ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE HARDENING EN SISTEMAS OPERATIVOS DE SERVIDOR

IMPLEMENTACIÓN DE HARDENING EN UN SISTEMA OPERATIVO DE SERVIDOR MICROSOFT

TRABAJO DE INTEGRACIÓN CURRICULAR PRESENTADO COMO REQUISITO PARA LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO SUPERIOR EN REDES Y TELECOMUNICACIONES

JUAN SEBASTIAN JANETA AULLA

juan.janeta@epn.edu.ec

DIRECTOR: GABRIELA KATHERINE CEVALLOS SALAZAR

gabriela.cevalloss@epn.edu.ec

DMQ, agosto 2023

CERTIFICACIONES

Yo, JUAN SEBASTIAN JANETA AULLA declaro que el siguiente trabajo de integración curricular aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

JUAN SEBASTIAN JANETA AULLA

juan.janeta@epn.edu.ec

sebas_janeta1996@outlook.com

Certifico que el presente trabajo de integración curricular fue desarrollado por JUAN SEBASTIAN JANETA AULLA, bajo mi supervisión.

GABRIELA KATHERINE CEVALLOS SALAZAR

DIRECTOR

gabriela.cevalloss@epn.edu.ec

DECLARACIÓN DE AUTORÍA

Mediante la presente declaración, afirmamos que el trabajo de integración curricular aquí descrito, así como el (los) producto(s) resultante(s) del mismo, son públicos y estarán a disposición de la comunidad a través del repositorio institucional de la Escuela Politécnica Nacional; sin embargo, la titularidad de los derechos patrimoniales nos corresponde a los autores que hemos contribuido en el desarrollo del presente trabajo; observando para el efecto las disposiciones establecidas por el órgano competente en propiedad intelectual, la normativa interna y demás normas.

JUAN SEBASTIAN JANETA

DEDICATORIA

A Dios por regalarme diariamente salud y vida, las cuales han sido factores principales para culminar esta gran meta, también por brindarme la sabiduría necesaria que a lo largo de este camino me ha ayudado a formarme como una persona profesional.

A mis padres Manuel Janeta y María Aulla, quienes han sido un ejemplo de sacrificio y esfuerzo, la confianza que han depositado en mi ha sido una gran motivación para lograr este gran paso hacia el campo profesional.

A mis hermanos, hermanas y familiares quienes me han acompañado en este camino de ardua labor, brindándome palabras de aliento y apoyo emocional. En especial a mi hermano Ángel Janeta quien se encuentra fuera del país, el cual fue un pilar principal para no rendirme y siempre me estuvo apoyando en las buenas y en las malas.

Juan

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por darme la vida y la salud, por brindarme unos padres maravillosos quienes me han guiado por el camino correcto, por otorgarme un sustento diario, la cual ha sido un factor primordial para este importante logro.

A mis padres quienes con gran esfuerzo me brindaron esta oportunidad de formarme como un profesional, gracias por ser mis pilares fundamentales en esta trayectoria, y sobre todo por confiar en mí, la cual ha sido mi mayor motivación para lograr este gran sueño.

También quiero agradecer a mi familia porque siempre han estado conmigo cuando los necesitaba, por nunca dejarme solo en este proceso que ha sido una experiencia inolvidable, gracias por brindarme esas palabras de aliento que me ayudaron en los momentos más difíciles de mi vida.

Agradezco a mi directora de tesis, Gabriela Katherine Cevallos Salazar, por su guía experta, paciencia y dedicación a lo largo de todo el proceso. Los conocimientos proporcionados y consejos han sido fundamentales para el desarrollo de este trabajo y para mi crecimiento académico.

Quiero expresar mi gratitud a mis profesores y mentores, por su inspiración y por compartir conmigo su vasto conocimiento. Sus enseñanzas y orientación han sido una fuente constante de motivación y crecimiento intelectual.

Finalmente, quiero agradecer a una persona en especial quien ha sido un apoyo económico en toda mi carrera académica, Dr. José Báez quien me brindo un trabajo en su empresa, la cual me ayudo para sustentarme en todas mis necesidades personales y académicas, gracias por la comprensión que me tuvo en toda mi formación profesional.

Juan

ÍNDICE DE CONTENIDOS

RESUMEN

El presente proyecto de titulación tiene como objetivo, la implementación de *hardening* en un sistema operativo de servidor Microsoft, con el fin de analizar, evaluar y solventar posibles problemas que se encuentren dentro del sistema. Para ello se cuenta de seis secciones los cuales se detallará a continuación:

En la primera sección se presenta la descripción del proyecto implementado, los objetivos, tanto general como específicos, el alcance y el marco teórico, en donde se explican las bases fundamentales tales como; sistemas operativos, *hardening*, herramientas de escaneo basados en el protocolo SCAP, marcos de referencia (NIST, CIS, ISO), esto con la finalidad de comprender e implementar el proyecto de titilación.

En la segunda sección se describe la metodología empleada en la implementación de este proyecto. La cual se detalla de manera general el proceso que se siguió para el cumplimento de cada uno de los objetivos planteados.

En la tercera sección se exponen los resultados, lo cual se detalla de manera exhaustiva el proceso de la implementación empezado por la instalación del *Windows Server* 2019, levantamiento de un servidor de correo, instalación de la herramienta de escaneo y la presentación del reporte de vulnerabilidades. Con ello se aplica una política de seguridad al servidor para obtener un segundo reporte con la finalidad de compararlos y solventar de manera manual los más críticos. Además, se presenta una guía con las mejores prácticas para la implementación de un sistema operativo de servidor con correo electrónico protegidos.

En la cuarta sección se tiene las conclusiones que se obtuvieron a partir de lo elaborado, así como también las recomendaciones que se deben tener en cuenta para la implementación de *hardening* en servidores.

Finalmente, en las últimas secciones de tiene las referencias en las que se basó la investigación y sus respectivos anexos.

PALABRAS CLAVE: *hardening*, protocolo SCAP, NIST, CIS, *Windows Server*.

ABSTRACT

The objective of this degree project is the implementation of hardening in a Microsoft server operating system, in order to analyze, evaluate and solve possible problems found within the system. For this purpose, there are six sections which will be detailed below:

In the first section the description of the implemented project is presented, the objectives, both general and specific, the scope and the theoretical framework, where the fundamental bases such as; operating systems, hardening, scanning tools based on the SCAP protocol, reference frameworks (NIST, CIS, ISO) are explained, this with the purpose of understanding and implementing the titilation project.

The second section describes the methodology used in the implementation of this project. It details in a general way the process followed for the fulfillment of each one of the proposed objectives.

The third section presents the results, which exhaustively details the implementation process, starting with the installation of Windows Server 2019, setting up a mail server, installing the scanning tool and presenting the vulnerability report. With this, a security policy is applied to the server to obtain a second report in order to compare them and manually solve the most critical ones. In addition, a guide with the best practices for the implementation of a server operating system with protected e-mail is presented.

The fourth section contains the conclusions obtained from the report, as well as the recommendations that should be taken into account for the implementation of server hardening.

Finally, the last sections contain the references on which the research was based and their respective annexes

KEYWORDS: *hardening, protocolo SCAP, NIST, CIS, Windows Server.*

1 DESCRIPCIÓN DEL COMPONENTE DESARROLLADO

El presente proyecto consiste en implementar un proceso de hardening en sistemas operativos de servidor, aplicando una política de seguridad basada en un marco de referencia. Con esto se asegura al sistema operativo de servidor, reduciendo significativamente los puntos vulnerables de ataques.

Se tiene un sistema operativo de servidor con alojamiento de servicio de correo electrónico, se escaneará el mismo mediante una herramienta de escaneo de configuración y vulnerabilidades basada en el protocolo SCAP, donde se obtendrá un reporte inicial el cual será comparado con un reporte luego de aplicar una política de seguridad. Este análisis determinará si las reglas especificadas por la política se han cumplido y si se ha mejorado la seguridad del sistema operativo.

1.1 Objetivo general

Implementar *hardening* en sistemas operativos de servidor.

1.2 Objetivos específicos

- Identificar las vulnerabilidades en un sistema operativo de servidor sin políticas de seguridad.
- Implementar una política de seguridad en un sistema operativo de servidor.
- Analizar los reportes, resultado de la aplicación de la herramienta de escaneo.
- Verificar el *hardening* del sistema operativo con base en los elementos de la triada CIA.

1.3 Alcance

En primera instancia, se llevará a cabo una investigación orientada hacia las herramientas relacionadas con el escaneo, configuración y detección de vulnerabilidades, haciendo uso del protocolo SCAP como base. A partir de este punto, se procederá a la instalación de un sistema operativo destinado a funciones de servidor, el cual será configurado sin aplicar ninguna política de seguridad específica. A través de la herramienta de escaneo, se generará un informe inicial de las vulnerabilidades presentes en dicho sistema.

Posteriormente, se llevará a cabo la implementación de una política de seguridad en el sistema operativo del servidor, con el objetivo de optimizar el informe de vulnerabilidades generado previamente por la herramienta de escaneo. Asimismo, se procederá a la puesta en marcha de un servidor de correo en el sistema operativo previamente endurecido. Se compararán los reportes para observar cuáles parámetros críticos se han solventado según el manual de buenas prácticas de seguridad emitido por organizaciones de estandarización en esta área.

Se realizará una guía que resuma las mejores prácticas, con esto se implementa *hardening* en un sistema operativo de servidor, reduciendo la superficie de ataques y por ende mitigando las debilidades que puedan ser aprovechadas por intrusos locales o remotos.

1.4 Marco Teórico

Sistemas operativos de servidor

Un sistema operativo de servidor es un *software* conformado por múltiples herramientas y dispositivos que permiten la gestión de distintos programas, los cuales tienen la finalidad de brindar uno o varios servicios a distintos usuarios. Existe una variedad de sistemas operativos algunos son de código libre y otros son privados, tal como lo es el *Windows Server* que hasta la actualidad muchas de las empresas emplean este sistema operativo por su facilidad de uso, instalación y soporte que brinda [1].

En el mercado hay varios sistemas operativos de servidor tales como:

UNIX: Este sistema operativo está diseñado para un entorno de cliente-servidor, el cual se emplea para multitareas y multi usuarios. La programación empleada para este sistema operativo es de alto nivel, la cual soporta varias arquitecturas de *software*. Hay algunas variantes de Unix como: Solaris, AIX, HP-UX y FreeBSD, que se utilizan en entornos empresariales y académicos. Una de las características de este servidor es que es de código abierto, lo que significa que está basado en la licencia de GNU abierta a todo el público permitiendo que su uso sea gratuito[2].

MacOS *Server*: Este sistema operativo de servidor fue fabricado por la compañía de *Apple,* la cual está basada en la arquitectura de Unix brindando una gran estabilidad, donde la seguridad sobresale. Además, este servidor cuenta con una interfaz gráfica de usuario, la cual hace que la configuración y gestión sea más fácil. Una de las características más destacadas es que cuenta con un sistema nativo para dispositivos móviles, la cual permite conectar con otros dispositivos *Apple*. Entre sus principales funciones se encuentra el servicio de correo, mensajería, VPN, web, entre otros [2].

Linux: Este sistema operativo de servidor está basado en código abierto, su arquitectura está basado en Unix lo que permite una estabilidad y una seguridad óptima para ser empleado a niveles empresariales. Es utilizado en varios servicios tales como web y base de datos. Lo que caracteriza de este servidor que es compatible con varios *software* y *hardware*. Otra característica que sobresale es la soportar una gran capacidad de carga de trabajo, sin perjudicar otros servicios [3].

Windows Server: Este sistema operativo de servidor fue desarrollado por Microsoft, una empresa conocida por desarrollar sistemas operativos que se familiariza con el usuario por su interfaz y su facilidad de uso. Su compatibilidad con otros *software* y *hardware* es amplia y es empleada en grandes centros de datos a nivel mundial y cuenta con un interfaz de usuario amigable. A nivel de seguridad proporciona diferentes actualizaciones periódicas con el fin de prevenir cualquier ataque o vulnerabilidad del sistema. De esta manera permite que las empresas se mantengan seguras y que sus servicios funcionen de

manera correcta sin interrupciones. Una de las características de este servidor es que es compatible con otros sistemas basados en Linux, además cuenta con una interfaz de usuario la cual permite que su gestión e instalación sea más sencilla [3].

Se tienen diversas versiones que se han ido desarrollando a lo largo del tiempo, entre las principales se encuentran:

Windows 2000 Server: El primer lanzamiento se realizó el 17 de febrero del año 2000, el cual fue diseñado para el reemplazo de *Windows* NT 4.0 funcionando como un servidor de archivos, intranet e infraestructura, generando de esta forma mejoras en la confiabilidad, escalabilidad y seguridad de los sistemas y la integración web [4].

Windows Server 2008: Se lanzó el 27 de febrero de 2008, fue el sucesor de *Windows Server 2003*, desarrollado con mejores características. Entre las principales características rige el de la creación de roles en donde se configura el servidor para la realización de tareas específicas tales como controlar el dominio, el servidor web, entre otros. Además, ofrece la implementación de la virtualización por medio de la plataforma Hyper-V, en donde el usuario puede crear y administrar entornos virtuales, lo cual resultó un ahorro en costos y una mayor flexibilidad [5] [6].

Windows Server 2008 R2: Esta versión se lanzó el 22 de octubre del 2009, la cual se destaca por ser el primer sistema operativo de 64 (bits) lanzado por Microsoft. Además, esta versión fue desarrollada con nuevas características entre ellas; mejora en el entorno virtual por medio de Hyper-V 2.0 agregando *Live Migration*, implementación de la función *Direct Access* que permite a los usuarios remotos acceder a la red de la empresa sin tener una conexión *VPN* tradicional, mejorando el rendimiento de las aplicaciones por medio de la funcionalidad *BranchCache* [6].

Windows Server 2012: Esta versión fue lanzada el 04 de septiembre de 2012, este sistema operativo trabaja como servidor basado en *Windows* 8 compartiendo características similares, además de tener de manera común el código base. Está diseñado para una arquitectura de 64 (bits), cuenta con

grandes cambios entre ellos; la interfaz de usuario implementado un aspecto moderno y óptimo, mejora considerable en la virtualización con el lanzamiento de Hyper-V 3, en donde se incluye el almacenamiento compartido por medio de clústeres compartidos. Luego mejoró a su versión *Windows Server* 2012 R2 [7].

Windows Server 2016: Fue lanzada el 12 de octubre del 2016 en el cual se introdujeron varias mejoras y nuevas características en comparación a las versiones anteriores. En primer lugar, se hizo una mejora considerable en la virtualización, por lo cual se incluye Hyper-V 2016. Otra de las características a destacar es la funcionalidad de *Nano Server*, que permite la instalación mínima para aplicaciones modernas basadas en contenedores, los cuales se incluyen por medio de *Dockers* proporcionando de esta forma un entorno ligero, mejorando la flexibilidad y la portabilidad [8].

Windows Server 2019: Es una versión consolidada de *Windows Server 2016,* que fue diseñada principalmente para entornos empresariales, ofrece nuevas características en el entorno de la administración híbrida permitiendo administrar un entorno local y la nube mediante *Azure*. Además, el almacenamiento es definido por *software* ya que mediante un *hardware* estándar permite crear soluciones de almacenamiento escalable, así como las características de S2D (*Storage Spaces Direct)* que básicamente permite crear un pool de almacenamiento compartido para máquinas virtuales y *clústeres*. En temas de seguridad también sobresale con respecto a otras versiones ya que ofrece actualizaciones de parches más seguido permitiendo que las posibles vulnerabilidades del sistema sean erradicadas [9].

Windows Server 2022: Esta versión es la más reciente, lanzada el 01 de marzo de 2022 el cual incluye mejoras considerables. Mejoras en la seguridad para la protección de los datos por medio de la inclusión de *Secured-core Server*, *Azure Integration* lo cual permite a las empresas extender la administración y las políticas a los entornos locales. Otra característica notable en este sistema es la mejora en el almacenamiento y HCI (*Hyper-Converged Infrastructure*) por medio de la implementación de *Storage Spaces Directory* que permite un almacenamiento escalable y resiliente [10].

El sistema operativo de servidor *Windows*, en sus diferentes versiones, requiere de varios requisitos para ser instalado tal como se observa en la Tabla 1.1 , en la cual se especifica la versión con sus respectivos requerimientos tanto en *hardware* como en *software*.

Tabla 1.1 Requisitos mínimos para instalar las diferentes versiones de *Windows Server*

Requisitos mínimos para instalar las versiones de *Windows*				
Versión de *Windows*	**Procesador**	**Memoria RAM**	**Disco duro mínimo**	**OTROS**
Windows server 2000	Compatible con Pentium con una velocidad mínima de 133 (MHz).	Min. 256 (MB)	Min. 2 (GB)	Adaptador de video, monitor con resolución VGA.
Windows server 2008	Velocidad mini. De 1 (GHz).	Min. 512 (MB)	Min. 8 (GB)	Pantalla con resolución Min. VGA (800 X 600) (pixeles)
Windows server 2012	Velocidad min. De 1.4 (GHz) primer procesador con arquitectura de 64 (bits).	Min. 512 (MB)	Min. 32 (GB)	Unidad DVD Pantalla con resolución mayor a (800 x 600) (pixeles)
Windows server 2016	Velocidad min. 1.4 (GHz) con una arquitectura de 64 (bits).	Min. 512 (MB)	Min. 32 (GB)	Unidad DVD Pantalla con Resolución 1024 x 768 (pixeles) Adaptador de red Gigabit Ethernet
Windows server 2019	Velocidad min. 1.4 (GHz) con arquitectura de 64	Min. 512 (MB), adicional 2	Min 32 (GB)	Resolución mínima de

	(bits) o también puede ser un procesador AMD64	(GB) si se instala la experiencia escritorio		pantalla de 1024 x 768 (pixeles) Unidad de DVD
Windows server 2022	Velocidad min. 1.4 (GHz) con arquitectura de 64 (bits)	Min. 512 (MB), y 2048 (MB) adicional para instalar el servidor escritorio.	Min. 32 (GB)	Tarjeta NIC con 1 GBPS mínimo para su optimo funcionamiento

En la Tabla 1.2 se visualizan las ventajas y desventajas que tiene *Windows Server*, en esta se recopila de todas las versiones ya que las actuales poseen más ventajas con respecto a versiones anteriores.

Tabla 1.2 Ventajas y desventajas de *Windows Server*

Windows Server	
Ventajas	**Desventajas**
Una de las ventajas que sobresale con respecto a otros sistemas operativos de servidor es la administración ya que el entorno gráfico de escritorio es más intuitivo y fácil de usar.	Una de las mayores desventajas es que para utilizar este sistema operativo de servidor hay que pagar un valor por la licencia.
En los motores de búsqueda se puede encontrar una variedad de documentación indicando cómo hay que utilizarlo.	En temas de seguridad, es uno de los sistemas con más probabilidad de ser afectado por un ataque cibernético para evitar estos inconvenientes se debe tener instalado los respectivos parches de seguridad actualizados.
El aprendizaje es más sencillo ya que el modo escritorio es amigable con el	En cuanto a *hardware* esta emplea más recursos en comparación con

usuario, y no tiene mucha complejidad al momento de utilizarlo.	otros sistemas de servidor, ya que al emplear el modo escritorio consume recursos como procesador y memoria RAM.
La migración de una versión anterior a una versión nueva es cómoda y sencilla ya que esto es posible gracias a una herramienta que posee *Windows server* como lo es el sistema de migración de almacenamiento, lo cual permite ahorrar el esfuerzo de instalar nuevamente desde cero el sistema operativo de servidor.	*Windows* detiene los servicios cuando se realizan cambios ya que es obligatorio reiniciar el sistema para que estos cambios sean efectuados. Lo que trae como consecuencia que los servicios que dependan de este equipo queden fuera de servicio por el tiempo que dura el reinicio.
Desde la versión 2019 se puede configurar para que el sistema sea más liviano dejando a un lado el modo escritorio y empleando el modo consola.	Para corregir fallos y vulnerabilidades actuales se requiere de manera obligatoria las nuevas actualizaciones, además se debe estar al día con las actualizaciones para evitar cualquier intruso que quiera ingresar al sistema.

Hardening

Se le conoce también como endurecimiento informático se refiere al proceso de asegurar y fortalecer un sistema informático o a su vez una red con la finalidad de reducir sus vulnerabilidades. Esto se logra, implementando medidas y configuraciones de seguridad para proteger los activos de información de amenazas y ataques [11]. El propósito de *Hardening* es obstruir la labor del atacante, minimizando el riesgo de que el sistema sea comprometido o explotado ya sea por *hackers, malware* y otras amenazas cibernéticas. Sin embargo, hay que tomar en cuenta que no necesariamente se logrará desarrollar equipos invulnerables [12].

Para la aplicación de *Hardening* se incluyen algunas medidas, entre ellas se encuentran [12]:

- **Protección de ataques físicos:** Entre estas actividades se destacan: establecer contraseñas complejas al momento que el equipo arranque, la configuración en la BIOS, la deshabilitación de inicio del sistema para cualquier unidad externa.
- **Sistema Operativo seguro:** Para esta medida es necesario considerar dos particiones principales, la primera para el sistema operativo y la segunda para la gestión de carpetas y archivos; evitando de esta manera la instalación de algún componente innecesario para el funcionamiento.
- **Activación de actualizaciones:** Para que un sistema minimice los riesgos en su seguridad es importante tener todos los parches que entrega el proveedor, por lo cual es adecuado instalar un servidor de actualizaciones.
- **Instalación y gestión de programas de seguridad:** En esta medida se destacan la instalación de Antivirus y filtros Anti-spam esto dependerá de las necesidades del sistema.
- **Configuración de políticas del sistema:** Para la aplicación de esta medida se tienen varios puntos como; políticas de contraseñas robustas añadiendo claves temporales, bloqueos de cuentas por intentos erróneos. Otro punto importante es el renombramiento y deshabilitación de cuentas, asignando el rol de administrador e invitado. Para finalizar, la asignación correcta de derechos de usuario.
- **Protocolos de Red:** En esta configuración es necesario usar sistemas de traducción de direcciones, deshabilitar protocolos innecesarios en el sistema y limitarlos al mínimo.

Al momento de fortalecer la seguridad, se busca mitigar los riesgos y garantizar aspectos importantes como: la integridad, confidencialidad y disponibilidad de los datos y servicios.

Integridad

Se define como la propiedad de los datos o de la información para mantenerse exactos y completos a lo largo del tiempo, generando de esta manera una garantía de que la información no ha sido alterada o modificada de manera no autorizada [13]. Entre los métodos y mecanismos para conservar la integridad se tiene [14]:

- **Control de Acceso:** Limitar el acceso a los datos en donde solo personas autorizadas con credenciales puedan modificar la información.
- **Firma Digital:** Se utiliza para asegurar que no haya modificación desde su creación, se lo realiza por medio de técnicas de criptografía asimétrica para la creación de firmas digitales.
- **Función de Hash:** Se genera un valor de resumen único al momento de alguna alteración en la información.
- **Auditorias y registros de eventos:** Es importante el registro y monitoreo de las actividades para identificar los cambios o accesos no autorizados y tomar medidas correctivas.

Disponibilidad

Hace referencia a que la información debe encontrarse a disposición para quienes quieran acceder, dentro de este ámbito están incluidas personas, aplicaciones, operaciones entre otras, en cuanto se necesite. Además, la capacidad de mantener los sistemas y servicios funcionando correctamente [15]. Entre los métodos y mecanismos para conservar la disponibilidad se tiene [16]:

- **Redundancia y alta disponibilidad:** Por medio de la utilización de tecnologías y configuración que permita la duplicación de *hardware*, sistemas y servicios, en caso de fallas o interrupciones.
- **Copias de Seguridad:** Se debe realizar copias de seguridad periódicas de los datos más relevantes y mantener planes de recuperación antes de que ocurra algún problema.

- **Monitorización y alertas:** Establecer sistemas de monitorización en tiempo real para poder responder de manera ágil ante posibles problemas.
- **Protección contra ataques cibernéticos:** Implementar medidas como *firewalls*, sistemas de detección y soluciones de seguridad, para la protección de sistemas y datos contra ataques.

Confidencialidad

Se refiere a la propiedad de los sistemas y los datos de funcionar de manera consistente, para operar de manera confiable, sin errores o fallas, asegurando que los datos sean precisos a lo largo del tiempo [17]. Entre los métodos y mecanismos para conservar la confiabilidad se tiene [18]:

- **Pruebas completas:** Para esta medida se realiza pruebas rigurosas de los sistemas y las aplicaciones para identificar y corregir posibles errores y fallas.
- **Programación de mantenimientos:** Se debe realizar mantenimiento regular de los sistemas, incluyendo actualizaciones de *software*, parches de seguridad y reemplazo de componentes obsoletos, ayudando a prevenir problemas futuros [18].
- **Documentación y procedimientos:** Se debe mantener una documentación clara y completa de los sistemas, las configuraciones y los procedimientos operativos, lo cual facilita la resolución de problemas [18].
- **Capacitación y concientización:** Proporcionar capacitación adecuada a los usuarios y al personal de TI sobre las mejores prácticas de seguridad y las políticas y procedimientos establecidos, para ayuda a garantizar que los sistemas se utilicen correctamente [18].

Herramientas de escaneo de vulnerabilidades basadas en el protocolo SCAP

Son un conjunto de estándares y protocolos que permite medir el nivel de seguridad de un sistema; mediante el SCAP (*Security Content Automation Protocol*) las empresas pueden seguir una guía con la cual pueden mejorar la seguridad de sus equipos. Lo más destacable es que el proceso que realiza es

de manera automática de ello viene las siglas SCAP (*Security Content Automation Protocol*), generando un informe al final del análisis en donde se detallan las vulnerabilidades [19]. Con ello se logra solventar los problemas encontrados y reduce posibles ataques por parte de los ciberdelincuentes [20].

Un elemento clave del Protocolo SCAP son los componentes los cuales incluyen [19]:

- ***Common Configuration Enumeration* (CCE):** Este formato contine un diccionario con las nomenclaturas para describir los problemas que existen dentro de la configuración del sistema.
- ***Common Platform Enumeration* (CPE*):*** Es un diccionario el cual contiene un formato estandarizado para relacionar nombres de productos y versiones [19].
- ***Open Vulnerability and Assessment Language* (OVAL):** Es el lenguaje empleado para presentar los informes de las vulnerabilidades generados después de realizar el escaneo.
- ***eXtensible Configuration Checklist Description Format* (XCCDF):** Este formato permite facilitar la preparación estandarizada de los resultados que se generan luego del análisis, presentando las vulnerabilidades del sistema mediante una plantilla XML.
- ***Open Checklist Interactive Language* (OCIL):** Es una guía, la cual se emplea para la interpretación de preguntas hacia el usuario y de la misma manera expresa la respuesta a las preguntas.

