8	14	Daños por agua	2	3	84
	14	Condiciones inadecuadas de temperatura o humedad	4	4	224
	14	Corte del suministro eléctrico	2	4	112
	14	Fuego	2	4	112
	14	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	84
	14	Errores de Configuración	2	3	84
	14	Desastres naturales	1	3	42
	14	Fuga de Información	2	4	112
	14	Fallo de servicios de comunicaciones	4	4	224
	14	Interrupción de otros servicios y suministros esenciales	4	3	168
	14	Degradación de los soportes de almacenamiento de la información	2	4	112
	14	Alteración de la Información	1	4	56
	14	Destrucción de la información	1	4	56
	14	Caída del sistema por sobrecarga	4	3	168
	14	abusos de privilegios de acceso	1	4	56
	14	Caída del sistema por agotamiento de recursos	0	0	0

	14	Difusión de software dañino	1	5	70
	14	Denegación de Servicio	3	4	168
	14	Errores de mantenimiento / Actualización de programas	3	4	168
	14	Acceso no autorizado	1	5	70
	14	Errores del administrador	2	3	84
	14	Indisponibilidad del personal	1	4	56
	14	Ingeniería Social	1	4	56
	14	Suplantación de identidad del usuario	1	4	56
	14	Interceptación de información (escucha)	1	4	56
SERVER9	15	Daños por agua	2	3	90
	15	Condiciones inadecuadas de temperatura o humedad	4	4	240
	15	Corte del suministro eléctrico	2	4	120
	15	Fuego	2	4	120
	15	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	90
	15	Errores de Configuración	2	3	90
	15	Desastres naturales	1	3	45
	15	Fuga de Información	2	4	120
	15	Fallo de servicios de comunicaciones	4	4	240
	15	Interrupción de otros servicios y suministros esenciales	4	3	180

	15	Degradación de los soportes de almacenamiento de la información	2	4	120
	15	Alteración de la Información	1	4	60
	15	Destrucción de la información	1	4	60
	15	Caída del sistema por sobrecarga	4	3	180
	15	abusos de privilegios de acceso	1	4	60
	15	Caída del sistema por agotamiento de recursos	0	0	0
	15	Difusión de software dañino	1	5	75
	15	Denegación de Servicio	3	4	180
	15	Errores de mantenimiento / Actualización de programas	3	4	180
	15	Acceso no autorizado	1	5	75
	15	Errores del administrador	2	3	90
	15	Indisponibilidad del personal	1	4	60
	15	Ingeniería Social	1	4	60
	15	Suplantación de identidad del usuario	1	4	60
	15	Interceptación de información (escucha)	1	4	60
SERVER10	19	Daños por agua	2	3	114
	19	Condiciones inadecuadas de temperatura o humedad	4	4	304
	19	Corte del suministro eléctrico	2	4	152
	19	Fuego	2	4	152

	19	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	114
	19	Errores de Configuración	2	3	114
	19	Desastres naturales	1	3	57
	19	Fuga de Información	2	4	152
	19	Fallo de servicios de comunicaciones	4	4	304
	19	Interrupción de otros servicios y suministros esenciales	4	3	228
	19	Degradación de los soportes de almacenamiento de la información	2	4	152
	19	Alteración de la Información	1	4	76
	19	Destrucción de la información	1	4	76
	19	Caída del sistema por sobrecarga	4	3	228
	19	abusos de privilegios de acceso	1	4	76
	19	Caída del sistema por agotamiento de recursos	0	0	0
	19	Difusión de software dañino	1	5	95
	19	Denegación de Servicio	3	4	228
	19	Errores de mantenimiento / Actualización de programas	3	4	228
	19	Acceso no autorizado	1	5	95
	19	Errores del administrador	2	3	114
	19	Indisponibilidad del personal	1	4	76

	19	Ingeniería Social	1	4	76
	19	Suplantación de identidad del usuario	1	4	76
	19	Interceptación de información (escucha)	1	4	76
TS2	19	Daños por agua	2	3	114
	19	Condiciones inadecuadas de temperatura o humedad	4	4	304
	19	Corte del suministro eléctrico	2	4	152
	19	Fuego	2	4	152
	19	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	114
	19	Errores de Configuración	2	3	114
	19	Desastres naturales	1	3	57
	19	Fuga de Información	2	4	152
	19	Fallo de servicios de comunicaciones	4	4	304
	19	Interrupción de otros servicios y suministros esenciales	4	3	228
	19	Degradación de los soportes de almacenamiento de la información	2	4	152
	19	Alteración de la Información	1	4	76
	19	Destrucción de la información	1	4	76
	19	Caída del sistema por sobrecarga	4	3	228
	19	abusos de privilegios de acceso	1	4	76
	19	Caída del sistema por agotamiento de recursos	0	0	0

	19	Difusión de software dañino	1	5	95
	19	Denegación de Servicio	3	4	228
	19	Errores de mantenimiento / Actualización de programas	3	4	228
	19	Acceso no autorizado	1	5	95
	19	Errores del administrador	2	3	114
	19	Indisponibilidad del personal	1	4	76
	19	Ingeniería Social	1	4	76
	19	Suplantación de identidad del usuario	1	4	76
	19	Interceptación de información (escucha)	1	4	76
SERVER11	29	Daños por agua	2	3	174
	29	Condiciones inadecuadas de temperatura o humedad	4	4	464
	29	Corte del suministro eléctrico	2	4	232
	29	Fuego	2	4	232
	29	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	174
	29	Errores de Configuración	2	3	174
	29	Desastres naturales	1	3	87
	29	Fuga de Información	2	4	232
	29	Fallo de servicios de comunicaciones	4	4	464
	29	Interrupción de otros servicios y suministros esenciales	4	3	348

	29	Degradación de los soportes de almacenamiento de la información	2	4	232
	29	Alteración de la Información	1	4	116
	29	Destrucción de la información	1	4	116
	29	Caída del sistema por sobrecarga	4	3	348
	29	abusos de privilegios de acceso	1	4	116
	29	Caída del sistema por agotamiento de recursos	0	0	0
	29	Difusión de software dañino	1	5	145
	29	Denegación de Servicio	3	4	348
	29	Errores de mantenimiento / Actualización de programas	3	4	348
	29	Acceso no autorizado	1	5	145
	29	Errores del administrador	2	3	174
	29	Indisponibilidad del personal	1	4	116
	29	Ingeniería Social	1	4	116
	29	Suplantación de identidad del usuario	1	4	116
	29	Interceptación de información (escucha)	1	4	116
AD	28	Daños por agua	2	3	168
	28	Condiciones inadecuadas de temperatura o humedad	4	4	448
	28	Corte del suministro eléctrico	2	4	224
	28	Fuego	2	4	224

	28	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	168
	28	Errores de Configuración	2	3	168
	28	Desastres naturales	1	3	84
	28	Fuga de Información	2	4	224
	28	Fallo de servicios de comunicaciones	4	4	448
	28	Interrupción de otros servicios y suministros esenciales	4	3	336
	28	Degradación de los soportes de almacenamiento de la información	2	4	224
	28	Alteración de la Información	1	4	112
	28	Destrucción de la información	1	4	112
	28	Caída del sistema por sobrecarga	4	3	336
	28	abusos de privilegios de acceso	1	4	112
	28	Caída del sistema por agotamiento de recursos	0	0	0
	28	Difusión de software dañino	1	5	140
	28	Denegación de Servicio	3	4	336
	28	Errores de mantenimiento / Actualización de programas	3	4	336
	28	Acceso no autorizado	1	5	140
	28	Errores del administrador	2	3	168
	28	Indisponibilidad del personal	1	4	112

	28	Ingeniería Social	1	4	112
	28	Suplantación de identidad del usuario	1	4	112
	28	Interceptación de información (escucha)	1	4	112
SAP	28	Daños por agua	2	3	168
	28	Condiciones inadecuadas de temperatura o humedad	4	4	448
	28	Corte del suministro eléctrico	2	4	224
	28	Fuego	2	4	224
	28	Errores de Mantenimiento / Actualización de equipos (Hardware)	2	3	168
	28	Errores de Configuración	2	3	168
	28	Desastres naturales	1	3	84
	28	Fuga de Información	2	4	224
	28	Fallo de servicios de comunicaciones	4	4	448
	28	Interrupción de otros servicios y suministros esenciales	4	3	336
	28	Degradación de los soportes de almacenamiento de la información	2	4	224
	28	Alteración de la Información	1	4	112
	28	Destrucción de la información	1	4	112
	28	Caída del sistema por sobrecarga	4	3	336
	28	abusos de privilegios de acceso	1	4	112
	28	Caída del sistema por agotamiento de recursos	0	0	0

	28	Difusión de software dañino	1	5	140
	28	Denegación de Servicio	3	4	336
	28	Errores de mantenimiento / Actualización de programas	3	4	336
	28	Acceso no autorizado	1	5	140
	28	Errores del administrador	2	3	168
	28	Indisponibilidad del personal	1	4	112
	28	Ingeniería Social	1	4	112
	28	Suplantación de identidad del usuario	1	4	112
	28	Interceptación de información (escucha)	1	4	112

Fuente: Elaboración Propia.

De acuerdo con lo identificado anteriormente se concluye que los servidores críticos serán los que presenten cuatro o más niveles de riesgos inaceptables, estos son:

Tabla 14. Servidores Críticos

SERVIDOR	AMENAZAS CRÍTICAS	VALOR RIESGO
SERVER1	Condiciones inadecuadas de temperatura o humedad	448
	Fallo de servicios de comunicaciones	448
	Interrupción de otros servicios y suministros esenciales	336
	Caída del sistema por sobrecarga	336
	Denegación de Servicio	336
	Errores de mantenimiento / Actualización de programas	336
SERVER11	Condiciones inadecuadas de temperatura o humedad	464
	Fallo de servicios de comunicaciones	464
	Interrupción de otros servicios y suministros esenciales	348
	Caída del sistema por sobrecarga	348
	Denegación de Servicio	348
	Errores de mantenimiento / Actualización de programas	348
AD	Condiciones inadecuadas de temperatura o humedad	448

	Fallo de servicios de comunicaciones	448
	Interrupción de otros servicios y suministros esenciales	336
	Caída del sistema por sobrecarga	336
	Denegación de Servicio	336
	Errores de mantenimiento / Actualización de programas	336
SAP	Condiciones inadecuadas de temperatura o humedad	448
	Fallo de servicios de comunicaciones	448
	Interrupción de otros servicios y suministros esenciales	336
	Caída del sistema por sobrecarga	336
	Denegación de Servicio	336
	Errores de mantenimiento / Actualización de programas	336

Fuente: Elaboración Propia.

Teniendo en cuenta que esa evaluación de riesgos fue levantada en el inicio del este proyecto aplicado (finales del 2021), y que varios de estos servidores han cambiado de roles y de sistema operativo, se plantea esta nueva lista de servidores críticos.

1. Server1: Este servidor (DELL R740) tenía un Windows Server 2012 R2 con rol de Hyper-V, en este servidor se tenía virtualizado el servidor TS (Terminal Server). En este servidor físico se instala un Proxmox VE 7.2.1 y se migra la máquina virtual TS. Por eso se reemplaza en la lista de servidores críticos Server1 por TS.
2. Server11. Este servidor tenía un Windows Server 2008 R2 con un SQL Server 2008 R2 con una sola base de datos, BD2, esta base de datos se migra al SQL Server 2012 R2 de SAP y se instala otro Proxmox VE 7.2.1 como parte del Clúster de virtualización. Por esto Server11 se elimina de la lista de servidores críticos.
3. AD y SAP se pasan de físicos a máquinas virtuales, migrándolas a un nuevo servidor DELL R740 adquirido por la compañía (Julio 2022); utilizando los servidores ProLiant DL380e Gen8 (AD) y PowerEdge R620 (SAP) como parte del clúster de Proxmox.

Una de las ventajas del entorno de virtualización Proxmox, entre muchas otras, es poder realizar migraciones en “caliente” de las máquinas virtuales entre equipos que hagan parte del clúster, pudiendo pasar entre servidores sin indisponer el servicio, sin perdida alguna de datos y sin que los clientes conectados si quiera lo noten.

Por lo anteriormente descrito, se van a realizar pruebas de Pentest directamente a los sistemas operativos y sus servicios, ya que al tener un clúster de virtualización no se depende de una máquina física como tal, por el contrario, que los servicios estén operativos y accesibles ya sea en uno u otro nodo del clúster, o en AWS cuando se active el DRP.

Tabla 15. Servidor Críticos - Revisión

Servidor	Rol	Servicios
TS	Terminal Server	SAP B1 Cliente, Infomante Cliente, ZKAccess Cliente.
AD	Active Directory	AD, DHCP, DNS, File Server
SAP	SAP B1 y BD	SAP B1 Aplicación, SQL Server

Fuente: Elaboración Propia.

5.2 ESTABLECER LA METODOLOGÍA PARA LA EVALUACIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA DE LOS SERVIDORES CRÍTICOS MEDIANTE LA CLASIFICACIÓN Y ANÁLISIS DE LAS MÁS RELEVANTES PARA SELECCIONAR LAS MÁS APROPIADA DE ACUERDO CON LA NATURALEZA DE LA ORGANIZACIÓN.

Existen varias metodologías para la realización de auditorías de seguridad o Pentest, todas ellas se encuentran estructuradas por diferentes fases y sus entregables son informes técnicos y gerenciales de los hallazgos de seguridad encontrados. Dependiendo de lo que se valla a auditar, una metodología es más aplicable que otra, por ejemplo, el OWAST TOP 10 su enfoque es a auditar software basado en nube, aunque se podría aplicar el concepto para otro tipo de software o sistema, su enfoque principal es la auditoria a aplicativos webs. Por el contrario, OSSTMM es más amplio en su enfoque y contempla, entre otros, la seguridad física de los servidores.

La mayoría de las metodologías de Pentest tienen como bases las siguientes fases:

5.2.1 **Pactar desde el comienzo el alcance de la prueba.** Se debe aclarar el alcance de las pruebas en una reunión previa a los análisis y dejarlo por escrito para aprobación del gerente previa revisión del encargado de TI. En este documento debe quedar plasmado que se va a analizar (servidores, dispositivos de red, aplicaciones, servicios web, etc.), como se va a actuar en caso de encontrar una vulnerabilidad, los tiempos en los que se va a realizar, los entregables y, sobre todo, los acuerdos de confidencialidad que se deban firmar.

5.2.2 **Recopilar toda la información posible, ya sea desde fuentes abiertas o desde escaneos a servicios o puertos.** Teniendo el alcance definido, se procede con el levantamiento de toda la información posible, tanto desde fuentes abiertas (usando Google Dorks, o las múltiples opciones que ofrece el Framework OSINT) como también realizando escaneos en la red en búsqueda de puertos y servicios publicados, puertos de red físicos accesibles sin ningún control, redes inalámbricas abiertas o con cifrado débil, engaño con dispositivos USB como los famosos Rubber Ducky, entre muchos otros.

5.2.3 **Clasificación de los resultados obtenidos en el paso anterior para depurar falsos positivos o falsos negativos y perfilar los ataques a realizar.** Toda la información recopilada en el paso anterior puede resultar abrumadora y confusa si no se clasifica y se ordena; además puede ayudar a que el analista se pierda o tenga un enfoque erróneo con falsos positivos o falsos negativos. La manera más ordenada y práctica es cotejar las amenazas encontradas contra bases de datos de vulnerabilidades para verificar si es o no vulnerable dicho servicio. Las bases de datos a consultar pueden ser: Exploit DataBase (https://www.exploit-db.com/), Vulnerability DataBase (https://vuldb.com/es/), OpenSource Vulnerability (https://osv.dev/), National Vulnerability Database del NIST (https://nvd.nist.gov/).

5.2.4 **Ejecutar ataques dirigidos a las vulnerabilidades encontradas para buscar comprometer el sistema o servicio.** Teniendo las amenazas identificadas y sabiendo que los servicios pueden ser vulnerables, se ejecutan los ataques para lograr comprometerlos. Estos ataques dependen de las vulnerabilidades, pueden ser PayLoad (carga útil), un Exploit, un envenenamiento de un protocolo de comunicación, Inyección SQL, Cross-site scripting, SMBRelay, enumeración de usuarios, crakeo de contraseñas por fuerza bruta y/o diccionario, y un gran etc.

5.2.5 **Si la máquina o servicio comprometida no contiene información o roles valiosos para el atacante, intentar realizar un pivoting (desplazamiento entre servidores) o escalamiento de privilegios.** En muchas ocasiones, vulnerar un servicio no significa necesariamente ganar acceso al sistema o comprometerlo, siempre y cuando el servicio se ejecute con permisos reducidos. Si es el caso, lo siguiente sería intentar ganar acceso a usuarios con más privilegios (NT AUTHORITY\SYSTEM o Administrator en entornos Windows o usuario root en GNU/Linux), teniendo esa elevación de privilegios, intentar realizar un pivoteo o desplazamiento lateral a otro equipo o escapar una Shell si el servicio comprometido está encapsulado en un contenedor. Si el atacante logra tener acceso al directorio activo de un entorno Windows y si tiene privilegios de administrador del dominio, prácticamente tiene acceso a todos los equipos de la red y podría hacer muchísimo daño.

5.2.6 **Intentar lograr persistencia en el equipo o sistema vulnerado, ya sea por puertas traseras o modificaciones al sistema.** Habiendo conseguido acceso, lo siguiente es intentar lograr persistencia, esto para ahorrar tiempo en futuras incursiones o mantener un canal de comunicaciones abierto y constante para lanzar otra serie de ataques. En la mayoría de los casos se configuran puertas traseras o BackDoor o se modifica el sistema para asignar permisos de conexión adicionales, por ejemplo, la habilitación de conexión por RDP, VNC, Telnet, SSH, usuarios de FTP, etc.

5.2.7 **Intentar eliminar todo rastro del ataque para que sea más difícil para los analistas forenses rastrear el ataque.** El atacante puede intentar eliminar todo rastro del ingreso al sistema comprometido, ya sea eliminando Logs de conexión, Logs de eventos, conexiones TCP, si se comprometió un servidor web se eliminarían los logs de Apache, limpieza del historial de comandos usados por consola (en caso de Linux), eliminar usuarios creados en el escalamiento de privilegios, eliminar las puertas traseras si ya no se necesitan, entre otros.

5.2.8 **Documentar todos los pasos realizados, las vulnerabilidades encontradas, los servicios comprometidos, etc.** El analista o Pentester debe tener la costumbre de documentar cada paso que dé en los análisis, los hallazgos encontrados, los resultados de los escaneos, comandos utilizados, logs generados, etc. Esto se convertirá en el insumo principal para la generación del informe de entrega final. Sin la evidencia de los hallazgos, difícilmente se podrá demostrar las vulnerabilidades y se perdería todo el trabajo realizado.

5.2.9 **Generar un informe detallado, uno técnico y otro gerencial como entregable del Pentest.** El entregable final de la prueba de intrusión o Pentest son dos informes de los hallazgos encontrados, uno con la mayor cantidad de información posible, de manera técnica, detallando todas las vulnerabilidades y servicios comprometidos, hasta donde se logró comprometer el servicio o sistema y el cómo se logró tener acceso; también debería contener información del cómo proteger el servicio para tapar esta vulnerabilidad. El otro informe es el gerencial; este informe es mucho más corto y concreto, debe contener un lenguaje entendible y no técnico, mostrando de manera resumida los hallazgos y el impacto que podría ocasionar si un ciberdelincuente lograra obtener estos accesos.

Es de aclarar que el alcance pactado de este proyecto aplicado no es el de vulnerar los sistemas o servidores de la compañía, por el contrario, es el de realizar diferentes análisis a los sistemas operativos, aplicaciones y puertos para lograr encontrar vulnerabilidades asociadas a estos y exponer la mejor manera de protegerlos para, de alguna manera, mitigar estos riesgos.

Para lograr encontrar dichas vulnerabilidades se deben realizar diferentes análisis, los cuales corresponderían a las fases 2 y 3 de un análisis de seguridad o Pentest. Teniendo en cuenta lo anterior, la metodología que se va a trabajar para este proyecto aplicado es la siguiente:

5.2.10 **Metodología aplicada.**

5.2.10.1 **Análisis previos.:**

- Caracterización de todos los servidores físicos y virtuales que tiene la compañía.
- Generación de tablas con información de las características de hardware de cada uno de los anteriores y de los servicios o roles que soportan.
- Aplicación de la metodología de Magerit Versión 3 para cuantificar los riesgos de cada uno.
- Con los resultados anteriores, determinar cuáles son los servidores críticos de la compañía.

5.2.10.2 **Análisis de vulnerabilidades en el Sistema operativo, aplicaciones, puertos y configuraciones de los servidores críticos.:**

- Montaje de un laboratorio con herramientas de auditoría de sistemas, dando apertura completa de puertos y quitando cualquier bloqueo a nivel de Firewall e IP que pueda limitar las pruebas.
- Análisis manual de puertos a cada servidor con Nmap para encontrar los abiertos y sus servicios.
- Análisis manual con Nmap dirigido esta vez a los puertos abiertos e incluyendo el script de análisis de vulnerabilidades de la suite.
- Análisis a cada servidor con la herramienta Nessus y generación de informe
- Análisis a cada servidor con la herramienta OpenVAS y generación de informe.

5.2.10.3 **Generación de recomendaciones de seguridad y pasos a seguir para solventar las vulnerabilidades encontradas.:**

- Generar recomendaciones específicas a cada servidor para corregir errores, tanto de configuraciones en el sistema operativo como de las aplicaciones o roles montados en ellos.
- Agrupar las amenazas generadas por cada servicio o aplicación vulnerable
- Contextualizar la amenaza y dar las pautas para eliminar o mitigar las vulnerabilidades.
- Generar recomendaciones adicionales de red, servidores o infraestructura que se evidenciaron en la ejecución de las pruebas.

5.3 EXAMINAR LA INFRAESTRUCTURA DE LOS SERVIDORES CRÍTICOS DE ECODIESEL COLOMBIA S.A. MEDIANTE LA METODOLOGÍA SELECCIONADA CON EL FIN DE IDENTIFICAR LAS VULNERABILIDADES.

Antes de empezar a realizar los análisis y pruebas se debe recalcar el tipo de análisis a realizar, los diferentes tipos son de caja blanca, caja negra o caja gris.