Con los avances de la investigación hoy en día existe una variedad de herramientas que permiten realizar el escaneo de vulnerabilidades, sin embargo, muchos de ellos no están basado en el protocolo SCAP, a continuación, se detalla las herramientas que más se han empleado para escanear Sistemas Operativos de Servidor basados en el protocolo SCAP.

OpenSCAP

Se trata de una herramienta de licencia abierta que se centra en la manipulación de la información de seguridad en base a un marco de referencia estandarizada. Realiza análisis de vulnerabilidades con el propósito de asegurar el cumplimiento

de los estándares mediante bibliotecas que ya vienen incluidas dentro de la herramienta. Al ser de licencia libre cualquier persona o entidad puede modificar su código fuente según sea su necesidad. Una característica de esta herramienta es la compatibilidad, ya que puede ser implementada en varios sistemas operativos tales como *Windows y Linux*.

Esta herramienta cuenta con algunas distribuciones que han sido desarrolladas de su código principal, entre los cuales están: *OpenSCAP Workbench* empleado para crear perfiles de seguridad mediante una interfaz de usuario. SCAP *Security Guide* (SSG) ha sido empleado para seguir una guía que ayuda a asegurar diferentes plataformas y sistemas informáticos. SCAP *Compliance Checker (SCC),* esta aplicación se ha utilizado para realizar prácticas de *harneding* en un sistema operativo mediante guías denominadas STIG (Guías de Implementación Técnica de Seguridad). Donde esta herramienta permite estandarizar protocolos de seguridad dentro de varias áreas tales como: servidores, redes, ordenadores, etc. [21] [22].

Nessus

Es un *software* enfocado para escanear vulnerabilidades de sistemas operativos, es muy conocida a nivel empresarial ya que muchas de ellas emplean este programa para analizar sus equipos, actualmente cuenta con dos versiones una de código abierto y otra que se debe pagar un valor mensual o anual para utilizarla. En la versión gratuita están limitadas algunas funciones y dura cierto tiempo, después se debe cancelar el pago correspondiente para ser utilizado, sin embargo, cuenta con varias características las cuales sobresalen al resto, entre ellas están el escaneo de puertos, así como también los dispositivos que están conectados a esa red con sus respectivos servicios, por último realiza un sondeo de los falsos positivos enumerándolos para su respectiva corrección [23].

OpenVAS

Se trata de una herramienta que es utilizada para el escaneo de vulnerabilidades, se desarrolló a partir de Nessus código abierto, por la empresa *Greenbone Networks* en el 2009, entre sus funciones principales están pruebas autenticadas y no autenticadas, para exploraciones a gran escala cuenta con ajustes que se

personalizan según la necesidad. Las características más destacables son: abundancia de información y tutoriales para el uso de la herramienta, ejecución en modo gráfico y línea de comandos. Por otro lado, tiene una versión de pago, donde se encuentran las herramientas completas en comparación con la versión gratuita en donde están habilitadas ciertas herramientas. Se puede ejecutar en varias plataformas como *Linux y Windows* [24].

Marcos de referencia

Un marco de referencia son un conjunto de protocolos, reglas y estándares que sirven de base para visualizar problemas dentro de un sistema y luego solventarlos. Mediante estos marcos de referencia los desarrolladores y los técnicos de TI pueden crear equipos que tengan características de consistencia y escalabilidad. En el área de seguridad un marco de referencia permite realizar una guía de mejores prácticas con el fin de reducir posibles vulnerabilidades dentro de un sistema, así también garantiza que se sigan prácticas adecuadas con el fin de proteger los bienes de una organización tal como lo es la información.

Existen varias organizaciones que desarrollan estos marcos de referencia en temas de seguridad entre los cuales se tiene:

CIS (*Center for Internet Security)*

Es una organización conformada por la comunidad de TI que tienen como objetivo desarrollar mejores prácticas para la defensa de ciberataques. Esta entidad sin fines de lucro permite identificar y desarrollar herramientas que solventen problemas de seguridad [25]. CIS es reconocido por sus controladores que proporcionan una lista priorizada dirigida a empresas de todo tamaño que al emplearlas en sus sistemas estas reducen significativamente posibles ataques [26].

El CIS cuenta con varios puntos de referencia donde se incluye varias recomendaciones sobre la configuración del sistema, teniendo en cuenta dos niveles de perfiles disponibles. En primer lugar, se encuentran los perfiles de nivel 1, donde está abarcado las configuraciones fundamentales, las cuales tienen efectos mínimos en el sistema y además son de fácil implementación. Por

otro lado se encuentra los perfiles de nivel 2, está en cambio están destinadas a entornos que requieren alta seguridad por lo cual demandan más coordinación y planificación en su implementación [26].

Existen 7 clasificaciones fundamentales sobre los puntos de referencia de CIS [26]:

- **Puntos de referencia de sistemas operativos:** Se trata de las configuraciones de seguridad de los sistemas operativos principales, como *Windows y Linux*, además, proporcionan pautas recomendadas para limitar el acceso tanto desde ubicaciones locales como remotas, perfiles de usuarios, protocolos de instalación y ajustes de los navegadores WEB.
- **Puntos de referencia de *software* de servidor:** Este contenido aborda las disposiciones relacionadas con la seguridad de distintas aplicaciones de *software*, englobando plataformas como Microsoft *Windows Server*, *SQL Server*, *VMware, Docker y Kubernetes*. Adicionalmente, estas medidas comprenden las configuraciones dirigidas a servidores de API, directrices de conectividad de red y limitaciones concernientes a la gestión de recursos de almacenamiento.
- **Puntos de referencia de proveedor de nube:** Se refieren a las disposiciones de seguridad presentadas por distintos servicios en línea, considerando las directrices para establecer la administración de identidades y accesos, los procedimientos de registro del sistema y las configuraciones de la red.
- **Puntos de referencia de dispositivos móviles:** Dentro de esta categoría abarca a los sistemas operativos móviles tales como iOS y Android. Esto generaliza tanto las opciones de configuración de privacidad inherentes al sistema operativo, como también la parametrización del navegador utilizado y la gestión de los permisos otorgados a las distintas aplicaciones.
- **Puntos de referencia de dispositivos de red:** Proporcionan directrices de configuración de seguridad de carácter tanto general como específico

del proveedor, destinadas a dispositivos de infraestructura de red y componentes *hardware* correspondientes.

- **Puntos de referencia de *software* de *desktop*:** Se trata de las configuraciones de seguridad correspondientes a ciertas aplicaciones de *software* de escritorio. Estas se enfocan en preservar la privacidad del correo electrónico y ajustar la configuración del servidor.
- **Puntos de referencia de dispositivo de impresión multifunción:** Empleado con el propósito de configurar impresoras multifuncionales en entornos de oficina, abordando asuntos tales como la actualización del *firmware*, la configuración de parámetros TCP/IP, la administración de usuarios y la compartición de archivos**.**

ISO 27001 SEGURIDAD DE LA INFORMACIÓN

Es un estándar internacional que tiene por objetivo gestionar la seguridad de la información. Fue desarrollado por la ISO (Organización Internacional de Normalización) junto con la colaboración de la IEC (Comisión Electrotécnica Internacional). Para las organizaciones fue desarrollada la SGSI (Sistema de Gestión de Seguridad de la Información), con el fin de implementar, desarrollar y mejorar de manera sistemática. Este estándar está diseñado principalmente para garantizar el triángulo de la CIA (Confidencialidad, Integridad, Disponibilidad) de la información [27].

En la implementación de un SGSI cubre aspectos importantes tales como: evaluación de riesgos, políticas de seguridad, gestión de activos de la información, seguridad física y del entorno. Una empresa que cuente con una certificación ISO 27001, puede garantizar la seguridad de la información de sus clientes dando una ventaja competitiva ante sus competencias [27].

NIST (*National Institute of Standards and Technology*)

Es una herramienta que permite gestionar a las empresas con el fin de reducir los ataques cibernéticos, sus principales funciones son: desarrollo de estándares para criptografía, promoción de buenas prácticas las cuales ayudan a las empresas a seguir una guía específica con el fin de salvaguardar la información, investigación científica que ayuda al desarrollo de nuevas tecnología, seguridad

cibernética mediante guías y pautas permitiendo gestionar y administrar la información de manera responsable [28].

El marco de ciberseguridad está compuesto por tres secciones principales estas son [29]:

- **Núcleo del marco:** El centro del marco está formado por actividades y metas de seguridad cibernética, organizados en grupos y alineados con estándares de la industria. Su objetivo es facilitar la comunicación entre equipos multidisciplinarios mediante un lenguaje claro y comprensible. El marco se divide en tres partes: Funciones, Categorías y Subcategorías. Las funciones agrupan las principales actividades de seguridad en un nivel más elevado: Identificar, Proteger, Detectar, Responder y Recuperar.
- **Niveles de implementación:** Los niveles de implementación se refieren al grado de adopción rigurosa de los estándares de ciberseguridad por parte de una organización y a la eficacia de sus procesos para mitigar los riesgos de ciberseguridad. Existen cuatro niveles Nivel parcial, Nivel riesgo informado, Nivel repetible y Nivel adaptado.
- **Perfiles del marco:** Los perfiles del marco tienen como objetivo concordar las funciones, categorías y subcategorías con los requisitos y metas comerciales, considerando su nivel de tolerancia al riesgo. Su propósito es describir el estado presente o deseado de las actividades de ciberseguridad. El perfil actual refleja los logros alcanzados hasta el momento, mientras que el perfil objetivo visualiza los hallazgos requeridos para cumplir de los objetivos de administración de riesgos de ciberseguridad [29].

2 METODOLOGÍA

En el presente proyecto se llevó a cabo una investigación sobre el endurecimiento de los sistemas operativos de servidor, enfocándose principalmente en *Windows Server* 2019, ya que en la mayoría de las instituciones se emplea este sistema operativo por su facilidad de administración, soporte e instalación. Para lo cual se siguieron las siguientes etapas para alcanzar el objetivo general:

En el primer objetivo se llevó a cabo la instalación del sistema operativo de servidor *Windows Server* 2019 junto con el levantamiento de un servidor de correo sin tomar en cuenta ninguna política de seguridad, para lo cual se empleó una máquina virtual en Hyper-V 5. Una vez instalado el servidor se procedió a levantar el servidor de correo con ayuda de la herramienta *HmailServer*. Mediante la herramienta *SCAP Compliance* se obtuvo el primer escaneo de vulnerabilidades.

En el segundo objetivo, se llevó a cabo la implementación de un nuevo sistema operativo de servidor. Dentro de este proceso, se procedió a aplicar una política de seguridad fundamentada en el marco de referencia CIS *Benchmark.* Para llevar a cabo esta tarea, se empleó la herramienta de *Power Shell*, mediante la cual se ejecutaron una serie de comandos con el propósito de aplicar un *script* que incluía las configuraciones de seguridad necesarias para el servidor. Posteriormente, una vez que el sistema operativo había sido endurecido en términos de seguridad, se procedió a habilitar el servicio de correo electrónico. Luego, se instaló una herramienta de escaneo con el objetivo de obtener un segundo informe acerca de las vulnerabilidades presentes en el sistema.

En el objetivo tres se analizó los reportes obtenidos con la finalidad de compararlos y visualizar las mejoras que se tienen en el último análisis, además se observó cuáles eran los parámetros críticos que se han solventado según el marco de referencia. Una vez realizado el análisis, de forma manual se solventaron seis recomendaciones, dos de ellas críticas, que no fueron implementadas por la política establecida. Esto con el fin de obtener una mejora en el *hardening* del sistema operativo, reflejado en un reporte final.

En el objetivo cuatro se analizó el reporte final, donde se verificó el impacto que tienen las políticas implementadas sobre los tres elementos del triángulo de seguridad informática: confiabilidad, integridad y disponibilidad. Además, se realizó una guía que resume las mejores prácticas para implementar un servidor endurecido, así como también el servidor de correo electrónico.

3 RESULTADOS

En la siguiente sección, se explica el proceso de *hardening* de un sistema operativo de servidor de Microsoft. Se emplea la versión 2019 de *Windows Server* para este propósito. Se comienza realizando la respectiva instalación junto con un servidor de correo electrónico, con el fin de obtener un análisis de vulnerabilidades del estado inicial del sistema. Una vez que se obtiene el primer análisis, se procede a realizar el *hardening* del servidor mediante un *script* en base en un marco de referencia. Esto se hace con la finalidad de endurecer las configuraciones del sistema. De esta manera, se levanta el servidor de correo nuevamente y se obtiene un segundo análisis con el fin de comparar los dos resultados.

Finalmente, de manera manual, se solucionan los problemas más críticos. Además, se crea una guía de buenas prácticas de seguridad para tener un sistema operativo de servidor con correo electrónico protegidos.

3.1 Vulnerabilidades en un sistema operativo de servidor sin políticas de seguridad

Instalación del sistema operativo de servidor

Primero para empezar se procedió a verificar las características de *hardware* del equipo principal con el objetivo de evitar cualquier inconveniente que hubiere al momento de levantar la máquina virtual, en la Figura 3.1 se visualiza las características de *hardware* de la máquina principal. En la cual se dispone de buenas características tanto de memoria RAM como de procesador, para lo cual se procedió a implementar la ISO del sistema operativo (SO) donde se empleó el hipervisor de Microsoft denominado Hyper-V, mediante esta herramienta se implementó el SO se servidor.

Figura 3.1 Características del *hardware* del equipo principal

En la Figura 3.2 se observa las características de la primera máquina virtual denominada SERVIDOR_WINDOWS_2019, la cual fue empleada para instalar el SO de servidor, así como también levantar el servicio de correo electrónico y la obtención del primer reporte de vulnerabilidades con la ayuda de la herramienta SCAP Compliance.

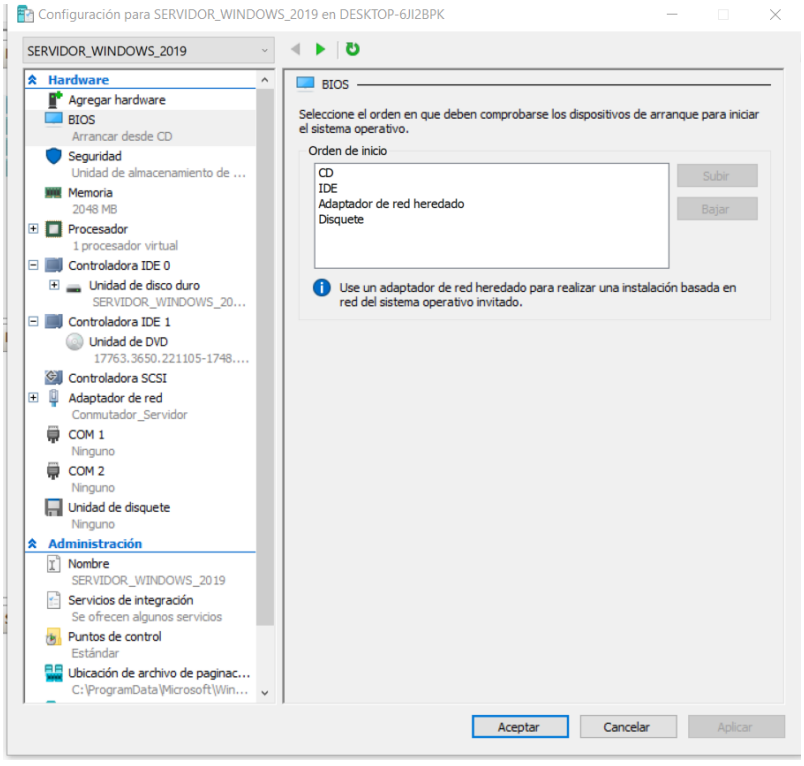


Figura 3.2 Características de la máquina virtual WINDOWS_SERVER_2019

En la Figura 3.3 se observa las características de la segunda máquina virtual denominada WINDOWS_SERVER_2019_2, la cual fue empleada para el segundo objetivo donde se enfoca en la aplicación de políticas de seguridad, levantamiento del SO de servidor y la obtención de un segundo reporte de vulnerabilidades.

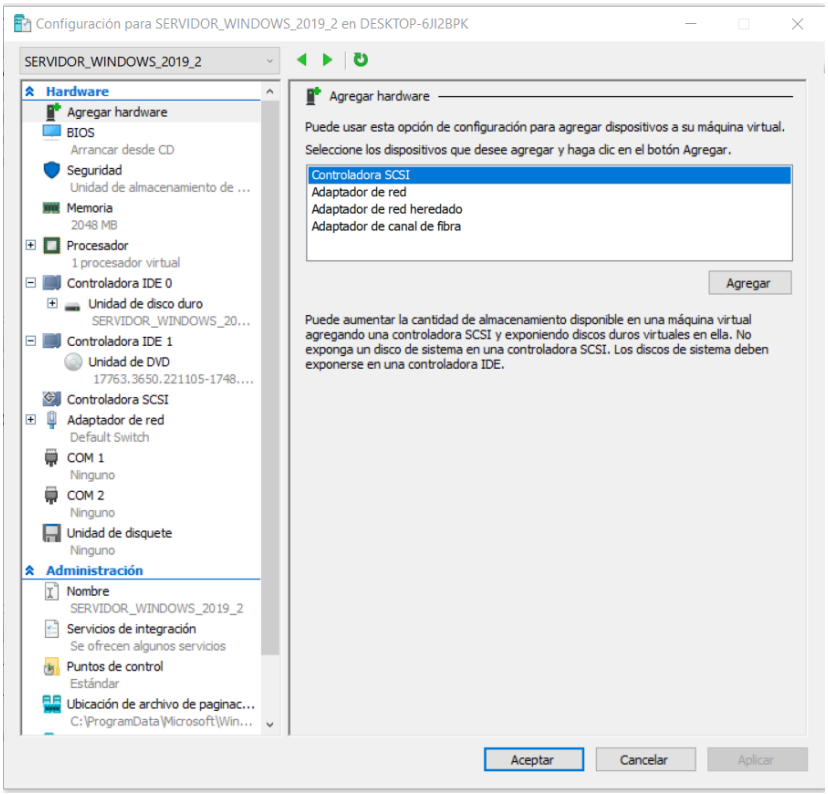


Figura 3.3 Características de la máquina virtual WINDOWS_SERVER_2019_2

Para la instalación del SO *Windows server* 2019, se ejecutó la máquina virtual denominada “SERVIDOR_WINDOWS_2019”, en el cual se escogió el idioma en que se va a instalar, así como también el entorno que se va a emplear en este caso el modo escritorio, con una arquitectura de x64. Finalmente, al terminar la instalación se precedió a registrar las credenciales para acceder al SO. En la Figura 3.4 se visualiza el resumen de los pasos que se siguió para la instalación.

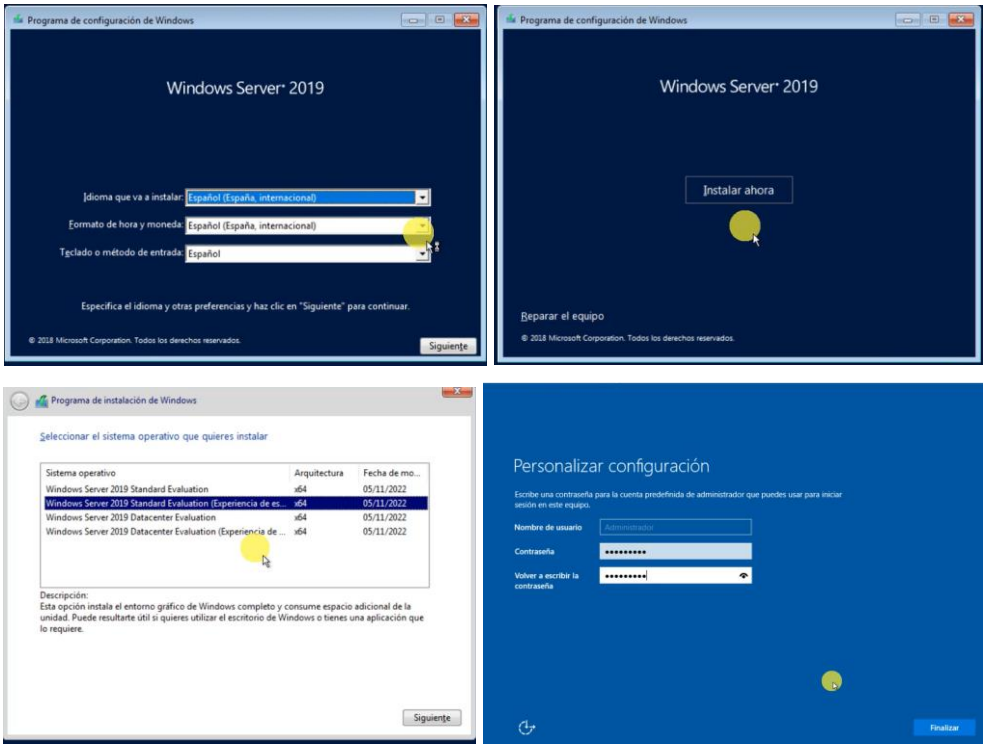


Figura 3.4 Instalación de SO *Windows Server* 2019

Al culminar la instalación se procedió a visualizar la configuración del SO, junto con las características. Así como en la Figura 3.5 se visualiza la información del *Windows Server* 2019.

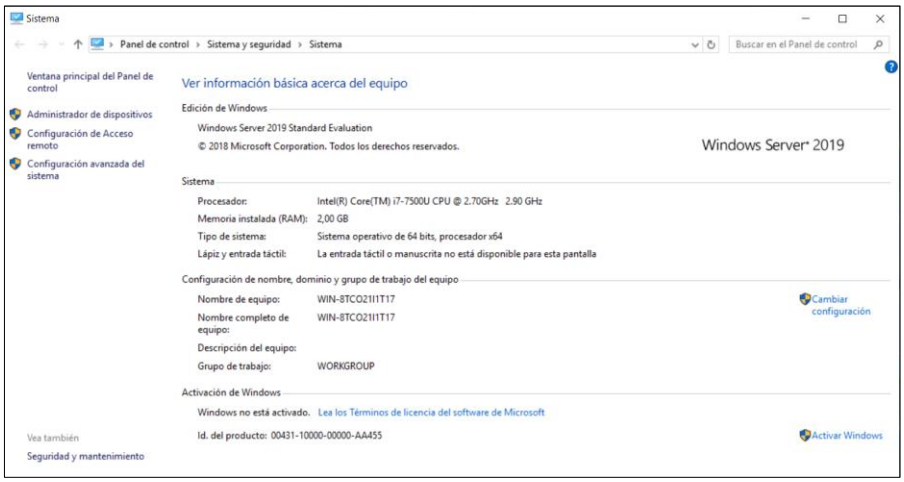


Figura 3.5 Características del SO *Windows Server* 2019

Creación de un conmutador virtual para la conexión del servidor con el cliente

El objetivo con el que se configuró este conmutador fue para la comunicación entre el servidor y el cliente, en este caso con un SO *Windows 10*, además mediante este conmutador, el servidor DHCP (Protocolo de configuración dinámica de host) permitió que le asignara una dirección IP dinámica al cliente.

Para la creación se colocó en la ventana de acciones, en la opción de administrador de conmutadores virtuales, se creó un nuevo conmutador virtual, se ingresó un nombre denominado “Conmutador_Servidor”, se escogió una red interna con la finalidad de que solo exista comunicación entre las máquinas virtuales. Finalmente se aplicó los cambios y se procedió a aceptar los cambios. En la Figura 3.6 se visualizan estas configuraciones.

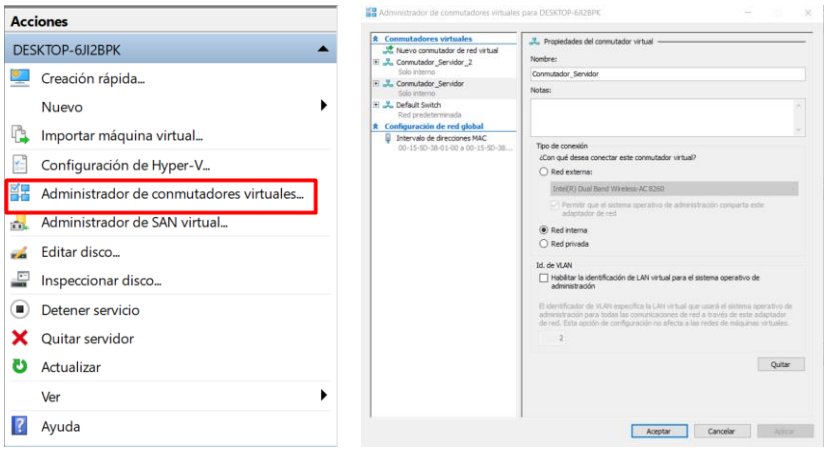


Figura 3.6 Creación del conmutador virtual

Instalación del sistema operativo *Windows* 10 configurado como usuario

Se instaló el sistema operativo *Windows* 10 con el objetivo de realizar las respectivas pruebas de conexión, recepción y gestión de correo electrónico, mediante la herramienta *Thunderbird*. Para empezar con esta instalación se descargó el archivo ISO de *Windows* 10 de la página oficial de Microsoft https://www.microsoft.com/es-es/software-download/windows10, una vez descargado el archivo se procedió a implementarla en una nueva máquina virtual denominada WINDOWS_10, en la Figura 3.7 se puede observar la asignación de la memoria RAM para el SO *Windows* 10.

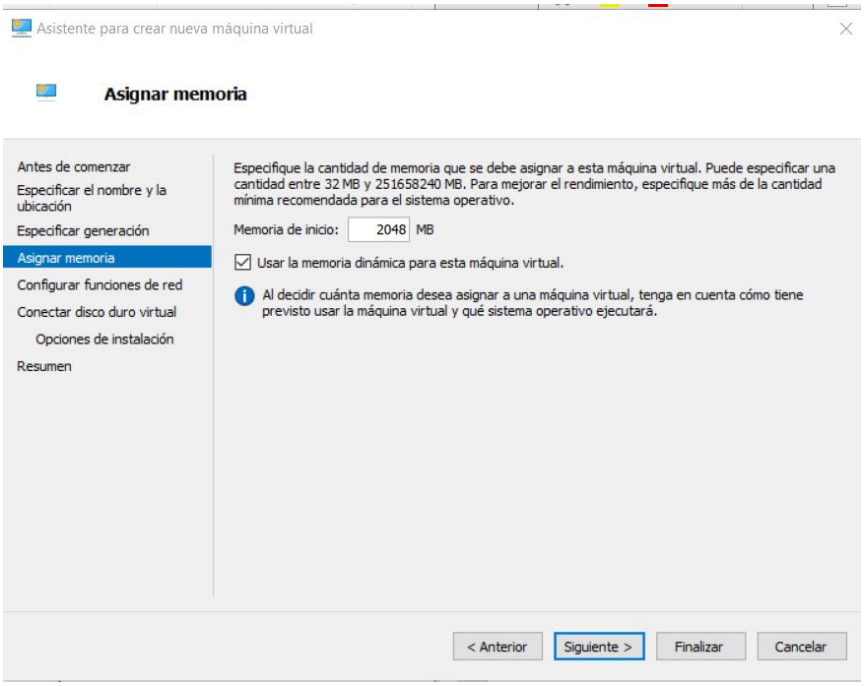


Figura 3.7 Asignación de la capacidad de memoria RAM

Con el fin de tener una comunicación entre la máquina WINDOWS_SERVER_2019 y la máquina WINDOWS_10, se escogió el conmutador virtual denominado Conmutador_Servidor, en la Figura 3.8 se obsreva esta configuración.

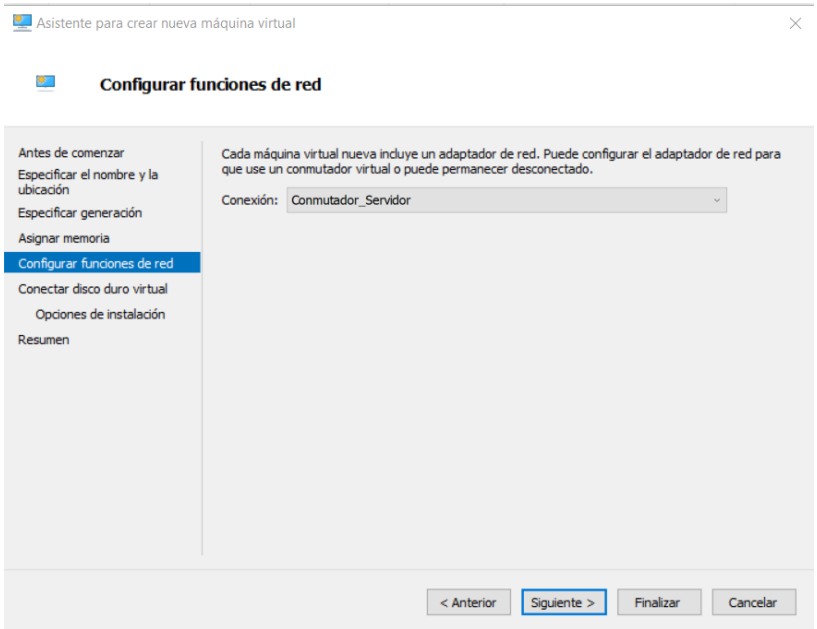


Figura 3.8 Asignación del conmutador virtual al SO WINDOWS_10

Para asignar una memoria de disco duro virtual se procedió a ingresar un valor de 90 (GB), en la Figura 3.9 se observa el respectivo proceso, finalmente se procedio a insertar la imagen ISO guardando los cambios realizados.

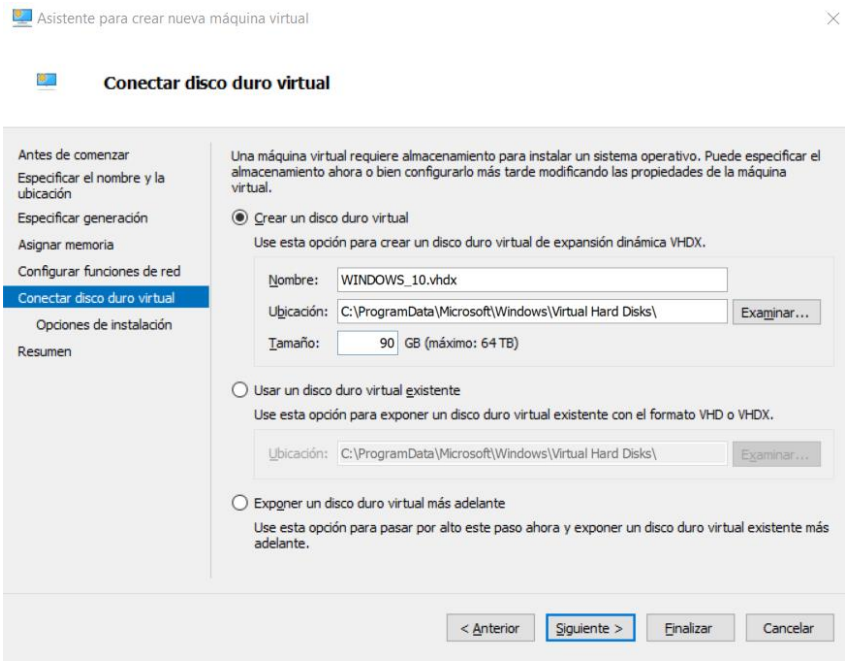


Figura 3.9 Asignacion de la capacidad del disco duro virtual para WINDOWS_10

Una vez que se creó el cliente se procedió a realizar la instalación, para ello se ejecutó la máquina *Windows_10* se siguió paso a paso el proceso de instalación. En la Figura 3.10 se presentan las primeras ventanas del proceso de instalación, en estas se encuentra la versión del SO a instalar y los términos de licencia.

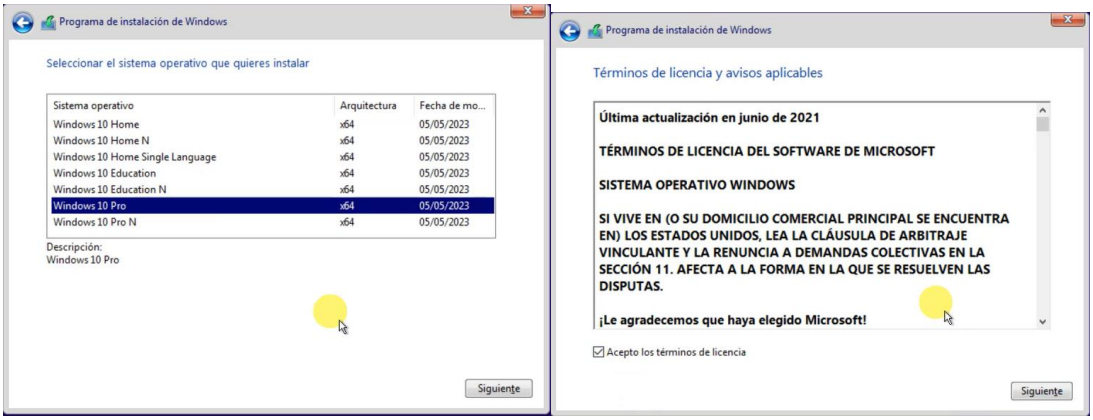


Figura 3.10 Versión del SO a instalar junto con los términos de licencia

En la Figura 3.11 se observa las siguientes ventanas del proceso de instalación, donde en la parte izquierda se observa el disco en la cual se va a instalar el SO, mientras que en la parte derecha se observa el proceso de la instalación.

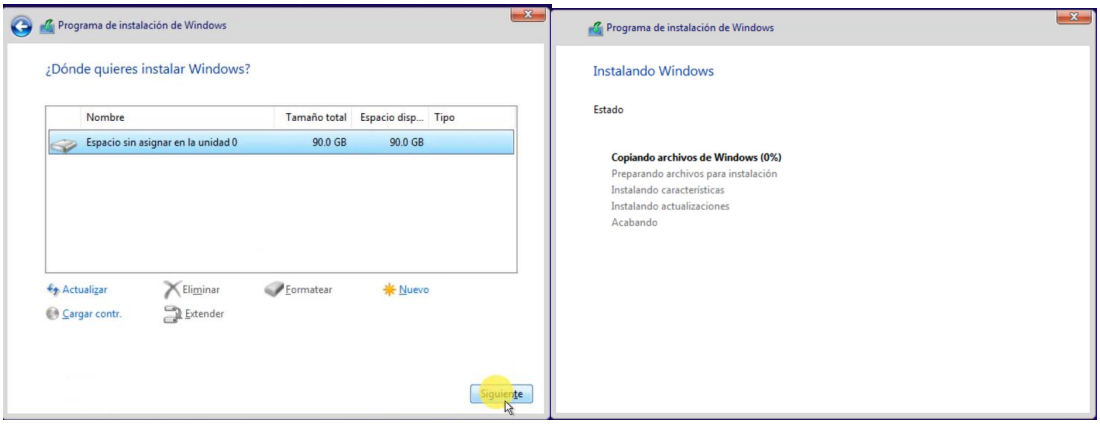


Figura 3.11 Ubicación para la instalación del SO y proceso de instalación

Para finalizar la configuración se procedió a configurar los conceptos básicos, tales como; la región en donde está ubicado el usuario, distribución del teclado, nombre del usuario del equipo, contraseña del usuario, preguntas de seguridad para las cuentas. Una vez que se registró estas configuraciones se procedió a iniciar el SO. En la Figura 3.12 se observa el escritorio del SO *Windows* 10 ya instalado.

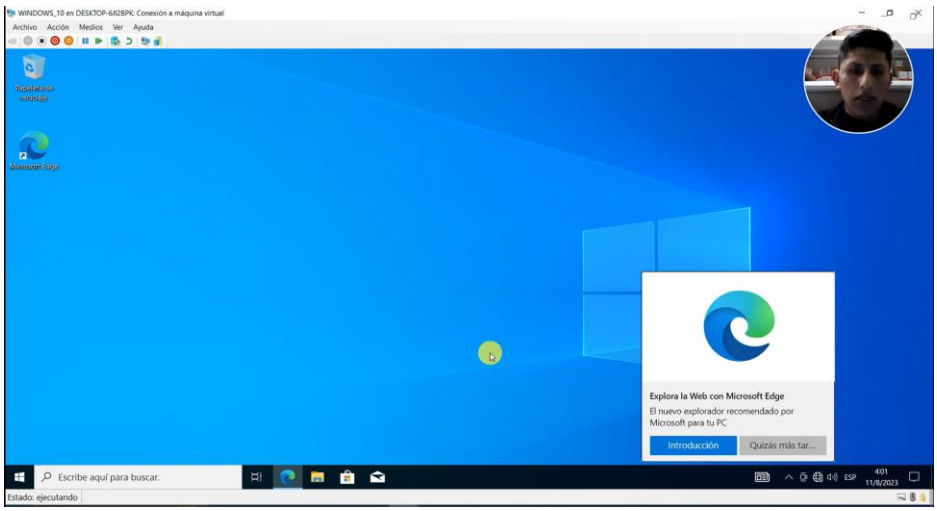


Figura 3.12 Escritorio del SO *Windows* 10

Configuración del servidor DHCP

Para configurar este servidor en *Windows Server*, en primera instancia se procedió a configurar una dirección IP estática con la finalidad mantener siempre esa dirección para el servidor y evitar que cuando se reinicie el servidor cambie de dirección. En la Figura 3.13 se observa la configuración de la dirección IP estática con las características siguientes:

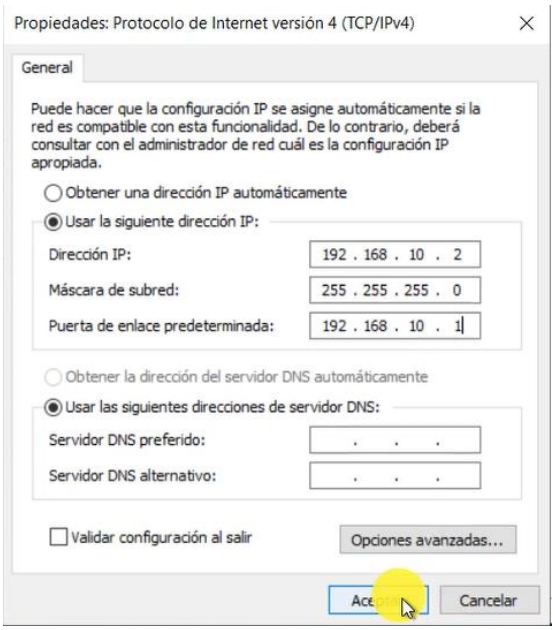


Figura 3.13 Configuración de la dirección IP

En la Figura 3.14 se visualiza el proceso de la instalación del servidor DHCP, empezando con la asignación de roles y características y selección del servidor a instalar.

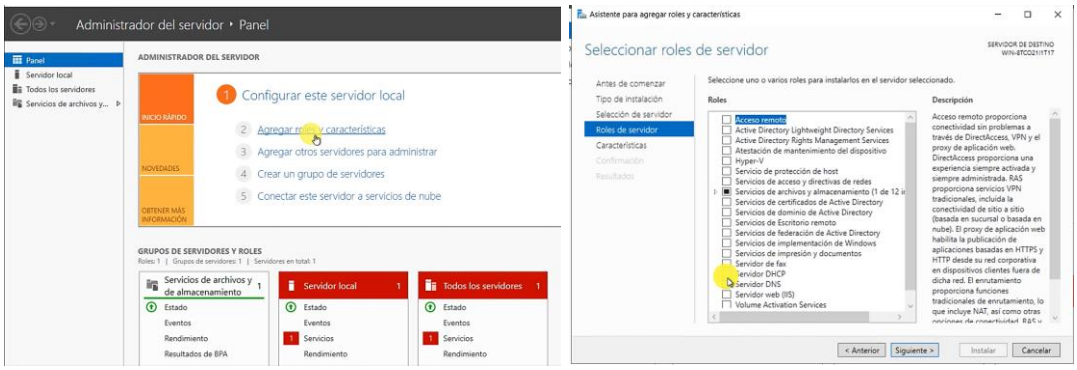


Figura 3.14 Proceso de instalación del servidor DHCP

Para la configuración del servidor DHCP se ingresó a la opción de herramientas DHCP, en esta ventana se configuró la dirección IPv4, en la cual se creó un nuevo ámbito con el nombre de “Servidor_DHCP”, pasando a la siguiente ventana donde se configuró los intervalos de la dirección IP. En la siguiente Figura 3.15 se observa este proceso de configuración.

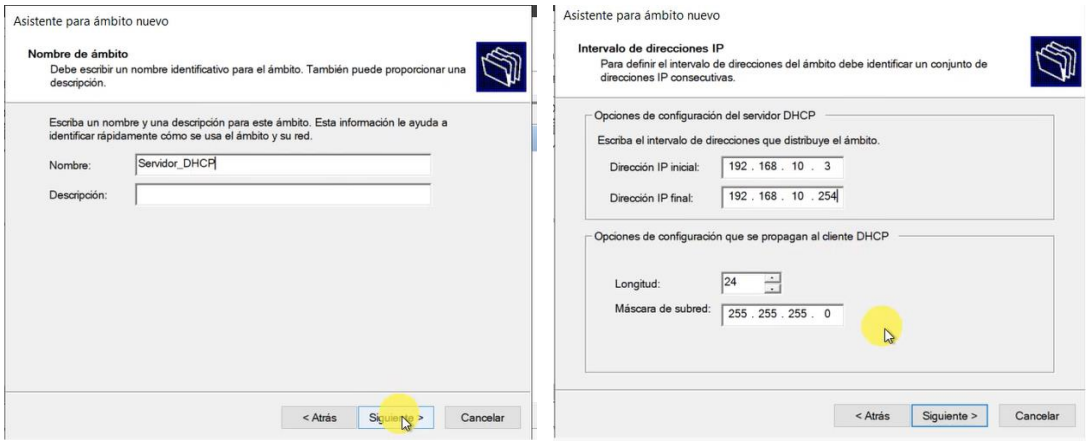


Figura 3.15 Configuración del nombre e intervalo en el servidor DHCP

Para la comunicación del servidor DHCP es importante ingresar la dirección IP que se configuró como estática en este caso la dirección IP 192.168.10.2, finalmente se procedió a finalizar la configuración. Es importante actualizar antes de realizar las pruebas de conexión.

Para la prueba de conexión se lo realizó desde el cliente *Windows* 10, en la cual se verificó mediante dos procesos:

Verificación de la dirección IP asignada: Para ello se ingresó al *cmd* en modo de administrador y se ejecutó el comando *ipconfig* para verificar si la IP reflejada está dentro del intervalo de configuración de direcciones, en la Figura 3.16 se evidencia la primera prueba de conexión.

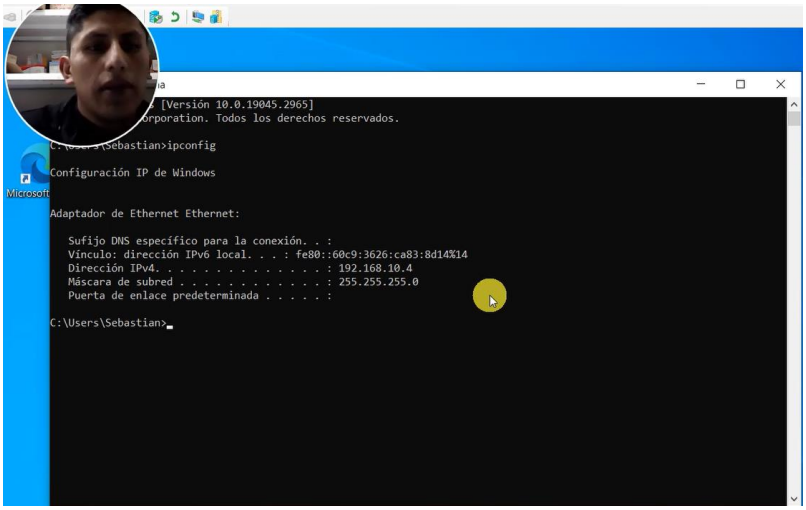


Figura 3.16 Asignación de la IP al cliente por medio de DHCP

Verificación de conexión mediante el comando *ping*: Para realizar esta prueba se procedió a ejecutar en el terminal el comando *ping* seguido por la dirección IP del servidor tal como se observa en la Figura 3.17, es importante que los *firewalls* estén desactivados para esta prueba.

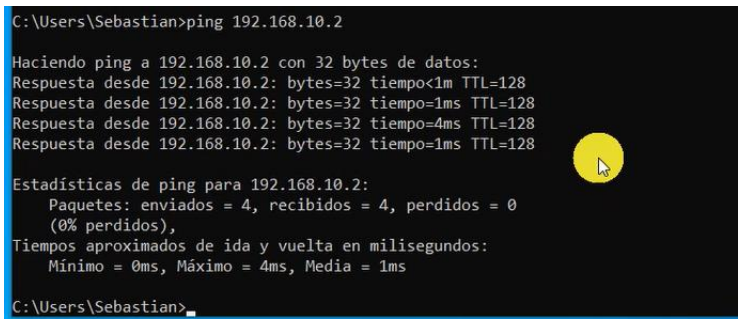


Figura 3.17 Prueba de conexión desde el cliente al servidor

Implementación del servidor de correo

Para levantar el servidor de correo se procedió a descargar la herramienta *HmailServer*, esta herramienta permite a las organizaciones y usuarios gestionar un servidor de correo electrónico. Mediante este *software* se puede realizar varias tareas tales como la gestión de cuentas de correo, envío, recepción de correos, seguridad, autenticación y almacenamiento [30]. Para ello se puede descargar de la siguiente página https://www.hmailserver.com/download tal como se observa en la siguiente Figura 3.18.

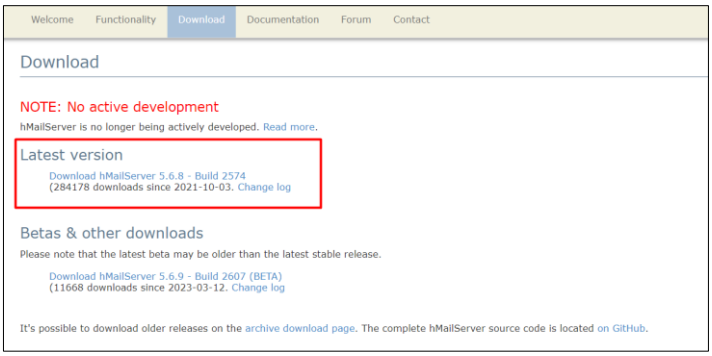


Figura 3.18 Página de descarga del software HmailServer [31]

Antes de ejecutar la herramienta, se procedió instalar el *.NET Framework*, el cual brinda una variedad de bibliotecas que permiten desarrollar aplicaciones en el entorno de *Windows*. En la Figura 3.19 se visualiza la instalación de esta herramienta. Un punto importante en esta instalación fue direccionar el archivo el cual se encuentra en la ISO del SO específicamente en la carpeta *sources-sxs,* una vez que se copió la dirección del archivo se procedió a pegar en la opción de origen, tal como se observa en la Figura 3.20. Esta instalación se lo realizó en la máquina virtual WINDOWS_SERVER_2019.

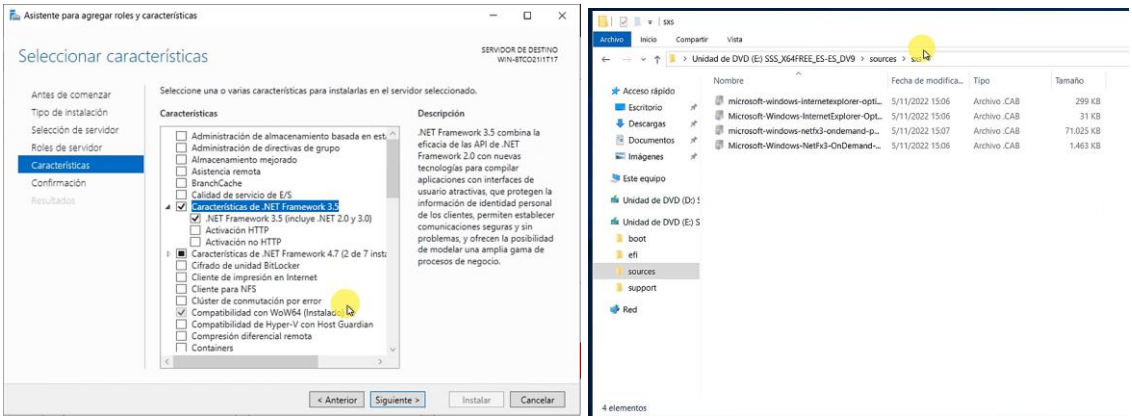


Figura 3.19 Proceso de configuración del .NET Framework

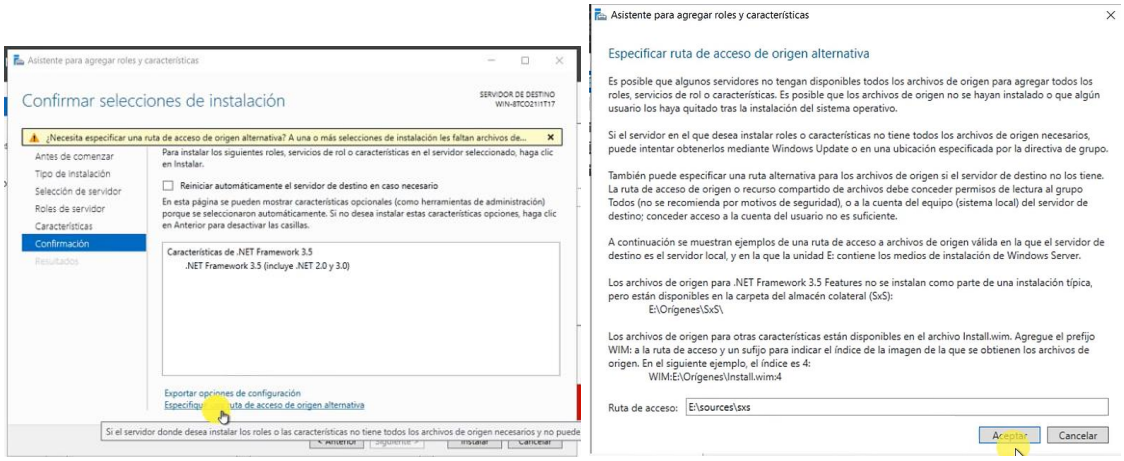


Figura 3.20 Instalación del .NET Framework

Una vez que se instaló el *Framework* se procedió a la instalación de la herramienta *HmailServer* para ello se ejecutó el archivo que se descargó, se aceptó los términos de licencia, se seleccionó la ubicación del archivo, se marcó los componentes que se requiere para que el servidor funcione sin problemas y finalmente instaló HmailServer. Al momento de correr el programa se visualiza una ventana de conexión al servidor tal como se observa en la Figura 3.21 en donde se procedió a insertar una clave para conectarse al servidor, dicha clave debe ser robusta con la finalidad de que solo un administrador pueda ingresar al servidor.

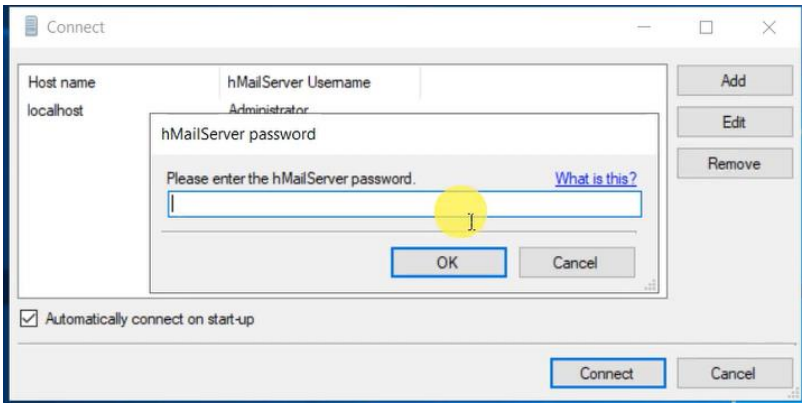


Figura 3.21 Conexión a la herramienta HmailServer

Una vez que se conectó al servidor se procedió a realizar las configuraciones para levantar el servicio de correo electrónico, entre las principales se encuentra las siguientes:

Creación de dominio. Para ello se procedió a agregar un nuevo dominio tal como se observa en la Figura 3.22 dicho dominio debe ser único.