- **Pruebas de caja Blanca:** En este tipo de pruebas se tiene de antemano toda la información de los objetivos, tanto de los servidores, infraestructura de red, tipo de aplicativos, sistemas operativos, tipos de control, entre otros.
- **Pruebas de caja negra:** Este tipo de prueba es la más cercana a un ataque real, ya que el pentester no conoce nada de los objetivos, debe empezar a realizar un levantamiento de información juiciosa y concienzuda de la infraestructura, tipo de sistema operativo, tipología de red y demás para poder realizar y enfocar muy bien los análisis posteriores.
- **Pruebas de caja Gris:** Este tipo de pruebas se puede decir que es un híbrido entre las dos anteriores, ya que el atacante o pentester tiene una información muy limitada de los objetivos y depende de su experiencia y experticia para realizar con éxito los análisis y ataques posteriores.

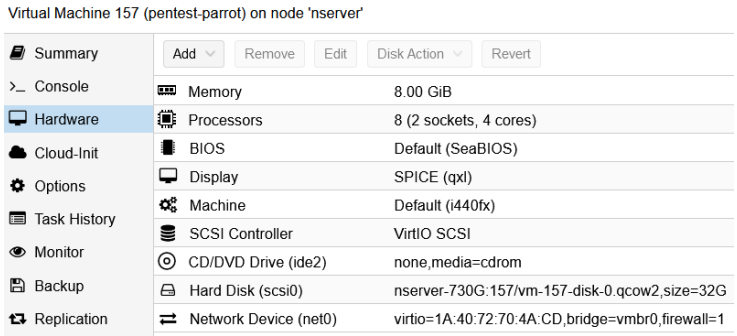
Teniendo en cuenta que en el desarrollo de las pruebas se tienen total conocimiento de toda la información de servidores, infraestructura, sistemas operativos, aplicaciones y demás, ya que la persona que va a desarrollar las pruebas trabaja directamente para la compañía y es el encargado de toda la infraestructura, las pruebas se encasillan en test de Caja Blanca.

Para el desarrollo de las pruebas, se utilizan varias herramientas, primero el sistema operativo es el Parrot Versión 5.1 (Electro Ara) x64, montado en un virtualizador Proxmox Virtual Environment versión 7.2-1, con 2 sockets, 4 Cores (8 Procesadores), 8GB de RAM y SSD de 32GB. (posteriormente actualizado a 16GB de RAM y 64GB de SSD).

Figura 7. Parrot versión 5.1

Fuente: Propia

Figura 8. VM Parrot, características.



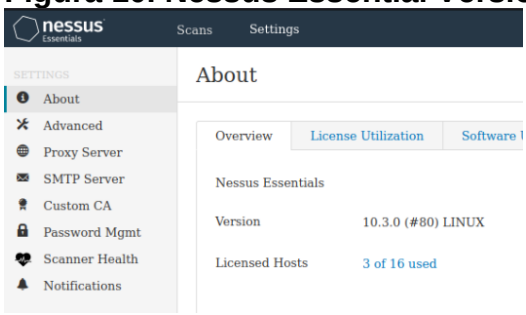
Fuente: Propia

Para los escaneos y análisis se utilizaron las siguientes herramientas:

Figura 9. OpenVAS – Greenbone Security Assistant Version 21.4.3

Fuente: Propia

Figura 10. Nessus Essential Versión 10.0.3



Fuente: Propia

Figura 11. Nmap Versión 7.92

Fuente: Propia

El resultado de los análisis a cada una de las máquinas se presenta a continuación:

Las direcciones IP, nombre de equipo, NetBIOS, FQDN, Dominio y aplicaciones sensibles, se han reemplazado por XXXX para cumplir el acuerdo de confidencialidad firmado con la empresa.

5.3.1 AD

5.3.1.1 **Resultados de escaneo con Nmap.**

Comando:

sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn XXXX

Resultado:

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 (https://nmap.org) at 2022-10-02 00:52 -05
Initiating ARP Ping Scan at 00:52
Scanning XXXX [1 port]
Completed ARP Ping Scan at 00:52, 0.07s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 00:52
Scanning XXXX [65535 ports]
Discovered open port 443/tcp on XXXX
Discovered open port 80/tcp on XXXX
Discovered open port 3389/tcp on XXXX

Discovered open port 445/tcp on XXXX
Discovered open port 135/tcp on XXXX
Discovered open port 139/tcp on XXXX
Discovered open port 53/tcp on XXXX
Discovered open port 636/tcp on XXXX
Discovered open port 10050/tcp on XXXX
Discovered open port 389/tcp on XXXX
Discovered open port 49155/tcp on XXXX
Discovered open port 49158/tcp on XXXX
Discovered open port 22270/tcp on XXXX
Discovered open port 53492/tcp on XXXX
Discovered open port 47001/tcp on XXXX
Discovered open port 53488/tcp on XXXX
Discovered open port 49154/tcp on XXXX
Discovered open port 49175/tcp on XXXX
Discovered open port 53630/tcp on XXXX
Discovered open port 3268/tcp on XXXX
Discovered open port 49153/tcp on XXXX
Discovered open port 49156/tcp on XXXX
Discovered open port 88/tcp on XXXX
Discovered open port 2260/tcp on XXXX
Discovered open port 9389/tcp on XXXX
Discovered open port 53620/tcp on XXXX
Discovered open port 593/tcp on XXXX
Discovered open port 53611/tcp on XXXX
Discovered open port 464/tcp on XXXX
Discovered open port 5722/tcp on XXXX
Discovered open port 49152/tcp on XXXX
Discovered open port 3269/tcp on XXXX
Discovered open port 7070/tcp on XXXX
Completed SYN Stealth Scan at 00:52, 11.63s elapsed (65535 total ports)
Nmap scan report for XXXX
Host is up, received arp-response (0.00073s latency).
Scanned at 2022-10-02 00:52:38 -05 for 11s
Not shown: 57596 closed tcp ports (reset), 7906 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE REASON
53/tcp open domain syn-ack ttl 128
80/tcp open http syn-ack ttl 128
88/tcp open kerberos-sec syn-ack ttl 128
135/tcp open msrpc syn-ack ttl 128
139/tcp open netbios-ssn syn-ack ttl 128
389/tcp open ldap syn-ack ttl 128
443/tcp open https syn-ack ttl 128

```
445/tcp   open  microsoft-ds     syn-ack ttl 128
464/tcp   open  kpasswd5         syn-ack ttl 128
593/tcp   open  http-rpc-epmap   syn-ack ttl 128
636/tcp   open  ldapssl          syn-ack ttl 128
2260/tcp  open  apc-2260         syn-ack ttl 128
3268/tcp  open  globalcatLDAP    syn-ack ttl 128
3269/tcp  open  globalcatLDAPssl syn-ack ttl 128
3389/tcp  open  ms-wbt-server    syn-ack ttl 128
5722/tcp  open  msdfsr           syn-ack ttl 128
7070/tcp  open  realserver       syn-ack ttl 128
9389/tcp  open  adws             syn-ack ttl 128
10050/tcp open  XXXX     syn-ack ttl 128
22270/tcp open  unknown          syn-ack ttl 128
47001/tcp open  winrm            syn-ack ttl 128
49152/tcp open  unknown          syn-ack ttl 128
49153/tcp open  unknown          syn-ack ttl 128
49154/tcp open  unknown          syn-ack ttl 128
49155/tcp open  unknown          syn-ack ttl 128
49156/tcp open  unknown          syn-ack ttl 128
49158/tcp open  unknown          syn-ack ttl 128
49175/tcp open  unknown          syn-ack ttl 128
53488/tcp open  unknown          syn-ack ttl 128
53492/tcp open  unknown          syn-ack ttl 128
53611/tcp open  unknown          syn-ack ttl 128
53620/tcp open  unknown          syn-ack ttl 128
53630/tcp open  unknown          syn-ack ttl 128
MAC Address: 46:05:16:50:86:02 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.92 seconds
        Raw packets sent: 82830 (3.645MB) | Rcvd: 57630 (2.305MB)
```

Ahora se van a analizar todos los puertos abiertos descubiertos en el paso anterior, pero esta vez con la opción “V” para que nos ofrezca más información del servicio que corre en ese puerto.

Comando:

```
sudo nmap -sCV -
p443,80,3389,445,135,139,53,636,10050,389,49155,49158,22270,53492,4
7001,53488,49154,49175,53630,3268,49153,49156,88,2260,9389,53620,5
93,53611,464,5722,49152,3269,7070 XXXX -oN AD
```

Resultado:

Nmap 7.92 scan initiated Sun Oct 2 01:34:05 2022 as: nmap -sCV -p443,80,3389,445,135,139,53,636,10050,389,49155,49158,22270,53492,47001,53488,49154,49175,53630,3268,49153,49156,88,2260,9389,53620,593,53611,464,5722,49152,3269,7070 -oN AD XXXX XXXX
Nmap scan report for XXXX
Host is up (0.00092s latency).

PORT	STATE	SERVICE	VERSION
53/tcp	filtered	domain	
80/tcp	filtered	http	
88/tcp	open	tcpwrapped	
135/tcp	filtered	msrpc	
139/tcp	filtered	netbios-ssn	
389/tcp	open	tcpwrapped	
443/tcp	filtered	https	
445/tcp	filtered	microsoft-ds	
464/tcp	open	tcpwrapped	
593/tcp	open	tcpwrapped	
636/tcp	open	tcpwrapped	
2260/tcp	open	tcpwrapped	
3268/tcp	open	tcpwrapped	
3269/tcp	open	tcpwrapped	
3389/tcp	filtered	ms-wbt-server	
5722/tcp	open	tcpwrapped	
7070/tcp	open	tcpwrapped	
9389/tcp	open	tcpwrapped	
10050/tcp	filtered	XXXX	
22270/tcp	open	tcpwrapped	
47001/tcp	open	tcpwrapped	
49152/tcp	open	tcpwrapped	
49153/tcp	open	tcpwrapped	
49154/tcp	open	tcpwrapped	
49155/tcp	open	tcpwrapped	
49156/tcp	open	tcpwrapped	
49158/tcp	open	tcpwrapped	
49175/tcp	open	tcpwrapped	
53488/tcp	open	tcpwrapped	
53492/tcp	open	tcpwrapped	
53611/tcp	open	tcpwrapped	
53620/tcp	filtered	unknown	
53630/tcp	open	tcpwrapped	

MAC Address: 46:05:16:50:86:02 (Unknown)

Nmap scan report for XXXX

Host is up (0.00091s latency).

PORT STATE SERVICE VERSION
53/tcp open domain Microsoft DNS 6.1.7601 (1DB15F75) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_ bind.version: Microsoft DNS 6.1.7601 (1DB15F75)
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2022-10-02 06:35:02Z)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: XXXX.wan, Site: Default-First-Site-Name)
443/tcp open ssl/https?
|_ssl-date: 2022-10-02T06:38:40+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=nls.XXXX.wan
| Not valid before: 2013-08-01T01:56:31
|_Not valid after: 2015-08-01T01:56:31
| sslv2:
| SSLv2 supported
| ciphers:
| SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
445/tcp open microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: XXXX)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
2260/tcp open apc-2260?
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: XXXX.wan, Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
3389/tcp open ssl/ms-wbt-server?
|_ssl-date: 2022-10-02T06:38:40+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=AD.XXXX.wan
| Not valid before: 2022-05-07T18:50:41
|_Not valid after: 2022-11-06T18:50:41
5722/tcp open msrpc Microsoft Windows RPC
7070/tcp open ssl/realserver?

| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2020-05-28T14:07:02
|_Not valid after: 2070-05-16T14:07:02
|_ssl-date: TLS randomness does not represent time
9389/tcp open mc-nmf   .NET Message Framing
10050/tcp open tcpwrapped
22270/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Bad Request
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open msrpc   Microsoft Windows RPC
49153/tcp open msrpc   Microsoft Windows RPC
49154/tcp open msrpc   Microsoft Windows RPC
49155/tcp open msrpc   Microsoft Windows RPC
49156/tcp open msrpc   Microsoft Windows RPC
49158/tcp open ncacn_http   Microsoft Windows RPC over HTTP 1.0
49175/tcp open msrpc   Microsoft Windows RPC
53488/tcp open msrpc   Microsoft Windows RPC
53492/tcp open msrpc   Microsoft Windows RPC
53611/tcp open msrpc   Microsoft Windows RPC
53620/tcp open msrpc   Microsoft Windows RPC
53630/tcp open msrpc   Microsoft Windows RPC
MAC Address: 46:05:16:50:86:02 (Unknown)
Service Info: Host: AD; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: required
| smb-os-discovery:
| OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
| Computer name: AD
| NetBIOS computer name: AD\x00
| Domain name: XXXX.wan
| Forest name: XXXX.wan
| FQDN: AD.XXXX.wan
|_ System time: 2022-10-02T01:37:32-05:00

|_nbstat: NetBIOS name: AD, NetBIOS user: <unknown>, NetBIOS MAC: 46:05:16:50:86:02 (unknown)
| smb2-time:
| date: 2022-10-02T06:37:33
|_ start_date: 2022-09-27T18:24:31
|_clock-skew: mean: 1h00m00s, deviation: 2h14m10s, median: 0s
| smb2-security-mode:
| 2.1:
|_   Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sun Oct 2 01:38:47 2022 -- 2 IP addresses (2 hosts up) scanned in 281.50 seconds

5.3.1.2 **Resultados de OpenVAS**

Tabla 16. AD - Resultados OpenVAS

Vulnerabilidad	Severidad	Puerto
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	443/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	443/tcp
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	135/tcp
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	3389/tcp
SSL/TLS: Certificate Expired	5.0 (Medium)	443/tcp
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	443/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	3389/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	443/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	443/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	443/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	3389/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4 (Low)	443/tcp

TCP timestamps	2.6 (Low)	general/tcp

Fuente: Elaboración Propia

5.3.1.3 **Resultados de NESSUS**

Tabla 17. AD - Resultados NESSUS

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.9	136507	KB4556843: Windows 7 and Windows Server 2008 R2 May 2020 Security Update
CRITICAL	9.9	149392	KB5003233: Windows 7 and Windows Server 2008 R2 Security Update (May 2021)
CRITICAL	9.8	142683	KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update
CRITICAL	9.8	144877	KB4598289: Windows 7 and Windows Server 2008 R2 January 2021 Security Update
CRITICAL	9.8	147231	KB5000851: Windows 7 and Windows Server 2008 R2 March 2021 Security Update
CRITICAL	9.8	150368	KB5003694: Windows 7 and Windows Server 2008 R2 Security Update (June 2021)
CRITICAL	9.8	151611	KB5004307: Windows 7 and Windows Server 2008 R2 Security Update (July 2021)
CRITICAL	9.8	152436	KB5005089: Windows 7 and Windows Server 2008 R2 Security Update (August 2021)
CRITICAL	9.8	153379	KB5005615: Windows 7 and Windows Server 2008 R2 September 2021 Security Update
CRITICAL	9.8	156069	KB5008282: Windows 7 and Windows Server 2008 R2 Security Update (December 2021)
CRITICAL	9.8	159672	KB5012649: Windows 7 and Windows Server 2008 R2 Security Update (April 2022)
CRITICAL	9.8	160937	KB5013999: Windows 7 and Windows Server 2008 R2 Security Update (May 2022)
CRITICAL	9.8	163952	KB5016679: Windows 7 and Windows Server 2008 R2 Security Update (August 2022)
CRITICAL	9.8	165002	KB5017373: Windows Server 2008 R2 Security Update (September 2022)
CRITICAL	9.8	94017	MS16-120: Security Update for Microsoft Graphics Component (3192884)
CRITICAL	9.8	58134	Microsoft Silverlight Unsupported Version Detection (Windows)

CRITICAL	9.8	134942	Microsoft Windows Type 1 Font Parsing Remote Code Execution Vulnerability (ADV200006)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	101367	Windows 7 and Windows Server 2008 R2 July 2017 Security Updates
CRITICAL	10.0	139491	KB4571719: Windows 7 and Windows Server 2008 R2 August 2020 Security Update
CRITICAL	10.0	146342	KB4601363: Windows 7 and Windows Server 2008 R2 February 2021 Security Update
CRITICAL	10.0	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	122615	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	8.8	100767	KB4023307: Security Update for the Windows Uniscribe Remote Code Execution Vulnerability for Microsoft Silverlight 5 (June 2017)
HIGH	8.8	134864	KB4537813: Windows 7 and Windows Server 2008 R2 February 2020 Security Update
HIGH	8.8	134865	KB4541500: Windows 7 and Windows Server 2008 R2 March 2020 Security Update
HIGH	8.8	135472	KB4550965: Windows 7 and Windows Server 2008 R2 April 2020 Security Update
HIGH	8.8	137260	KB4561669: Windows 7 and Windows Server 2008 R2 June 2020 Security Update
HIGH	8.8	138460	KB4565539: Windows 7 and Windows Server 2008 R2 July 2020 Security Update
HIGH	8.8	140422	KB4577053: Windows 7 and Windows Server 2008 R2 September 2020 Security Update
HIGH	8.8	141431	KB4580387: Windows 7 and Windows Server 2008 R2 October 2020 Security Update
HIGH	8.8	148466	KB5001335: Windows 7 and Windows Server 2008 R2 Security Update (Apr 2021)
HIGH	8.8	151476	KB5004951: Windows 7 and Windows Server 2008 R2 OOB Security Update RCE (July 2021)
HIGH	8.8	154984	KB5007233: Windows 7 and Windows Server 2008 R2 Security Update (November 2021)
HIGH	8.8	156627	KB5009621: Windows 7 and Windows Server 2008 R2 Security Update (January 2022)
HIGH	8.8	158718	KB5011529: Windows 7 and Windows Server 2008 R2 (March 2022) Security Update
HIGH	8.8	162191	KB5014742: Windows 7 and Windows Server 2008 R2 Security Update (June 2022)

HIGH	8.8	163050	KB5015862: Windows 7 and Windows Server 2008 R2 Security Update (July 2022)
HIGH	8.8	87880	MS16-006: Security Update for Silverlight to Address Remote Code Execution (3126036)
HIGH	8.8	93468	MS16-109: Security Update for Silverlight (3182373)
HIGH	8.8	135475	Security Updates for Internet Explorer (April 2020)
HIGH	8.8	152432	Security Updates for Internet Explorer (August 2021)
HIGH	8.8	151597	Security Updates for Internet Explorer (July 2021)
HIGH	8.8	152587	Security Updates for Internet Explorer (June 2021)
HIGH	8.8	154032	Security Updates for Internet Explorer (October 2021)
HIGH	8.8	140428	Security Updates for Internet Explorer (September 2020)
HIGH	8.8	164090	Security Updates for Microsoft Visual Studio Products (August 2022)
HIGH	8.8	158715	Security Updates for Microsoft Visual Studio Products (March 2022)
HIGH	8.8	149436	Security Updates for Microsoft Visual Studio Products (May 2021)
HIGH	8.6	154344	Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)
HIGH	7.8	91230	7-Zip < 16.00 Multiple Vulnerabilities
HIGH	7.8	109800	7-Zip < 18.00 Multiple Vulnerabilities
HIGH	7.8	109730	7-Zip < 18.05 Memory Corruption Arbitrary Code Execution
HIGH	7.8	143572	KB4592503: Windows 7 and Windows Server 2008 R2 December 2020 Security Update
HIGH	7.8	154035	KB5006728: Windows 7 and Windows Server 2008 R2 Security Update (October 2021)
HIGH	7.8	157427	KB5010422: Windows 7 and Windows Server 2008 R2 Security Update (February 2022)
HIGH	7.8	97794	MS17-013: Security Update for Microsoft Graphics Component (4013075)
HIGH	7.8	63155	Microsoft Windows Unquoted Service Path Enumeration
HIGH	7.8	153374	Security Updates for Internet Explorer (September 2021)

HIGH	7.8	139598	Security Updates for Microsoft .NET Framework (August 2020)
HIGH	7.8	159733	Security Updates for Microsoft Visual Studio Products (April 2022)
HIGH	7.8	156194	Security Updates for Microsoft Visual Studio Products (December 2021)
HIGH	7.8	162317	Security Updates for Microsoft Visual Studio Products (June 2022)
HIGH	7.8	161118	Security Updates for Microsoft Visual Studio Products (May 2022)
HIGH	7.8	155018	Security Updates for Microsoft Visual Studio Products (November 2021)
HIGH	7.8	153428	Security Updates for Microsoft Visual Studio Products (September 2021)
HIGH	7.5	109799	7-Zip < 16.03 NULL Pointer Dereference DoS
HIGH	7.5	152020	Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU)
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	139498	Security Updates for Internet Explorer (August 2020)
HIGH	7.5	138467	Security Updates for Internet Explorer (July 2020)
HIGH	7.5	137266	Security Updates for Internet Explorer (June 2020)
HIGH	7.5	147228	Security Updates for Internet Explorer (March 2021)
HIGH	7.5	136512	Security Updates for Internet Explorer (May 2020)
HIGH	7.5	149386	Security Updates for Internet Explorer (May 2021)
HIGH	7.5	142691	Security Updates for Internet Explorer (November 2020)
HIGH	7.5	104896	Security Updates for Internet Explorer (September 2017)
HIGH	7.5	157841	Security Updates for Microsoft Visual Studio Products (February 2022)
HIGH	7.5	150418	Security Updates for Microsoft Visual Studio Products (June 2021)
HIGH	7.5	165107	Security Updates for Microsoft Visual Studio Products (Sep 2022)

HIGH	7.4	154051	Security Updates for Microsoft Visual Studio Products (October 2021)
HIGH	9.3*	48762	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
HIGH	9.3*	65211	MS13-022: Vulnerability in Microsoft Silverlight Could Allow Remote Code Execution (2814124)
HIGH	9.3*	67209	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (2861561)
HIGH	7.1*	72932	MS14-014: Vulnerability in Silverlight Could Allow Security Feature Bypass (2932677)
HIGH	9.0*	73984	MS14-025: Vulnerability in Group Policy Preferences Could Allow Elevation of Privilege (2962486)
HIGH	8.3*	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
HIGH	9.3*	83440	MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)
HIGH	9.3*	83354	MS15-049: Vulnerability in Silverlight Could Allow Elevation of Privilege (3058985)
HIGH	9.3*	85348	MS15-080 : Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)
HIGH	9.3*	87257	MS15-128: Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)
HIGH	9.3*	87258	MS15-129: Security Update for Silverlight to Address Remote Code Execution (3106614)
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	99289	KB4017094: Security Update for the libjpeg Information Disclosure Vulnerability for Microsoft Silverlight 5 (April 2017)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	57582	SSL Self-Signed Certificate
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	6.5	132101	Windows Speculative Execution Configuration Check
MEDIUM	5.9	148960	Oracle Java SE 1.7.0_301 / 1.8.0_291 / 1.11.0_11 / 1.16.0_1 Multiple Vulnerabilities (Apr 2021 CPU)

MEDIUM	5.9	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.5	152423	Security Updates for Microsoft Visual Studio Products (August 2021)
MEDIUM	5.3	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	156887	Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (January 2022 CPU)
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3*	78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)
MEDIUM	4.3*	70339	MS13-087: Vulnerability in Silverlight Could Allow Information Disclosure (2890788)
LOW	3.7	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.3	140501	Security Updates for Microsoft .NET Framework (September 2020)
LOW	3.1	134204	MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (3125869)
LOW	3.3*	10663	DHCP Server Detection

Fuente: Elaboración Propia

5.3.2 TS

5.3.2.1 **Resultados de escaneo con Nmap.**

Comando:

sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn XXXX -oN TS.txt

Resultado:

Nmap 7.92 scan initiated Sun Oct 2 01:56:15 2022 as: nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN TS.txt XXXX
Nmap scan report for XXXX
Host is up, received arp-response (0.00090s latency).
Scanned at 2022-10-02 01:56:15 -05 for 12s
Not shown: 59354 closed tcp ports (reset), 6160 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack ttl 128
135/tcp	open	msrpc	syn-ack ttl 128
139/tcp	open	netbios-ssn	syn-ack ttl 128
443/tcp	open	https	syn-ack ttl 128
445/tcp	open	microsoft-ds	syn-ack ttl 128
593/tcp	open	http-rpc-epmap	syn-ack ttl 128
3388/tcp	open	cbserver	syn-ack ttl 128
3389/tcp	open	ms-wbt-server	syn-ack ttl 128
5357/tcp	open	wsdapi	syn-ack ttl 128
5504/tcp	open	fcp-cics-gw1	syn-ack ttl 128
5800/tcp	open	vnc-http	syn-ack ttl 128
5900/tcp	open	vnc	syn-ack ttl 128
5985/tcp	open	wsman	syn-ack ttl 128
10050/tcp	open	XXXX	syn-ack ttl 128
49153/tcp	open	unknown	syn-ack ttl 128
49155/tcp	open	unknown	syn-ack ttl 128
49186/tcp	open	unknown	syn-ack ttl 128
58537/tcp	open	unknown	syn-ack ttl 128
58559/tcp	open	unknown	syn-ack ttl 128
58615/tcp	open	unknown	syn-ack ttl 128
58757/tcp	open	unknown	syn-ack ttl 128

MAC Address: 76:F7:F0:DE:07:79 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done at Sun Oct 2 01:56:27 2022 -- 1 IP address (1 host up) scanned in 12.25 second

Comando:

sudo nmap -sCV -p80,135,139,443,445,593,3388,3389,5357,5504,5800,5900,5985,10050,49153,49155,49186,58537,58559,58615,58757 -oN TS2.txt XXXX

Resultado:

```
# Nmap 7.92 scan initiated Sun Oct  2 02:03:49 2022 as: nmap -sCV -p80,135,139,443,445,593,3388,3389,5357,5504,5800,5900,5985,10050,49153,49155,49186,58537,58559,58615,58757 -oN TS2.txt XXXX
Nmap scan report for XXXX
Host is up (0.0017s latency).

PORT      STATE SERVICE           VERSION
80/tcp    open  http              Microsoft IIS httpd 8.5
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
443/tcp   open  ssl/http          Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_ssl-date: 2022-10-02T07:05:01+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=4.ECODIESELCOLOMBIAS.A
| Subject Alternative Name: DNS:4.ECODIESELCOLOMBIAS.A
| Not valid before: 2022-09-04T21:41:30
|_Not valid after:  2023-09-04T22:01:30
445/tcp   open  microsoft-ds      Windows Server 2012 R2 Standard 9600 microsoft-ds
593/tcp   open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
3388/tcp  open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=1.ECODIESELCOLOMBIAS.A
| Subject Alternative Name: DNS:1.ECODIESELCOLOMBIAS.A
| Not valid before: 2022-09-04T21:38:09
|_Not valid after:  2023-09-04T21:58:09
|_ssl-date: 2022-10-02T07:05:01+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: XXXX
|   NetBIOS_Domain_Name: XXXX
|   NetBIOS_Computer_Name: TS
|   DNS_Domain_Name: XXXX.wan
|   DNS_Computer_Name: TS.XXXX.wan
```

```
|   DNS_Tree_Name: XXXX.wan
|   Product_Version: 6.3.9600
|_  System_Time: 2022-10-02T07:04:56+00:00
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5504/tcp  open  msrpc           Microsoft Windows RPC
5800/tcp  open  vnc-http        TightVNC (user: TS; VNC TCP port: 5900)
|_http-title: TightVNC desktop [TS]
5900/tcp  open  vnc             VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication (2)
|     Tight (16)
|   Tight auth subtypes:
|_    STDV VNCAUTH_ (2)
5985/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
10050/tcp open  tcpwrapped
49153/tcp open  msrpc           Microsoft Windows RPC
49155/tcp open  msrpc           Microsoft Windows RPC
49186/tcp open  msrpc           Microsoft Windows RPC
58537/tcp open  msrpc           Microsoft Windows RPC
58559/tcp open  msrpc           Microsoft Windows RPC
58615/tcp open  msrpc           Microsoft Windows RPC
58757/tcp open  msrpc           Microsoft Windows RPC
MAC Address: 76:F7:F0:DE:07:79 (Unknown)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled and required
|_clock-skew: mean: 50m00s, deviation: 2h02m28s, median: 0s
|_nbstat: NetBIOS name: TS, NetBIOS user: <unknown>, NetBIOS MAC:
76:f7:f0:de:07:79 (unknown)
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2
Standard 6.3)
|   OS CPE: cpe:/o:microsoft:windows_server_2012::-
|   Computer name: TS
|   NetBIOS computer name: TS\x00
```

| Domain name: XXXX.wan
| Forest name: XXXX.wan
| FQDN: TS.XXXX.wan
|_ System time: 2022-10-02T02:04:55-05:00
| smb2-time:
| date: 2022-10-02T07:04:56
|_ start_date: 2022-09-29T16:37:55
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done at Sun Oct 2 02:05:07 2022 -- 1 IP address (1 host up) scanned in 78.64 seconds

5.3.2.2 **Resultados de OpenVAS**

Tabla 18. TS - Resultados OpenVAS

Vulnerabilidad	**Severidad**	**Puerto**
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	443/tcp
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	443/tcp
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	3389/tcp
SSL/TLS: Report Weak Cipher Suites	5.0 (Medium)	443/tcp
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	135/tcp
VNC Server Unencrypted Data Transmission	4.8 (Medium)	5900/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	3389/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)	443/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	443/tcp
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4 (Low)	443/tcp
TCP timestamps	2.6 (Low)	general/tcp

Fuente: Elaboración Propia

5.3.2.3 **Resultados de NESSUS**

Tabla 19. TS - Resultados NESSUS

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	156860	Apache Log4j 1.x Multiple Vulnerabilities
CRITICAL	9.8	157229	Foxit PDF Reader < 11.2.1 Multiple Vulnerabilities
CRITICAL	9.8	141217	Foxit Reader < 10.1 Multiple Vulnerabilities
CRITICAL	9.8	135849	Foxit Reader < 9.7.2 Multiple Vulnerabilities
CRITICAL	9.8	165005	KB5017365: Windows Server 2012 R2 Security Update (September 2022)
CRITICAL	9.8	58134	Microsoft Silverlight Unsupported Version Detection (Windows)
CRITICAL	9.8	130011	Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows)
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.8	147946	Security Update for .NET Core (March 2021)
CRITICAL	9.0	156057	Apache Log4j 2.x < 2.16.0 RCE
CRITICAL	9.0	124198	Oracle Java SE 1.7.0_221 / 1.8.0_211 / 1.11.0_3 / 1.12.0_1 Multiple Vulnerabilities (Apr 2019 CPU)
CRITICAL	10.0	156002	Apache Log4j < 2.15.0 Remote Code Execution (Windows)
CRITICAL	10.0	156032	Apache Log4j Unsupported Version Detection
CRITICAL	10.0	62758	Microsoft XML Parser (MSXML) and XML Core Services Unsupported
HIGH	8.8	152161	Foxit Reader < 11.0.1 Multiple Vulnerabilities
HIGH	8.8	158744	Security Updates for Microsoft .NET core (March 2022)
HIGH	8.8	138473	Security Updates for Microsoft Visual Studio Products (July 2020)
HIGH	8.8	158715	Security Updates for Microsoft Visual Studio Products (March 2022)
HIGH	8.8	149436	Security Updates for Microsoft Visual Studio Products (May 2021)
HIGH	8.6	154344	Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU)
HIGH	8.4	65057	Insecure Windows Service Permissions
HIGH	8.3	135592	Oracle Java SE 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1 Multiple Vulnerabilities (Apr 2020 CPU)
HIGH	8.3	138522	Oracle Java SE 1.7.0_271 / 1.8.0_261 / 1.11.0_8 / 1.14.0_2 Multiple Vulnerabilities (Jul 2020 CPU)

HIGH	8.1	132992	Oracle Java SE 1.7.0_251 / 1.8.0_241 / 1.11.0_6 / 1.13.0_2 Multiple Vulnerabilities (Jan 2020 CPU)
HIGH	7.8	154004	Foxit PDF Reader < 11.1 Multiple Vulnerabilities
HIGH	7.8	160718	Foxit PDF Reader < 11.2.2 Multiple Vulnerabilities
HIGH	7.8	63155	Microsoft Windows Unquoted Service Path Enumeration
HIGH	7.8	138465	Security Update for .NET Core (July 2020)
HIGH	7.8	156227	Security Updates for Microsoft ASP.NET Core (December 2021)
HIGH	7.8	148552	Security Updates for Microsoft Visual Studio Products (April 2021)
HIGH	7.8	143573	Security Updates for Microsoft Visual Studio Products (December 2020)
HIGH	7.8	156194	Security Updates for Microsoft Visual Studio Products (December 2021)
HIGH	7.8	146426	Security Updates for Microsoft Visual Studio Products (February 2021)
HIGH	7.8	144977	Security Updates for Microsoft Visual Studio Products (January 2021)
HIGH	7.8	155018	Security Updates for Microsoft Visual Studio Products (November 2021)
HIGH	7.8	140465	Security Updates for Microsoft Visual Studio Products (September 2020)
HIGH	7.8	153428	Security Updates for Microsoft Visual Studio Products (September 2021)
HIGH	7.5	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
HIGH	7.5	163575	Foxit PDF Reader < 12.0.1 Multiple Vulnerabilities
HIGH	7.5	152020	Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU)
HIGH	7.5	161241	Oracle Java SE Multiple Vulnerabilities (April 2022 CPU)
HIGH	7.5	163304	Oracle Java SE Multiple Vulnerabilities (July 2022 CPU)
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	152488	Security Update for .NET Core (August 2021)
HIGH	7.5	145041	Security Update for .NET Core (January 2021)
HIGH	7.5	139496	Security Update for Microsoft ASP.NET Core (DoS) (August 2020)
HIGH	7.5	145040	Security Update for Microsoft ASP.NET Core (January 2021)
HIGH	7.5	140425	Security Update for Microsoft ASP.NET Core (September 2020)

HIGH	7.5	104896	Security Updates for Internet Explorer (September 2017)
HIGH	7.5	165077	Security Updates for Microsoft .NET Core (September 2022)
HIGH	7.5	161167	Security Updates for Microsoft .NET core (May 2022)
HIGH	7.5	165076	Security Updates for Microsoft ASP.NET Core (September 2022)
HIGH	7.5	139506	Security Updates for Microsoft Visual Studio Products (August 2020)
HIGH	7.5	157841	Security Updates for Microsoft Visual Studio Products (February 2022)
HIGH	7.5	150418	Security Updates for Microsoft Visual Studio Products (June 2021)
HIGH	7.5	147749	Security Updates for Microsoft Visual Studio Products (March 2021)
HIGH	7.4	154051	Security Updates for Microsoft Visual Studio Products (October 2021)
HIGH	8.3*	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.6	156327	Apache Log4j 2.0 < 2.3.2 / 2.4 < 2.12.4 / 2.13 < 2.17.1 RCE
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	57582	SSL Self-Signed Certificate
MEDIUM	6.5	146328	Security Update for .NET Core (February 2021)
MEDIUM	6.5	150708	Security Update for .NET Core (June 2021)
MEDIUM	6.5	146344	Security Update for Microsoft ASP.NET Core (February 2021)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	6.5	132101	Windows Speculative Execution Configuration Check
MEDIUM	5.9	156183	Apache Log4j 2.x < 2.17.0 DoS
MEDIUM	5.9	148960	Oracle Java SE 1.7.0_301 / 1.8.0_291 / 1.11.0_11 / 1.16.0_1 Multiple Vulnerabilities (Apr 2021 CPU)
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.9	163974	Security Updates for Microsoft .NET Core (August 2022)
MEDIUM	5.5	152528	Security Update for Microsoft ASP.NET Core (August 2021)
MEDIUM	5.5	162314	Security Updates for Microsoft .NET core (June 2022)
MEDIUM	5.5	152423	Security Updates for Microsoft Visual Studio Products (August 2021)

MEDIUM	5.5	142694	Security Updates for Microsoft Visual Studio Products (November 2020)
MEDIUM	5.3	126821	Oracle Java SE 1.7.0_231 / 1.8.0_221 / 1.11.0_4 / 1.12.0_2 Multiple Vulnerabilities (Jul 2019 CPU)
MEDIUM	5.3	141800	Oracle Java SE 1.7.0_281 / 1.8.0_271 / 1.11.0_9 / 1.15.0_1 Multiple Vulnerabilities (Oct 2020 CPU)
MEDIUM	5.3	145218	Oracle Java SE 1.7.0_291 / 1.8.0_281 / 1.11.0_10 / 1.15.0_2 Information Disclosure (Windows Jan 2021 CPU)
MEDIUM	5.3	156887	Oracle Java SE 1.7.0_331 / 1.8.0_321 / 1.11.0_14 / 1.17.0_2 Multiple Vulnerabilities (January 2022 CPU)
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3*	78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)
LOW	3.7	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.3	164808	Foxit PDF Reader < 12.0 Multiple Vulnerabilities
LOW	3.1	134204	MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (3125869)

Fuente: Elaboración Propia

5.3.3 SAP

5.3.3.1 **Resultados de escaneo con Nmap:**

Comando:

sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn XXXX -oN SAP1.txt

Resultado:

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.

Starting Nmap 7.92 (https://nmap.org) at 2022-10-02 02:10 -05

Initiating ARP Ping Scan at 02:10

Scanning XXXX [1 port]

Completed ARP Ping Scan at 02:10, 0.05s elapsed (1 total hosts)

Initiating SYN Stealth Scan at 02:10

Scanning XXXX [65535 ports]

Discovered open port 445/tcp on XXXX

Discovered open port 80/tcp on XXXX

Discovered open port 8080/tcp on XXXX

Discovered open port 139/tcp on XXXX

Discovered open port 135/tcp on XXXX

Discovered open port 3389/tcp on XXXX

Discovered open port 30001/tcp on XXXX

Discovered open port 40000/tcp on XXXX

Discovered open port 5357/tcp on XXXX

Discovered open port 30000/tcp on XXXX

Discovered open port 49154/tcp on XXXX

Discovered open port 5985/tcp on XXXX

Discovered open port 49156/tcp on XXXX

Discovered open port 10050/tcp on XXXX

Discovered open port 1433/tcp on XXXX

Discovered open port 2701/tcp on XXXX

Discovered open port 8443/tcp on XXXX

Completed SYN Stealth Scan at 02:10, 11.89s elapsed (65535 total ports)

Nmap scan report for XXXX

Host is up, received arp-response (0.0033s latency).

Scanned at 2022-10-02 02:10:03 -05 for 12s

Not shown: 58549 closed tcp ports (reset), 6969 filtered tcp ports (no-response)

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

```
PORT      STATE SERVICE        REASON
80/tcp    open  http           syn-ack ttl 128
135/tcp   open  msrpc          syn-ack ttl 128
139/tcp   open  netbios-ssn    syn-ack ttl 128
445/tcp   open  microsoft-ds   syn-ack ttl 128
1433/tcp  open  ms-sql-s       syn-ack ttl 128
2701/tcp  open  sms-rcinfo     syn-ack ttl 128
3389/tcp  open  ms-wbt-server  syn-ack ttl 128
5357/tcp  open  wsdapi         syn-ack ttl 128
5985/tcp  open  wsman          syn-ack ttl 128
8080/tcp  open  http-proxy     syn-ack ttl 128
8443/tcp  open  https-alt      syn-ack ttl 128
10050/tcp open  XXXX   syn-ack ttl 128
30000/tcp open  ndmps          syn-ack ttl 128
30001/tcp open  pago-services1 syn-ack ttl 128
40000/tcp open  safetynetp     syn-ack ttl 128
49154/tcp open  unknown        syn-ack ttl 128
49156/tcp open  unknown        syn-ack ttl 128
MAC Address: 2E:B8:ED:B5:00:CC (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.15 seconds
        Raw packets sent: 83423 (3.671MB) | Rcvd: 58567 (2.343MB)
```

Comando:

sudo nmap -sCV -p80,135,139,445,1433,2701,3389,5357,5985,8080,8443,10050,30000,30001,40000,49154,49156 XXXX -oN SAP2.txt

Resultado:

Nmap 7.92 scan initiated Sun Oct 2 02:14:39 2022 as: nmap -sCV -p80,135,139,445,1433,2701,3389,5357,5985,8080,8443,10050,30000,30001,40000,49154,49156 -vvv -oN SAP2.txt XXXX

Nmap scan report for XXXX

Host is up, received arp-response (0.0014s latency).

Scanned at 2022-10-02 02:14:40 -05 for 71s

PORT STATE SERVICE REASON VERSION

80/tcp open http syn-ack ttl 128 Microsoft IIS httpd 8.5

| http-methods:

| Supported Methods: OPTIONS TRACE GET HEAD POST

|_ Potentially risky methods: TRACE

|_http-title: IIS Windows Server

|_http-server-header: Microsoft-IIS/8.5

135/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

139/tcp open netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn

445/tcp open microsoft-ds syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

1433/tcp open ms-sql-s syn-ack ttl 128 Microsoft SQL Server 2012 11.00.7507.00; SP4+

| ms-sql-ntlm-info:

| Target_Name: XXXX

| NetBIOS_Domain_Name: XXXX

| NetBIOS_Computer_Name: SAP

| DNS_Domain_Name: XXXX.wan

| DNS_Computer_Name: SAP.XXXX.wan

| DNS_Tree_Name: XXXX.wan

|_ Product_Version: 6.3.9600

| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback

| Issuer: commonName=SSL_Self_Signed_Fallback

| Public Key type: rsa

| Public Key bits: 1024

| Signature Algorithm: sha1WithRSAEncryption

| Not valid before: 2022-09-27T18:35:04

| Not valid after: 2052-09-27T18:35:04

| MD5: 5c88 97ab 7891 dff5 7ae5 a8c3 8552 222a

| SHA-1: efb2 63ea e828 43ff f242 7d60 2353 8d1b d870 6c24

| -----BEGIN CERTIFICATE-----

|
MIIB+zCCAWSgAwIBAgIQPCyA7XhblodGTM9KYfOZJzANBgkqhkiG9w0BAQUFADA7

|
MTkwNwYDVQQDHjAAUwBTAEwAXwBTAGUAbABmAF8AUwBpAGcAbgBlAGQAXwBGAGEA

|
bABsAGIAYQBjAGswIBcNMjIwOTI3MTgzNTA0WhgPMjA1MjA5MjcxODM1MDRaMDsx

|
OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGU
AZABfAEYAYQBs

|
AGwAYgBhAGMAazCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtu
sGAfUx+e+D

|
cmcXtfSRktcwjGRFhesLpHvZ27uIO+T8DIFpNg4XhJOPmTWI5T6DBgK0Yg
hHaPjh

|
d0CZug4LCtgdlm3xcQ9yjH7pXZmiF7laMc8ruyOPIg1egshhydwnPwTzn+DO
5+yl

|
luWFLFUFUz+cEuL1vMpRpDWRzrJ2xTkCAwEAATANBgkqhkiG9w0BAQU
FAAOBgQAj

|
kQ5TfmYNQ5MkYsvd9iwen3aumlbVuPlMGdY15arclDTtPopNFxJG7vYrWm
l2SNOK

|
hlNGA31pzZBiTHdWlz0vR554f6XeUqbdMtVt+A9GJfBHh13/InpwWKN7DW
wuWNg3

| dHJ0DCssRo93UeRuj6mNdkSAZYdzMNj1YdyRU+Chfg==

|_-----END CERTIFICATE-----

|_ssl-date: 2022-10-02T07:15:52+00:00; +1s from scanner time.