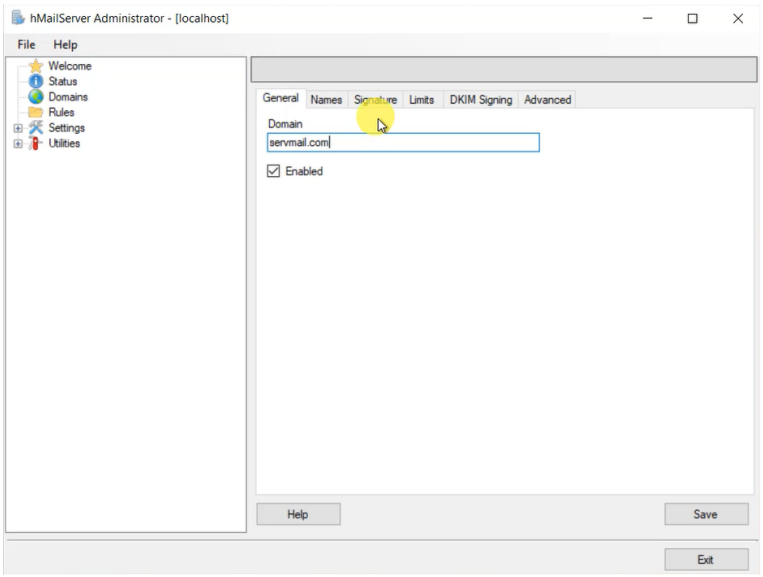


Figura 3.22 Creación del nuevo dominio

Creación de usuarios. Para la creación de los usuarios se dirigió a la carpeta de *accounts*, en esta carpeta se almacenaron los usuarios creados, para ello cada usuario tuvo diferentes nombres con sus respectivas contraseñas. En la Figura 3.23 se observa la creación del primer usuario con la dirección de correo **juan@servmail.com** con su respectiva contraseña, nombre de usuario **JUAN JANETA**.

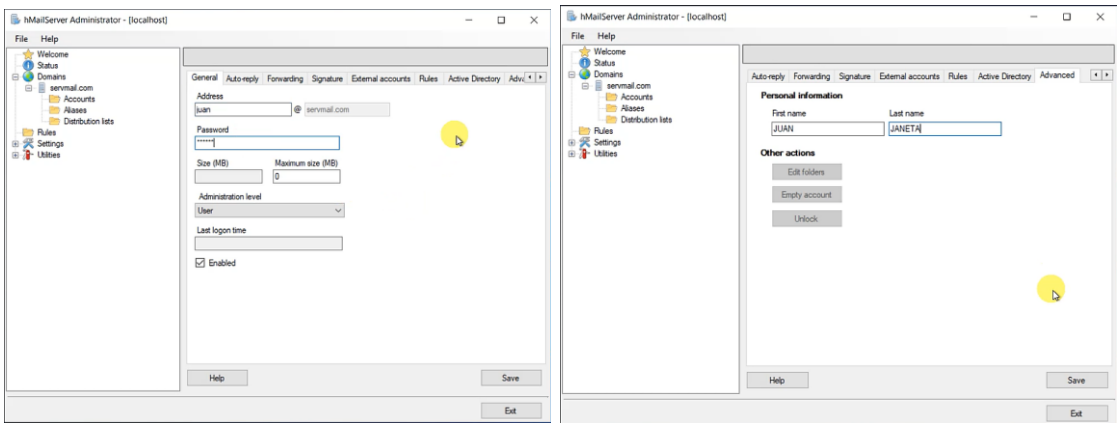


Figura 3.23 Creación del primer usuario

De la misma manera se crearon dos usuarios restantes, para las respectivas pruebas. En la Figura 3.24 se evidencia la creacion del segundo usuario en la cual se registró el correo electrónico con su respectiva contraseña.

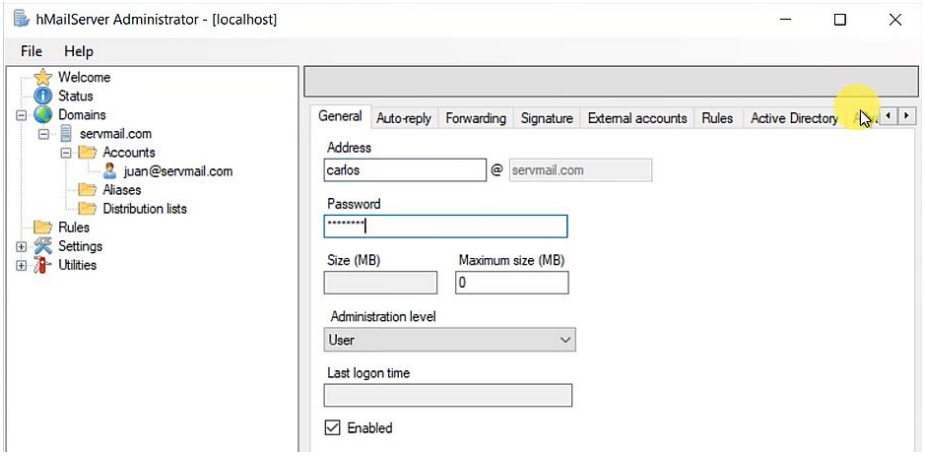


Figura 3.24 Creación del segundo usuario

Para la finalización de la creación del segundo usuario se procedió a ingresar la información personal del usuario, como su primer nombre y su primer apellido. Esta configuración se evidencia en la Figura 3.25.

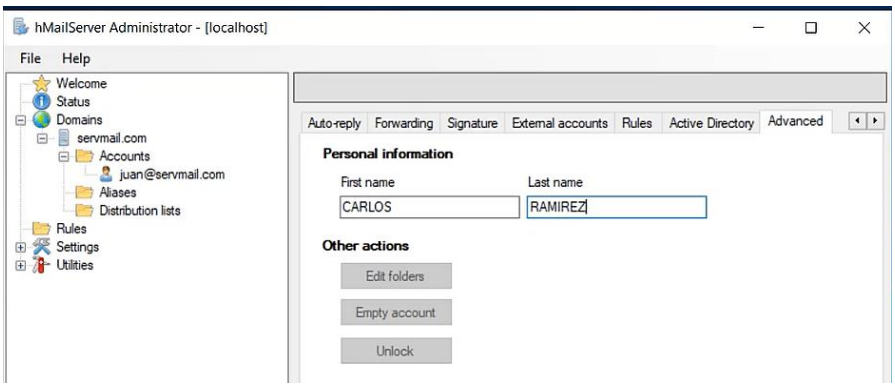


Figura 3.25 Registro de datos personales del segundo usuario

Para la creación del tercer usuario se procedió a seguir la misma configuración que del primer y segundo usuario con la diferencia del correo electrónico y la contraseña tal como se observa en la Figura 3.26.

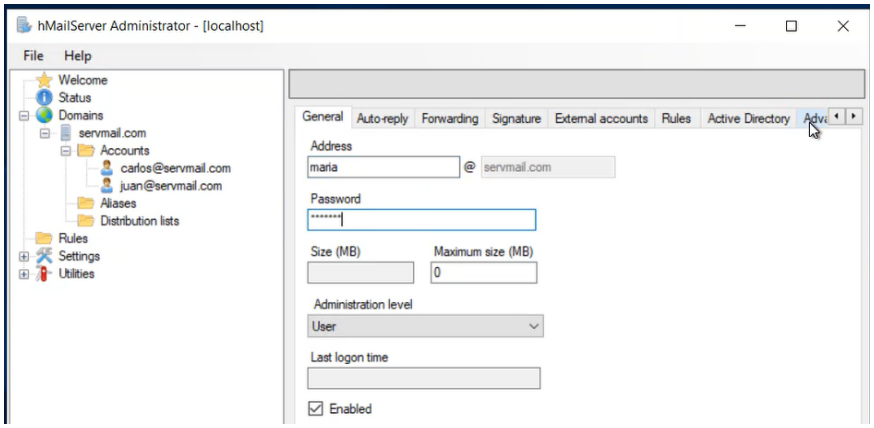


Figura 3.26 Creacion del tercer usuario

Asi tambien se registró los datos personales del tercer usuario tal como se observa en la Figura 3.27.

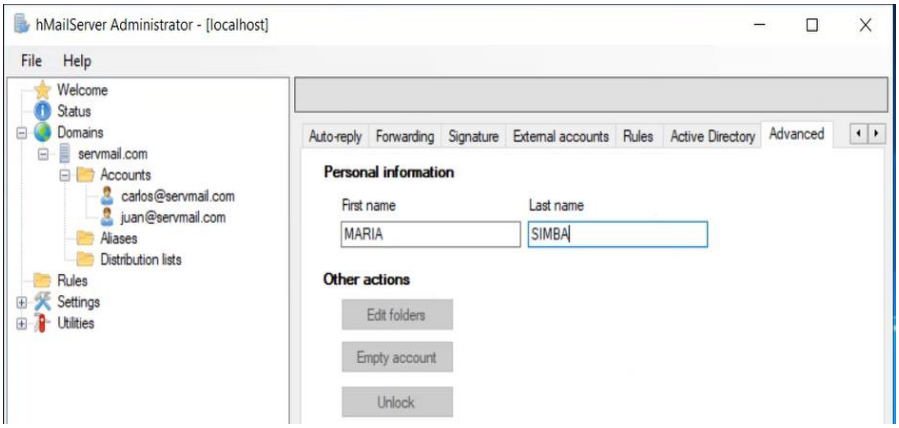


Figura 3.27 Creación del segundo y tercer usuario.

Por otro lado en la Tabla 3.1 se detalalla las credenciaes empleadas en la creación de los usuarios:

Tabla 3.1 Credenciales de usuarios

Dirección de correo	Contraseña	Nombre de usuario
juan@servmail.com	juan23	JUAN JANETA
carlos@servmail.com	carlos23	CARLOS RAMIREZ
maria@servmail.com	maria23	MARIA SIMBA

Instalación de *Thunderbird*

Para realizar las respectivas pruebas se empleó *Thunderbird,* esta herramienta es un gestor de correo electrónico con múltiples características, tales como; ligero, gratuito ideal para empresarios y profesionales, permite recibir, archivar y enviar correos a distintos usuarios [32]. Para la instalación de esta herramienta se la descargó de la siguiente página https://www.thunderbird.net/es-ES/, para ello se procedió a ejecutarlo, tomando en cuenta, el tipo de instalación, la cual se escogió la opción estándar, se seleccionó la ubicación del archivo y se procedió a instalar. En la Figura 3.28 se evidencia el proceso de instalación del *software Thunderbird* la cual fue instalada en el SO de servidor.

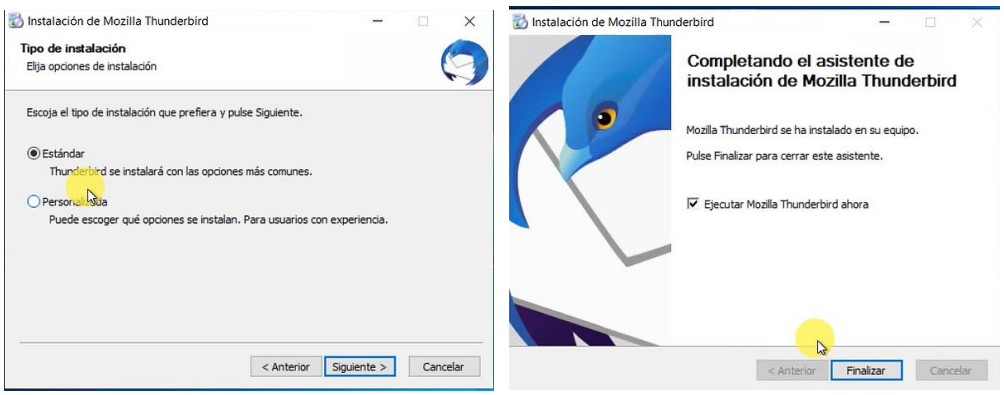


Figura 3.28 Instalación de la herramienta *Thunderbird*

Para la configuración de las cuentas de correo ya anteriormente creadas, se procedió a registrar en el gestor de correo para lo cual se ingresó las credenciales del primer usuario. Tal como se observa en la Figura 3.29.

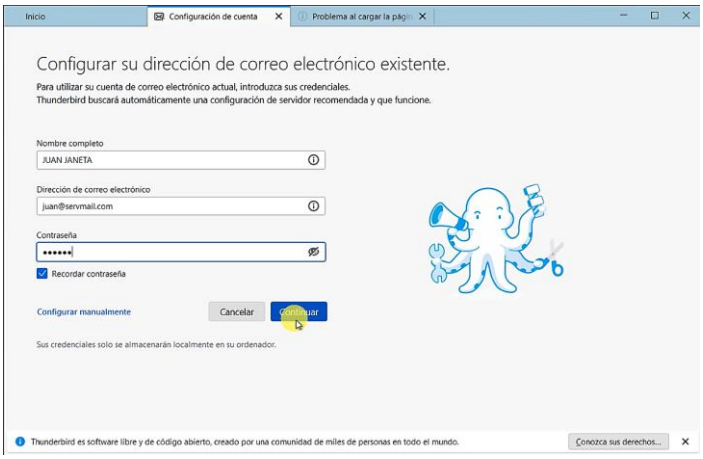


Figura 3.29 Registro de credenciales del primer usuario

Una vez insertado las credenciales se procedió a validar, al momento de validar se desplegó nuevos campos en los que se procedió a configurar algunos parámetros tal como se evidencia en la Figura 3.30. Estos parámetros son de mucha importancia para que la herramienta permita enviar o recibir los correos.

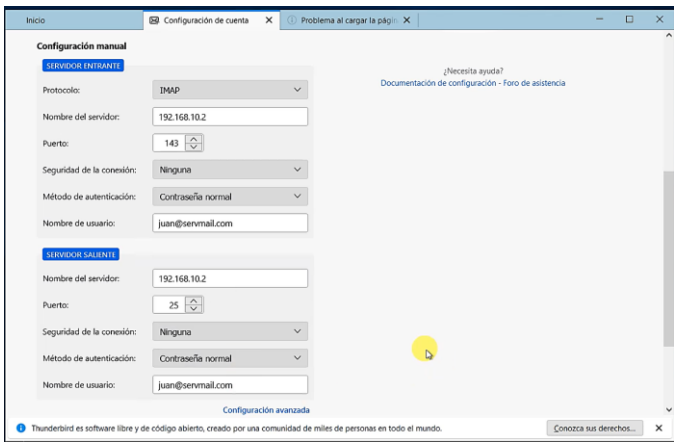


Figura 3.30 Configuración de parámetros para la recepción y envío de correos

Para la creación de las dos cuentas restantes se procedió a instalar la herramienta de *Thunderbird* en la máquina virtual de WINDOWS_10 configurada como cliente, para la instalación se siguió la misma configuración que al momento de instalar esta herramienta en el servidor.

Para ingresar la segunda cuenta en la herramienta Thunderbird se procedió a ingresar las credenciales del usuario Carlos, tal como se evidencia en la Figura 3.31. En esta ventana se ingresó los datos personales como el nombre y el apellido, seguido por el correo electrónico y su contraseña.

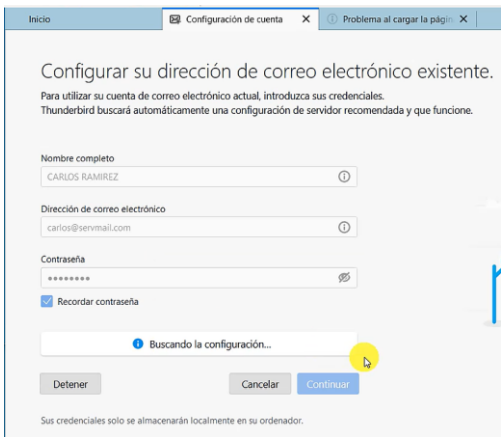


Figura 3.31 Inicio de sesión del usuario CARLOS RAMIREZ

Al validar la cuenta se presentó una nueva ventana, en la cual se realizó configuraciones tales como protocolo de entrada, direccion IP del servidor, puerto de entrada, seguridad de conexión, metodo de autentificacion, nombre de ususario, de la misma manera se configuración para el protocolo de salida, dirección del servidor, puerto de salida, seguridad de conexión, metodo de autentificación finalmete nombre de usuario que en este caso fué el correo electrónico. Esta configuracion se evidencia en la Figura 3.32.

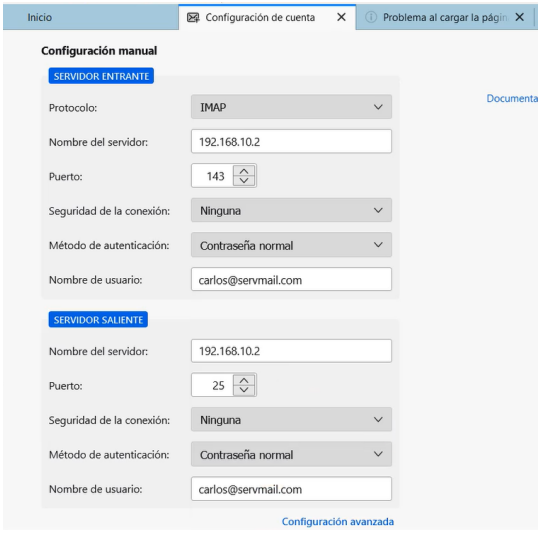


Figura 3.32 Configuración de los puertos de entrada y salida del usuario Carlos

Una vez configurado los protocolos se procedió a crear la cuenta, en la cual al lograr conectar con el servidor y verificar los datos nos presentó una nueva ventana con la notificación de la cuenta creada con éxito tal como se observa en la Figura 3.33.

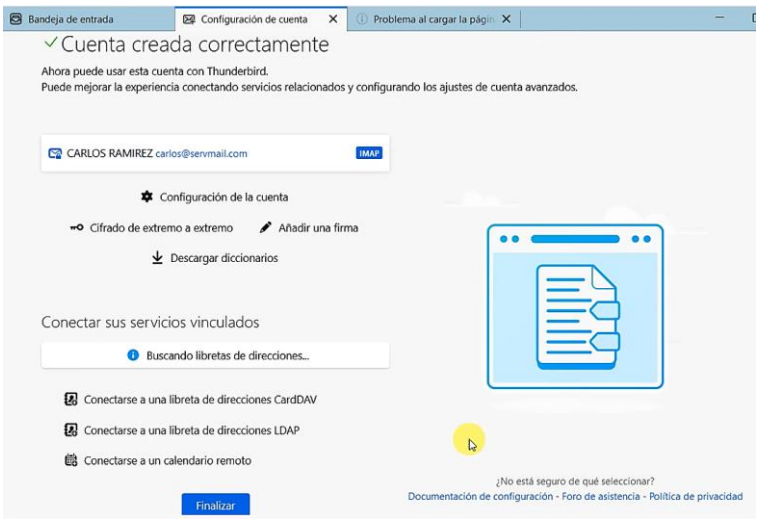


Figura 3.33 Registro de cuenta creada con éxito del usuario Carlos

De la misma manera se procedió a crear la tercera cuenta denominada María Simba, para lo cual se ingresó las credenciales tales como nombre completo, correo electrónico y contraseña. Tal como se observa en la Figura 3.34.

Figura 3.34 Inicio de sesión del usuario MARIA SIMBA

Una vez que se ingresó las credenciales se prcedió a configurar los protocolos tanto de entrada como de salida, tal como se observa en la Figura 3.35.

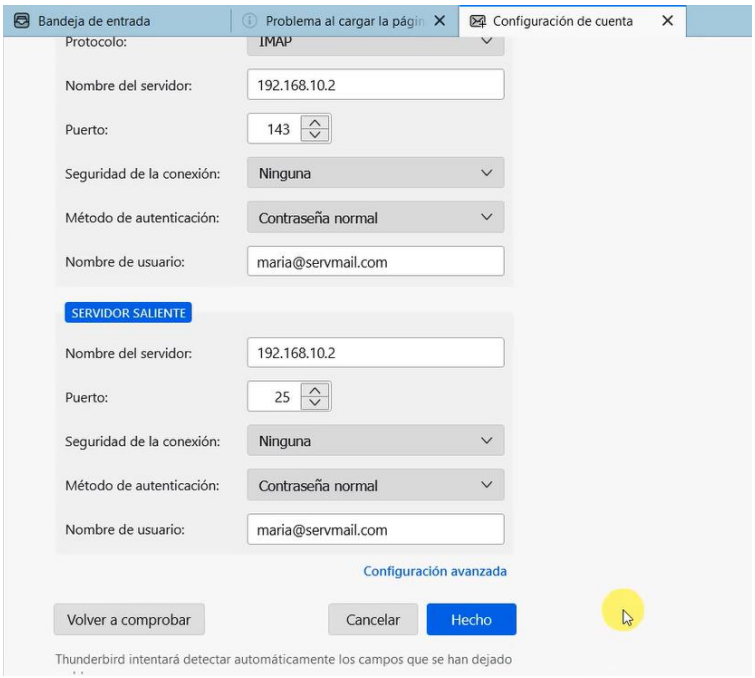


Figura 3.35 Configuración de los puertos de entrada y salida del usuario María

Al validar la cuenta con el servidor se presentó una nueva ventana con la notificación de cuenta creada correctamente tal como se observa en la Figura 3.36.

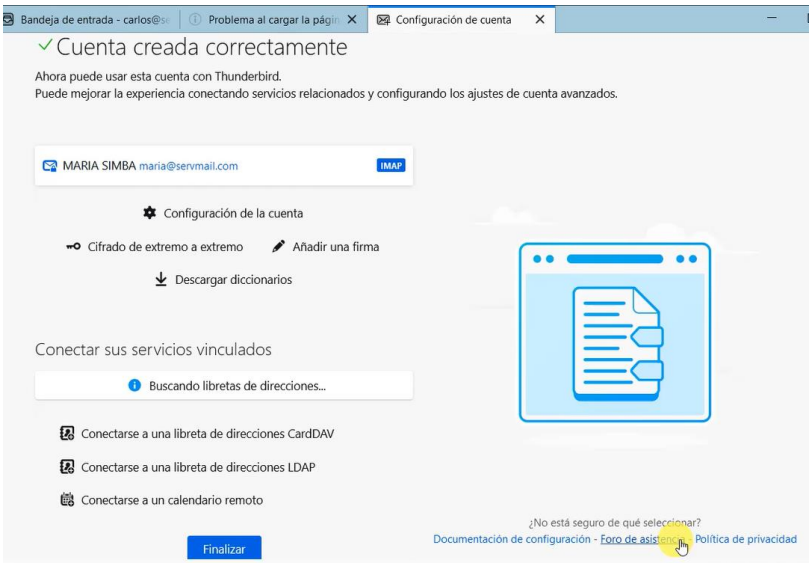


Figura 3.36 Registro de cuenta creada con éxito del usuario Carlos

Pruebas de gestión de correos electrónicos

Para comprobar el funcionamiento del servidor de correo se procedió a enviar correos entre los tres usuarios, en la Tabla 3.2 se visualizan los mensajes enviados de cada usuario.

Tabla 3.2 Envió de mensajes de los diferentes usuarios

Usuario quien envía el correo	Mensaje enviado	Usuario quien recibe el correo
JUAN JANETA	Saludos estimado Carlos	CARLOS RAMIREZ
JUAN JANETA	Saludos estimada María	MARIA SIMBA
CARLOS RAMIREZ	Saludos estimado Juan	JUAN JANETA
CARLOS RAMIREZ	Saludos estimada María	MARIA SIMBA
MARIA SIMBA	Saludos estimado Juan	JUAN JANETA
MARIA SIMBA	Saludo estimado Carlos	CARLOS RAMIREZ

En la Figura 3.37 se evidencia las pruebas de envío y recepción de correo electrónico desde la cuenta de Carlos Ramírez hacia María Simba en la parte superior y en la parte inferior María Simba hacia Carlos Ramírez.

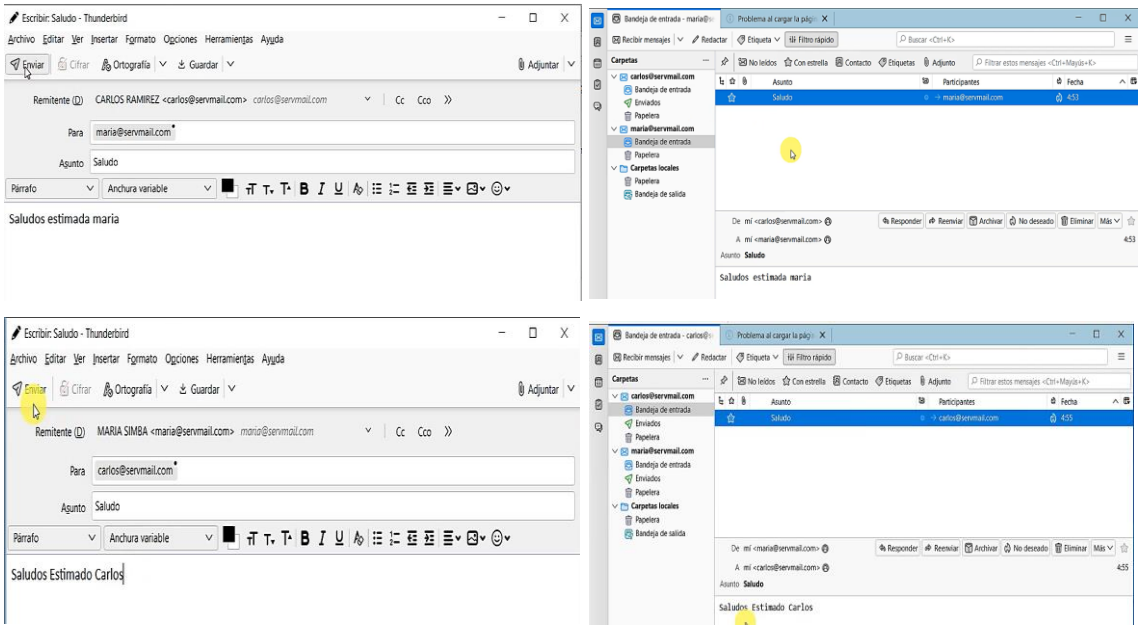


Figura 3.37 Mensaje enviado de Carlos hacia María y viceversa

En la Figura 3.38 se evidencia las pruebas de envío y recepción de correo electrónico desde la cuenta de Carlos Ramírez hacia Juan Janeta en la parte superior y en la parte inferior Juan Janeta hacia Carlos Ramírez.