2701/tcp open cmrcservice syn-ack ttl 128 Microsoft Configuration Manager Remote Control service (CmRcService.exe)

3389/tcp open ssl/ms-wbt-server? syn-ack ttl 128

| ssl-cert: Subject: commonName=SAP.XXXX.wan

| Issuer: commonName=SAP.XXXX.wan

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2022-07-02T22:30:41

| Not valid after: 2023-01-01T22:30:41

| MD5:   2151 c3f0 6e50 fbef a4ac 27b1 dc88 2613

| SHA-1: 3614 f7f2 c3dc 3a65 a719 c403 a7b6 baba c9d1 d662

| -----BEGIN CERTIFICATE-----

| MIIC8DCCAdigAwIBAgIQVjIiUqCOIKBP9ZLJiKPbEzANBgkqhkiG9w0BAQsFADAh

| MR8wHQYDVQQDExZTRVJWSVNBUC5yZWRwcm9waWEud2FuMB4XDTIyMDcwMjIyMzA0

| MVoXDTIzMDEwMTIyMzA0MVowITEfMB0GA1UEAxMWU0VSVklTQVAucmVkcHJvcGlh

| LndhbjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKqePEcCVtCe3Suw

| mNhfL+C8eCQRV/7Ug8E0qyrvEp0yrfRo+Fj5iIyhATLy/Tm8EuiuF1Ac70fH0ncH

| bMyPWlgTXEbLjz9ntiY3cBSMqtzU1GIu/+5JzzoyqgXKoFNtQF+ex1h5HZQe8fjK

| 4aimWri8jOUfMsFXWd9X1EMh9GN+C9MtyBvD6hh0/2THR0GJi3BnPR2h87kVkGFK

|
0BZnRGppt2A1glzGDZ1gzcyCzU/JdjWT6edpOqXP95AfKoERwt2IxII6qyTvq
uC6

|
tqqTsYIM2ZVIQ2wIfRvVpPYglDPRGDikhVMz63+/LEQvd9fcg7P5MT+/mJz0
XOUX

|
Whr6wYcCAwEAAaMkMCIwEwYDVR0lBAwwCgYIKwYBBQUHAwEwCwY
DVR0PBAQDAgQw

|
MA0GCSqGSIb3DQEBCwUAA4IBAQCPDTkn8a5TnUBvw+Td3vRIaOGoI8
BqJkN7cJp0

|
0kOGEGag+KPhJN9w5hn5Y8KPU748AsWwbn19hUzYb2JUJ9EjeIAqd1ST
X6AQoZTy

|
oDid2wg8iUopQ38uMBuMNf31wt/gI6RsZE1Otg//y37Mqak2z7GjQPbQVZsG
3d+v

|
/xG8dKj9TiH6iMPO4IJ+eFDjCkt0jL8qXELXbzs9ChWkAnAsSu98F97pTyYO
y5l+

|
04GrxU/l1sIrYLi0GkeK6AunmfX4nFGj6gpJkgABBnv8oPMKR5sf3cfLbus1Y
Hac

| ikTBERUfDSwR//7Z2E9stqLFHu4E/jCMd9B6PWil7T/7xFel

|_-----END CERTIFICATE-----

|_ssl-date: 2022-10-02T07:15:52+00:00; +1s from scanner time.

5357/tcp open http syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Service Unavailable

5985/tcp open http syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|_http-title: Not Found

|_http-server-header: Microsoft-HTTPAPI/2.0

8080/tcp open http syn-ack ttl 128 Apache Tomcat 8.5.41

|_http-favicon: Apache Tomcat

| http-methods:

| Supported Methods: GET HEAD POST PUT DELETE OPTIONS

|_ Potentially risky methods: PUT DELETE

|_http-open-proxy: Proxy might be redirecting requests

|_http-title: Site doesn't have a title (text/html).

|_http-server-header: <empty>

8443/tcp open ssl/https-alt syn-ack ttl 128

|_http-title: Site doesn't have a title (text/plain;charset=ISO-8859-1).

|_ssl-date: 2022-10-02T07:15:52+00:00; +1s from scanner time.

| ssl-cert: Subject: commonName=SAP

| Issuer: commonName=SAP

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2014-09-24T15:21:43

| Not valid after: 2024-09-21T15:21:43

| MD5: 641e 6e3f a507 340a 4209 1fec e970 0099

| SHA-1: 9c79 e5d2 cf61 9a75 7c74 65fd 63ec 4157 3a52 a0bb

| -----BEGIN CERTIFICATE-----

|
MIICxTCCAa2gAwIBAgIEbwaNlTANBgkqhkiG9w0BAQsFADATMREwDwY
DVQQDEwhT

|
RVJWSVNBUDAeFw0xNDA5MjQxNTIxNDNaFw0yNDA5MjExNTIxNDNaM
BMxETAPBgNV

|
BAMTCFNFUlZJU0FQMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK
CAQEAgW6Y

|
mowgSqU2lUk3V5yEXHOa+2P9u9ylNp0DQwdhudTS+E9Fh93x8SrDStf4x5
rgL/jF

|
/ASAr7pOLdDTJcVzE8d/iOQek8wleifrCkWdMvd8N8+AB0SYpSCsPJHcGY
vziZm2

|
Fa4Q6K4TiPUd8wSJK1YFEvlqmbfBgZq+qavCl2Vpt18wU6aDExgvXpE9/b0
LrFqG

|
iHDjZ8Uv93whQ5mmbnm8RAgE19YjU1O6YvT/9hkTB50lDjWzC1P7uzmrQ
58OmPqf

|
drcT34y8QVDOaBNLyuEYusi6ZbhZj2mglWBDQORP2k8uDwnR8rzjY7VQw
6nsLOaK

|
xy5+hpueGqJwB2SupQIDAQABoyEwHzAdBgNVHQ4EFgQUEYC5kty1nD
mF2RuUvb7C

|
DvPTJqowDQYJKoZIhvcNAQELBQADggEBAEr1nYjMMtAXyOqGa9e1nbV
MNT+YOhQ7

|
PnDDu3k5adN57U3/KEVJ8BlHhS7CZtF6HRbIshohTdjHbOFI6UTmuWk8WRRoK4dq

|
qX+Jwk3mTZeQ5ge0Ae8RXn/Y2anJlMmfUma7swBa/fSfWnA1JtFuOjEVHToHdYYR

|
I6F0YyKcQeoIO4EdmKgcwCCedag5onYPOrj+vJBRiPruQkgwJcbCEqS9Cfaiw3TU

|
O70GCv+Z/jmfssANXXt7wS4tTvV7G5pVf6tnwujYFyxx34xR9Rz6NJA4vwiS54rD

| XAsfJBYo+92Wx9vT1y/Uk6FIwW6VMPmii8JBfkpnNdb98zXBJ5OdrGg=

|_-----END CERTIFICATE-----

10050/tcp open tcpwrapped   syn-ack ttl 128

30000/tcp open giop   syn-ack ttl 128 omg.org CORBA naming service

|_giop-info: ERROR: Script execution failed (use -d to debug)

30001/tcp open giop   syn-ack ttl 128 omg.org CORBA naming service

|_giop-info: ERROR: Script execution failed (use -d to debug)

40000/tcp open ssl/http   syn-ack ttl 128 Apache Tomcat 8.5.41

|_http-title: HTTP Status 404 \xE2\x80\x93 Not Found

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=Administrator/organizationName=SAP/countryName=CN/organizationalUnitName=B1

| Issuer:
commonName=Administrator/organizationName=SAP/countryName=CN/organizationalUnitName=B1

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2021-05-25T13:57:17

| Not valid after: 2031-05-23T13:57:17

| MD5: 65e4 0768 39c1 8ee8 85a8 886f 0bd3 9ab5

| SHA-1: e13f e868 ab95 d7c5 78ff 3eff 0586 8ebd 8961 631f

| -----BEGIN CERTIFICATE-----

|
MIIDHzCCAgegAwIBAgIEC7mNmDANBgkqhkiG9w0BAQsFADBAMQswCQYDVQQGEwJD

|
TjEMMAoGA1UEChMDU0FQMQswCQYDVQQLEwJCMTEWMBQGA1UEAxMNQWRtaW5pc3Ry

|
YXRvcjAeFw0yMTA1MjUxMzU3MTdaFw0zMTA1MjMxMzU3MTdaMEAxCzAJBgNVBAYT

|
AkNOMQwwCgYDVQQKEwNTQVAxCzAJBgNVBAsTAkIxMRYwFAYDVQQDEw1BZG1pbmlz

|
dHJhdG9yMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlBdHlBuLEA8J

|
uUQi7SYhodACY36D1r5KSdQINk0Gbl5UJ1Y4a7jfmxzskpAp+d3MkNM9u/3Aax1n

|
QBcTeucjN0pgF4n0tFOkTyNWjFKPdn/N+7SNioqIzB1BmXVJKDQ2o9gNZ
GupoJkW

|
/VN0kRGgGGb5t4bX3fqeejqYONY2J4UBI+FYjd8uNK1htn/nIuK0VXO7gosY
Vfei

|
/dvPlWnC9fcKBXIw2Nu+Jcz22QrtoKV65pFHoLF06wXBD2p1VWSKJEoRH
4MUlTCn

|
09ypyjplLnfdSyrI0+QYSEzxx4/Wq1ByJA1zzjJT9Af8TSfFgWgJ9pn1GjvWHG
Sg

|
KWOV7ixuMwIDAQABoyEwHzAdBgNVHQ4EFgQUYS6WHbcdQMxGPI7P
MJfHBHx5gKYw

|
DQYJKoZIhvcNAQELBQADggEBAIEtdjCSV+Z1dBoLIWzl44YEVAdQ42Xc4
9Ei5ouK

|
U90SQKUGJQtxVgCUUplEie5QiDJ4cDJvstn1ZDNIUBg/xp7ApCu+zjzNI9JX
FIgj

|
BXhEaGPr/q8gaIgFsNnEbgGxHP1OG67kqVH557VEuxZgJiS6gj8BOD6YI/+
E20u8

|
mkHqMZ4GUOuCeA7A88vtgJ2URfNlMgFHBWvG41vAdq62NqG4zRwKqW
soNLe2Juh6

|
xjs76n+blNlEvmQpZqDf8Cw5rfsBpG3NagJbheBdPjCaMJz9JcAxQUBXLunI
Qucd

| +uV8oJK8YYdGWgu7LBmHFmIwpG69YapUC4v+kAEV3Ku1OfQ=

|_-----END CERTIFICATE-----

49154/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

49156/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC

MAC Address: 2E:B8:ED:B5:00:CC (Unknown)

Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:

| smb-security-mode:

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| ms-sql-info:

| XXXX:1433:

| Version:

| name: Microsoft SQL Server 2012 SP4+

| number: 11.00.7507.00

| Product: Microsoft SQL Server 2012

| Service pack level: SP4

| Post-SP patches applied: true

|_   TCP port: 1433

| smb2-security-mode:

| 3.0.2:

|_   Message signing enabled but not required

|_clock-skew: mean: 0s, deviation: 0s, median: 0s

| smb2-time:

| date: 2022-10-02T07:15:47

|_ start_date: 2022-09-27T18:25:59

| nbstat: NetBIOS name: SAP, NetBIOS user: <unknown>, NetBIOS MAC: 96:bd:06:ff:e9:32 (unknown)

| Names:

| SAP<00>   Flags: <unique><active>

| XXXX<00>   Flags: <group><active>

| SAP<20>   Flags: <unique><active>

| Statistics:

| 96 bd 06 ff e9 32 00 00 00 00 00 00 00 00 00 00

| 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

|_ 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

| p2p-conficker:

| Checking for Conficker.C or higher...

| Check 1 (port 59371/tcp): CLEAN (Couldn't connect)

| Check 2 (port 46807/tcp): CLEAN (Couldn't connect)

| Check 3 (port 30920/udp): CLEAN (Timeout)

| Check 4 (port 18447/udp): CLEAN (Failed to receive data)

|_ 0/4 checks are positive: Host is CLEAN or ports are blocked

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done at Sun Oct 2 02:15:51 2022 -- 1 IP address (1 host up) scanned in 72.30 seconds

5.3.3.2 **Resultados de OpenVAS**

Tabla 20. SAP - Resultados OpenVAS

Vulnerabilidad	Severidad	Puerto
Microsoft SQL Server End Of Life Detection	10.0	1433/tcp
Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)	9.8	8443/tcp
Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)	9.8	40000/tcp
Apache Tomcat Multiple Vulnerabilities - Feb20 (Windows)	9.8	8080/tcp
Apache Tomcat Request Mix-up Vulnerability (May 2022) - Windows	8.6	8443/tcp
Apache Tomcat Request Mix-up Vulnerability (May 2022) - Windows	8.6	8080/tcp
Apache Tomcat Request Mix-up Vulnerability (May 2022) - Windows	8.6	40000/tcp
Apache Tomcat DoS Vulnerability (Sep 2021) - Windows	7.5	8080/tcp
Apache Tomcat DoS Vulnerability (Sep 2021) - Windows	7.5	40000/tcp
Apache Tomcat HTTP/2 Vulnerability - Dec20 (Windows)	7.5	8443/tcp
Apache Tomcat DoS Vulnerability - June20 (Windows)	7.5	40000/tcp
Apache Tomcat HTTP/2 Vulnerability - Dec20 (Windows)	7.5	8080/tcp
Apache Tomcat HTTP/2 Vulnerability - Dec20 (Windows)	7.5	40000/tcp
Apache Tomcat Information Disclosure Vulnerability (Mar21) - Windows	7.5	8443/tcp
Apache Tomcat Information Disclosure Vulnerability (Mar21) - Windows	7.5	8080/tcp
Apache Tomcat Information Disclosure Vulnerability (Mar21) - Windows	7.5	40000/tcp
Apache Tomcat DoS Vulnerability - June20 (Windows)	7.5	8443/tcp
Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows)	7.5	8443/tcp
Apache Tomcat DoS Vulnerability - June20 (Windows)	7.5	8080/tcp

Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows)	7.5	8080/tcp
Apache Tomcat Multiple DoS Vulnerabilities - July20 (Windows)	7.5	40000/tcp
Apache Tomcat Session Fixation Vulnerability - Dec19 (Windows)	7.5	40000/tcp
Apache Tomcat Session Fixation Vulnerability - Dec19 (Windows)	7.5	8080/tcp
Apache Tomcat Session Fixation Vulnerability - Dec19 (Windows)	7.5	8443/tcp
Apache Tomcat DoS Vulnerability (Sep 2021) - Windows	7.5	8443/tcp
Apache Tomcat RCE Vulnerability (Mar21) - Windows	7.0	8080/tcp
Apache Tomcat Privilege Escalation Vulnerability - Dec19 (Windows)	7.0	8443/tcp
Apache Tomcat RCE Vulnerability (Mar21) - Windows	7.0	8443/tcp
Apache Tomcat Privilege Escalation Vulnerability - Dec19 (Windows)	7.0	8080/tcp
Apache Tomcat Privilege Escalation Vulnerability - Dec19 (Windows)	7.0	40000/tcp
Apache Tomcat RCE Vulnerability (Mar21) - Windows	7.0	40000/tcp
Apache Tomcat RCE Vulnerability - May20 (Windows)	7.0	8443/tcp
Apache Tomcat RCE Vulnerability - May20 (Windows)	7.0	8080/tcp
Apache Tomcat RCE Vulnerability - May20 (Windows)	7.0	40000/tcp
Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Windows	6.5	8443/tcp
Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Windows	6.5	8080/tcp
Apache Tomcat JNDI Realm Authentication Weakness Vulnerability (Jul 2021) - Windows	6.5	40000/tcp
Apache Tomcat Information Disclosure Vulnerability - Jan21 (Windows)	5.9	8080/tcp
Apache Tomcat Information Disclosure Vulnerability - Jan21 (Windows)	5.9	8443/tcp
Apache Tomcat Information Disclosure Vulnerability - Jan21 (Windows)	5.9	40000/tcp
Apache Tomcat HTTP Request Smuggling Vulnerability (Jul 2021) - Windows	5.3	40000/tcp
Apache Tomcat HTTP Request Smuggling Vulnerability (Jul 2021) - Windows	5.3	8443/tcp
Apache Tomcat HTTP Request Smuggling Vulnerability (Jul 2021) - Windows	5.3	8080/tcp
SSL/TLS: Report Weak Cipher Suites	5.0	3389/tcp

DCE/RPC and MSRPC Services Enumeration Reporting	5.0	135/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol	4.3	40000/tcp
Apache Tomcat HTTP/2 Vulnerability - Oct20	4.3	40000/tcp
Apache Tomcat HTTP/2 Vulnerability - Oct20	4.3	8080/tcp
Apache Tomcat HTTP/2 Vulnerability - Oct20	4.3	8443/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3	3389/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3	8443/tcp
Apache Tomcat Information Disclosure Vulnerability (Sep 2022) - Windows	4.3	8443/tcp
Apache Tomcat Information Disclosure Vulnerability (Sep 2022) - Windows	4.3	8080/tcp
Apache Tomcat Information Disclosure Vulnerability (Sep 2022) - Windows	4.3	40000/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0	8443/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0	3389/tcp
TCP timestamps	2.6	general/tcp

Fuente: Elaboración Propia

5.3.3.3 **Resultados de NESSUS**

Tabla 21. SAP - Resultados NESSUS

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	139574	Apache 2.4.x < 2.4.46 Multiple Vulnerabilities
CRITICAL	9.8	150280	Apache 2.4.x < 2.4.47 Multiple Vulnerabilities
CRITICAL	9.8	161454	Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow
CRITICAL	9.8	158900	Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL	9.8	161948	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities
CRITICAL	9.8	156255	Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF
CRITICAL	9.8	153584	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	9.8	58134	Microsoft Silverlight Unsupported Version Detection (Windows)
CRITICAL	9.1	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities

CRITICAL	9.0	153583	Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL	10.0	40362	Mozilla Foundation Unsupported Application Detection
HIGH	8.8	137364	Dell SupportAssist Multiple Vulnerabilities (DSA-2019-051)
HIGH	8.8	150122	Mozilla Firefox ESR < 78.11
HIGH	8.8	151574	Mozilla Firefox ESR < 78.12
HIGH	8.8	152414	Mozilla Firefox ESR < 78.13
HIGH	8.8	153090	Mozilla Firefox ESR < 78.14
HIGH	8.8	153877	Mozilla Firefox ESR < 78.15
HIGH	8.8	164090	Security Updates for Microsoft Visual Studio Products (August 2022)
HIGH	8.8	158715	Security Updates for Microsoft Visual Studio Products (March 2022)
HIGH	8.8	149436	Security Updates for Microsoft Visual Studio Products (May 2021)
HIGH	8.4	65057	Insecure Windows Service Permissions
HIGH	7.8	123642	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities
HIGH	7.8	153806	Dell SupportAssist < 3.10 Multiple Vulnerabilities (DSA-2021-163)
HIGH	7.8	138149	Dell SupportAssist PC Doctor Vulnerability (DSA-2019-084)
HIGH	7.8	138151	Dell SupportAssist Uncontrolled Search Path Vulnerability (DSA-2020-005)
HIGH	7.8	63155	Microsoft Windows Unquoted Service Path Enumeration
HIGH	7.8	159733	Security Updates for Microsoft Visual Studio Products (April 2022)
HIGH	7.8	156194	Security Updates for Microsoft Visual Studio Products (December 2021)
HIGH	7.8	162317	Security Updates for Microsoft Visual Studio Products (June 2022)
HIGH	7.8	161118	Security Updates for Microsoft Visual Studio Products (May 2022)
HIGH	7.8	155018	Security Updates for Microsoft Visual Studio Products (November 2021)
HIGH	7.8	153428	Security Updates for Microsoft Visual Studio Products (September 2021)
HIGH	7.5	121355	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities
HIGH	7.5	153585	Apache >= 2.4.17 < 2.4.49 mod_http2
HIGH	7.5	153586	Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi
HIGH	7.5	104896	Security Updates for Internet Explorer (September 2017)

HIGH	7.5	157841	Security Updates for Microsoft Visual Studio Products (February 2022)
HIGH	7.5	150418	Security Updates for Microsoft Visual Studio Products (June 2021)
HIGH	7.5	165107	Security Updates for Microsoft Visual Studio Products (Sep 2022)
HIGH	7.4	154051	Security Updates for Microsoft Visual Studio Products (October 2021)
HIGH	7.1	127910	Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161)
HIGH	8.3*	81264	MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
MEDIUM	6.5	149255	Mozilla Firefox ESR < 78.10.1
MEDIUM	6.5	132101	Windows Speculative Execution Configuration Check
MEDIUM	6.1	135290	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities
MEDIUM	5.9	117807	Apache 2.4.x < 2.4.35 DoS
MEDIUM	5.5	152423	Security Updates for Microsoft Visual Studio Products (August 2021)
MEDIUM	4.8	87875	MS KB3123479: Deprecation of SHA-1 Hashing Algorithm for Microsoft Root Certificate Program
MEDIUM	4.3*	78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)
LOW	3.1	134204	MS15-124: Cumulative Security Update for Internet Explorer (CVE-2015-6161) (3125869)

Fuente: Elaboración Propia

5.4 PROPONER UNAS BUENAS PRÁCTICAS ARTICULADAS CON ESTÁNDARES INTERNACIONALES CON EL FIN DE MITIGAR LOS RIESGOS Y DAR CONTINUIDAD AL NEGOCIO.

Para el desarrollo de este objetivo, se dividirá en varias secciones, una con la resolución que se debe aplicar inmediatamente con los resultados catalogados “Críticos”, “Altos” y “Medios” de cada uno de los servidores. Luego en las recomendaciones que se sugieren en el IDS/IPS Wazuh, el Firewall perimetral; y en el caso de los servidores SAP y TS, los resultados de un script de hardening llamado HardeningKitty.

Las recomendaciones Generales se tratarán en el apartado “Recomendaciones” al final del documento

5.4.1 AD

Primero que nada y antes siquiera de empezar a parchear vulnerabilidades, se debe contemplar la eliminación de este servidor, ya que se trata de un Windows Server 2008 R2, con fecha de final de vida (EOL) 1/14/2020, el cual ya no está recibiendo soporte oficial por parte de Microsoft y se están recibiendo actualizaciones únicamente de aplicaciones instaladas y de parches de seguridad viralizadas, por ejemplo, PrintNightmare o Eternal Blue.

5.4.1.1 **Microsoft DNS Server Remote Code Execution (SIGRed).** Para solucionar esta vulnerabilidad, se debe aplicar los parches de seguridad liberados por Microsoft. Una contramedida puede ser la limitación del tamaño de las peticiones DNS por un valor de 0xFF00 para evitar el desbordamiento.

Solución: Aplicar este cambio en el registro de Windows del DNS Server:

```
reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DN
S\Parameters" /v "TcpReceivePacketSize" /t REG_DWORD /d
0xFF00 /f
net stop DNS && net start DNS
```

5.4.1.2 **SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE).** Esta vulnerabilidad encontrada va de la mano de la obsolescencia del certificado SSLv3, publicado en 1996 y depreciado del todo en el año 2015. SSL paso a ser reemplazado por TLS el cual ya se encuentra en la versión 1.3 lanzado en el 2018.

Esta vulnerabilidad solo se puede subsanar eliminando la compatibilidad con SSLv3 en el servidor. Las aplicaciones que aún necesiten de este para funcionar significan que están en una versión muy antigua y se necesitan actualizar inmediatamente.

Solución: Desactivar SSL de versión 3.

5.4.1.3 **SSL Certificate Signed Using Weak Hashing Algorithm.** Esta vulnerabilidad consta del uso de un pobre algoritmo de las claves del certificado SSL, por ejemplo, MD2, MD4, MD5 o SHA1.

En este caso, los dos certificados del servidor utilizan SHA1 con RSA.

Solución: Se debe poner en contacto por la autoridad de certificación para volver a emitir el certificado.

5.4.1.4 **SSL Medium Strength Cipher Suites Supported (SWEET32).** En la máquina objetivo se está soportando el uso de cifrado de nivel medio, por ejemplo, de longitudes de claves de entre 64 y 112 o que use 3DES. Un atacante puede obtener la cookie de sesión de HTTPS capturando alrededor de 785GB[12] de información (Sniffeando la red).

Solución:
Reconfigurar las aplicaciones para que trabajen con un cifrado más actual y robusto, y en el servidor retirar esta retrocompatibilidad inversa del cifrado.

5.4.1.5 **SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam).** El host remoto permite conexiones SSL/TLS con uno o más módulos Diffie-Hellman menores o iguales a 1024 bits. A través del criptoanálisis, un tercero puede encontrar el secreto compartido en poco tiempo (según el tamaño del módulo y los recursos del atacante). Esto puede permitir que un atacante recupere el texto sin formato o potencialmente viole la integridad de las conexiones.

Solución:

[12] https://sweet32.info/

Vuelva a configurar el servicio para usar módulos Diffie-Hellman únicos de 2048 bits o más.

5.4.1.6 **SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption).** Esta vulnerabilidad va de la mano con la retrocompatibilidad o soporte que se tiene con versiones anteriores de SSL, en este caso, al ser compatible con SSLv2, un ciberdelincuente puede realizar un ataque tipo Men-In-The-Middle para explotar esta vulnerabilidad y poder descifrar el tráfico TLS previamente capturado.

Solución:
Desactive SSLv2 en el servidor. Además, asegúrese que las llaves privadas no se utilicen en ningún otro lugar o software que admita conexiones SSLv2.

5.4.1.7 **SSL RC4 Cipher Suites Supported (Bar Mitzvah).** RC4 es un cifrado que está en desuso y tiene vulnerabilidades conocidas. Una de estas es que, si el texto sin formato se cifra repetidamente y un atacante puede obtener muchos textos cifrados, el atacante puede obtener el texto sin formato.

Solución:
Reconfigurar el servidor o la aplicación que utilice este cifrado para seleccionar otro tipo de cifrado más robusto, como por ejemplo TLS 1.2.

5.4.1.8 **Certificados Expirados.** Los dos certificados del servidor se encuentran expirados, uno el 2015-08-01 y el otro el 2022-11-06.

Solución:
Volver a generar los certificados para renovarlos.

5.4.1.9 **Deprecated TLSv1.0 and TLSv1.1 Protocol Detection.** *Al igual que con los certificados SSL, también se están admitiendo versiones muy antiguas y obsoletas de TLS, el 1.0 y 1.1.*

Solución:
De ser posible, deshabilitar completamente la compatibilidad con TLS 1.0 y 1.1, y permitir únicamente las versiones 1.2 y 1.3

5.4.1.10 **Paquetes de seguridad no aplicados (Criticidad alta).** Algunos paquetes de seguridad no están instalados.

Solución:
Es necesario que se aplique de manera inmediata todos los paquetes de seguridad faltantes, la lista de KB es la siguiente:

- KB4556843
- KB5003233
- KB4586805
- KB4598289
- KB5000851
- KB5003694
- KB5004307
- KB5005089
- KB5005615
- KB5008282
- KB5012649
- KB5013999
- KB5016679
- KB5017373
- KB4571719
- KB4601363
- KB4023307
- KB4537813
- KB4541500
- KB4550965
- KB4561669
- KB4565539
- KB4577053
- KB4580387
- KB5001335
- KB5004951
- KB5007233
- KB5009621
- KB5011529
- KB5014742
- KB5015862
- KB4592503
- KB5006728
- KB5010422
- KB2269637
- KB4017094

- KB3009008
- MS16-006
- MS16-109
- KB4550964
- KB4550905
- KB4550951
- KB4550961

5.4.1.11 **7-Zip < 18.00, < 16.00 Multiple Vulnerabilities.** Las versiones de 7zip inferiores a la 18.00 y 16.00 tienen múltiples vulnerabilidades conocidas.

Solución:
Actualizar la versión de 7zip a la más reciente.

5.4.1.12 **Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU) - Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU).** Múltiples vulnerabilidades encontradas en versiones antiguas de Java.

Solución: Actualizar a la última versión Java de Oracle.

5.4.2 TS

Este servidor tiene un sistema operativo Windows Server 2012 R2 Standard; aunque actualmente está siendo soportado de manera oficial por parte de Microsoft, se recomienda encarecidamente la actualización de este, ya que su EOF es el 10 oct 2023.

5.4.2.1 **SSL/TLS: Report Vulnerable Cipher Suites for HTTPS - SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection - SSL/TLS: Report Weak Cipher Suites - SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection - SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE).** Estas vulnerabilidades se trataron en el análisis del servidor “AD”; prácticamente son basados en la compatibilidad y habilitación de SSL en cualquiera de sus versiones (1, 2 o 3), adicional de TLS en versiones 1.0, y 1.1, e incluso 1.2. Adicional se tiene habilitado encriptación pobre o vulnerable.

Solución: Deshabilitar SSL versión 1, 2 y 3, igual TLS 1.0, 1.1 y de ser posible, 1.2

5.4.2.2 **VNC Server Unencrypted Data Transmission.** En este server se tiene instalado un servidor VNC, que, aunque se tiene bajo contraseña tanto las conexiones como la configuración de este; no se tiene encriptación en su transporte por la red.

Solución: Actualizar el servidor VNC y habilitar la encriptación en la conexión.

5.4.2.3 **Apache Log4j 1.x Multiple Vulnerabilities.** Este servidor utiliza para alguno de sus roles la herramienta Log4j en versiones 1.x. Este tiene múltiples vulnerabilidades asociadas.

Solución: Actualizar de manera inmediata esta herramienta por una versión no vulnerable, sobre todo a Log4Shell.

5.4.2.4 **Foxit PDF Reader < 11.2.1 , < 10.1 , < 9.7.2 Multiple Vulnerabilities.** El lector de PDF de la empresa Foxit, el PDF Reader, tiene múltiples vulnerabilidades conocidas en versiones inferiores a la 11.2.1

Solución: Actualizar a la última versión disponible de esta herramienta.

5.4.2.5 **Oracle Java SE 1.7.0_241 / 1.8.0_231 / 1.11.0_5 / 1.13.0_1 Multiple Vulnerabilities (Oct 2019 CPU) (Windows) - Oracle Java SE 1.7.0_221 / 1.8.0_211 / 1.11.0_3 / 1.12.0_1 Multiple Vulnerabilities (Apr 2019 CPU) - Oracle Java SE 1.7.0_321 / 1.8.0_311 / 1.11.0_13 / 1.17.0_1 Multiple Vulnerabilities (October 2021 CPU) - Oracle Java SE 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1 Multiple Vulnerabilities (Apr 2020 CPU) - Oracle Java SE 1.7.0_271 / 1.8.0_261 / 1.11.0_8 / 1.14.0_2 Multiple Vulnerabilities (Jul 2020 CPU) - Oracle Java SE 1.7.0_251 / 1.8.0_241 / 1.11.0_6 / 1.13.0_2 Multiple Vulnerabilities (Jan 2020 CPU) - Oracle Java SE 1.7.0_311 / 1.8.0_301 / 1.11.0_12 / 1.16.0_2 Multiple Vulnerabilities (July 2021 CPU) - Oracle Java SE Multiple Vulnerabilities (April 2022 CPU).** Este servidor tiene instalado el Java de Oracle, pero está bastante desactualizado. Se debe revisar si se necesita una versión en específico de Java para alguna tarea o si se puede llegar a actualizar a una versión segura.

Solución: Actualizar Java a la última versión.

5.4.2.6 **Apache Log4j 2.x < 2.16.0 RCE.** Se separó esta vulnerabilidad de la otra, ya que esta permite la Ejecución Remota de Comandos; lo que la vuelve una puerta de entrada para un cibercriminal.

Solución: Actualizar inmediatamente la versión del Apache Log4j por la última versión disponible, o al menos a una versión que no sea vulnerable a este RCE.

5.4.2.7 **Security Update for .NET Core (March 2021).** Versión de .NET Core desactualizada, esta actualización acumulativa soluciona muchos errores encontrados.

Solución: Actualizar .NET Core a su última versión disponible.

5.4.2.8 **Security Updates for Microsoft Visual Studio Products (July 2020) – ASP.NET.** Este servidor tiene software de Visual Studio instalado, pero no se encuentran actualizados.

Solución: Aplicar actualizaciones de seguridad o acumulativas de Visual Studio o de ser posible, actualizar a la última versión de este.

5.4.2.9 **SSL Certificate Cannot Be Trusted - SSL Self-Signed Certificate.** Los certificados de seguridad SSL son auto firmados y esto no permite la validación de su seguridad.

Solución: Contratar los servicios de una empresa certificadora externa y adquirir un certificado de seguridad válido.

5.4.2.10 **Actualizaciones de seguridad no aplicados.** Algunos de los paquetes de seguridad recomendados no están instalados. Alguno de estos es:

- KB5017365
- KB5017367
- KB3009008
- KB3125869

5.4.2.11 **MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483).** Existe una vulnerabilidad conocida en las políticas de grupo, que puede ser explotada y convertirse en un RCE.

Solución: Aplicar los paquetes de parches de seguridad liberados por Microsoft.

5.4.3 SAP. Al igual que el servidor anterior, este es un Windows Server 2012 R2 Standard, el cual tiene varios aplicativos a considerar, como el SQL Server 2012. Es altamente recomendable actualizar tanto el sistema operativo como el motor de la base de datos, ya que se consideran vulnerables, vencidos o muy próximos a su EOL, el cual para la base de datos es el 12 jul 2022 (soporte finalizado) y para el sistema operativo es 10 oct 2023.

5.4.3.1 **Microsoft SQL Server End Of Life Detection.** Se detecta que el software Microsoft SQL Server ya se encuentra por fuera de soporte, el cual venció el Julio 12 de este 2022. Por parte de Microsoft solo se entregarán paquetes de actualizaciones críticos y la periodicidad en la entrega es mucho mayor.

Solución: Considerar la adquisición de paquetes de extensión de soporte, Microsoft tiene estas ofertas, Extended Security Update Year 1, Extended Security Update Year 2 o Extended Security Update Year 3, los cuales extienden la duración del soporte hasta el 11 jul 2023, 9 jul 2024 y 8 jul 2025 respectivamente.

Otra solución que se debe tener presente es la compra del software a una nueva versión, actualmente ya se encuentra la versión 2022 liberada.

5.4.3.2 **Apache Tomcat Multiple Vulnerabilities - Apache Tomcat Request Mix-up Vulnerability - Apache Tomcat DoS Vulnerability - Apache Tomcat HTTP/2 Vulnerability - Apache Tomcat Information Disclosure Vulnerability - Apache Tomcat Session Fixation Vulnerability - Apache Tomcat Privilege Escalation Vulnerability - Apache Tomcat RCE Vulnerability.** Existen múltiples vulnerabilidades encontradas en el servidor Apache Tomcat instalado en este servidor, esto puede conllevar, entre otros, en ataque de DoS, escalamiento de privilegios, ejecución remota de comandos RCE.

Solución: Actualizar de manera inmediata la versión del servidor Tomcat instalado en esta máquina a la última liberada por la fundación Apache. Si esto no es posible debido a incompatibilidades con software interno, actualizar por lo menos a una versión que no esté comprometida y cuando el proveedor tecnológico (desarrollador del software heredado) lo permita, actualizar a una versión mayor.

5.4.3.3 **Mozilla Firefox ESR versiones < 78.15.** En este servidor se encuentra instalado el navegador de la fundación Mozilla, el Firefox en su versión 78.10. Esta versión y las anteriores tienen vulnerabilidades conocidas y publicadas por Mozilla en su página de seguridad. https://www.mozilla.org/en-US/security/known-vulnerabilities/

Solución: Actualizar dicho navegador a la última versión disponible, que, para la fecha de redacción de este proyecto, es la versión 105.0.1.

5.4.3.4 **Dell SupportAssist Multiple Vulnerabilities (DSA-2019-051) - Dell SupportAssist PC Doctor Vulnerability (DSA-2019-084) - Dell SupportAssist Uncontrolled Search Path Vulnerability (DSA-2020-005).** En este servidor se encuentra instalo el Dell SupportAssist y sus herramientas, la versión instalada tiene varias vulnerabilidades conocidas; por lo que se recomienda actualizar.

Solución: Actualizar a la última versión liberada por DELL, o de ser posible, desinstalar esta aplicación y gestionar las actualizaciones de software, firmware y demás, por medio del Windows Update o manualmente.

5.4.3.5 **Security Updates for Microsoft Visual Studio Products.** Se encuentra instalado el Visual Studio en este servidor, pero no se encuentra actualizado.

Solución: Aplicar las actualizaciones de seguridad liberadas por Microsoft para el Visual Studio y sus herramientas asociadas.

5.4.3.6 **Insecure Windows Service Permissions.** Se detectó al menos un ejecutable de servicio de Windows con permisos no seguros en el host remoto. Los servicios configurados para usar un ejecutable con permisos débiles son vulnerables a los ataques de escalada de privilegios.

Un usuario sin privilegios podría modificar o sobrescribir el ejecutable con código arbitrario, que se ejecutaría la próxima vez que se inicie el servicio. Dependiendo del usuario con el que se ejecuta el servicio, esto podría resultar en una escalada de privilegios.

Solución: Este plugin de Nessus tiene en cuenta los siguientes grupos de usuarios de dominio.

- Everyone
- Users
- Domain Users
- Authenticated Users

Asegúrese de que los grupos enumerados anteriormente no tengan permisos para modificar o escribir ejecutables de servicio. Además, asegúrese de que estos grupos no tengan permiso de Control total para ningún directorio que contenga ejecutables de servicio.

5.4.3.7 **Microsoft Windows Unquoted Service Path Enumeration.** El host remoto de Windows tiene al menos un servicio instalado que usa una ruta de servicio sin comillas, que contiene al menos un espacio en blanco. Un atacante local puede obtener privilegios elevados insertando un archivo ejecutable en la ruta del servicio afectado.

Solución: Este plugin de Nessus encontró varios servicios los cuales en su ruta tienen un espacio en blanco, y en este caso se debe colocar comillas (“) en la ruta

para evitar que un ciberdelincuente no pueda vulnerar aprovecharse de esto insertando código propio en la ruta del servicio afectado y poder así obtener elevación de privilegios.

La solución a esto es listar todas las rutas de los servicios que se están ejecutando, ya sea de manera manual o automático, y colocar las comillas al principio y al final de cada uno, para evitar que un atacante pueda utilizarlo.

5.4.3.8 **Microsoft Defender Elevation of Privilege Vulnerability (CVE-2019-1161).** En este servidor se encuentra instalado el Microsoft Defender, y el ejecutable Microsoft Malware Protection Signature Update Stub (MpSigStub.exe) se encuentra en la versión 1.1.16200.1. Esta versión tiene una vulnerabilidad conocida de gravedad alta, con puntaje 7.1; un atacante puede explotar esta vulnerabilidad y ganar privilegios de administrador.

Solución: Actualizar la versión del software a la última versión liberada por Microsoft.

5.4.3.9 **Windows Speculative Execution Configuration Check.** El host remoto no ha mitigado adecuadamente una serie de vulnerabilidades de ejecución especulativa conocidas. Por lo tanto, puede verse afectado por:

- Branch Target Injection (BTI) (CVE-2017-5715)
- Bounds Check Bypass (BCB) (CVE-2017-5753)
- Rogue Data Cache Load (RDCL) (CVE-2017-5754)
- Rogue System Register Read (RSRE) (CVE-2018-3640)
- Speculative Store Bypass (SSB) (CVE-2018-3639)
- L1 Terminal Fault (L1TF) (CVE-2018-3615, CVE-2018-3620, CVE-2018-3646)
- Microarchitectural Data Sampling Uncacheable Memory (MDSUM) (CVE-2019-11091)
- Microarchitectural Store Buffer Data Sampling (MSBDS) (CVE-2018-12126)
- Microarchitectural Load Port Data Sampling (MLPDS) (CVE-2018-12127)
- Microarchitectural Fill Buffer Data Sampling (MFBDS) (CVE-2018-12130)
- TSX Asynchronous Abort (TAA) (CVE-2019-11135)

Solución: Aplicar las contramedidas y recomendaciones de seguridad sugeridas por los fabricantes para cada una de las vulnerabilidades listadas.

5.4.3.10 **MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483).** El host remoto de Windows se ve afectado por una vulnerabilidad de ejecución remota de código debido a la forma en que el servicio de directiva de grupo administra los datos de la directiva cuando un sistema unido a un dominio se conecta a un controlador de dominio. Un atacante, utilizando una red controlada, puede explotar esto para obtener el control total del host.

Solución: Aplicar los parches de seguridad liberados por Microsoft.

5.4.4 Hardening – Recomendaciones de Script HardeningKitty

5.4.4.1 TS

Tabla 22. HardeningKitty – TS

Aprobadas	**79**
Catalogadas Riesgo Bajo	56
Catalogadas Riesgo Medio	192
Catalogadas Riesgo Alto	2
Total	**329**

Fuente: Propia

Ejemplo de las recomendaciones del script para aplicar Hardening a este servidor:

Riesgo Alto:

[ ] ID 1000, SMBv1 Support, Result=Enabled, Recommended=Disabled, Severity=High

[ ] ID 1708, BitLocker Drive Encryption: Volume status, Result=FullyDecrypted, Recommended=FullyEncrypted, Severity=High

Riesgo Medio:

[ ] ID 1203, Deny access to this computer from the network, Result=, Recommended=BUILTIN\Guests;NT AUTHORITY\Local acco
unt, Severity=Medium

[ ] ID 1313, Network security: LAN Manager authentication level, Result=3, Recommended=5, Severity=Medium

[ ] ID 1403, Log size limit (Domain Profile, Policy), Result=4096, Recommended=16384, Severity=Medium

[ ] ID 1404, Log dropped packets (Domain Profile, Policy), Result=0, Recommended=1, Severity=Medium

[😾] ID 1601, DNS Client: Turn off multicast name resolution (LLMNR), Result=1, Recommended=0, Severity=Medium

Riesgo Bajo:

[😾] ID 1405, Log successful connections (Domain Profile, Policy), Result=0, Recommended=1, Severity=Low

[😾] ID 1300, Accounts: Block Microsoft accounts, Result=0, Recommended=3, Severity=Low

[😾] ID 1304, Interactive logon: Don't display username at sign-in, Result=0, Recommended=1, Severity=Low

[😾] ID 1405, Log successful connections (Domain Profile, Policy), Result=0, Recommended=1, Severity=Low

[😾] ID 1502, User Account Management, Result=Success, Recommended=Success and Failure, Severity=Low

[😾] ID 1503, DPAPI Activity, Result=No Auditing, Recommended=Success and Failure, Severity=Low

[😾] ID 1504, Plug and Play Events, Result=No Auditing, Recommended=Success, Severity=Low

[😾] ID 1505, Process Creation, Result=No Auditing, Recommended=Success, Severity=Low

[😾] ID 1506, Account Lockout, Result=Success, Recommended=Failure, Severity=Low

[😾] ID 1507, Group Membership, Result=, Recommended=Success, Severity=Low

5.4.4.2 **SAP.** El puntaje obtenido por la herramienta HardeningKitty: **3.25.**

Tabla 23. HardeningKitty para SAP

Aprobadas	**69**
Catalogadas Riesgo Bajo	58
Catalogadas Riesgo Medio	200
Catalogadas Riesgo Alto	2
Total	**329**

Fuente: Propia

Ejemplo de las recomendaciones del script para aplicar Hardening a este servidor:

Riesgo Alto:

[🦊] ID 1708, BitLocker Drive Encryption: Volume status, Result=FullyDecrypted, Recommended=FullyEncrypted, Severity=High

[🦊] ID 1000, SMBv1 Support, Result=Enabled, Recommended=Disabled, Severity=High

Riesgo Medio:

[🦊] ID 1601, DNS Client: Turn off multicast name resolution (LLMNR), Result=1, Recommended=0, Severity=Medium

[🦊] ID 1602, Lanman Workstation: Enable insecure guest logons, Result=1, Recommended=0, Severity=Medium

[🦊] ID 1603, Turn off Microsoft Peer-to-Peer Networking Services, Result=0, Recommended=1, Severity=Medium

[🦊] ID 1601, DNS Client: Turn off multicast name resolution (LLMNR), Result=1, Recommended=0, Severity=Medium

[🦊] ID 1602, Lanman Workstation: Enable insecure guest logons, Result=1, Recommended=0, Severity=Medium

[🦊] ID 1603, Turn off Microsoft Peer-to-Peer Networking Services, Result=0, Recommended=1, Severity=Medium

[🦊] ID 1623, Device Guard: Require UEFI Memory Attributes Table (Policy), Result=, Recommended=1, Severity=Medium

Riesgo Bajo:

[🦊] ID 1631, Group Policy: Process even if the Group Policy objects have not changed, Result=1, Recommended=0, Severity=Low

[🦊] ID 1747, Windows Game Recording and Broadcasting: Enables or disables Windows Game Recording and Broadcasting, Result=1, Recommended=0, Severity=Low

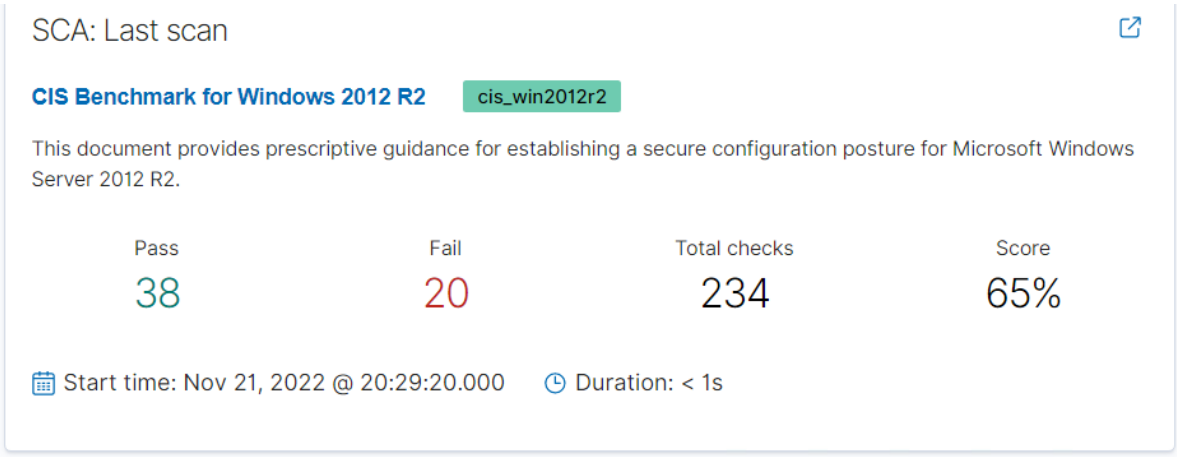
[😾] ID 2101, Turn on PowerShell Script Block Logging (Invocation), Result=0, Recommended=1, Severity=Low
[😾] ID 1002, Turn on PowerShell Transcription, Result=0, Recommended=1, Severity=Low
[😾] ID 2201, Lsass.exe audit mode, Result=, Recommended=8, Severity=Low

5.4.4.3 **AD.** Lastimosamente el script de powershell HardeningKitty es compatible con versiones de Windows Server desde la 2012 en adelante, AD al ser un 2008 R2 no es compatible con él y genera un error al intentar ejecutarlo.