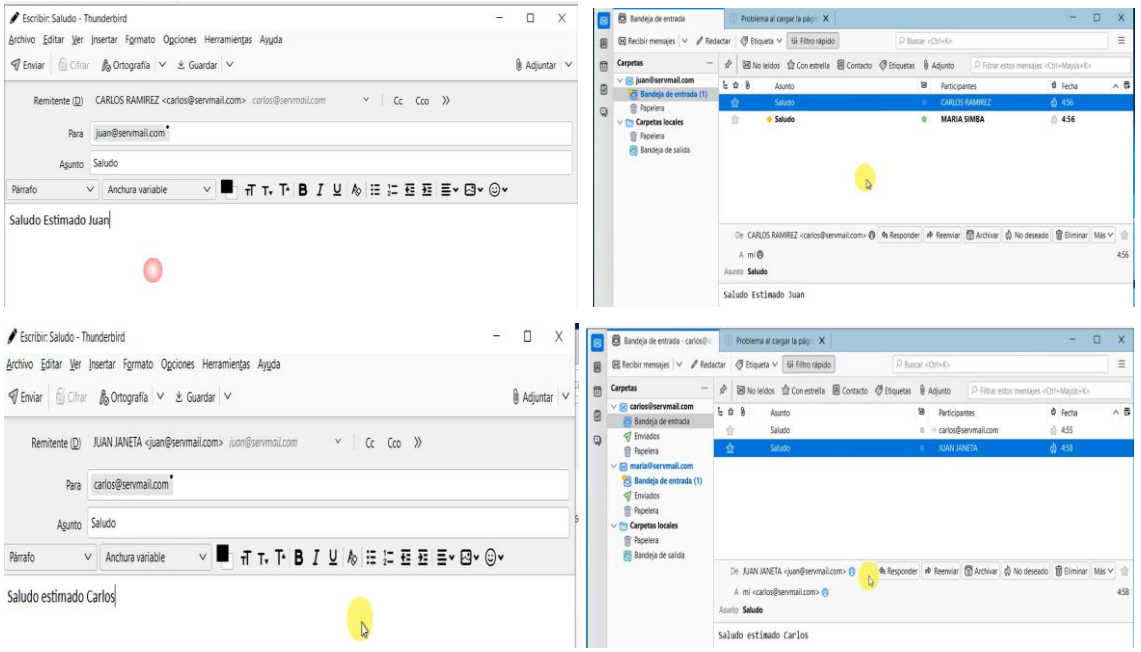


Figura 3.38 Mensaje enviado de Carlos hacia Juan y viceversa

En la Figura 3.39 se evidencia las pruebas de envío y recepción de correo electrónico desde la cuenta de María Simba hacia Juan Janeta en la parte superior y en la parte inferior Juan Janeta hacia María Simba.

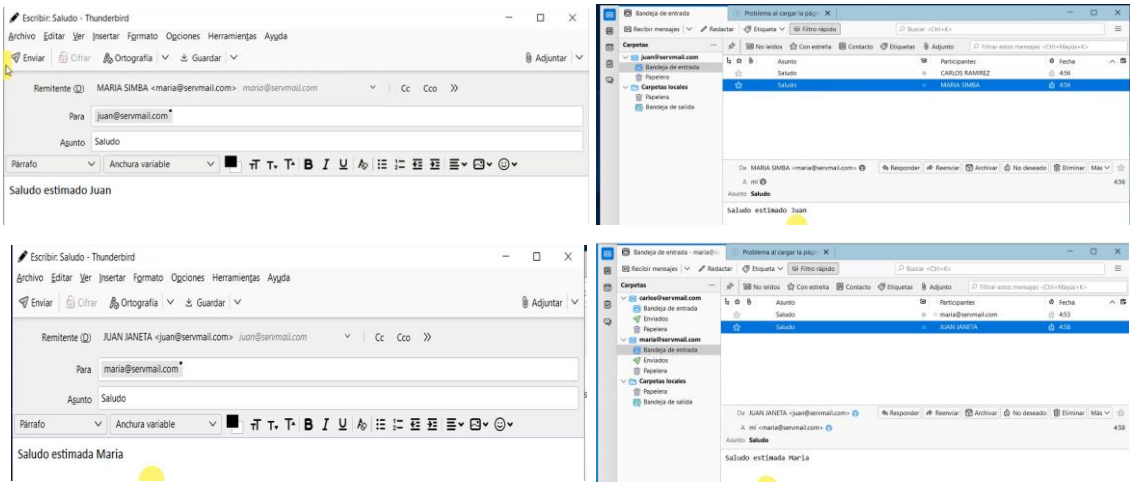


Figura 3.39 Mensaje enviado de María hacia Juan y viceversa

Instalación de la herramienta de escaneo

Para visualizar el reporte de vulnerabilidades se empleó la herramienta SCAP *Compliance*, se escogió esta herramienta ya que posee una variedad de características empezando por la facilidad de uso hasta la implementación de STIG. Para la instalación de la herramienta de escaneo se procedió a descargar de la siguiente página https://public.cyber.mil/stigs/scap/, una vez descargado se procedió a ejecutarlo como administrador. En la Figura 3.40 se visualiza el proceso de instalación, en la cual se empieza por aceptar los términos de licencia del programa, seguido por seleccionar todos los paquetes del programa, creación de un ícono en el escritorio, finalmente con su respectiva instalación.

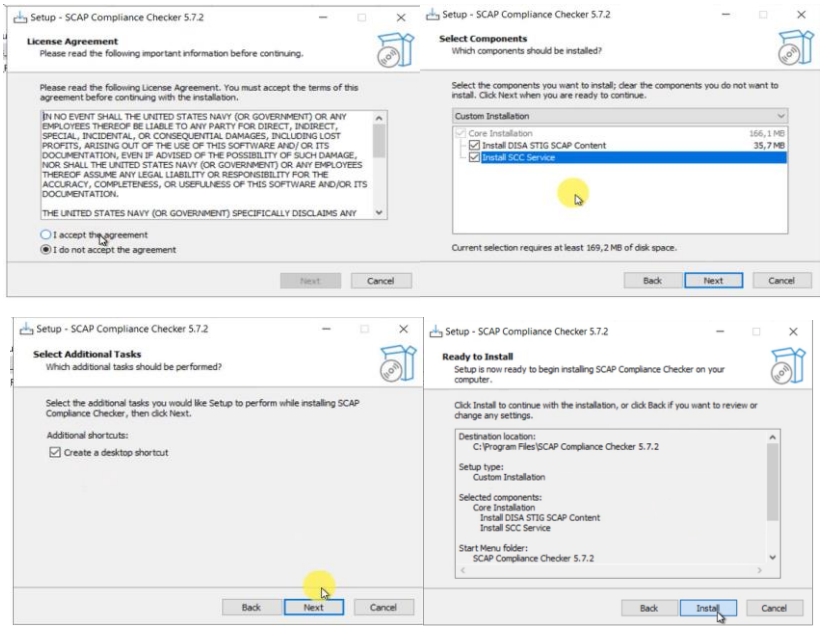


Figura 3.40 Instalación de la herramienta de escaneo SCAP *Compliance Cheker*

Una vez instalado el programa se procedió a ejecutarlo como administrador, una vez dentro se presentó la interfaz del programa la cual cuenta con varias características, empezando por su estructura la cual se puede visualizar en la Figura 3.41. donde se detalla cada una de sus partes:

1. ***Choose a Scan Type****:* Corresponde a escoger un tipo de escaneo, esta puede ser local, remota a un usuario *Windows*, remota a varios usuarios de *Windows*, escaneo mediante CISCO de forma remota, etc.
2. ***Select Content***: Es un indicador de cuantos equipos se va a realizar el escaneo.
3. ***Start Scan****:* Permite iniciar el escaneo de los usuarios seleccionados.
4. ***View Results****:* En la presente sección, es posible visualizar tanto la cantidad de exploraciones llevadas a cabo, como la eventual presencia de un escaneo reciente.
5. ***SCAP****:* En esta ventana se visualiza todos los archivos, programas a los cuales se puede realizar un escaneo mediante un STIG.
6. ***Install****:* Esta opción permite instalar los respectivos STIG que han sido desarrollados por personal de la TI.
7. ***Refresh****:* Mediante esta opción actualizamos los archivos, programas, STIG que han sido instalados.

8. ***Show All****:* Con esta opción se visualiza todos los archivos existentes en dicho programa.
9. ***Computer Status, stream status, current stream****:* Es un indicador en el cual se refleja los resultados arrojados una vez que se empieza a realizar el escaneo.
10. ***Log****.* Son los registros con los que están cargados el programa, una vez realizado el escaneo, en base a esos formatos se presenta los resultados.

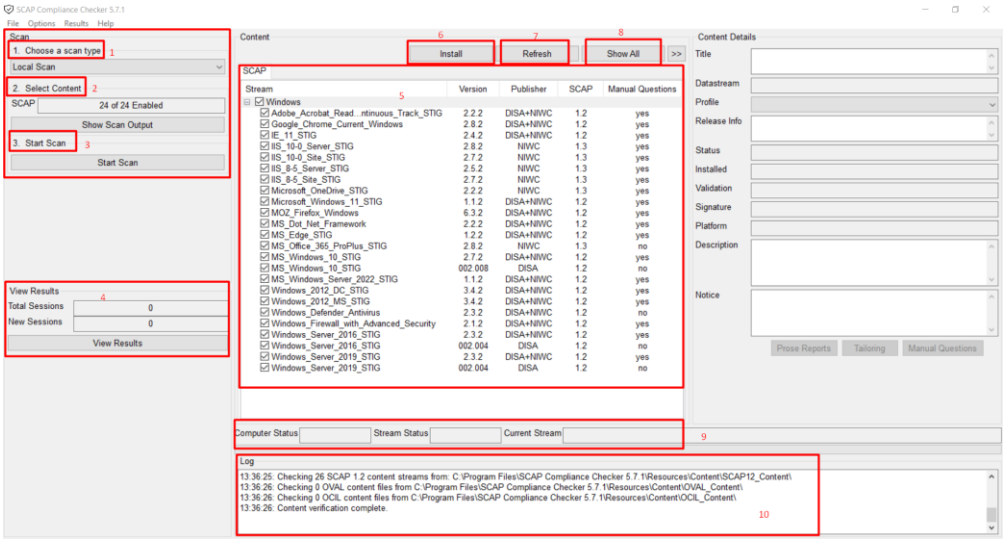


Figura 3.41 Interfaz de la herramienta SCAP *Compliance*

Reporte de vulnerabilidades

Para obtener el reporte de vulnerabilidades primero se procedió a escanear el SO de Servidor, para ello se procedió a descargar STIG, que es una guía de referencia de implementación de seguridad para diferentes sistemas operativos esto se descargó del siguiente repositorio https://www.niwcatlantic.navy.mil/Technology/SCAP/SCAP-Content-Repository/, una vez descargado, se procedió a ejecutarla. Se procedió a instalar la STIG correspondiente al SO *Windows Server 2019.* En la Figura 3.42 se observa la respectiva instalación.

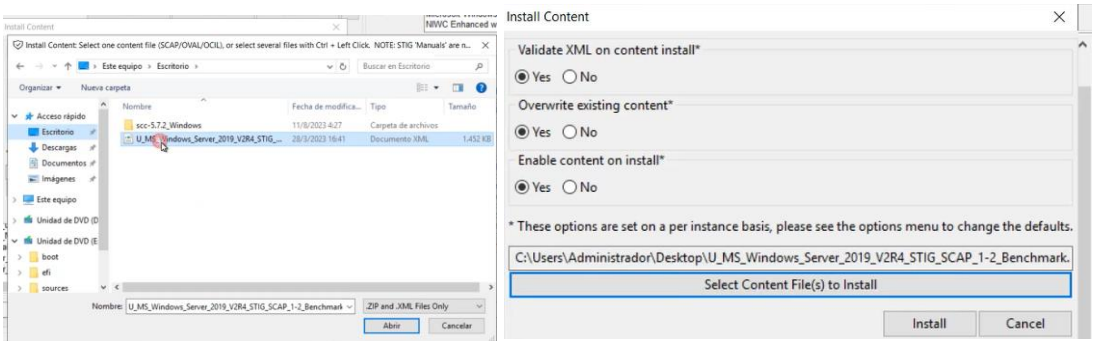


Figura 3.42 Instalación de las STIG de *Windows Server* 2019

En la Figura 3.43 se observa el proceso de escaneo del SO *Windows Server*, en lo cual se escogió un escaneo local ya que la herramienta se lo instaló directamente en el SO, se verificó que esté seleccionada STIG correspondiente al Servidor, finalmente se procedió a escanear, ver la Figura 3.44.

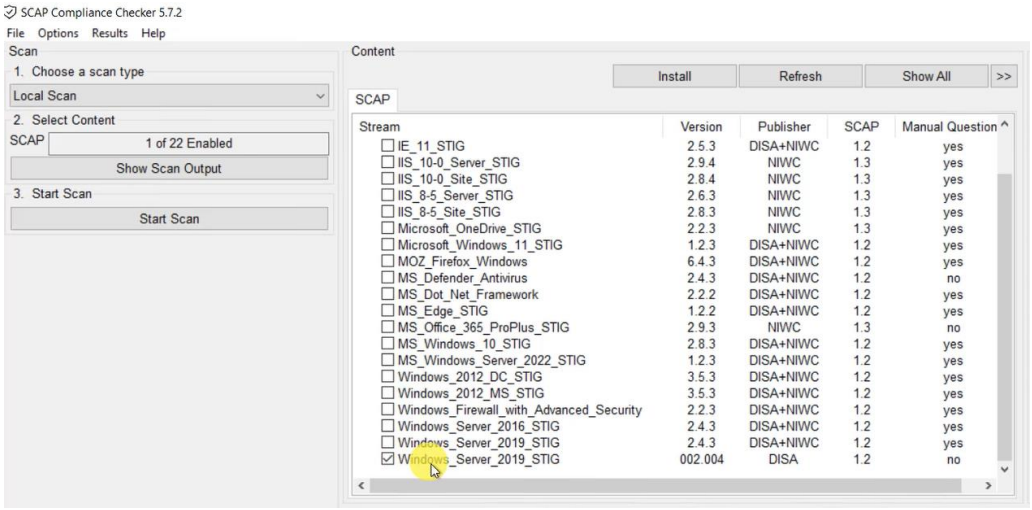


Figura 3.43 Proceso de escaneo en el Servidor

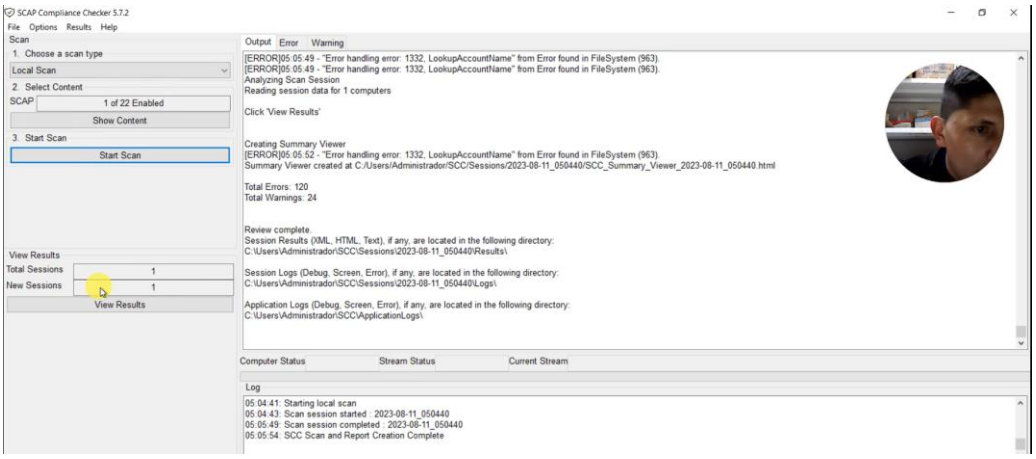


Figura 3.44 Finalización del escaneo

Al ingresar en la opción de resultados se encontró dos documentos, en los cuales se encontraban los reportes obtenidos después del escaneo, esto se evidencia en la Figura 3.45 donde, en el primero reporte se encuentra toda la configuración del sistema, mientras que en el segundo reporte se encuentran solo las configuraciones con problemas en el sistema.

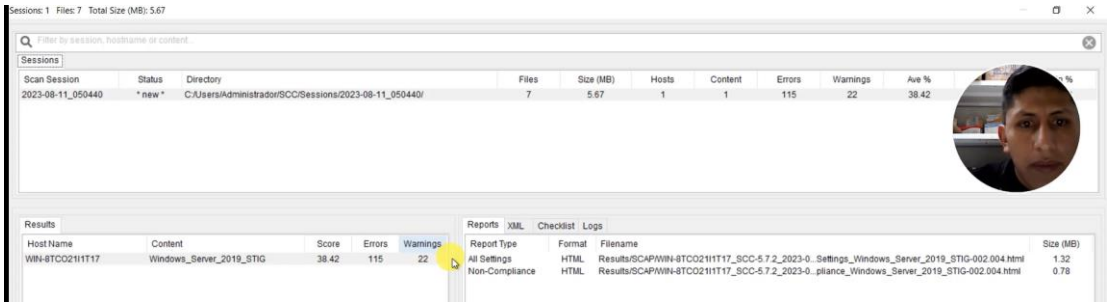


Figura 3.45 Documentos con el reporte de vulnerabilidades

En la Figura 3.46 se observa que al abrir el primer documento se presentan los siguientes detalles:

El porcentaje con el que está asegurado el sistema inicial, el cual es de 38,42 %, es decir que el 61.58 % del sistema tiene configuraciones con falencias, los cuales deben ser corregidas para reducir los riesgos de vulnerabilidades del sistema.

El total de configuraciones que se ha analizado son 202, de estos 69 cumplen con el STIG, mientras que 109 no cumplen con lo establecido y hacen que el sistema sea vulnerable. Por otro lado 25 no son aplicables, esto hace referencia a que estas configuraciones no pueden ser modificadas por seguridad del sistema.

También en la Figura 3.46 se observa el estado de cumplimiento del sistema representado en un color rojo. También en esta figura se indican los puntajes y colores asignados, si la puntuación es igual a 100 esto se representará en color azul; el color verde está representado por una puntuación de mayor o igual a 90; por otro lado, el amarillo se verá reflejado si la puntuación se encuentra de 80 para arriba. Pero si la puntuación esta entre 0 y menos de 80 se reflejara un color rojo tal como se observa en la Figura 3.47.

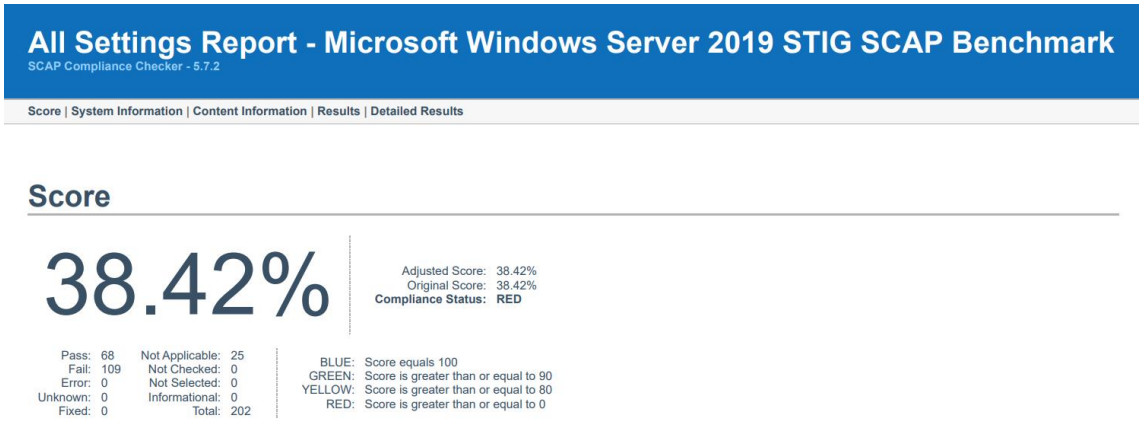


Figura 3.46 Porcentaje de aseguramiento del sistema

En este documento también se encuentra las configuraciones con los niveles de gravedad o severidad en el sistema, también se representan como categoria I, II, III. En la Figura 3.47 se observa las configuraciones de alta gravedad, en las cuales se han analizado un total de 18 configuraciones, de estas, 9 estan en estado azul y 9 estan en estado rojo, los de estado azul cumplen con los STIG establecidos, mientras que los de estado rojo deben ser solventados para evitar futuros daños en el sistema.

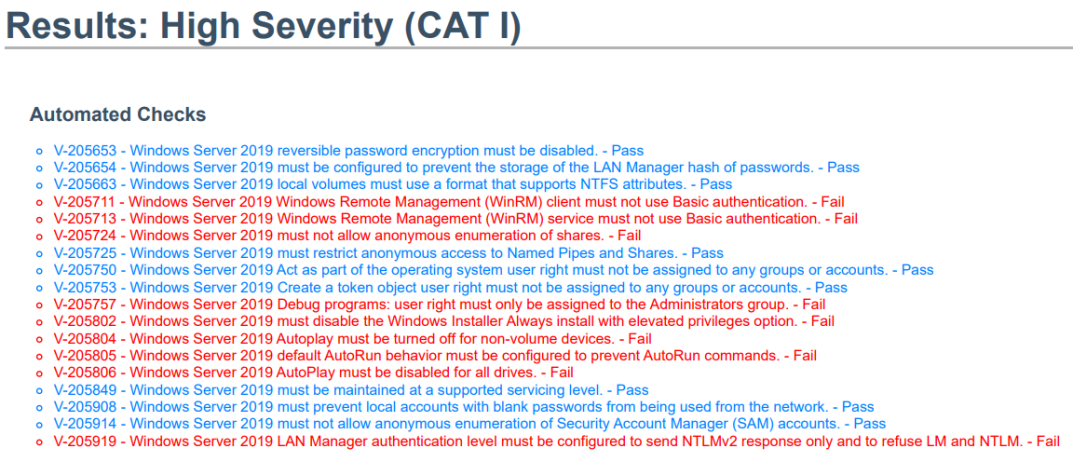
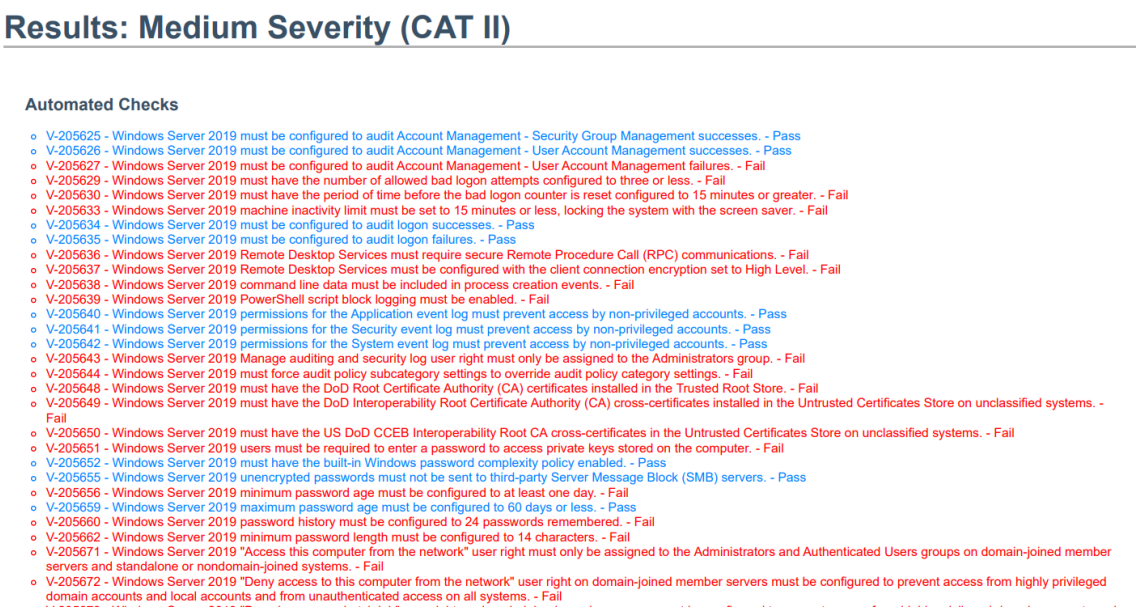


Figura 3.47 Reporte de configuraciones de categoría I

En la Figura 3.48 se observa las configuraciones de categoría II o también denominados gravedad media, en este nivel se analizaron un total de 154 configuraciones, de los cuales 58 están representado por el color azul es decir que cumplen con los STIG, mientras que 96 configuraciones están representadas por color rojo, estos también deben ser solventados para asegurar el servidor.



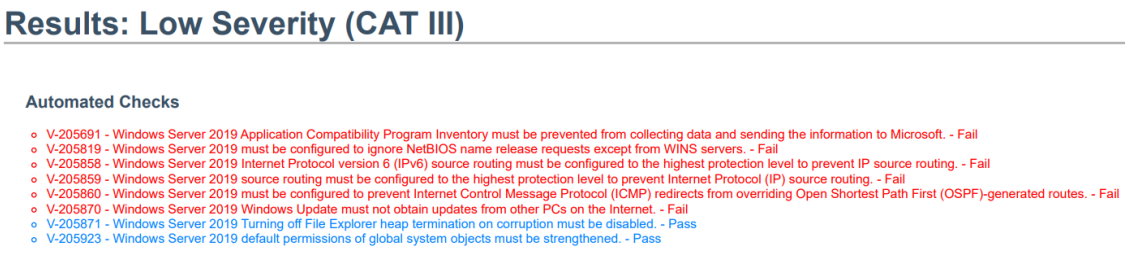
Results: Medium Severity (CAT II)

Automated Checks

- V-205625 - Windows Server 2019 must be configured to audit Account Management - Security Group Management successes. - Pass
- V-205626 - Windows Server 2019 must be configured to audit Account Management - User Account Management successes. - Pass
- V-205627 - Windows Server 2019 must be configured to audit Account Management - User Account Management failures. - Fail
- V-205629 - Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less. - Fail
- V-205630 - Windows Server 2019 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater. - Fail
- V-205633 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver. - Fail
- V-205634 - Windows Server 2019 must be configured to audit logon successes. - Pass
- V-205635 - Windows Server 2019 must be configured to audit logon failures. - Pass
- V-205636 - Windows Server 2019 Remote Desktop Services must require secure Remote Procedure Call (RPC) communications. - Fail
- V-205637 - Windows Server 2019 Remote Desktop Services must be configured with the client connection encryption set to High Level. - Fail
- V-205638 - Windows Server 2019 command line data must be included in process creation events. - Fail
- V-205639 - Windows Server 2019 PowerShell script block logging must be enabled. - Fail
- V-205640 - Windows Server 2019 permissions for the Application event log must prevent access by non-privileged accounts. - Pass
- V-205641 - Windows Server 2019 permissions for the Security event log must prevent access by non-privileged accounts. - Pass
- V-205642 - Windows Server 2019 permissions for the System event log must prevent access by non-privileged accounts. - Pass
- V-205643 - Windows Server 2019 Manage auditing and security log user right must only be assigned to the Administrators group. - Fail
- V-205644 - Windows Server 2019 must force audit policy subcategory settings to override audit policy category settings. - Fail
- V-205648 - Windows Server 2019 must have the DoD Root Certificate Authority (CA) certificates installed in the Trusted Root Store. - Fail
- V-205649 - Windows Server 2019 must have the DoD Interoperability Root Certificate Authority (CA) cross-certificates installed in the Untrusted Certificates Store on unclassified systems. - Fail
- V-205650 - Windows Server 2019 must have the US DoD CCEB Interoperability Root CA cross-certificates in the Untrusted Certificates Store on unclassified systems. - Fail
- V-205651 - Windows Server 2019 users must be required to enter a password to access private keys stored on the computer. - Fail
- V-205652 - Windows Server 2019 must have the built-in Windows password complexity policy enabled. - Pass
- V-205655 - Windows Server 2019 unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers. - Pass
- V-205656 - Windows Server 2019 minimum password age must be configured to at least one day. - Fail
- V-205659 - Windows Server 2019 maximum password age must be configured to 60 days or less. - Pass
- V-205660 - Windows Server 2019 password history must be configured to 24 passwords remembered. - Fail
- V-205662 - Windows Server 2019 minimum password length must be configured to 14 characters. - Fail
- V-205671 - Windows Server 2019 "Access this computer from the network" user right must only be assigned to the Administrators and Authenticated Users groups on domain-joined member servers and standalone or nondomain-joined systems. - Fail
- V-205672 - Windows Server 2019 "Deny access to this computer from the network" user right on domain-joined member servers must be configured to prevent access from highly privileged domain accounts and local accounts and from unauthenticated access on all systems. - Fail

Figura 3.48 Reporte de configuraciones de categoría II

Por último, en la Figura 3.49 se presenta los de categoría III o también denominado como de baja gravedad, en esta se analizaron un total de 8 configuraciones, de estas 6 son de configuraciones que deben ser solventadas ya que están representadas por color rojo, mientras dos configuraciones cumplen con el STIG representadas por el color azul.