5.4.4.4 **Hardening – Puntaje y Recomendaciones de IDS/IPS Wazuh**

5.4.4.5 **SAP**

Figura 12. Wazuh Score - SAP



Fuente: Propia

- **15015. Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'**

Razón fundamental
Un atacante con acceso a la consola (por ejemplo, alguien con acceso físico o alguien que puede conectarse al servidor a través de Servicios de escritorio remoto) podría ver el nombre del último usuario que inició sesión en el servidor. Luego, el atacante podría intentar adivinar la contraseña, usar un diccionario o usar un ataque de fuerza bruta para intentar iniciar sesión.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Inicio de sesión interactivo: no mostrar el último nombre de usuario.

Descripción
Esta configuración de directiva determina si el nombre de cuenta del último usuario que inició sesión en los equipos cliente de su organización se mostrará en la pantalla de inicio de sesión de Windows respectiva de cada equipo. Habilite esta configuración de directiva para evitar que los intrusos recopilen nombres de cuentas

de forma visual desde las pantallas de las computadoras de escritorio o portátiles de su organización. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> DontDisplayLastUserName -> 1

- **15018. Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)'**

Razón fundamental

El número que se asigna a esta configuración de directiva indica el número de usuarios cuya información de inicio de sesión la computadora almacenará en caché localmente. Si el número se establece en 4, la computadora almacena en caché la información de inicio de sesión de 4 usuarios. Cuando un quinto usuario inicia sesión en la computadora, el servidor sobrescribe la sesión de inicio de sesión en caché más antigua. Los usuarios que accedan a la consola de la computadora tendrán sus credenciales de inicio de sesión almacenadas en caché en esa computadora. Un atacante que pueda acceder al sistema de archivos de la computadora podría ubicar esta información almacenada en caché y usar un ataque de fuerza bruta para intentar determinar las contraseñas de los usuarios. Para mitigar este tipo de ataque, Windows cifra la información y oculta su ubicación física.

Remediación

Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en 4 o menos inicios de sesión: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Inicio de sesión interactivo: número de inicios de sesión anteriores en caché (en caso de que el controlador de dominio no esté disponible)

Descripción

Esta configuración de directiva determina si un usuario puede iniciar sesión en un dominio de Windows utilizando la información de cuenta almacenada en caché. La información de inicio de sesión para cuentas de dominio se puede almacenar en caché localmente para permitir que los usuarios inicien sesión incluso si no se puede contactar a un controlador de dominio. Esta configuración de directiva determina la cantidad de usuarios únicos para quienes la información de inicio de sesión se almacena en caché localmente. Si este valor se establece en 0, la función de caché de inicio de sesión está deshabilitada. Un atacante que pueda acceder al sistema de archivos del servidor podría ubicar esta información almacenada en caché y usar un ataque de fuerza bruta para determinar las contraseñas de los usuarios. El estado recomendado para esta configuración es: 4 o menos inicios de sesión.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon -> CachedLogonsCount -> n:^(\d+) compare <= 4

- **15020. Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'**

Razón fundamental

De manera predeterminada, la computadora almacena en caché en la memoria las credenciales de cualquier usuario autenticado localmente. La computadora usa estas credenciales almacenadas en caché para autenticar a cualquier persona que intente desbloquear la consola. Cuando se utilizan credenciales almacenadas en caché, los cambios que se hayan realizado recientemente en la cuenta, como las asignaciones de derechos de usuario, el bloqueo de la cuenta o la desactivación de la cuenta, no se tienen en cuenta ni se aplican después de autenticar la cuenta. Los privilegios de usuario no se actualizan y (lo que es más importante) las cuentas deshabilitadas aún pueden desbloquear la consola de la computadora.

Remediación

Para implementar la configuración recomendada a través de GP, establezca la siguiente ruta de la interfaz de usuario en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Inicio de sesión interactivo: Requerir autenticación del controlador de dominio para desbloquear la estación de trabajo.

Descripción

Se requiere información de inicio de sesión para desbloquear una computadora bloqueada. Para las cuentas de dominio, esta configuración de seguridad determina si es necesario comunicarse con un controlador de dominio para desbloquear una computadora. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon -> ForceUnlockLogon -> 1

- **15021. Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher.**

Razón fundamental
Los usuarios a veces se olvidan de bloquear sus estaciones de trabajo cuando están lejos de ellas, lo que permite la posibilidad de que usuarios maliciosos accedan a sus computadoras. Si se usan tarjetas inteligentes para la autenticación, la computadora debe bloquearse automáticamente cuando se retira la tarjeta para garantizar que solo el usuario con la tarjeta inteligente acceda a los recursos usando esas credenciales.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de IU para Bloquear estación de trabajo (o, si corresponde para su entorno, Forzar cierre de sesión o Desconexión si se trata de una sesión de Servicios de escritorio remoto): Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales \Opciones de seguridad\Inicio de sesión interactivo: Comportamiento de eliminación de tarjeta inteligente.

Descripción
Esta configuración de directiva determina lo que sucede cuando la tarjeta inteligente de un usuario que ha iniciado sesión se quita del lector de tarjetas inteligentes. El estado recomendado para esta configuración es: Bloquear estación de trabajo. Configurar esta opción para Forzar cierre de sesión o Desconectar si una sesión de Servicios de Escritorio remoto también se ajusta al punto de referencia.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon -> ScRemoveOption -> r:^1$|^2$|^3$

- **15022. Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'.**

Razón fundamental
El secuestro de sesiones utiliza herramientas que permiten a los atacantes que tienen acceso a la misma red que el cliente o el servidor interrumpir, finalizar o robar una sesión en curso. Los atacantes pueden potencialmente interceptar y modificar paquetes SMB no firmados y luego modificar el tráfico y reenviarlo para que el servidor pueda realizar acciones no deseadas. Alternativamente, el atacante podría hacerse pasar por el servidor o el cliente después de una autenticación legítima y obtener acceso no autorizado a los datos. SMB es el protocolo de uso compartido de recursos que es compatible con muchos sistemas operativos Windows. Es la base de NetBIOS y muchos otros protocolos. Las firmas SMB autentican tanto a los

usuarios como a los servidores que alojan los datos. Si alguna de las partes falla en el proceso de autenticación, no se realizará la transmisión de datos.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Cliente de red de Microsoft: firmar digitalmente las comunicaciones (siempre).

Descripción
Esta configuración de directiva determina si el componente de cliente SMB requiere la firma de paquetes. Nota: Cuando las computadoras basadas en Windows Vista tienen esta configuración de política habilitada y se conectan a recursos compartidos de archivos o impresoras en servidores remotos, es importante que la configuración esté sincronizada con su configuración complementaria, Servidor de red de Microsoft: Firmar digitalmente las comunicaciones (siempre), en esos servidores. Para obtener más información acerca de estas configuraciones, consulte la sección 'Cliente y servidor de red de Microsoft: firma digital de comunicaciones (cuatro configuraciones relacionadas)' en el Capítulo 5 de la guía Amenazas y contramedidas. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters -> RequireSecuritySignature -> 1

- **15026. Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'.**

Razón fundamental
El secuestro de sesiones utiliza herramientas que permiten a los atacantes que tienen acceso a la misma red que el cliente o el servidor interrumpir, finalizar o robar una sesión en curso. Los atacantes pueden potencialmente interceptar y modificar paquetes SMB no firmados y luego modificar el tráfico y reenviarlo para que el servidor pueda realizar acciones no deseadas. Alternativamente, el atacante podría hacerse pasar por el servidor o el cliente después de una autenticación legítima y obtener acceso no autorizado a los datos. SMB es el protocolo de uso compartido de recursos que es compatible con muchos sistemas operativos Windows. Es la base de NetBIOS y muchos otros protocolos. Las firmas SMB autentican tanto a los usuarios como a los servidores que alojan los datos. Si alguna de las partes falla en el proceso de autenticación, no se realizará la transmisión de datos.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre).

Descripción
Esta configuración de directiva determina si el componente del servidor SMB requiere la firma de paquetes. Habilite esta configuración de directiva en un entorno mixto para evitar que los clientes posteriores utilicen la estación de trabajo como un servidor de red. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters -> RequireSecuritySignature -> 1

- **15027. Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'.**

Razón fundamental
El secuestro de sesiones utiliza herramientas que permiten a los atacantes que tienen acceso a la misma red que el cliente o el servidor interrumpir, finalizar o robar una sesión en curso. Los atacantes pueden potencialmente interceptar y modificar paquetes SMB no firmados y luego modificar el tráfico y reenviarlo para que el servidor pueda realizar acciones no deseadas. Alternativamente, el atacante podría hacerse pasar por el servidor o el cliente después de una autenticación legítima y obtener acceso no autorizado a los datos. SMB es el protocolo de uso compartido de recursos que es compatible con muchos sistemas operativos Windows. Es la base de NetBIOS y muchos otros protocolos. Las firmas SMB autentican tanto a los usuarios como a los servidores que alojan los datos. Si alguna de las partes falla en el proceso de autenticación, no se realizará la transmisión de datos.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Servidor de red de Microsoft: Firme digitalmente las comunicaciones (si el cliente está de acuerdo).

Descripción
Esta configuración de directiva determina si el servidor SMB negociará la firma de paquetes SMB con los clientes que lo soliciten. Si no llega ninguna solicitud de firma

del cliente, se permitirá una conexión sin una firma si el servidor de red de Microsoft: la configuración Firmar digitalmente las comunicaciones (siempre) no está habilitada. Nota: Habilite esta configuración de política en clientes SMB en su red para que sean completamente efectivos para la firma de paquetes con todos los clientes y servidores en su entorno. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters -> EnableSecuritySignature -> 1

- **Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'.**

Razón fundamental

Un usuario no autorizado podría enumerar de forma anónima nombres de cuentas y recursos compartidos y usar la información para intentar adivinar contraseñas o realizar ataques de ingeniería social. (Los ataques de ingeniería social intentan engañar a los usuarios de alguna manera para obtener contraseñas o algún tipo de información de seguridad).

Remediación

Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta U en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Acceso a la red: no permitir la enumeración anónima de cuentas y recursos compartidos SAM.

Descripción

Esta configuración de directiva controla la capacidad de los usuarios anónimos para enumerar cuentas SAM y recursos compartidos. Si habilita esta configuración de política, los usuarios anónimos no podrán enumerar los nombres de usuario de la cuenta de dominio y los nombres de recursos compartidos de red en los sistemas de su entorno. El estado recomendado para esta configuración es: Habilitado. Nota: esta política no tiene efecto en los controladores de dominio.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa -> RestrictAnonymous -> 1

- **15032. Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'.**

Razón fundamental
El usuario puede acceder a las contraseñas que se almacenan en caché cuando inicia sesión en la computadora. Aunque esta información puede parecer obvia, puede surgir un problema si el usuario, sin saberlo, ejecuta un código hostil que lee las contraseñas y las reenvía a otro usuario no autorizado.

Remediación
Para establecer la configuración recomendada a través de la GP, establezca la siguiente ruta de la interfaz de usuario en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Acceso a la red: no permitir el almacenamiento de contraseñas y credenciales para la autenticación de red.

Descripción
Esta configuración de directiva determina si Credential Manager (anteriormente denominado Nombres de usuario y contraseñas almacenados) guarda contraseñas o credenciales para su uso posterior cuando obtiene la autenticación de dominio. El estado recomendado para esta configuración es: Habilitado. Nota: Los cambios en esta configuración no surtirán efecto hasta que se reinicie Windows.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa -> DisableDomainCreds -> 1

- **15034. Configure 'Network access: Named Pipes that can be accessed anonymously'.**

Razón fundamental
Limitar las canalizaciones con nombre a las que se puede acceder de forma anónima reducirá la superficie de ataque del sistema.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de interfaz de usuario: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Acceso a la red: canalizaciones con nombre a las que se puede acceder de forma anónima.

Descripción
Esta configuración de directiva determina qué sesiones de comunicación o canalizaciones tendrán atributos y permisos que permitan el acceso anónimo. El estado recomendado para esta configuración es: - Nivel 1 - Controlador de dominio. El estado recomendado para esta configuración es: LSARPC, NETLOGON, SAMR y (cuando el servicio de navegador de computadora heredado está habilitado) NAVEGADOR. - Nivel 1 - Servidor miembro. El estado recomendado para esta configuración es: <en blanco> (es decir, ninguno) o (cuando el servicio antiguo del Explorador de equipos está habilitado) NAVEGADOR. Nota: Un servidor miembro que tenga la función de servicios de escritorio remoto con el servicio de función de licencia de escritorio remoto requerirá una excepción especial a esta recomendación, para permitir el acceso anónimo a las canalizaciones con nombre de HydraLSPipe y TermServLicensing.

Check (Condition: all)
r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters -> NullSessionPipes -> r:lsarpc && r:netlogon && r:samr

- **15048. Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'.**

Razón fundamental
Puede habilitar ambas opciones para esta configuración de política para ayudar a proteger el tráfico de red que usa el proveedor de soporte de seguridad NTLM (NTLM SSP) para que no sea expuesto o manipulado por un atacante que haya obtenido acceso a la misma red. En otras palabras, estas opciones ayudan a proteger contra los ataques de intermediarios.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de IU para Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Seguridad de red: Seguridad de sesión mínima para NTLM Clientes basados en SSP (incluido RPC seguro).

Descripción
Esta configuración de directiva determina qué comportamientos permiten los clientes para las aplicaciones que usan el proveedor de soporte de seguridad (SSP) NTLM. La interfaz SSP (SSPI) es utilizada por aplicaciones que necesitan servicios de autenticación. La configuración no modifica cómo funciona la secuencia de

autenticación, sino que requiere ciertos comportamientos en las aplicaciones que usan SSPI. El estado recomendado para esta configuración es: Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits. Nota: Estos valores dependen del valor de configuración de Seguridad de red: nivel de autenticación de LAN Manager (regla 2.3.11.7).

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0 -> NTLMMinClientSec -> 537395200

- **15049. Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'.**

Razón fundamental

Puede habilitar todas las opciones de esta configuración de política para ayudar a proteger el tráfico de red que usa el proveedor de soporte de seguridad NTLM (NTLM SSP) para que no sea expuesto o manipulado por un atacante que haya obtenido acceso a la misma red. Es decir, estas opciones ayudan a proteger contra los ataques de intermediarios.

Remediación

Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de IU para Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Seguridad de red: Seguridad de sesión mínima para NTLM Servidores basados en SSP (incluyendo RPC seguro).

Descripción

Esta configuración de directiva determina qué comportamientos permiten los servidores para las aplicaciones que usan el proveedor de soporte de seguridad (SSP) NTLM. La interfaz SSP (SSPI) es utilizada por aplicaciones que necesitan servicios de autenticación. La configuración no modifica cómo funciona la secuencia de autenticación, sino que requiere ciertos comportamientos en las aplicaciones que usan SSPI. El estado recomendado para esta configuración es: Requerir seguridad de sesión NTLMv2, Requerir cifrado de 128 bits. Nota: Estos valores dependen del valor de configuración de Seguridad de red: nivel de autenticación de LAN Manager (regla 2.3.11.7).

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0 -> NTLMMinServerSec -> 537395200

- **15053. Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'.**

Razón fundamental
Uno de los riesgos que la función Control de cuentas de usuario introducida con Windows Vista está tratando de mitigar es el software malicioso que se ejecuta con credenciales elevadas sin que el usuario o el administrador estén al tanto de su actividad. Un vector de ataque de estos programas era descubrir la contraseña de la cuenta denominada 'Administrador' porque esa cuenta de usuario se creó para todas las instalaciones de Windows. Para abordar este riesgo, en Windows Vista y posteriores, la cuenta de administrador integrada ahora está deshabilitada de forma predeterminada. En una instalación predeterminada de una computadora nueva, las cuentas con control administrativo sobre la computadora se configuran inicialmente de una de estas dos maneras: - Si la computadora no está unida a un dominio, la primera cuenta de usuario que cree tiene los permisos equivalentes como usuario local. administrador. -Si la computadora está unida a un dominio, no se crean cuentas de administrador local. El administrador de la empresa o del dominio debe iniciar sesión en la computadora y crear una si se garantiza una cuenta de administrador local. Una vez que se instala Windows, la cuenta de administrador integrada se puede habilitar manualmente, pero recomendamos enfáticamente que esta cuenta permanezca deshabilitada.

Remediación
Para establecer la configuración recomendada a través de la GP, establezca la siguiente ruta de la interfaz de usuario en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Control de cuentas de usuario: modo de aprobación de administrador para la cuenta de administrador integrada.

Descripción
Esta configuración de política controla el comportamiento del modo de aprobación de administrador para la cuenta de administrador integrada. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> FilterAdministratorToken -> 1

- **15055. Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'.**

Razón fundamental
Uno de los riesgos que la función UAC introducida con Windows Vista está tratando de mitigar es el software malicioso que se ejecuta con credenciales elevadas sin que el usuario o el administrador estén al tanto de su actividad. Esta configuración alerta al administrador de las operaciones con privilegios elevados y le permite evitar que un programa malicioso eleve sus privilegios cuando el programa intenta hacerlo.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de la IU para Solicitar consentimiento en el escritorio seguro: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Control de cuentas de usuario: Comportamiento de la solicitud de elevación para administradores en el modo de aprobación del administrador.

Descripción
Esta configuración de directiva controla el comportamiento de la solicitud de elevación para los administradores. El estado recomendado para esta configuración es: Solicitar consentimiento en el escritorio seguro.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> ConsentPromptBehaviorAdmin -> 2

- **15056. Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'.**

Razón fundamental
Uno de los riesgos que la característica de Control de cuentas de usuario introducida con Windows Vista está tratando de mitigar es el de los programas maliciosos que se ejecutan con credenciales elevadas sin que el usuario o el administrador estén al tanto de su actividad. Esta configuración alerta al usuario de que un programa requiere el uso de operaciones con privilegios elevados y requiere que el usuario pueda proporcionar credenciales administrativas para que el programa se ejecute.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de la interfaz de usuario para denegar automáticamente las solicitudes de elevación: Configuración del equipo\Políticas\Configuración de

Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Control de cuentas de usuario: Comportamiento de la solicitud de elevación para usuarios estándar.

Descripción
Esta configuración de directiva controla el comportamiento de la solicitud de elevación para los usuarios estándar. El estado recomendado para esta configuración es: Denegar automáticamente las solicitudes de elevación.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> ConsentPromptBehaviorUser -> 0

- **15090. Ensure LAPS AdmPwd GPO Extension / CSE is installed.**

Razón fundamental
Debido a la dificultad de administrar las contraseñas de los administradores locales, muchas organizaciones optan por utilizar la misma contraseña en todas las estaciones de trabajo y/o servidores miembros cuando los implementan. Esto crea un riesgo de seguridad de superficie de ataque grave porque si un atacante logra comprometer un sistema y conoce la contraseña de su cuenta de administrador local, entonces puede aprovechar esa cuenta para obtener acceso instantáneo a todas las demás computadoras que también usan esa contraseña para su administrador local. cuenta.

Remediación
Para utilizar LAPS, se requiere una actualización menor del esquema de Active Directory y se debe instalar una extensión del lado del cliente (CSE) de la política de grupo en cada computadora administrada. Cuando se instala LAPS, el archivo AdmPwd.dll debe estar presente en la siguiente ubicación y registrado en Windows (la instalación de LAPS AdmPwd GPO Extension / CSE hace esto por usted): C:\Program Files\LAPS\CSE\AdmPwd.dll

Descripción
En mayo de 2015, Microsoft lanzó la herramienta Solución de contraseña de administrador local (LAPS), que es un software gratuito y compatible que permite a una organización establecer automáticamente contraseñas de cuenta de administrador locales únicas y aleatorias en estaciones de trabajo conectadas a un dominio y servidores miembros. Las contraseñas se almacenan en un atributo confidencial de la cuenta de la computadora del dominio y los administradores de sistemas aprobados pueden recuperarlas de Active Directory cuando sea necesario. La herramienta LAPS requiere una pequeña actualización del esquema de Active Directory para poder implementarse, así como la instalación de una extensión del

lado del cliente (CSE) de la directiva de grupo en los equipos de destino. Consulte la documentación de LAPS para obtener más información. LAPS es compatible con Windows Vista o sistemas operativos de estación de trabajo más nuevos, y Server 2003 o sistemas operativos de servidor más nuevos. LAPS no admite computadoras independientes; deben estar unidas a un dominio. Nota: Las organizaciones que utilizan software comercial de terceros para administrar contraseñas de administrador local únicas y complejas en miembros del dominio pueden optar por ignorar estas recomendaciones de LAPS. Nota n.º 2: LAPS solo está diseñado para administrar contraseñas de administrador local y, por lo tanto, no se recomienda (ni se admite) para usar directamente en controladores de dominio, que no tienen una cuenta de administrador local tradicional. Le recomendamos encarecidamente que solo implemente la configuración de LAPS CSE y LAPS GPO en estaciones de trabajo y servidores miembros.

Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}
- r:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA} -> DllName

- **15097. Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver'.**

Razón fundamental

Desde septiembre de 2016, Microsoft ha recomendado enfáticamente que SMBv1 se deshabilite y ya no se use en las redes modernas, ya que es un diseño de 30 años que es mucho más vulnerable a los ataques que los diseños mucho más nuevos, como SMBv2 y SMBv3.

Remediación

Para establecer la configuración recomendada a través de la GP, establezca la siguiente ruta de la interfaz de usuario en Habilitado: Deshabilitar controlador: Configuración del equipo\Políticas\Plantillas administrativas\Guía de seguridad de MS\Configurar controlador de cliente SMB v1. Nota: esta ruta de directiva de grupo no existe de forma predeterminada. Se requiere una plantilla de directiva de grupo adicional (SecGuide.admx/adml); está disponible en Microsoft

Descripción

Esta opción configura el tipo de inicio para el servicio de controlador de cliente (MRxSmb10) del Bloque de mensajes del servidor versión 1 (SMBv1), que se

recomienda desactivar. El estado recomendado para esta configuración es: Habilitado: deshabilitar el controlador. Nota: Bajo ninguna circunstancia, configure esta configuración general como Deshabilitada, ya que al hacerlo se eliminará por completo la entrada de registro subyacente, lo que causará problemas graves.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10 -> Start -> 4

- **15014. Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'.**

Razón fundamental

Se espera este comportamiento. El problema es que el período de tiempo de espera de 10 minutos para las rutas de redirección de ICMP crea temporalmente una situación de red en la que el tráfico ya no se enrutará correctamente para el host afectado. Ignorar dichos redireccionamientos ICMP limitará la exposición del sistema a ataques que afectarán su capacidad para participar en la red.

Remediación

Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de la interfaz de usuario en Deshabilitada: Configuración del equipo\Políticas\Plantillas administrativas\MSS (heredado)\MSS: (EnableICMPRedirect) Permitir redireccionamientos ICMP para anular rutas generadas por OSPF Nota: esta ruta de directiva de grupo no existe por defecto. Se requiere una plantilla de directiva de grupo adicional (MSS-legacy.admx/adml); está disponible en esta publicación de blog de TechNet: La configuración de MSS: blog de orientación de seguridad de Microsoft.

Descripción

Los redireccionamientos del Protocolo de mensajes de control de Internet (ICMP) hacen que la pila IPv4 conecte las rutas del host. Estas rutas anulan las rutas generadas Open Shortest Path First (OSPF). El estado recomendado para esta configuración es: Deshabilitado.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -> EnableICMPRedirect -> 0

- **15153. Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'.**

Razón fundamental
Un usuario puede ser engañado y aceptar una oferta de asistencia remota no solicitada de un usuario malintencionado.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de UI en Deshabilitada: Configuración del equipo\Políticas\Plantillas administrativas\Sistema\Asistencia remota\Configurar oferta de asistencia remota Nota: Es posible que esta ruta de directiva de grupo no exista de forma predeterminada. Lo proporciona la plantilla de directiva de grupo RemoteAssistance.admx/adml que se incluye con las plantillas administrativas (o posteriores) de Microsoft Windows 8.0 y Server 2012 (no R2).

Descripción
Esta configuración de política le permite activar o desactivar Ofrecer asistencia remota (no solicitada) en esta computadora. La mesa de ayuda y el personal de soporte no podrán ofrecer asistencia de manera proactiva, aunque aún pueden responder a las solicitudes de asistencia de los usuarios. El estado recomendado para esta configuración es: Deshabilitado.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services -> fAllowUnsolicited -> 0

- **15154. Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'.**

Razón fundamental
Existe un ligero riesgo de que un administrador deshonesto obtenga acceso a la sesión de escritorio de otro usuario; sin embargo, no puede conectarse a la computadora de un usuario sin previo aviso ni controlarla sin el permiso del usuario. Cuando un experto intenta conectarse, el usuario aún puede optar por denegar la conexión o otorgar al experto privilegios de solo lectura. El usuario debe hacer clic explícitamente en el botón Sí para permitir que el experto controle la estación de trabajo de forma remota.

Remediación
Para establecer la configuración recomendada a través de la GP, establezca la siguiente ruta de la interfaz de usuario en Deshabilitada: Configuración del equipo\Políticas\Plantillas administrativas\Sistema\Asistencia remota\Configurar asistencia remota solicitada Nota: es posible que esta ruta de directiva de grupo no exista de forma predeterminada. Lo proporciona la plantilla de directiva de grupo

RemoteAssistance.admx/adml que se incluye con las plantillas administrativas (o posteriores) de Microsoft Windows 8.0 y Server 2012 (no R2).

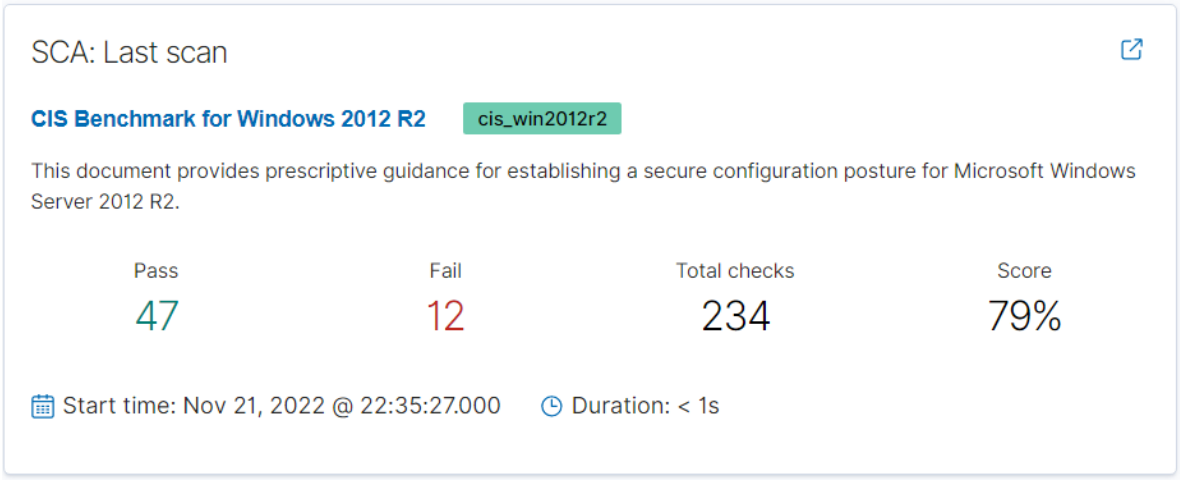
Descripción
Esta configuración de directiva le permite activar o desactivar la asistencia remota solicitada (Solicitar) en esta computadora. El estado recomendado para esta configuración es: Deshabilitado.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services -> fAllowToGetHelp -> 0

5.4.4.6 **TS**

Figura 13. Wazuh Score - TS



Fuente: Propia.

- **15018. Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)'.**

Razón fundamental
El número que se asigna a esta configuración de directiva indica el número de usuarios cuya información de inicio de sesión la computadora almacenará en caché localmente. Si el número se establece en 4, la computadora almacena en caché la información de inicio de sesión de 4 usuarios. Cuando un quinto usuario inicia sesión en la computadora, el servidor sobrescribe la sesión de inicio de sesión en caché más antigua. Los usuarios que accedan a la consola de la computadora tendrán sus credenciales de inicio de sesión almacenadas en caché en esa computadora. Un atacante que pueda acceder al sistema de archivos de la computadora podría ubicar esta información almacenada en caché y usar un ataque de fuerza bruta para intentar determinar las contraseñas de los usuarios. Para mitigar este tipo de ataque, Windows cifra la información y oculta su ubicación física.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de la interfaz de usuario en 4 o menos inicios de sesión: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Inicio de sesión interactivo: Número de inicios de sesión anteriores en caché (en caso de que el controlador de dominio no esté disponible).

Descripción
Esta configuración de directiva determina si un usuario puede iniciar sesión en un dominio de Windows utilizando la información de cuenta almacenada en caché. La información de inicio de sesión para cuentas de dominio se puede almacenar en caché localmente para permitir que los usuarios inicien sesión incluso si no se puede contactar a un controlador de dominio. Esta configuración de directiva determina la cantidad de usuarios únicos para quienes la información de inicio de sesión se almacena en caché localmente. Si este valor se establece en 0, la función de caché de inicio de sesión está deshabilitada. Un atacante que pueda acceder al sistema de archivos del servidor podría ubicar esta información almacenada en caché y usar un ataque de fuerza bruta para determinar las contraseñas de los usuarios. El estado recomendado para esta configuración es: 4 o menos inicios de sesión.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon -> CachedLogonsCount -> n:^(\d+) compare <= 4

- **15020. Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'.**

Razón fundamental
De manera predeterminada, la computadora almacena en caché en la memoria las credenciales de cualquier usuario autenticado localmente. La computadora usa estas credenciales almacenadas en caché para autenticar a cualquier persona que intente desbloquear la consola. Cuando se utilizan credenciales almacenadas en caché, los cambios que se hayan realizado recientemente en la cuenta, como las asignaciones de derechos de usuario, el bloqueo de la cuenta o la desactivación de la cuenta, no se tienen en cuenta ni se aplican después de autenticar la cuenta. Los privilegios de usuario no se actualizan y (lo que es más importante) las cuentas deshabilitadas aún pueden desbloquear la consola de la computadora.

Remediación
Para implementar la configuración recomendada a través de GP, establezca la siguiente ruta de la interfaz de usuario en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Inicio de sesión interactivo: Requerir autenticación del controlador de dominio para desbloquear la estación de trabajo.

Descripción
Se requiere información de inicio de sesión para desbloquear una computadora bloqueada. Para las cuentas de dominio, esta configuración de seguridad determina

si es necesario comunicarse con un controlador de dominio para desbloquear una computadora. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon -> ForceUnlockLogon -> 1

- **15034. Configure 'Network access: Named Pipes that can be accessed anonymously'.**

Razón fundamental
Limitar las canalizaciones con nombre a las que se puede acceder de forma anónima reducirá la superficie de ataque del sistema.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de interfaz de usuario: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Acceso a la red: canalizaciones con nombre a las que se puede acceder de forma anónima.

Descripción
Esta configuración de directiva determina qué sesiones de comunicación o canalizaciones tendrán atributos y permisos que permitan el acceso anónimo. El estado recomendado para esta configuración es: - Nivel 1 - Controlador de dominio. El estado recomendado para esta configuración es: LSARPC, NETLOGON, SAMR y (cuando el servicio de navegador de computadora heredado está habilitado) NAVEGADOR. - Nivel 1 - Servidor miembro. El estado recomendado para esta configuración es: <en blanco> (es decir, ninguno) o (cuando el servicio antiguo del Explorador de equipos está habilitado) NAVEGADOR. Nota: Un servidor miembro que tenga la función de servicios de escritorio remoto con el servicio de función de licencia de escritorio remoto requerirá una excepción especial a esta recomendación, para permitir el acceso anónimo a las canalizaciones con nombre de HydraLSPipe y TermServLicensing.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters -> NullSessionPipes -> r:lsarpc && r:netlogon && r:samr

- **15053. Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'.**

Razón fundamental
Uno de los riesgos que la función Control de cuentas de usuario introducida con Windows Vista está tratando de mitigar es el software malicioso que se ejecuta con credenciales elevadas sin que el usuario o el administrador estén al tanto de su actividad. Un vector de ataque de estos programas era descubrir la contraseña de la cuenta denominada 'Administrador' porque esa cuenta de usuario se creó para todas las instalaciones de Windows. Para abordar este riesgo, en Windows Vista y posteriores, la cuenta de administrador integrada ahora está deshabilitada de forma predeterminada. En una instalación predeterminada de una computadora nueva, las cuentas con control administrativo sobre la computadora se configuran inicialmente de una de estas dos maneras: - Si la computadora no está unida a un dominio, la primera cuenta de usuario que cree tiene los permisos equivalentes como usuario local. administrador. -Si la computadora está unida a un dominio, no se crean cuentas de administrador local. El administrador de la empresa o del dominio debe iniciar sesión en la computadora y crear una si se garantiza una cuenta de administrador local. Una vez que se instala Windows, la cuenta de administrador integrada se puede habilitar manualmente, pero recomendamos enfáticamente que esta cuenta permanezca deshabilitada.

Remediación
Para establecer la configuración recomendada a través de la GP, establezca la siguiente ruta de la interfaz de usuario en Habilitado: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Control de cuentas de usuario: modo de aprobación de administrador para la cuenta de administrador integrada.

Descripción
Esta configuración de política controla el comportamiento del modo de aprobación de administrador para la cuenta de administrador integrada. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> FilterAdministratorToken -> 1

- **15055. Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'.**

Razón fundamental
Uno de los riesgos que la función UAC introducida con Windows Vista está tratando de mitigar es el software malicioso que se ejecuta con credenciales elevadas sin que el usuario o el administrador estén al tanto de su actividad. Esta configuración alerta al administrador de las operaciones con privilegios elevados y le permite evitar que un programa malicioso eleve sus privilegios cuando el programa intenta hacerlo.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de la IU para Solicitar consentimiento en el escritorio seguro: Configuración del equipo\Políticas\Configuración de Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Control de cuentas de usuario: Comportamiento de la solicitud de elevación para administradores en el modo de aprobación del administrador.

Descripción
Esta configuración de directiva controla el comportamiento de la solicitud de elevación para los administradores. El estado recomendado para esta configuración es: Solicitar consentimiento en el escritorio seguro.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> ConsentPromptBehaviorAdmin -> 2

- **15056. Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'.**

Razón fundamental
Uno de los riesgos que la característica de Control de cuentas de usuario introducida con Windows Vista está tratando de mitigar es el de los programas maliciosos que se ejecutan con credenciales elevadas sin que el usuario o el administrador estén al tanto de su actividad. Esta configuración alerta al usuario de que un programa requiere el uso de operaciones con privilegios elevados y requiere que el usuario pueda proporcionar credenciales administrativas para que el programa se ejecute.

Remediación
Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de la interfaz de usuario para denegar automáticamente las solicitudes de elevación: Configuración del equipo\Políticas\Configuración de

Windows\Configuración de seguridad\Políticas locales\Opciones de seguridad\Control de cuentas de usuario: Comportamiento de la solicitud de elevación para usuarios estándar.

Descripción
Esta configuración de directiva controla el comportamiento de la solicitud de elevación para los usuarios estándar. El estado recomendado para esta configuración es: Denegar automáticamente las solicitudes de elevación.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System -> ConsentPromptBehaviorUser -> 0

- **15090. Ensure LAPS AdmPwd GPO Extension / CSE is installed.**

Razón fundamental
Debido a la dificultad de administrar las contraseñas de los administradores locales, muchas organizaciones optan por utilizar la misma contraseña en todas las estaciones de trabajo y/o servidores miembros cuando los implementan. Esto crea un riesgo de seguridad de superficie de ataque grave porque si un atacante logra comprometer un sistema y conoce la contraseña de su cuenta de administrador local, entonces puede aprovechar esa cuenta para obtener acceso instantáneo a todas las demás computadoras que también usan esa contraseña para su administrador local. cuenta.

Remediación
Para utilizar LAPS, se requiere una actualización menor del esquema de Active Directory y se debe instalar una extensión del lado del cliente (CSE) de la política de grupo en cada computadora administrada. Cuando se instala LAPS, el archivo AdmPwd.dll debe estar presente en la siguiente ubicación y registrado en Windows (la instalación de LAPS AdmPwd GPO Extension / CSE hace esto por usted): C:\Program Files\LAPS\CSE\AdmPwd.dll

Descripción
En mayo de 2015, Microsoft lanzó la herramienta Solución de contraseña de administrador local (LAPS), que es un software gratuito y compatible que permite a una organización establecer automáticamente contraseñas de cuenta de administrador locales únicas y aleatorias en estaciones de trabajo conectadas a un dominio y servidores miembros. Las contraseñas se almacenan en un atributo confidencial de la cuenta de la computadora del dominio y los administradores de sistemas aprobados pueden recuperarlas de Active Directory cuando sea necesario. La herramienta LAPS requiere una pequeña actualización del esquema de Active Directory para poder implementarse, así como la instalación de una extensión del

lado del cliente (CSE) de la directiva de grupo en los equipos de destino. Consulte la documentación de LAPS para obtener más información. LAPS es compatible con Windows Vista o sistemas operativos de estación de trabajo más nuevos, y Server 2003 o sistemas operativos de servidor más nuevos. LAPS no admite computadoras independientes; deben estar unidas a un dominio. Nota: Las organizaciones que utilizan software comercial de terceros para administrar contraseñas de administrador local únicas y complejas en miembros del dominio pueden optar por ignorar estas recomendaciones de LAPS. Nota n.º 2: LAPS solo está diseñado para administrar contraseñas de administrador local y, por lo tanto, no se recomienda (ni se admite) para usar directamente en controladores de dominio, que no tienen una cuenta de administrador local tradicional. Le recomendamos encarecidamente que solo implemente la configuración de LAPS CSE y LAPS GPO en estaciones de trabajo y servidores miembros.

Checks (Condition: all)

- r:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}
- r:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA} -> DllName

- **15097. Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver'.**

Razón fundamental

Desde septiembre de 2016, Microsoft ha recomendado enfáticamente que SMBv1 se deshabilite y ya no se use en las redes modernas, ya que es un diseño de 30 años que es mucho más vulnerable a los ataques que los diseños mucho más nuevos, como SMBv2 y SMBv3.

Remediación

Para establecer la configuración recomendada a través de la GP, establezca la siguiente ruta de la interfaz de usuario en Habilitado: Deshabilitar controlador: Configuración del equipo\Políticas\Plantillas administrativas\Guía de seguridad de MS\Configurar controlador de cliente SMB v1. Nota: esta ruta de directiva de grupo no existe de forma predeterminada. Se requiere una plantilla de directiva de grupo adicional (SecGuide.admx/adml); está disponible en Microsoft

Descripción

Esta opción configura el tipo de inicio para el servicio de controlador de cliente (MRxSmb10) del Bloque de mensajes del servidor versión 1 (SMBv1), que se recomienda desactivar. El estado recomendado para esta configuración es:

Habilitado: deshabilitar el controlador. Nota: Bajo ninguna circunstancia, configure esta configuración general como Deshabilitada, ya que al hacerlo se eliminará por completo la entrada de registro subyacente, lo que causará problemas graves.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10 -> Start -> 4

- **15104. Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'.**

Razón fundamental

Se espera este comportamiento. El problema es que el período de tiempo de espera de 10 minutos para las rutas de redirección de ICMP crea temporalmente una situación de red en la que el tráfico ya no se enrutará correctamente para el host afectado. Ignorar dichos redireccionamientos ICMP limitará la exposición del sistema a ataques que afectarán su capacidad para participar en la red.

Remediación

Para establecer la configuración recomendada a través de GP, configure la siguiente ruta de la interfaz de usuario en Deshabilitada: Configuración del equipo\Políticas\Plantillas administrativas\MSS (heredado)\MSS: (EnableICMPRedirect) Permitir redireccionamientos ICMP para anular rutas generadas por OSPF Nota: esta ruta de directiva de grupo no existe por defecto. Se requiere una plantilla de directiva de grupo adicional (MSS-legacy.admx/adml); está disponible en esta publicación de blog de TechNet: La configuración de MSS: blog de orientación de seguridad de Microsoft.

Descripción

Los redireccionamientos del Protocolo de mensajes de control de Internet (ICMP) hacen que la pila IPv4 conecte las rutas del host. Estas rutas anulan las rutas generadas Open Shortest Path First (OSPF). El estado recomendado para esta configuración es: Deshabilitado.

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -> EnableICMPRedirect -> 0

- **15191. Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled'.**

Razón fundamental
Esta configuración garantiza que los usuarios y administradores que utilicen el escritorio remoto en un servidor seguirán utilizando la misma sesión; si se desconectan y se vuelven a conectar, volverán a la misma sesión que estaban utilizando antes, evitando la creación de una segunda sesión simultánea. Esto evita el uso innecesario de recursos al hacer que el servidor aloje sesiones adicionales innecesarias (lo que supondría una carga adicional para el servidor) y también garantiza una experiencia coherente para el usuario.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en Habilitado: Configuración del equipo\Políticas\Plantillas administrativas\Componentes de Windows\Servicios de escritorio remoto\Host de sesión de escritorio remoto\Conexiones\Restringir usuarios de Servicios de escritorio remoto a una sola sesión de Servicios de escritorio remoto . Nota: Esta ruta de directiva de grupo la proporciona la plantilla de directiva de grupo TerminalServer.admx/adml que se incluye con todas las versiones de las plantillas administrativas de Microsoft Windows. Nota n.º 2: en las plantillas administrativas de Microsoft Windows anteriores, esta configuración se denominaba Restringir a los usuarios de Servicios de Terminal Server a una única sesión remota, pero se cambió el nombre a partir de las Plantillas administrativas de Windows 7 y Server 2008 R2.

Descripción
Esta configuración de política le permite restringir a los usuarios a una única sesión de Servicios de Escritorio remoto. El estado recomendado para esta configuración es: Habilitado.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services -> fSingleSessionPerUser -> 1

- **15199. Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'.**

Razón fundamental
Esta configuración ayuda a evitar que las sesiones activas de Escritorio remoto ocupen la computadora durante largos períodos de tiempo mientras no está en uso, lo que evita que una gran cantidad de sesiones inactivas consuman los recursos informáticos. Además, las sesiones antiguas y olvidadas de Escritorio remoto que aún están activas pueden causar bloqueos de contraseña si la contraseña del

usuario ha cambiado pero la sesión anterior aún se está ejecutando. Para los sistemas que limitan la cantidad de usuarios conectados (por ejemplo, servidores en el modo administrativo predeterminado: solo 2 sesiones), las sesiones antiguas pero aún activas de otros usuarios pueden evitar que otro usuario se conecte, lo que resulta en una denegación de servicio efectiva.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en Habilitado: 15 minutos o menos: Configuración del equipo\Políticas\Plantillas administrativas\Componentes de Windows\Servicios de escritorio remoto\Host de sesión de escritorio remoto\Límites de tiempo de sesión\Establecer límite de tiempo para activo pero sesiones inactivas de Servicios de Escritorio remoto. Nota: Esta ruta de directiva de grupo la proporciona la plantilla de directiva de grupo TerminalServer.admx/adml que se incluye con todas las versiones de las plantillas administrativas de Microsoft Windows. Nota n.º 2: en las plantillas administrativas de Microsoft Windows anteriores, esta configuración se denominaba Establecer límite de tiempo para las sesiones de Servicios de Terminal Server activas pero inactivas, pero se le cambió el nombre a partir de las plantillas administrativas de Windows 7 y Server 2008 R2.