Results: Low Severity (CAT III)

Automated Checks

- V-205691 - Windows Server 2019 Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft. - Fail
- V-205819 - Windows Server 2019 must be configured to ignore NetBIOS name release requests except from WINS servers. - Fail
- V-205858 - Windows Server 2019 Internet Protocol version 6 (IPv6) source routing must be configured to the highest protection level to prevent IP source routing. - Fail
- V-205859 - Windows Server 2019 source routing must be configured to the highest protection level to prevent Internet Protocol (IP) source routing. - Fail
- V-205860 - Windows Server 2019 must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF)-generated routes. - Fail
- V-205870 - Windows Server 2019 Windows Update must not obtain updates from other PCs on the Internet. - Fail
- V-205871 - Windows Server 2019 Turning off File Explorer heap termination on corruption must be disabled. - Pass
- V-205923 - Windows Server 2019 default permissions of global system objects must be strengthened. - Pass

Figura 3.49 Reporte de configuraciones de categoría III

3.2 Implementación de una política de seguridad basado en el marco de referencia CIS

Aplicación de la política de seguridad en *Windows Server* 2019

Para proceder a realizar la aplicación de una política de seguridad, antes se creó una nueva máquina virtual donde se instaló un nuevo SO de servidor *Windows Server* 2019, esto se realizó siguiendo los mismos pasos que se emplearon al momento de levantar el primer SO de servidor. En la Figura 3.50 se visualiza el

nuevo sistema operativo implementado, la diferencia con el anterior es la configuración del conmutador virtual ya que en el primero se creó un conmutador nuevo, mientras que para este SO de servidor se va a emplear el conmutador por *default* este conmutador de red viene preconfigurado con la finalidad de brindar conexión con redes externas, es decir que nuestro router podrá asignar una dirección ip valida a la máquina virtual, esto se lo realiza con la finalidad de descargar módulos DSC que permiten que la aplicación de la política de seguridad permanezca latente en el sistema operativo.

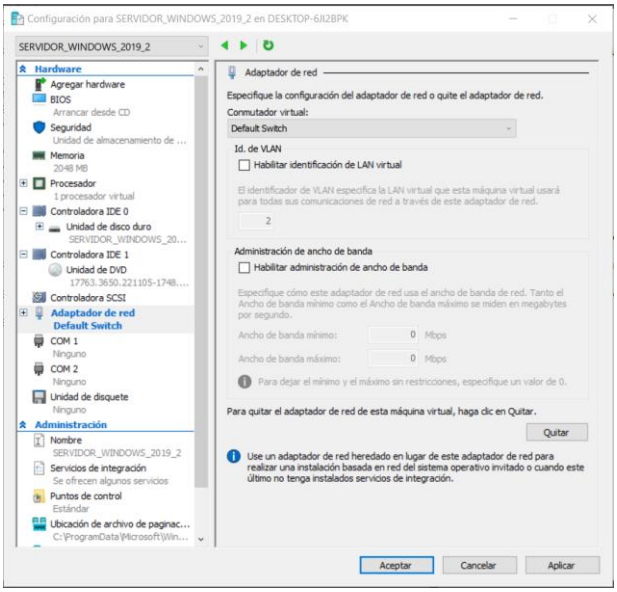


Figura 3.50 Características de la nueva máquina virtual

Una vez instalado el SO de servidor nuevo se procedió a ejecutarlo para realizar las configuraciones en la interfaz de usuario, una vez dentro del Servidor se procedió a verificar la versión del *Power Shell* mediante el comando $PSVersionTable.PSVersion esto se puede visualizar en la Figura 3.51, donde se observa que la versión es 5, con lo cual se ejecutó sin problemas los siguientes comandos ya que se cumple el requisito mínimo.

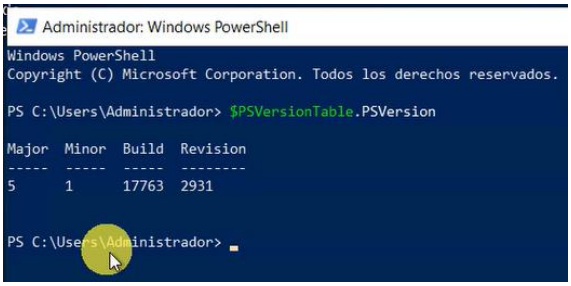


Figura 3.51 Versión de *Power Shell* del SO servidor

Instalación de módulos DSC y aplicación de la política de seguridad

Estos módulos DSC son los encargados de la administración del estado deseado del sistema, manteniendo esa configuración en todo momento sin que vuelva al estado inicial. Para ello se procedió instalar los siguientes módulos:

***AuditPolicyDsc**:* Este módulo se utiliza para especificar la configuración de políticas de auditoría en un sistema Windows. Las políticas de auditoría son reglas que determinan qué eventos se registran en el registro de eventos de Windows y cómo se manejan esos registros. Estos registros pueden ser críticos para la seguridad y la administración de sistemas, ya que pueden ayudar a identificar actividades sospechosas o problemas en un sistema. En la Figura 3.52 se evidencia la instalación de este módulo.

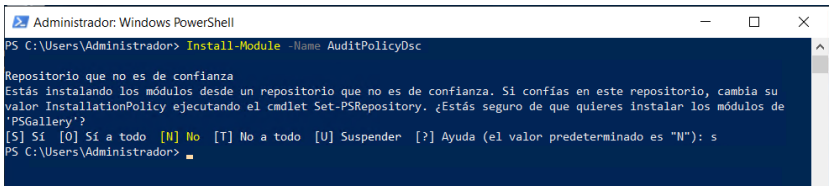


Figura 3.52 Instalación del módulo *AuditPolicyDsc*

SecurityPolicyDsc: Es un contenedor alrededor de la aplicación secedit.exe, a fin de otorgar al usuario la capacidad de ajustar las políticas de seguridad en el ámbito local. Este componente específico demanda la presencia de un sistema operativo Windows equipado con el programa secedit.exe. En la Figura 3.53 se visualiza la instalación de este módulo.

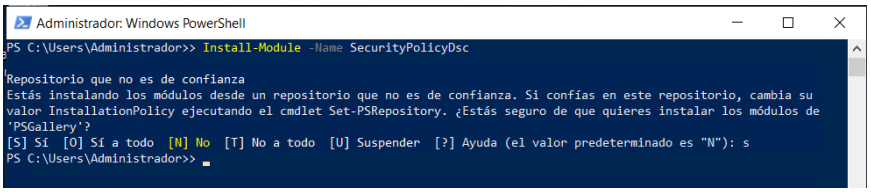


Figura 3.53 Instalación del módulo *SecurityPolicyDsc*

NetworkingDsc: Mediante el siguiente módulo se puede configurar el estado deseado de una red reduciendo los errores cometidos por el usuario, manteniendo la seguridad de la red y aumentando la eficiencia de la red. Algunas de las configuraciones principales de este módulo son: ajustes de interfaces de red, configuración de *firewall*, configuración de adaptadores de red virtuales,

configuración de VPN y configuración de nombres de host y dominio. En la Figura 3.54 se visualiza la instalación de este módulo.

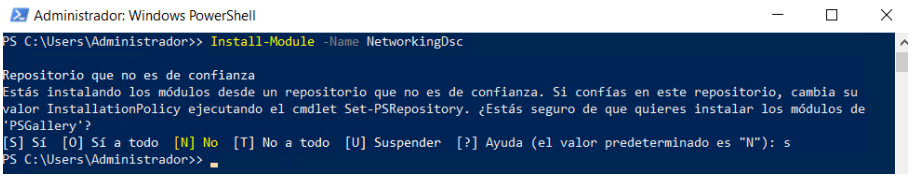


Figura 3.54 Instalación del módulo *NetworkingDsc*

Una vez descargado e instalado los módulos DSC, se procedió a verificar si se instalaron de manera correcta, en la siguiente Figura 3.55 se observa el proceso de verificación de los módulos DSC.

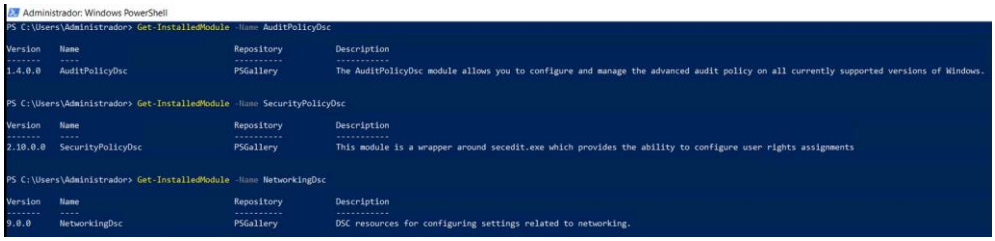


Figura 3.55 Verificación de la instalación de los módulos DSC

El paso siguiente que se realizó fue descargarse el *script* del siguiente repositorio https://raw.githubusercontent.com/Cloudneeti/os-harderning-scripts/master/WindowsServer2019/CIS_Benchmark_WindowsServer2019_v100.ps1, en la Figura 3.56 se visualiza el proceso de descarga del *script*.

Figura 3.56 Descarga del *script Windows Server* 2019 CIS BENCHMARK

En la Figura 3.57 se visualiza el proceso de ejecución del *script*, lo cual al momento de ejecutarlo se creó un archivo MOF en el directorio.

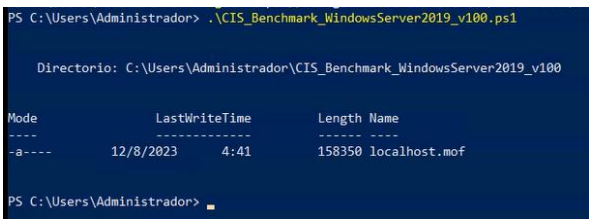


Figura 3.57 Creación del archivo MOF en el directorio

Finalmente se procedió a ejecutar el archivo en el código base del sistema, en la Figura 3.58 se observa el proceso de aplicación y las respectivas configuraciones que se van solventando.

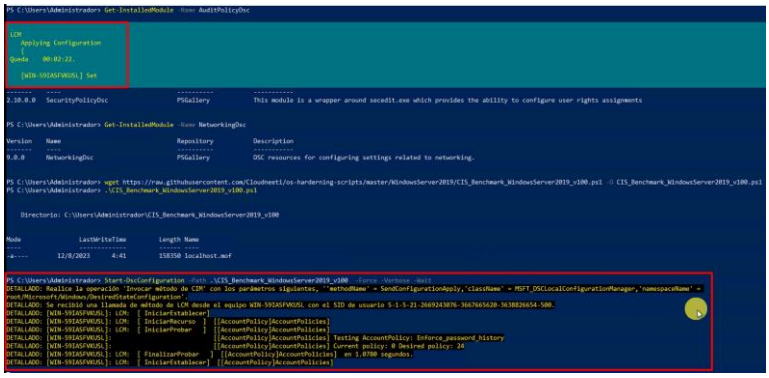


Figura 3.58 Aplicación de las políticas de seguridad en el código base del sistema

En la Figura 3.59 se refleja una configuracion que no se ha completado correctamenta, esto indica que ciertas configuraciones no se han logrado solventar con el *script*, por lo que se requiere configurar de manera manual.

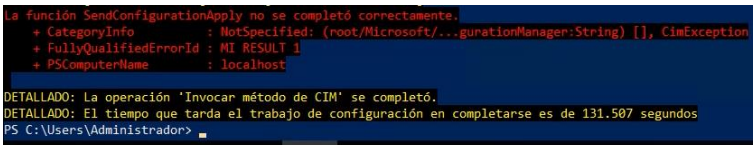


Figura 3.59 Configuraciones que no se han solventado con el *script*

Implementación del servidor DHCP

Antes de realizar este proceso se procedió a crear un nuevo conmutador virtual denominado “Conmutador_Servidor_2”, tal como se observa en la siguiente Figura 3.60.

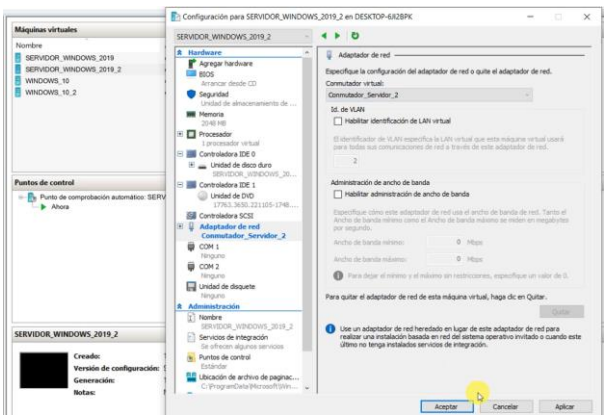


Figura 3.60 Creación de un nuevo conmutador virtual

Al momento de modificar la dirección IP se presenta un mensaje de control de cuentas de usuario tal como se observa en la Figura 3.61. Al principio este mensaje no se presentó, sin embargo, una vez aplicado la política de seguridad presenta un control, ya que esta configuración solo debe realizar un administrador.

Figura 3.61 Control de cuentas de usuario

La dirección IP registrada para este segundo servidor fue la misma que se empleó para el primero, esto con la finalidad de visualizar los posibles cambios que exista al momento de levantar el servidor de correo. De la misma manera se procedió a configurar el servidor DHCP con las mismas especificaciones que el primero, esta configuración se pude visualizar en la sección Configuración del servidor DHCP

Un detalle importante que resaltó al momento de realizar las pruebas de conexión fue cuando se realizó la prueba de *ping* del cliente al servidor ya que, al tener activados los *firewalls* no fue posible realizar la conexión, para lo cual se procedió a configurar una regla de entrada. En la Figura 3.62 se visualiza el proceso de agregación de regla de entrada, en esta se escogió la opción de archivos e impresoras compartidos y permitir conexión.

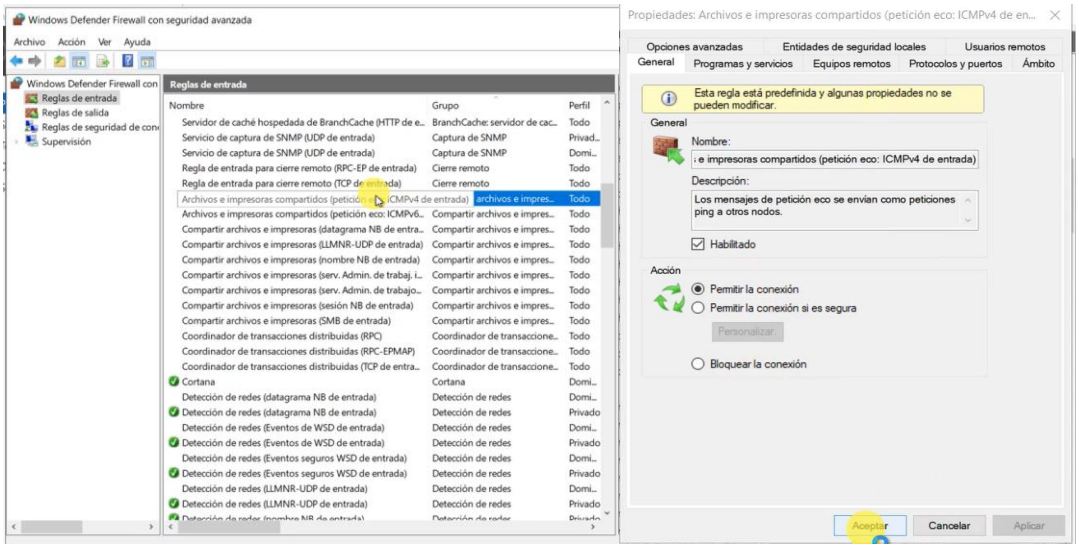


Figura 3.62 Agregación de la regla de entrada

Una vez realizado el cambio se procedió a comprobar la conexión, así como se observa en la Figura 3.63 en la parte izquierda se tiene una prueba de conexión al servidor sin agregar la regla de entrada, mientras en la parte derecha la prueba de conexión exitosa una vez que se agregó la regla de entrada.

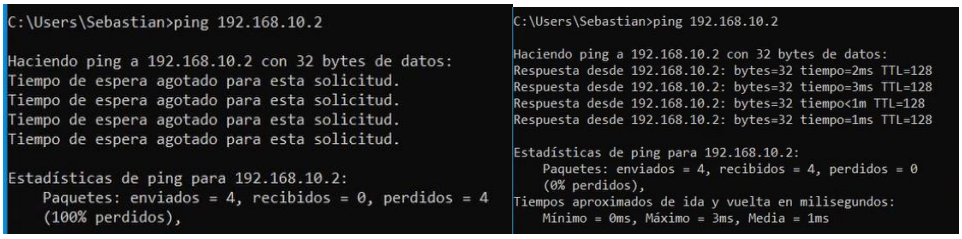


Figura 3.63 Pruebas de conexión al servidor

Implementación del servidor de correo electrónico

Para la implementación de servidor de correo una vez endurecido el sistema, se siguió el mismo proceso que en el capítulo uno, Implementación del servidor de correo**;** el proceso que se siguió para la instalación fue con los mismos pasos, de esta manera se creó las cuentas, tal como se observa en la Figura 3.64. En dicho servidor se registró tres usuarios de los cuales, dos se registraron en el mismo SO de servidor y el otro se registró en el cliente *Windows* 10. Esto se evidencia en la Figura 3.65. Donde los usuarios Juan y Carlos están registrados en el servidor Windows Server.

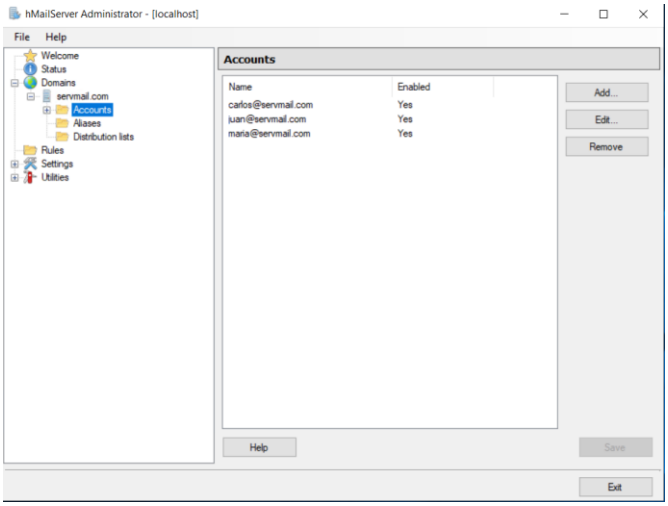


Figura 3.64 Usuarios creados en el servidor *HmailServer*

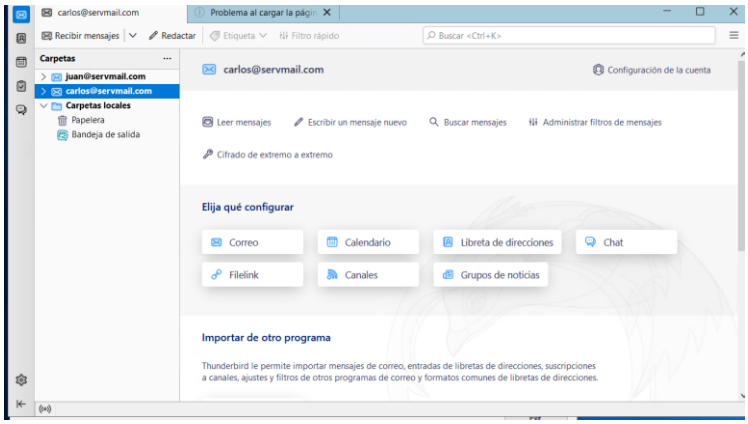


Figura 3.65 Registro de cuentas en la herramienta *Thunderbird*

Para el registro de la cuenta en el cliente *Windows* 10, se tuvo algunos inconvenientes tal como se observa en la Figura 3.66. Se puede observar que la cuenta de usuario no se conecta con el servidor debido a que los *firewalls* no permiten la conexión.

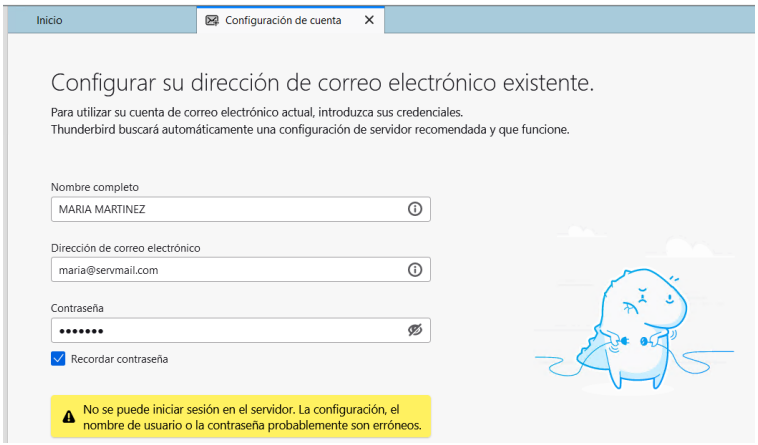


Figura 3.66 Registro erróneo de cuenta

Para solventar este problema se procedió a crear reglas de entrada y salida que permitan tener conexión del cliente al servidor, para ello primero se creó una regla de entrada tal como se observa en la Figura 3.67, en esta figura se observa que el tipo de regla que se escogió fue la de un puerto local específico 143 con protocolo TCP.

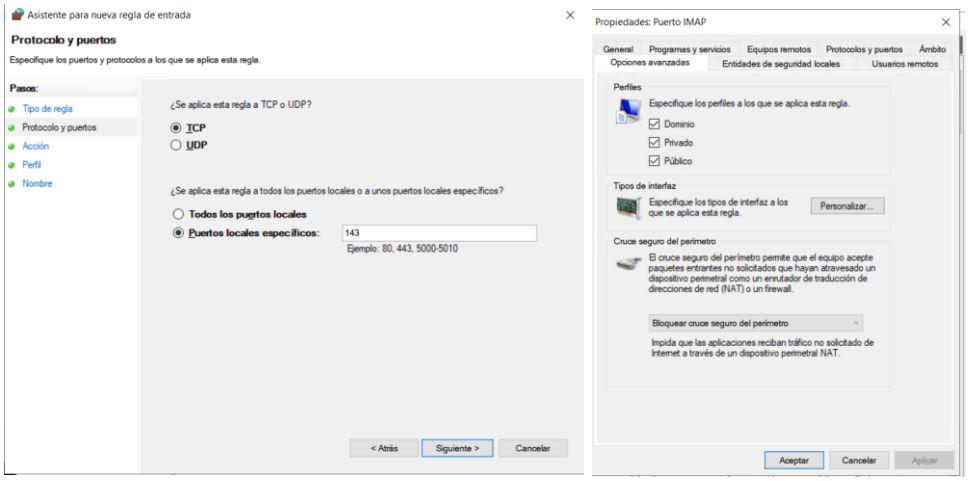


Figura 3.67 Creación de regla de entrada IMAP

Para crear la regla de salida se procedió a la opción Nueva Regla, en la cual se escogió la opción de puerto remoto específico 25 con protocolo TCP. En la Figura 3.68 se visualizan los detalles de la regla saliente creada.

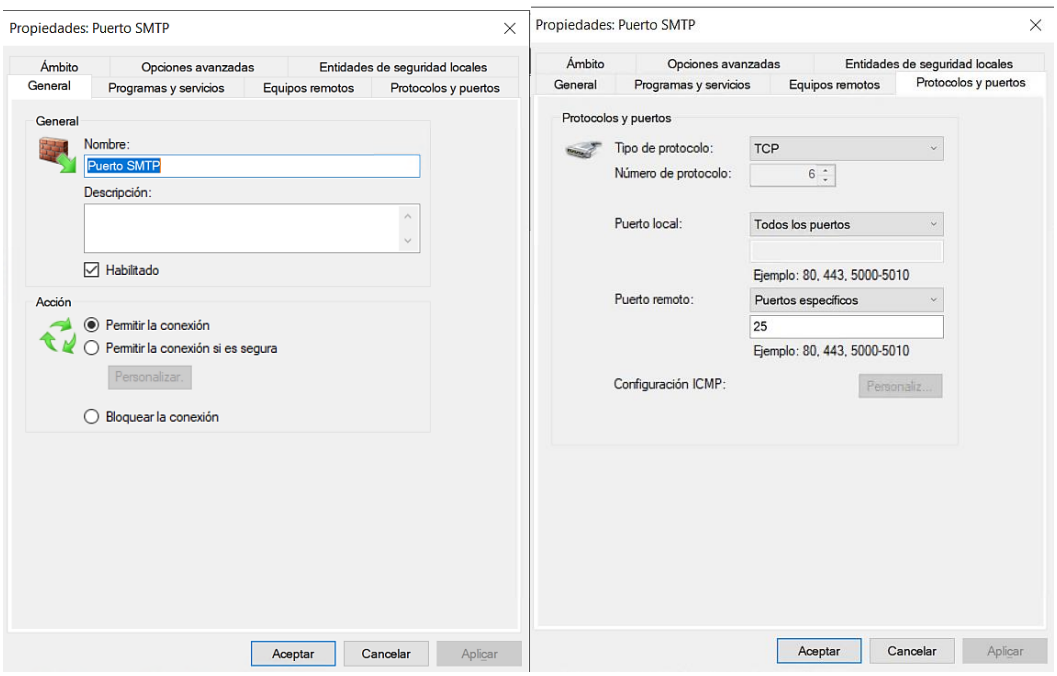


Figura 3.68 Propiedades de la regla de salida SMTP

Una vez que se realizó estos cambios, la cuenta se registró sin problemas, tal como se observa en la Figura 3.69.

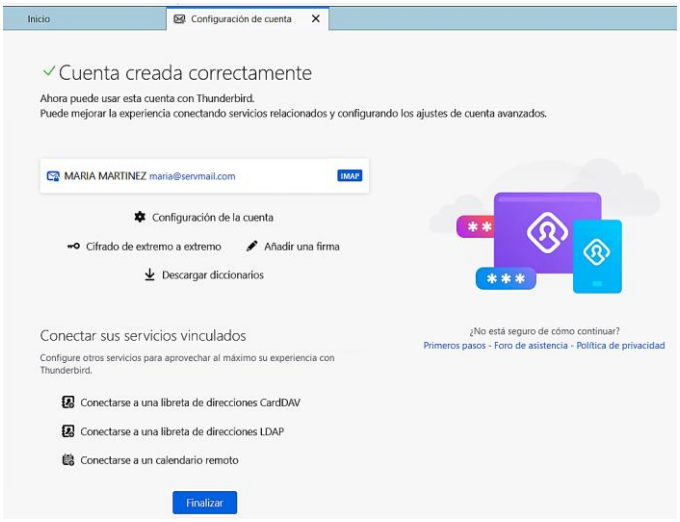


Figura 3.69 Registro de la cuenta creado con éxito del usuario Maria

Prueba de correos electronicos en la herramienta *Thunderbird*

Para comprobar la gestión de correos en las distintas cuentas, se procedió a realizar el envío de correos a las diferentes cuentas, en la Figura 3.70 se visualiza los mensajes enviados desde el usuario JUAN JANETA hacia CARLOS RAMIREZ.

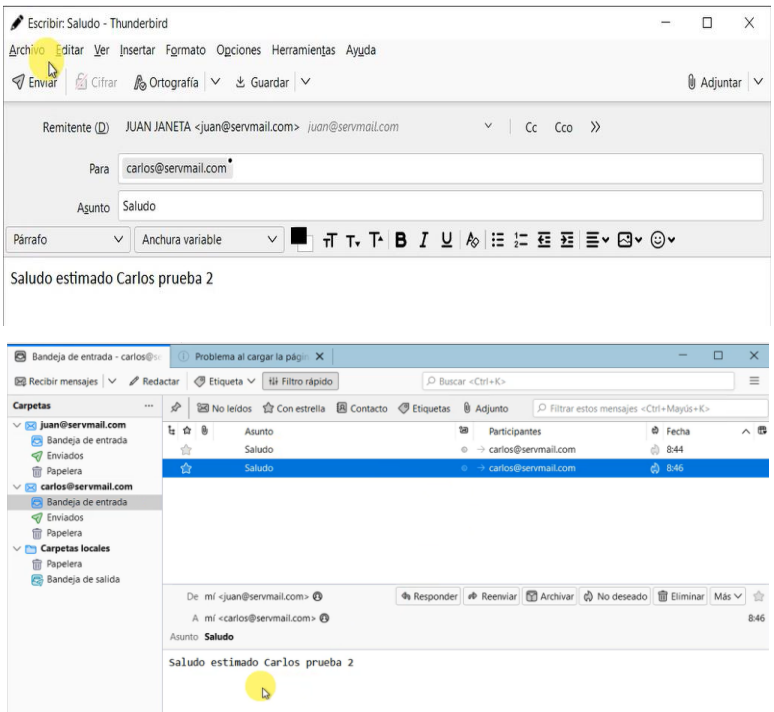


Figura 3.70 Envío y recepción de correo del usuario Juan hacia Carlos

En la Figura 3.71 se visualiza que de la misma manera el envío de un correo desde el usuario CARLOS RAMIREZ hacia JUAN JANETA.

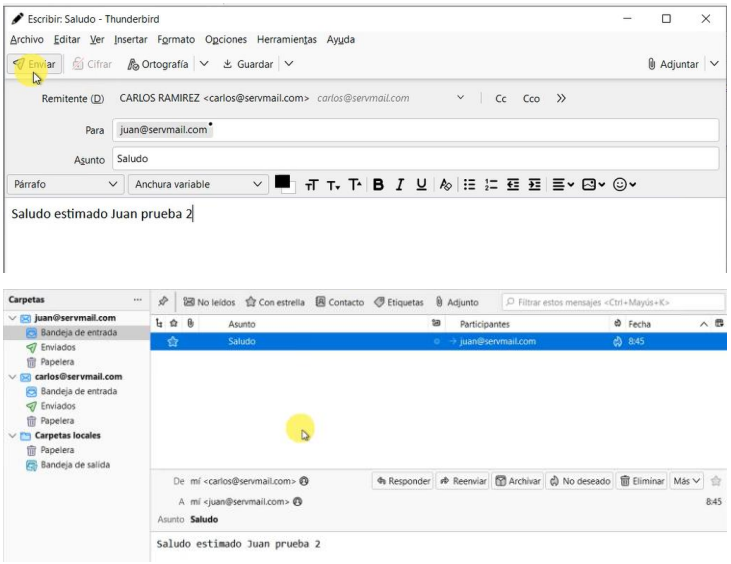


Figura 3.71 Envío y recepción de correo del usuario Carlos hacia Juan

Por último, se realizó la prueba de envío y recepción de correos dede la cuenta de María hacia Carlos, tal como se observa en la Figura 3.72.

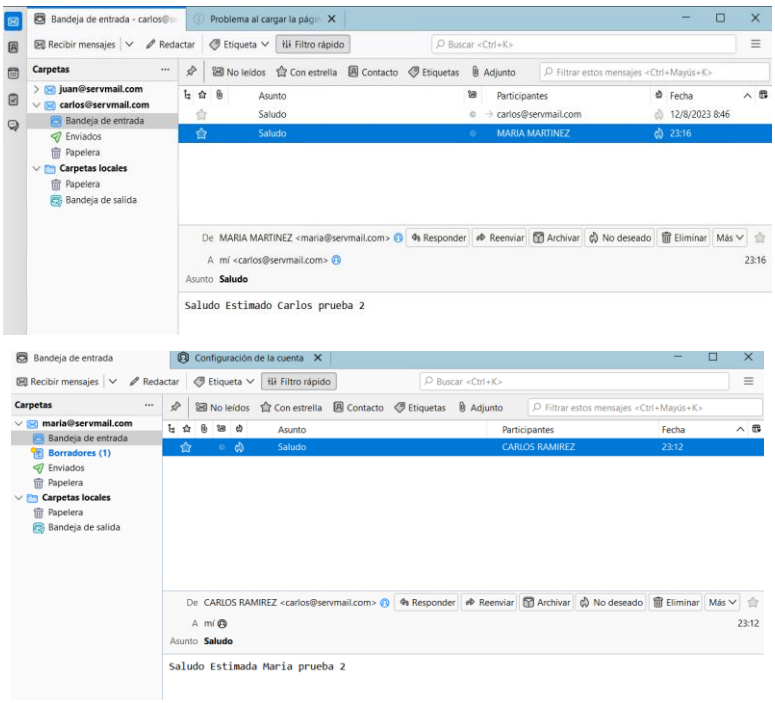


Figura 3.72 Envío y recepción de correo del usuario Maria hacia Carlos

Reporte de vulnerabilidades

Para obtener el reporte de vulnerabilidades se procedió a instalar la herramienta de escaneo, en este proceso no se vio reflejado grandes cambios solo las de notificación al momento de ejecutar el programa. Para el resto de la instalación el proceso fue el mismo que en la seccion de Instalación de la herramienta de escaneo del capitulo I.

El la Figura 3.73 se visualiza el segundo reporte generado por la herramienta, en la imagen se evidencia que el porcentaje de aseguramiento del sistema ha mejorado considerablemente, ya que en el primer reporte se tuvo un valor de 30.42 % y en este segundo reporte refleja un valor 60.45 %. Además, de las 202 configuraciones que se analizaron 107 han logrado pasar las pruebas basadas en el STIG mientras que 70 configuraciones aún tienen problemas de configuración. El valor de aseguramiento del servidor es inferior al 80% por ende el sistema sigue entando en estado rojo.

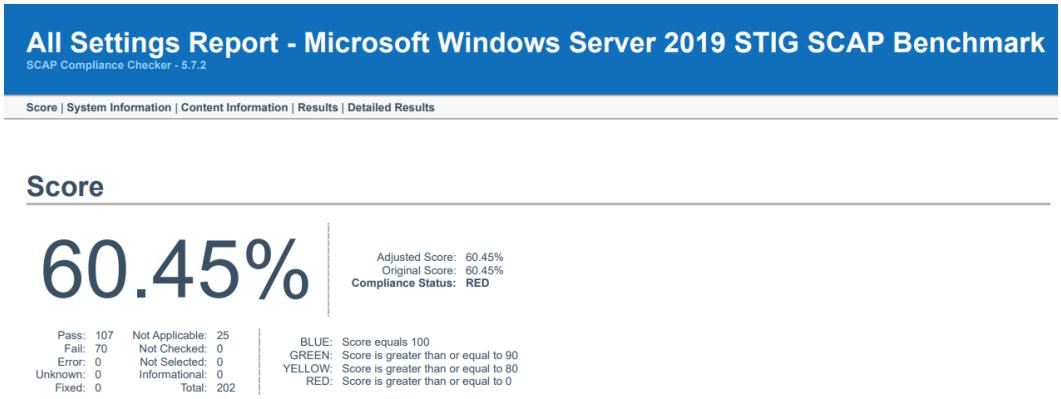
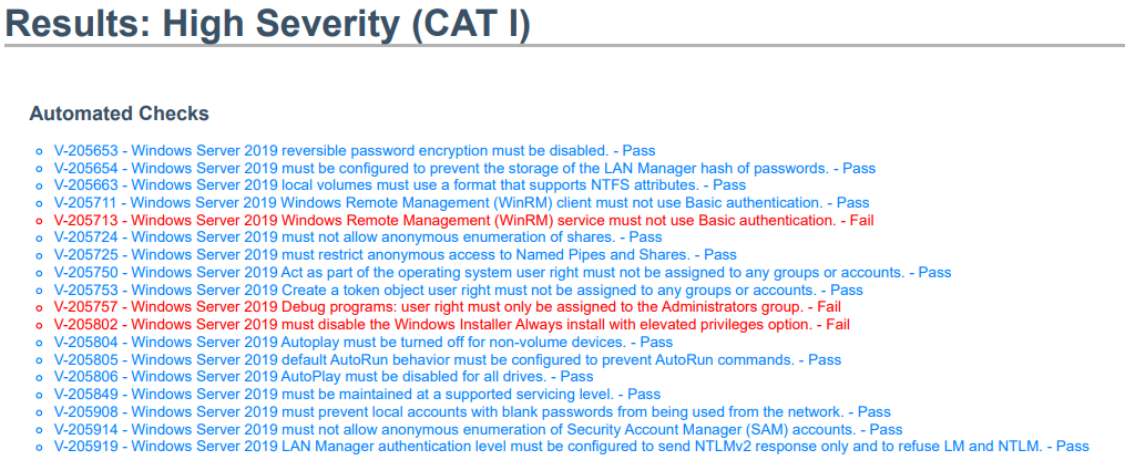


Figura 3.73 Segundo reporte de vulnerabilidades

También se obtuvo de forma detallada las 70 configuraciones con problemas, las cuales se dividen en las tres categorías, en la primera categoría, también conocida como gravedad alta, se tienen tres configuraciones que se ven reflejadas en color rojo, mientras que las demás se ven reflejadas de color azul. Esto se puede evidenciar en la Figura 3.74.



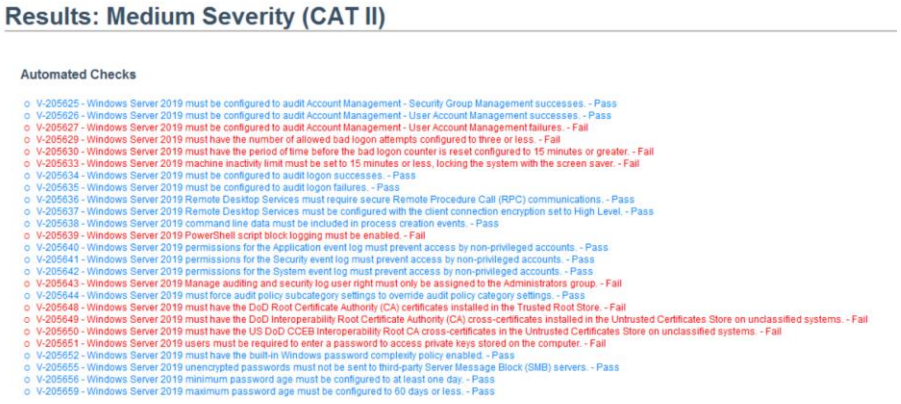
Results: High Severity (CAT I)

Automated Checks

- V-205653 - Windows Server 2019 reversible password encryption must be disabled. - Pass
- V-205654 - Windows Server 2019 must be configured to prevent the storage of the LAN Manager hash of passwords. - Pass
- V-205663 - Windows Server 2019 local volumes must use a format that supports NTFS attributes. - Pass
- V-205711 - Windows Server 2019 Windows Remote Management (WinRM) client must not use Basic authentication. - Pass
- V-205713 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication. - Fail
- V-205724 - Windows Server 2019 must not allow anonymous enumeration of shares. - Pass
- V-205725 - Windows Server 2019 must restrict anonymous access to Named Pipes and Shares. - Pass
- V-205750 - Windows Server 2019 Act as part of the operating system user right must not be assigned to any groups or accounts. - Pass
- V-205753 - Windows Server 2019 Create a token object user right must not be assigned to any groups or accounts. - Pass
- V-205757 - Windows Server 2019 Debug programs: user right must only be assigned to the Administrators group. - Fail
- V-205802 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option. - Fail
- V-205804 - Windows Server 2019 Autoplay must be turned off for non-volume devices. - Pass
- V-205805 - Windows Server 2019 default AutoRun behavior must be configured to prevent AutoRun commands. - Pass
- V-205806 - Windows Server 2019 AutoPlay must be disabled for all drives. - Pass
- V-205849 - Windows Server 2019 must be maintained at a supported servicing level. - Pass
- V-205908 - Windows Server 2019 must prevent local accounts with blank passwords from being used from the network. - Pass
- V-205914 - Windows Server 2019 must not allow anonymous enumeration of Security Account Manager (SAM) accounts. - Pass
- V-205919 - Windows Server 2019 LAN Manager authentication level must be configured to send NTLMv2 response only and to refuse LM and NTLM. - Pass

Figura 3.74 Segundo reporte de configuraciones de categoria I

De la misma manera se presenta en la siguiente Figura 3.75 el reporte detallado de las configuraciones de categoria II, también conocido como de gravedad media, en esta se encuntran 60 configuraciones representadas en color rojo y 94 en color azul. La mayoría de estas configuraciones logran pasar con lo establecido en por la STIG, mientras que las demás deben ser solventados para asegurar aun más el sistema.



Results: Medium Severity (CAT II)

Automated Checks

- V-205625 - Windows Server 2019 must be configured to audit Account Management - Security Group Management successes. - Pass
- V-205626 - Windows Server 2019 must be configured to audit Account Management - User Account Management successes. - Pass
- V-205627 - Windows Server 2019 must be configured to audit Account Management - User Account Management failures. - Fail
- V-205629 - Windows Server 2019 must have the number of allowed bad logon attempts configured to three or less. - Fail
- V-205630 - Windows Server 2019 must have the period of time before the bad logon counter is reset configured to 15 minutes or greater. - Fail
- V-205633 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver. - Fail
- V-205634 - Windows Server 2019 must be configured to audit logon successes. - Pass
- V-205635 - Windows Server 2019 must be configured to audit logon failures. - Pass
- V-205636 - Windows Server 2019 Remote Desktop Services must require secure Remote Procedure Call (RPC) communications. - Pass
- V-205637 - Windows Server 2019 Remote Desktop Services must be configured with the client connection encryption set to High Level. - Pass
- V-205638 - Windows Server 2019 command line data must be included in process creation events. - Pass
- V-205639 - Windows Server 2019 PowerShell script block logging must be enabled. - Fail
- V-205640 - Windows Server 2019 permissions for the Application event log must prevent access by non-privileged accounts. - Pass
- V-205641 - Windows Server 2019 permissions for the Security event log must prevent access by non-privileged accounts. - Pass
- V-205642 - Windows Server 2019 permissions for the System event log must prevent access by non-privileged accounts. - Pass
- V-205643 - Windows Server 2019 Manage auditing and security log user right must only be assigned to the Administrators group. - Fail
- V-205644 - Windows Server 2019 must force audit policy subcategory settings to override audit policy category settings. - Pass
- V-205648 - Windows Server 2019 must have the DoD Root Certificate Authority (CA) certificates installed in the Trusted Root Store. - Fail
- V-205649 - Windows Server 2019 must have the DoD Interoperability Root Certificate Authority (CA) cross-certificates installed in the Untrusted Certificates Store on unclassified systems. - Fail
- V-205650 - Windows Server 2019 must have the US DoD CCEB Interoperability Root CA cross-certificates in the Untrusted Certificates Store on unclassified systems. - Fail
- V-205651 - Windows Server 2019 users must be required to enter a password to access private keys stored on the computer. - Fail
- V-205652 - Windows Server 2019 must have the built-in Windows password complexity policy enabled. - Pass
- V-205655 - Windows Server 2019 unencrypted passwords must not be sent to third-party Server Message Block (SMB) servers. - Pass
- V-205656 - Windows Server 2019 minimum password age must be configured to at least one day. - Pass
- V-205659 - Windows Server 2019 maximum password age must be configured to 60 days or less. - Pass

Figura 3.75 Segundo reporte de configuraciones de categoría II

Por último se presenta las configuraciones de categoría 3, también consideras como de gravedad baja, en estas se encuentran un total de 8 configuraciones de ellas la mayor parte son configuraciones representadas por color rojo, sin embargo estas configuraciones al ser de nivel 3 no afectan el SO de servidor. Esto queda a consideración del administrador si desea solventar dichas configuraciones. Estos resultados se evidencia en la Figura 3.76.

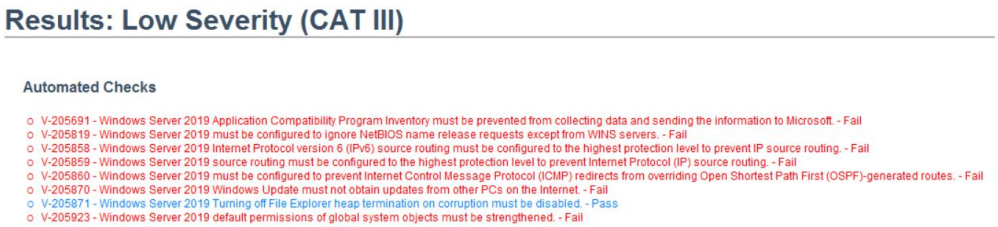


Figura 3.76 Segundor reporte de configuraciones de categoría III

3.3 Análisis de los reportes de vulnerabilidades

Análisis de los dos reportes obtenidos

En la Figura 3.77, se visualizan los dos reportes obtenidos, en la parte izquierda, la imagen corresponde al primer reporte en la cual se evidencia un valor de 38.42 %, este valor corresponde al porcentaje del servidor sin política de seguridad aplicada, también se tiene que el estado del SO de servidor es grave. Por otro lado, en la parte derecha se visualiza el segundo reporte, el valor de aseguramiento del servidor se ha elevado a un porcentaje de 60.45 %, este resultado se obtuvo después de aplicar las políticas de seguridad. Sin embargo, el estado sigue en estado grave por lo cual se debe realizar cambios manuales para aumentar este porcentaje.

También se puede visualizar que el total de configuraciones que se han analizado en los dos reportes son de 202; en el primero, 68 configuraciones cumplen con lo establecido por el STIG, mientras que la diferencia tiene problemas de configuraciones. En el segundo reporte el valor de configuraciones ha aumentado a 107, mientras que la diferencia corresponde a configuraciones con posibles problemas de seguridad.

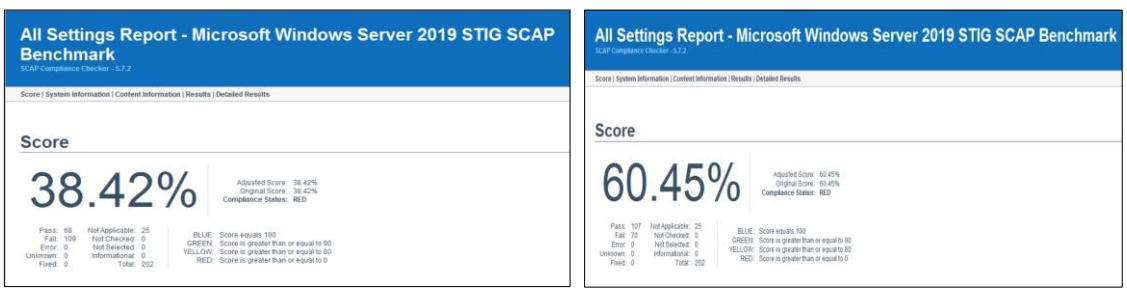


Figura 3.77 Reporte de aseguramiento de *Windows Server* 2019

También se pueden analizar las diferentes categorías que presenta la herramienta de escaneo, empezando por la categoria I tal como se observa en la Figura 3.78. En el primer reporte se visualiza 18 configuraciones de los cuales la mitad pasa la pruebas, mientras que la otra mitad tiene problemas de configuración de seguridad. En la otra imagen también se visualiza la categoria I pero esta corresponde al segundo reporte donde se aplicaron las políticas de seguridad, evidentemente se confirma que se han obtenido mejoras considerables, de estos resultados solo tres configuraciones son considerados de gravedad, las cuales posteriormente serán solventadas.

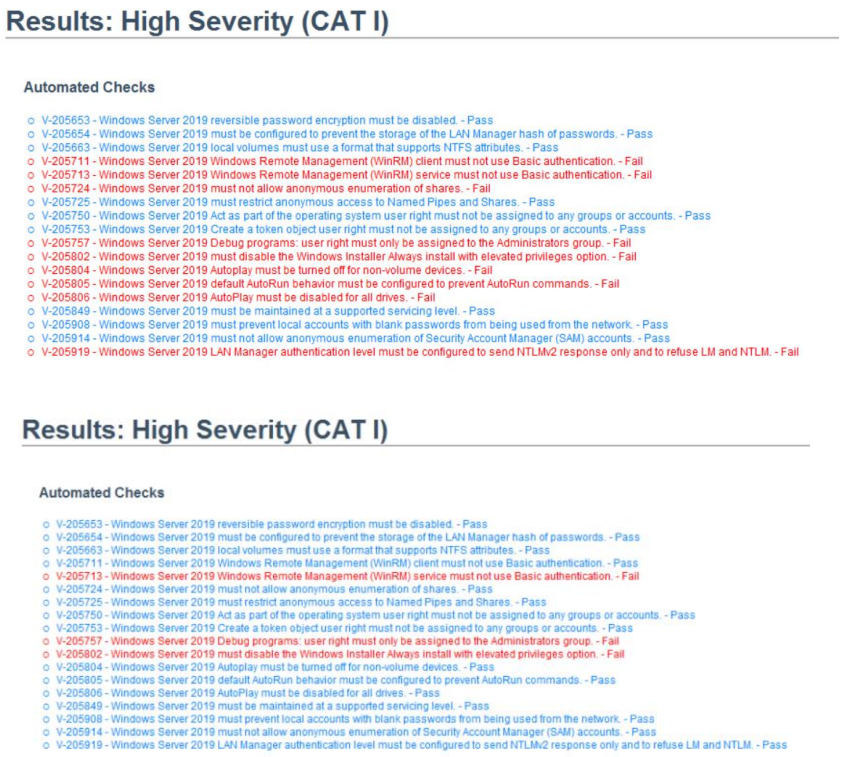


Figura 3.78 Análisis de reportes de categoria I

Así también se obtuvo los resultados de categoria II, la cual se analiza en base a la Figura 3.79. En el primer reporte realizado, lado izquierdo, se visualiza que existe la mayor cantidad de configuraciones con problemas, específicamente 96 configuraciones con problemas de seguriad. Por otro, parte derecha de la figura, se observa que la mayoría de los problemas se han solventado con la aplicación de las políticas de seguridad, específicamente 94 configuraciones sin problemas y 60 configuraciones con problemas.

Figura 3.79 Análisis de reportes de categoria II

Finalmente, en la Figura 3.80 se tiene los reportes de la categoría III, no se visualizan cambios considerables ya que en el primer reporte ubicado en la parte superior se han encontrado 8 configuraciones de ellas solo una logra cumplir con las reglas del STIG. El segundo reporte, ubicado en la parte inferior, evidencia que son dos las reglas que cumplen, dando como resultado que la mayor parte de configuraciones tienen problemas, sin embargo, estas configuraciones al pertenecer a la categoría III el SO de servidor no se ve afectado ya que son mínimos los problemas de seguridad.

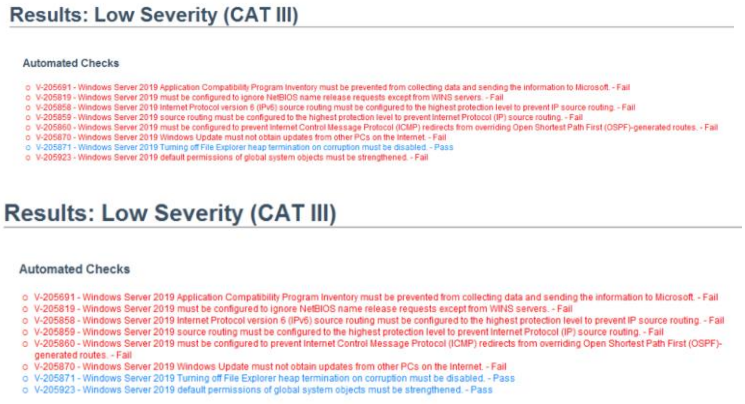


Figura 3.80 Análisis de reportes de categoria III

Reporte de problemas que se han solventado en las tres categorías

En la Tabla 3.3 se detalla los problemas que se solventó con la aplicación de las políticas de seguridad, además se detalla cada uno de los problemas y qué efecto tienen en el servidor.