Descripción
Esta configuración de política le permite especificar la cantidad máxima de tiempo que una sesión activa de Servicios de Escritorio remoto puede estar inactiva (sin intervención del usuario) antes de que se desconecte automáticamente. El estado recomendado para esta configuración es: Habilitado: 15 minutos o menos.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services -> MaxIdleTime -> n:^(\d+) compare <= 900000

- **15200. Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'.**

Razón fundamental
Esta configuración ayuda a evitar que las sesiones activas de Escritorio remoto ocupen la computadora durante largos períodos de tiempo mientras no está en uso, lo que evita que los recursos informáticos se consuman por un gran número de sesiones desconectadas pero aún activas. Además, las sesiones antiguas y olvidadas de Escritorio remoto que aún están activas pueden causar bloqueos de contraseña si la contraseña del usuario ha cambiado pero la sesión anterior aún se está ejecutando. Para los sistemas que limitan la cantidad de usuarios conectados (por ejemplo, servidores en el modo administrativo predeterminado: solo 2 sesiones), las sesiones antiguas pero aún activas de otros usuarios pueden evitar

que otro usuario se conecte, lo que resulta en una denegación de servicio efectiva. Esta configuración es importante para garantizar que una sesión desconectada finalice correctamente.

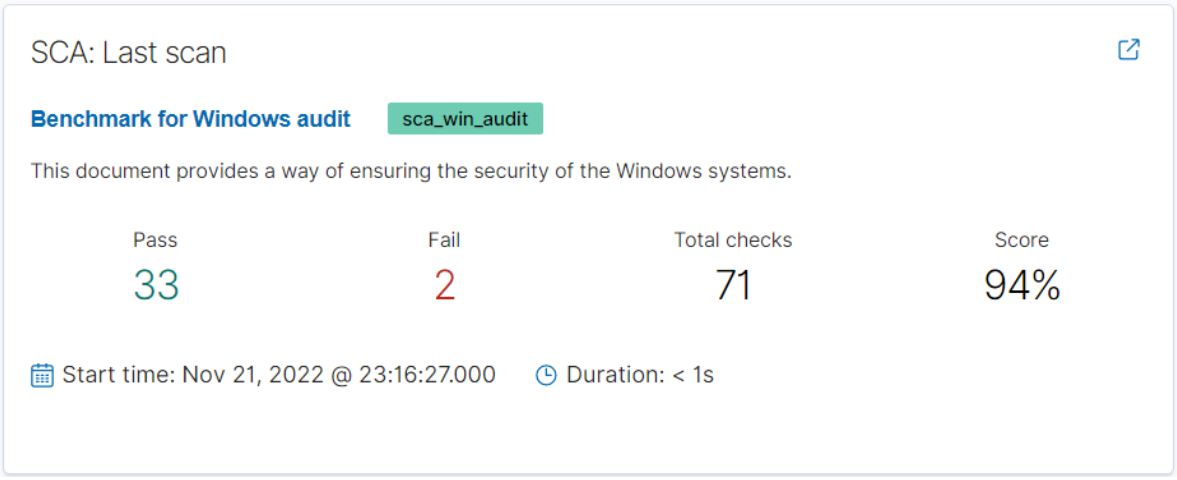
Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de IU en Habilitado: 1 minuto: Configuración del equipo\Políticas\Plantillas administrativas\Componentes de Windows\Servicios de escritorio remoto\Host de sesión de escritorio remoto\Límites de tiempo de sesión\Establecer límite de tiempo para sesiones desconectadas. Nota: Esta ruta de directiva de grupo la proporciona la plantilla de directiva de grupo TerminalServer.admx/adml que se incluye con todas las versiones de las plantillas administrativas de Microsoft Windows.

Descripción
Esta configuración de directiva le permite configurar un límite de tiempo para las sesiones de Servicios de Escritorio remoto desconectadas. El estado recomendado para esta configuración es: Habilitado: 1 minuto.

Check (Condition: all)
- r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services -> MaxDisconnectionTime -> 60000

5.4.4.7 **AD**

Figura 14. Wazuh Score - AD



Fuente: Propia

- **14553. Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'.**

Razón fundamental
Un usuario puede ser engañado y aceptar una oferta de asistencia remota no solicitada de un usuario malintencionado.

Remediación
Para establecer la configuración recomendada a través de GP, establezca la siguiente ruta de UI en Deshabilitada: Configuración del equipo\Políticas\Plantillas administrativas\Sistema\Asistencia remota\Configurar oferta de asistencia remota Nota: Es posible que esta ruta de directiva de grupo no exista de forma predeterminada. Lo proporciona la plantilla de directiva de grupo RemoteAssistance.admx/adml que se incluye con las plantillas administrativas (o posteriores) de Microsoft Windows 8.0 y Server 2012 (no R2).

Descripción
Esta configuración de política le permite activar o desactivar Ofrecer asistencia remota (no solicitada) en esta computadora. La mesa de ayuda y el personal de soporte no podrán ofrecer asistencia de manera proactiva, aunque aún pueden responder a las solicitudes de asistencia de los usuarios. El estado recomendado para esta configuración es: Deshabilitado

Check (Condition: all)

- r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services -> fAllowUnsolicited -> 0

- **14554. Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'.**

Razón fundamental

Existe un ligero riesgo de que un administrador deshonesto obtenga acceso a la sesión de escritorio de otro usuario; sin embargo, no puede conectarse a la computadora de un usuario sin previo aviso ni controlarla sin el permiso del usuario. Cuando un experto intenta conectarse, el usuario aún puede optar por denegar la conexión o otorgar al experto privilegios de solo lectura. El usuario debe hacer clic explícitamente en el botón Sí para permitir que el experto controle la estación de trabajo de forma remota.

Remediación

Para establecer la configuración recomendada a través de la GP, establezca la siguiente ruta de la interfaz de usuario en Deshabilitada: Configuración del equipo\Políticas\Plantillas administrativas\Sistema\Asistencia remota\Configurar asistencia remota solicitada Nota: es posible que esta ruta de directiva de grupo no exista de forma predeterminada. Lo proporciona la plantilla de directiva de grupo RemoteAssistance.admx/adml que se incluye con las plantillas administrativas (o posteriores) de Microsoft Windows 8.0 y Server 2012 (no R2).

Descripción

Esta configuración de directiva le permite activar o desactivar la asistencia remota solicitada (Solicitar) en esta computadora. El estado recomendado para esta configuración es: Deshabilitado.

Check (Condition: all)

r:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services -> fAllowToGetHelp -> 0

6 CONCLUSIONES

- Ecodiesel Colombia cuenta con un esquema de red muy robusto, teniendo alta disponibilidad tanto en sus Firewall como en sus canales de comunicación.

- Se tienen varios servidores críticos sin respaldo, y en caso de alguna contingencia el tiempo de indisponibilidad sería alto.

- El tener el ERP y la base de datos en el mismo servidor constituye un riesgo latente, se debe manejar por separado el servidor de aplicaciones y de Base de Datos.

7 RECOMENDACIONES

7.1 RECOMENDACIONES GENERALES

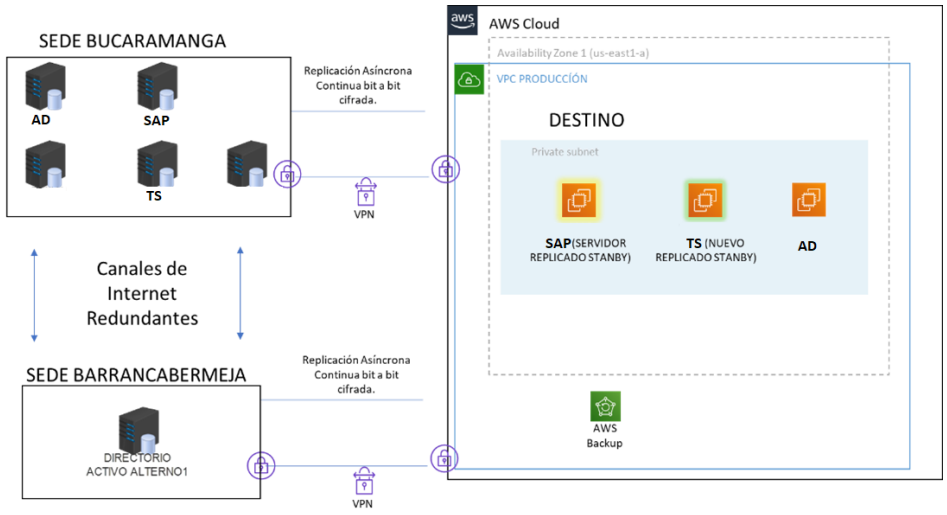
7.1.1 Data Center Alterno o migración a nube. Teniendo en cuenta que toda la infraestructura de la compañía está soportada por servidores ubicados en Data Center On Premise, y no se cuenta con replicación de los servidores en otras ubicaciones, es altamente susceptible a indisponibilidad en caso de fallas de origen natural o humana en los equipos servidores o de red, como lo pueden ser, fallas en el fluido eléctrico, incendio, agua, cortes en las fibras de comunicación, daños eléctricos en ambos Firewall por sobrecarga, etc. En caso de que esto ocurra, toda comunicación proveniente desde la planta industrial hacia el Data Center se perdería, no teniendo contingencia rápida para solucionarlo.

Para lograr subsanar esto, se recomienda migrar toda la infraestructura a servidores en nube, como lo es Azure de Microsoft, Google Cloud de Alphabet (Google) o AWS de Amazon; o por lo menos implementar un Disaster Recovery Plan o DRP dentro del Plan Estratégico de TI PETI con el Data Center alterno en alguna de estas nubes, teniéndolas como respaldo en caso de cualquier impase del Data Center y estando, sincronizándose, de manera continua.

Esta solución también es aplicable si cualquiera de los servidores críticos de la compañía es afectado por un malware de tipo Ransomware, ya que desde la nube se puede recuperar la información a un estado anterior y limpio del malware y luego recuperarlo en el servidor On Premise.

El esquema básico en AWS para los servidores críticos sería el representado en la siguiente gráfica.

Figura 15. Esquema Diseño general comunicaciones y centros de computo



Fuente: Propia.

Tal como se observa en la figura, se han establecido 2 VPN una contra cada sede con el objetivo de garantizar en todo momento la operación y dar flexibilidad ante posibles eventos que afecten la operación.

7.1.2 Actualización de todos los servidores. Partiendo de la base que el Active Directory principal está montado en un Windows Server 2008 R2, y que esto arrastra un sinfín de amenazas, es recomendable migrar inmediatamente versiones más actualizadas de Windows Server, actualmente ya fue liberada la versión 2022.

El End Of Life para esta versión de Windows Server 2008 R2 fue el 14 de Enero del 2020.

El End Of Life para la versión Windows Server 2012 R2 es el 10 de Octubre del 2023.

El End Of Life para la versión del motor de base de datos SQL Server 2012 R2 fue el 12 de Julio de 2022.

Como se aprecia, los sistemas operativos ya están vencidos o les falta muy poco para vencerse, pasado esto, ya no se entregan actualizaciones o parches de seguridad y los sistemas quedan expuestos.

Se recomienda encarecidamente se incluya en el presupuesto del próximo año la adquisición de estas nuevas licencias para migrarlos a la última versión posible.

Se recomiendo de igual manera, migrar la totalidad de los servidores, no solo unos cuantos, ya que se continuaría arrastrando amenazas embebidas a la tecnología de estos sistemas.

7.1.3 Renovación de los certificados TLS. Muchas de las vulnerabilidades encontradas tenían un común denominador, el uso de cifrados antiguos y vulnerables, como lo es SSL en versiones 1.1, 1.2 y 1.3.

Se evidencia que en el servidor de dominio principal (AD) tiene el rol de Servicios de Certificados del Active Directory(AD CS), solo que todos los certificados generados e implementados ya se encuentran caducados u obsoletos. Se recomienda realizar el pago a un ente certificador para renovar estos certificados, preferiblemente migrándolos a TLS 1.3 y aplicarlos en todas las comunicaciones internas o locales entre servidores y los clientes o EndPoint.

7.1.4 Implementar un servidor de Backup Seguro. Aunque esto no surge de los análisis realizados, se recomienda implementar un servidor de Backup seguro, donde se puedan realizar copias de seguridad de manera incremental, diferencial y full, se almacenen en ubicaciones seguras, donde no se tenga acceso ni siquiera al administrador de dominio solo un usuario restringido y habilitado por el tiempo de la copia, al igual que se encripten a nivel del sistema de archivos y de ser posible, replicar estas copias en otras dos ubicaciones por fuera de las oficinas o en nube.

La información por respaldar sería completa, desde información de los usuarios, snapshot de servidores y las bases de datos.

7.1.5 Segregación de la red de servidores. Por norma general o buenas prácticas, no es recomendable tener los servidores en el mismo rango de IP de los usuarios, y los servidores que tengan algún servicio publicado en internet, deben estar aislados en una DMZ.

Se recomienda segregar todos los servidores en una red independiente, crear la DMZ y colocar en esta el servidor TS y crear las reglas de Firewall para interconectarlos y sobre todo limitar las comunicaciones entre estas redes e internet y usuarios.

7.1.6 Separar el servidor de aplicaciones con el servidor de Base de datos. Como buena práctica, no es recomendable mantener en el mismo servidor la aplicación y la base de datos.

Se recomienda separar, en dos servidores independientes, cada uno de estos servicios e implementar un Firewall de Base de datos para dar una protección extra a la misma.

7.1.7 Quitar roles en servidor de directorio activo. Como buena práctica se recomienda que el servidor de AD tenga los mínimos roles asignados.

Se evidencia que en el servidor AD se tienen los roles de AD, AD CS, DCHP, DNS, File Server, SSO, entre otros.

Se recomienda distribuir dichos roles en otros servidores para mantener lo más simple y liviano este servidor.

7.1.8 Aplicar cifrado a los sistemas de archivos. Por seguridad y como buena práctica, se recomienda aplicar un cifrado al sistema de archivo de cada End Point de la Organización, priorizando los equipos Laptop de cargos de directivos, Gerencia, Profesionales y Auxiliares.

Al tener ecosistema Microsoft, se puede utilizar BitLocker para este cifrado, y al tenerlo configurado se pueden administrar permisos por medio de GPO del AD.

Aplicar esta recomendación de seguridad disminuiría el riesgo de fuga de información en caso de pérdida o robo de los equipos, ya que no se tendría acceso a la información almacenada en el disco.

7.1.9 Resultados generales. Para los dos servidores testeados con la herramienta Hardening Kitty, el puntaje es muy bajo, el margen de mejora es muy alto, si revisamos lo resultados matemáticamente tenemos que SAP solo pasa el 20.97% de las pruebas, y AD el 24.01%; los cuales son extremadamente bajos.

Aunque se debe analizar muy a detalle las pruebas realizadas, ya que muchas de estas pueden no ser acordes o tomando una contramedida se podría aprobar varios test simultáneamente.

Pero en general es un muy buen ejercicio tratar de aprobar la mayor cantidad de pruebas para garantizar la seguridad del servidor.

8 BIBLIOGRAFÍA

ECHEVERRY PARADA, JUAN SEBASTIAN. [en línea]. Metodología para el diagnóstico continúo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada. [Consultado el 18 de Diciembre 2021]. Disponible en: http://hdl.handle.net/10654/10200

GÓMEZ NOVA, ARELIS. [en línea]. Diseño de una metodología para auditar la seguridad de la información en productos de software orientados a servicios de gestión e información en instituciones de educación superior. [Consultado el 18 de Diciembre 2021]. Disponible en: http://hdl.handle.net/20.500.12749/3441

LIRA PLAZA, RICARDO CESAR. [en línea]. Metodologías de penetración de sistemas, análisis de resultados y modelo de protección. [Consultado el 18 de Diciembre 2021]. Disponible en: https://repositorio.tec.mx/bitstream/handle/11285/628456/CEM274344.pdf

GOBIERNO DE ESPAÑA. MINISTERIO DE HACIENDA Y ADMINISTRACIÓN PÚBLICAS. [en línea]. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [Consultado el 7 de Diciembre 2021]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

PINZÓN RUGE, JEISON NICOLAS. [en línea]. Metodología para identificación y valoración de riesgos y salvaguarda en una mesa de ayuda tecnológica. [Consultado el 30 de Noviembre 2021]. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/8310/PROYECTO%20DE%20GRADO.pdf

ANEXOS

Anexo 1. Acuerdo de Confidencialidad

V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE GABRIEL RICARDO PABON CASTILLO Y ECODIESEL COLOMBIA S.A.

Por la parte reveladora
Nombre: Ecodiesel Colombia S.A.
Dirección: Cra. 31 # 51-74 edificio Torre Mardel oficina 201 Bucaramanga, Santander
Teléfono: 607 6837308
E-mail: ecodiesel@ecodieselcolombiasa.com

Por la parte receptora de la información
Nombre: Gabriel Ricardo Pabón Castillo
Dirección: Calle 73 # 20-40 Apto. 302 Barrancabermeja, Santander
Teléfono: 3164344798
E-mail: gpabon@ecodieselcolombiasa.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la *Ecodiesel Colombia S.A.*, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto *aplicado con el título: Evaluación de seguridad a la infraestructura de servidores críticos de la empresa Ecodiesel Colombia S.A.*

2. Que la información de propiedad de *Ecodiesel Colombia S.A.* ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación *Evaluación de seguridad a la infraestructura de servidores críticos de la empresa Ecodiesel Colombia S.A., Gabriel Ricardo Pabón Castillo* que, para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de *Ecodiesel Colombia S.A.*

En consecuencia, las partes se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad, la parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al ***Ecodiesel Colombia S.A.***, así como también a no utilizar dicha información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento de la ***empresa Ecodiesel Colombia S.A.***

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión del proyecto aplicado y extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto *Evaluación de seguridad a la infraestructura de servidores críticos de la empresa Ecodiesel Colombia S.A.* lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, **la parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora de la información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legítima poseedora de la misma *Ecodiesel Colombia S.A.*, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de ***Ecodiesel Colombia S.A.***

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: *Marca, Modelo, Serial o identificador único de los servidores, así como sus características y roles, tipos de aplicativos que están ejecutándose en ellos, como servidores web, de aplicaciones o microservicios, servidores de bases de datos, contenedores, máquinas virtuales, entre otros; con el fin de determinar su criticidad, superficies de ataques, vulnerabilidades, etc. No se recolectará, almacenará ni compartirá información sensible de empleados, clientes o proveedores.*

10. La información capturada por la **parte receptora** se observará como *información cualitativa*, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad de todo el personal de ***Ecodiesel Colombia S.A.*** no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de ***Ecodiesel Colombia S.A.***, ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante *Gabriel Ricardo Pabón Castillo* se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa *Ecodiesel Colombia S.A.* para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la emresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora**, esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la

inobservancia del presente acuerdo, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *(Gabriel Ricardo Pabón Castillo – Ecodiesel Colombia S.A.)* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente acuerdo. En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las clausulas del presente acuerdo de confidencialidad por parte de *Gabriel Ricardo Pabón Castillo*.

Novena. Legislación aplicable: Este acuerdo se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente Acuerdo y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Las partes reconocen y aceptan que el presente documento, podrá ser firmado a través de firma digital y/o cualquier mecanismo de firma electrónica, las cuales tendrán plenos efectos de acuerdo con la Ley 527 de 1999 y para el caso de la firma electronica, adicionalmente de acuerdo con el Decreto 2364 de 2012 y demás normas que las modifiquen, complementen o sustituyan.

Firman en Bucaramanga S.S., a los (14) días del mes de (Octubre) de 2021

Como Parte Receptora:

Gabriel Ricardo Pabón Castillo
Estudiante UNAD.
C.C. No. 1098618630 de Bucaramanga

Por la parte reveladora:

Lina Reyes Salazar
Ecodiesel Colombia S.A.
C.C. No. 63325400 de Bucaramanga

Anexo 2. Carta autorización para ejecución de proyecto aplicado

Bucaramanga, 14 de octubre de 2021

Señora:
Lina Reyes Salazar
Gerente General
ECODIESEL COLOMBIA S.A.

Asunto: Autorización para la ejecución del proyecto titulado: Evaluación de seguridad a la infraestructura de servidores críticos de la empresa Ecodiesel Colombia S.A.

Cordial saludo estimada Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a Ecodiesel Colombia S.A., de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: Evaluación de seguridad a la infraestructura de servidores críticos de la empresa Ecodiesel Colombia S.A. el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "Evaluar la seguridad de la infraestructura de los servidores críticos de Ecodiesel Colombia S.A. mediante un enfoque metodológico con el fin de acoplar buenas prácticas de seguridad articuladas a estándares internacionales."; al mismo tiempo será apoyado por los objetivos específicos: "Argumentar la selección de los servidores críticos de Ecodiesel Colombia S.A. mediante una caracterización de cada uno de ellos con el fin de determinar los servidores que presentan un alto riesgo a ser vulnerados.", "Establecer la metodología para la evaluación de seguridad de la infraestructura de los servidores críticos mediante la clasificación y análisis de las más relevantes para seleccionar las más apropiada de acuerdo con la naturaleza de la organización.", "Examinar la infraestructura de los servidores críticos de Ecodiesel Colombia S.A. mediante la metodología seleccionada con el fin de identificar las vulnerabilidades."

y "Proponer unas buenas prácticas articuladas con estándares internacionales con el fin de mitigar los riesgos y dar continuidad al negocio." para obtener como resultado un alto impacto en la seguridad de la empresa Ecodiesel Colombia S.A..

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

1. Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por Ecodiesel Colombia S.A.
2. La empresa Ecodiesel Colombia S.A. deberá establecer que tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
3. La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
4. La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
5. Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.

Firman en Bucaramanga S.S., a los (14) días del mes de (Octubre) de 2021.

Cordialmente,

Gabriel Ricardo Pabón Castillo
Estudiante UNAD.

En señal de aceptación de lo comunicado por medio del presente documento, firma en calidad de Gerente y Representante legal;

Lina Reyes Salazar
Gerente General y Representante Legal
ECODIESEL COLOMBIA S.A.