Tabla 3.3 Detalle de problemas de categoría I solventados

Categoría I	
Configuraciones solventadas mediante el script	**Detalle del problema**
Administración remota de Windows (WinRM)	La autenticación básica emplea contraseñas en formato de texto sin cifrar, lo que podría resultar en la vulnerabilidad del sistema.
Windows Server 2019 debe abstenerse de permitir la enumeración anónima de recursos compartidos.	Posibilitar que los usuarios sin identificación puedan listar todos los nombres de cuentas y visualizar todos los recursos compartidos podría generar un esquema de ubicaciones susceptibles para dirigir posibles ataques al sistema.
La reproducción automática debe estar desactivada para dispositivos sin volumen.	Las cuentas de usuario comunes no deben contar con privilegios elevados. Permitir que *Windows Installer* incremente los privilegios durante la instalación de programas podría abrir la puerta para que individuos y programas maliciosos logren tomar el control total de un sistema.
El comportamiento predeterminado de ejecución automática debe configurarse para evitar los comandos de ejecución automática.	Posibilitar la ejecución de comandos *AutoRun* puede abrir la puerta a la inserción de código perjudicial en un sistema. Ajustar esta configuración impide la ejecución de los mencionados comandos *AutoRun.*

La reproducción automática debe estar deshabilitada para todas las unidades.	Posibilitar la ejecución de *AutoPlay* puede dar paso a la inserción de códigos dañinos en un sistema. Activar esta directriz implica desactivar la reproducción automática en todas las unidades.
Es necesario ajustar la configuración del nivel de autenticación de LAN *Manager* con el propósito de permitir únicamente la emisión de una respuesta NTLMv2, y proceder a denegar tanto LM como NTLM.	El protocolo de autenticación Kerberos versión 5 es el método estándar para verificar la identidad de los usuarios que acceden a cuentas de dominio. Aunque NTLM, que es menos seguro, se mantiene en las versiones más recientes de *Windows*, esto se hace por razones de compatibilidad con sistemas anteriores y aplicaciones que dependen de él, a pesar de sus limitaciones de seguridad.

De la misma manera se detalla en la Tabla 3.4 los problemas solventados de la categoría II.

Tabla 3.4 Detalle de problemas de categoría II solventados

Categoría II	
Configuraciones solventadas en Windows server 2019	**Detalle del problema**
Los servicios de escritorio remoto deben requerir comunicaciones seguras de llamada a procedimiento remoto (RPC).	Habilitar la comunicación insegura de procedimiento remoto (RPC) pone en riesgo el sistema frente a posibles ataques de intermediarios y divulgación de datos.
Los servicios de escritorio remoto deben configurarse con el cifrado de conexión del cliente establecido en nivel alto.	Es esencial encriptar las conexiones remotas para prevenir el acceso no autorizado a datos sensibles o información confidencial. Optar por la opción "Alto nivel"

	asegurará que las sesiones estén cifradas en ambas direcciones.
Es necesario incorporar los datos provenientes de la línea de comandos dentro de los registros de eventos relacionados con la generación de procesos.	Activar la opción de "Registrar información de la línea de comandos en eventos de inicio de procesos" permitirá almacenar los detalles de la línea de comandos junto con los eventos de inicio de procesos en el registro.
Windows Server 2019 debe forzar la configuración de la subcategoría de la política de auditoría para anular la configuración de la categoría de la política de auditoría.	La recolección de esta información resulta fundamental para examinar la protección de los recursos de datos e identificar indicios de conducta dudosa e imprevista.
La antigüedad mínima de la contraseña debe configurarse en al menos un día.	Habilitar la posibilidad de modificar contraseñas en rápida sucesión durante un mismo día posibilita a los usuarios alterar las contraseñas utilizando su registro de contraseñas previas.
El historial de contraseñas debe configurarse para recordar 24 contraseñas	Esto posibilita a los usuarios desactivar de manera efectiva la necesidad de solicitar modificaciones regulares de contraseña. Por defecto, se establece en "24" para los sistemas dentro del dominio de Windows.
Es necesario establecer una longitud mínima de 14 caracteres para la contraseña.	Los sistemas de información desprotegidos por contraseñas débiles abren la posibilidad de que cualquier individuo pueda descifrar la contraseña, lo que le daría acceso al sistema y pondría en riesgo el dispositivo, los datos y la red interna.
Debe evitar la visualización de presentaciones de diapositivas en la pantalla de bloqueo.	Deshabilitar esta característica restringirá el acceso a la información únicamente para usuarios que han iniciado sesión.

La pantalla de inicio de sesión no debe exhibir la interfaz de usuario (IU) destinada a la selección de red.	Habilitar la participación con la pantalla de selección de redes capacita a los usuarios para modificar las conexiones a redes disponibles sin necesidad de iniciar sesión.
Windows Defender *SmartScreen* debe estar habilitado.	Activar *SmartScreen* tiene la capacidad de impedir la ejecución de programas descargados de Internet que podrían ser peligrosos, o de notificar a los usuarios al respecto.
Debe evitar la indexación de archivos cifrados.	La indexación de documentos encriptados puede revelar información confidencial. Esta configuración impide la indexación de los documentos que están protegidos mediante cifrado.
El empleo de la autenticación Digest no debe ser realizado en el cliente de administración remota de Windows (WinRM).	La seguridad de la autenticación Digest no es tan robusta como otras alternativas y podría ser vulnerable a ataques de intermediarios. Optar por no habilitar la autenticación Digest disminuirá esta posibilidad.
Las cuentas de administrador no deben enumerarse durante la elevación.	Esta disposición establece el sistema de manera que siempre demande a los usuarios ingresar tanto un nombre de usuario como una contraseña para elevar una aplicación en curso.
El Control de cuentas de usuario debe, como mínimo, solicitar el consentimiento de los administradores en el escritorio seguro.	Este ajuste establece las condiciones necesarias para que los administradores que han accedido al sistema finalicen una acción que demanda mayores niveles de autorización.
Es necesario establecer la configuración del registro de eventos de la aplicación en un	Esto podría impedir el registro adecuado de eventos de auditoría, lo que resultaría en la

valor igual o superior a 32768 (KB).	necesidad constante de atención por parte del equipo administrativo.
Es necesario establecer la dimensión del registro de sucesos de seguridad en 196608 (KB) o superior.	Esto puede evitar que los eventos de auditoría se registren correctamente y requieran atención frecuente por parte del personal administrativo.
Es fundamental prevenir la modificación de las opciones de instalación por parte de los usuarios.	Esta disposición impide que los usuarios modifiquen las preferencias de instalación, lo cual podría resultar en el descuido de las medidas de seguridad.
No debe guardar contraseñas en Remote Desktop Client.	Almacenar contraseñas en el Cliente de Escritorio Remoto podría posibilitar que un individuo sin autorización inicie una sesión de escritorio remoto en un sistema ajeno.
Los servicios de escritorio remoto deben invariablemente requerir al cliente las contraseñas al momento de establecer la conexión.	Desactivar esta configuración posibilitaría que cualquier individuo utilice las credenciales guardadas en un objeto de enlace para establecer conexión con el servidor de terminales.
El almacenamiento de credenciales RunAs no debe ser llevado a cabo por el Servicio de Administración Remota de Windows (WinRM).	Si se impide guardar las credenciales de RunAs para la gestión remota de *Windows*, se impedirá su uso con extensiones.
El modo de aprobación del Control de cuentas de usuario para el administrador integrado debe estar habilitado	Esta disposición establece la cuenta de administrador incorporada para operar en un modo que requiere la aprobación del administrador.
El sistema de Control de Cuentas de Usuario tiene la responsabilidad de rechazar de manera automática las peticiones de elevación	Este ajuste regula cómo se maneja la elevación cuando es requerida por una cuenta de usuario normal.

realizadas por usuarios de nivel estándar.	
El uso de tráfico no encriptado no debe ser permitido en el Cliente de Administración Remota de Windows (WinRM).	El acceso no encriptado desde una ubicación remota a un sistema puede poner en riesgo la confidencialidad de la información sensible. Por lo tanto, es necesario aplicar encriptación para prevenir esta situación.
La configuración del cliente de red de Microsoft debe establecer que las comunicaciones con firma digital estén permanentemente habilitadas.	La implementación de firmas digitales en los paquetes SMB contribuye a evitar posibles ataques de intermediarios. Cuando esta configuración está activada, el cliente SMB solamente establecerá comunicación con un servidor SMB que aplique firmas a los paquetes SMB.
La configuración del Servidor de Red de Microsoft requiere que las comunicaciones con firma digital se configuren como "Habilitadas" en caso de consentimiento por parte del cliente.	La implementación de firmas digitales en los paquetes SMB contribuye a evitar posibles ataques de intermediarios. Cuando esta configuración está activada, el cliente SMB solamente establecerá comunicación con un servidor SMB que aplique firmas a los paquetes SMB.
Los inicios de sesión no seguros en un servidor SMB deben estar deshabilitados.	La implementación de firmas digitales en los paquetes SMB contribuye a evitar posibles ataques de intermediarios. Cuando esta configuración está activada, el cliente SMB solamente establecerá comunicación con un servidor SMB que aplique firmas a los paquetes SMB.
La telemetría debe configurarse en Seguridad o Básico.	Restringir esta habilidad impedirá la transmisión de datos posiblemente sensibles fuera de la compañía. La alternativa denominada "Seguridad" en

	cuanto a Telemetría establece el nivel mínimo de información compartida, mientras que la configuración de telemetría para el cliente en modo "Básico" envía datos fundamentales de diagnóstico.
Debe evitar que se descarguen archivos adjuntos de fuentes RSS.	Los archivos que se agregan en los feeds RSS podrían no ser seguros. Este ajuste impedirá la descarga de archivos adjuntos desde fuentes RSS.
Los servicios que emplean el sistema local para llevar a cabo la negociación durante el proceso de autenticación NTLM, deben utilizar la identidad de la máquina en vez de autenticarse de manera anónima.	Los servicios que emplean la función del Sistema local que involucra la autenticación NTLM al reiniciar pueden experimentar accesos no autorizados si se les concede la posibilidad de autenticarse de manera anónima en vez de emplear la identidad de la máquina.
Debe evitar que NTLM vuelva a una sesión nula.	Las sesiones NTLM que tienen la capacidad de utilizar sesiones sin autenticación pueden obtener acceso de manera no autorizada.
Debe evitar la autenticación PKU2U mediante identidades en línea.	PKU2U es un sistema de autenticación punto a punto que impide que las identidades en línea se autentiquen en sistemas que están conectados a un dominio.
Es necesario establecer la configuración de seguridad de la sesión para los clientes que utilizan NTLM SSP de manera que se exija la implementación de seguridad de sesión NTLMv2 y un nivel de cifrado de 128 bits.	Microsoft ha integrado diversos proveedores de apoyo de seguridad destinados a utilizarse con sesiones de llamada a procedimiento remoto (RPC). Es esencial activar todas las alternativas para asegurar el más alto grado de protección.

Es necesario establecer la configuración de seguridad de la sesión en servidores que utilizan NTLM SSP de manera que se exija la implementación de seguridad de sesión NTLMv2, así como el empleo de cifrado de 128 (bits).	Microsoft ha integrado diversos proveedores de apoyo de seguridad destinados a utilizarse con sesiones de llamada a procedimiento remoto (RPC). Es esencial activar todas las alternativas para asegurar el más alto grado de protección.

En la Tabla 3.5 se presenta los problemas solventados de la categoría III.

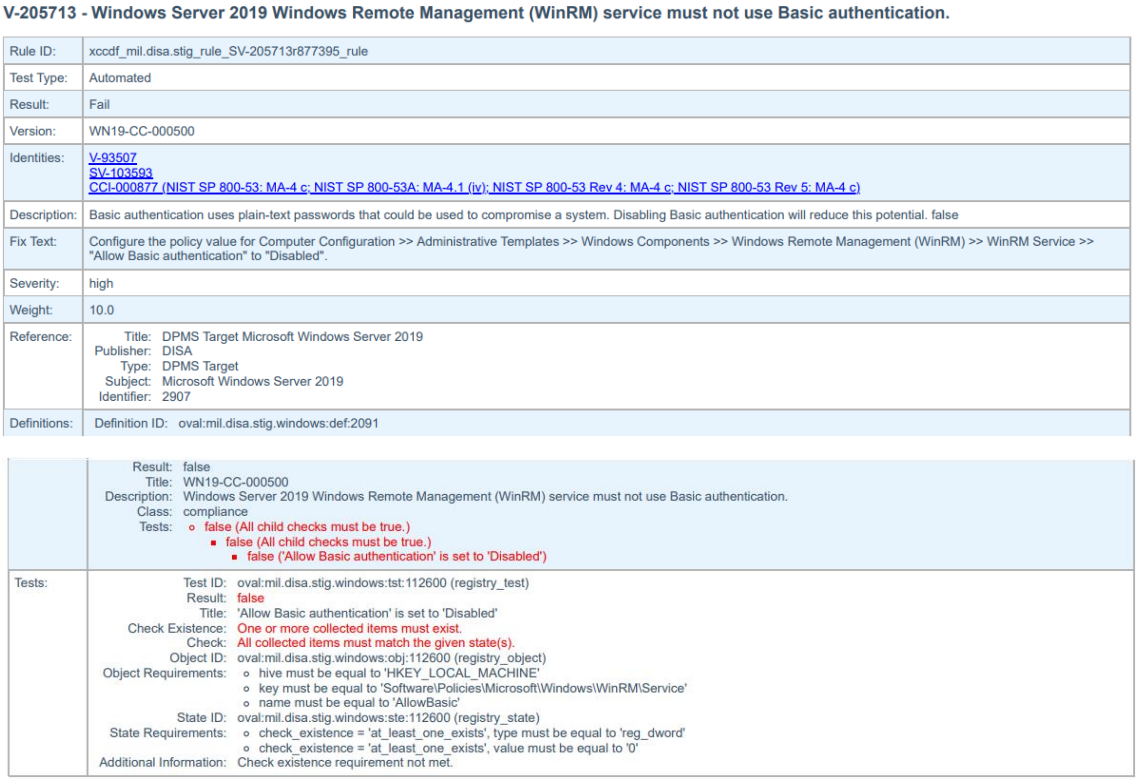
Tabla 3.5 Detalle de problemas de categoría III solventados

Categoría III	
Configuraciones solventadas en Windows server 2019	**Detalle del problema**
Es necesario fortalecer los permisos por defecto de los elementos en el contexto del sistema global.	Los sistemas operativos *Windows* cuentan con un registro global de recursos compartidos del sistema. Cada tipo de recurso se origina con una lista de control de acceso discrecional (DACL) predefinida que establece quiénes tienen la capacidad de acceder a los recursos y con qué permisos. Cuando se activa esta política, la DACL predefinida se vuelve más restrictiva, lo que posibilita que usuarios no administrativos puedan visualizar los recursos compartidos, pero no realizar cambios en aquellos que no hayan creado.

Aplicación de recomendaciones de forma manual

Primer problema de categoría I: Servicio de administración remota de Windows (WinRM)

Para solventar los problemas de seguridad presentes en la categoría I se procedió a ingresar a los detalles de dicho problema, para lo cual al dar clic sobre la configuración representadas en color rojo se desplegó los detalles, tal como se observa en la Figura 3.81 también se puede observar que se presenta una breve descripción, así como también el proceso que se debe seguir para solventar el inconveniente.



V-205713 - Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication.

Rule ID:	xccdf_mil.disa.stig_rule_SV-205713r877395_rule
Test Type:	Automated
Result:	Fail
Version:	WN19-CC-000500
Identities:	V-93507 SV-103593 CCI-000877 (NIST SP 800-53: MA-4 c; NIST SP 800-53A: MA-4.1 (iv); NIST SP 800-53 Rev 4: MA-4 c; NIST SP 800-53 Rev 5: MA-4 c)
Description:	Basic authentication uses plain-text passwords that could be used to compromise a system. Disabling Basic authentication will reduce this potential. false
Fix Text:	Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> "Allow Basic authentication" to "Disabled".
Severity:	high
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2019 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2019 Identifier: 2907
Definitions:	Definition ID: oval:mil.disa.stig.windows:def:2091

	Result: false Title: WN19-CC-000500 Description: Windows Server 2019 Windows Remote Management (WinRM) service must not use Basic authentication. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Allow Basic authentication' is set to 'Disabled')
Tests:	Test ID: oval:mil.disa.stig.windows:tst:112600 (registry_test) Result: false Title: 'Allow Basic authentication' is set to 'Disabled' Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.stig.windows:obj:112600 (registry_object) Object Requirements: ○ hive must be equal to 'HKEY_LOCAL_MACHINE' ○ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Service' ○ name must be equal to 'AllowBasic' State ID: oval:mil.disa.stig.windows:ste:112600 (registry_state) State Requirements: ○ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword' ○ check_existence = 'at_least_one_exists', value must be equal to '0' Additional Information: Check existence requirement not met.

Figura 3.81 Detalles de la configuración de servicio de administración remota de Windows (WinRM)

Para la solución del problema se procedió a ingresar al editor de directivas de grupo local, ejecutando el comando gpedit.msc. Dentro de esta ventana, se optó por elegir la alternativa correspondiente a la configuración del equipo. Una vez en esta sección, se procedió a seleccionar las plantillas administrativas, seguido por los componentes de *Windows*. En la Figura 3.82 se evidencia este proceso

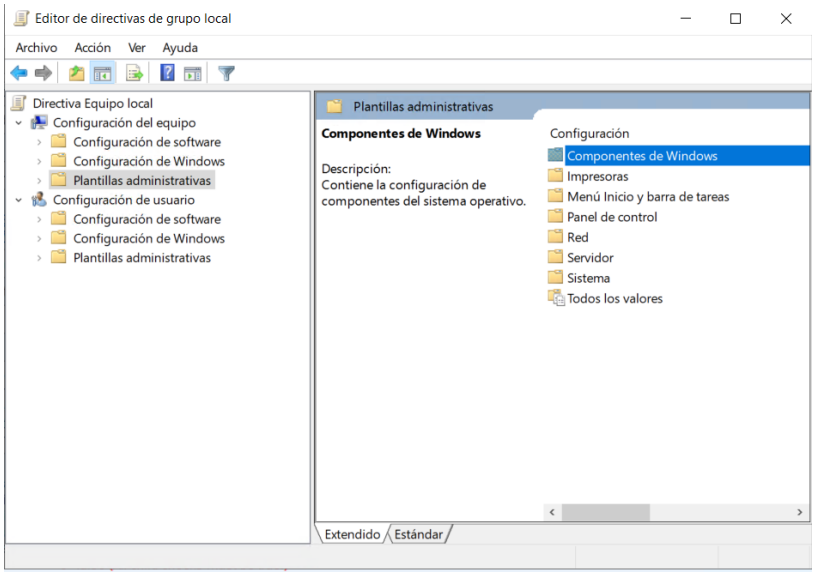


Figura 3.82 Ventana de plantillas administrativas en configuración del equipo

Dentro de esta categoría, se escogió específicamente la opción relacionada con la administración remota de *Windows* (WinRM) - Cliente WinRM. En el marco de esta configuración, se llevó a cabo la acción de permitir la autenticación básica, estableciéndola en el estado "Deshabilitado". Esta configuración se evidencia en la Figura 3.83.

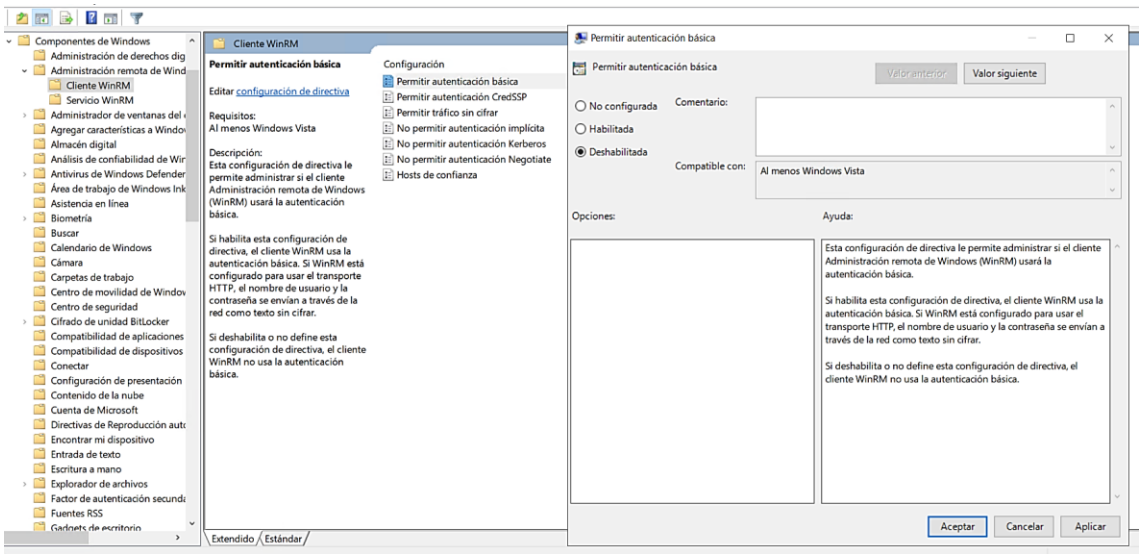
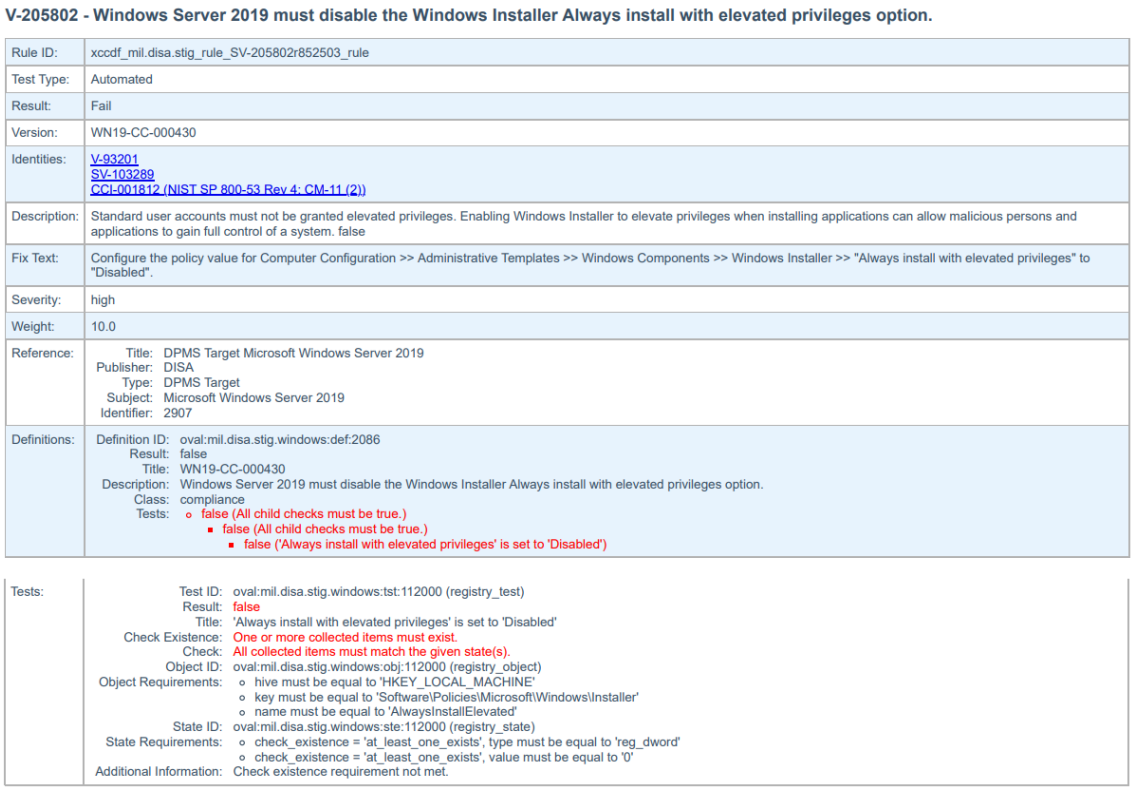


Figura 3.83 Configuración manual de la configuración de servicio de administración remota de Windows (WinRM)

Segundo problema de categoría I: “Windows Installer” Instalar siempre con privilegios elevados

De la misma manera se procedió a solventar el segundo problema de la categoría I, en la Figura 3.84 se visualizan los detalles el problema, que efectos tiene en el sistema y cómo se solventa el problema.



V-205802 - Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option.

Rule ID:	xccdf_mil.disa.stig_rule_SV-205802r852503_rule
Test Type:	Automated
Result:	Fail
Version:	WN19-CC-000430
Identities:	V-93201 SV-103289 CCI-001812 (NIST SP 800-53 Rev 4: CM-11 (2))
Description:	Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system. false
Fix Text:	Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Always install with elevated privileges" to "Disabled".
Severity:	high
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2019 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2019 Identifier: 2907
Definitions:	Definition ID: oval:mil.disa.stig.windows:def:2086 Result: false Title: WN19-CC-000430 Description: Windows Server 2019 must disable the Windows Installer Always install with elevated privileges option. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Always install with elevated privileges' is set to 'Disabled')
Tests:	Test ID: oval:mil.disa.stig.windows:tst:112000 (registry_test) Result: false Title: 'Always install with elevated privileges' is set to 'Disabled' Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.stig.windows:obj:112000 (registry_object) Object Requirements: ○ hive must be equal to 'HKEY_LOCAL_MACHINE' ○ key must be equal to 'Software\Policies\Microsoft\Windows\Installer' ○ name must be equal to 'AlwaysInstallElevated' State ID: oval:mil.disa.stig.windows:ste:112000 (registry_state) State Requirements: ○ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword' ○ check_existence = 'at_least_one_exists', value must be equal to '0' Additional Information: Check existence requirement not met.

Figura 3.84 Detalles del segundo problema de categoría I

Para solventar dicho problema se procedió a dirigirse a la configuración del equipo luego a plantillas administrativas, dentro de esa ventana se escogió componentes de *Windows* en la opción de instalador de *Windows* se buscó la opción "Instalar siempre con privilegios elevados" y se procedió a “deshabilitarlo”. Esta configuración se evidencia en la Figura 3.85.

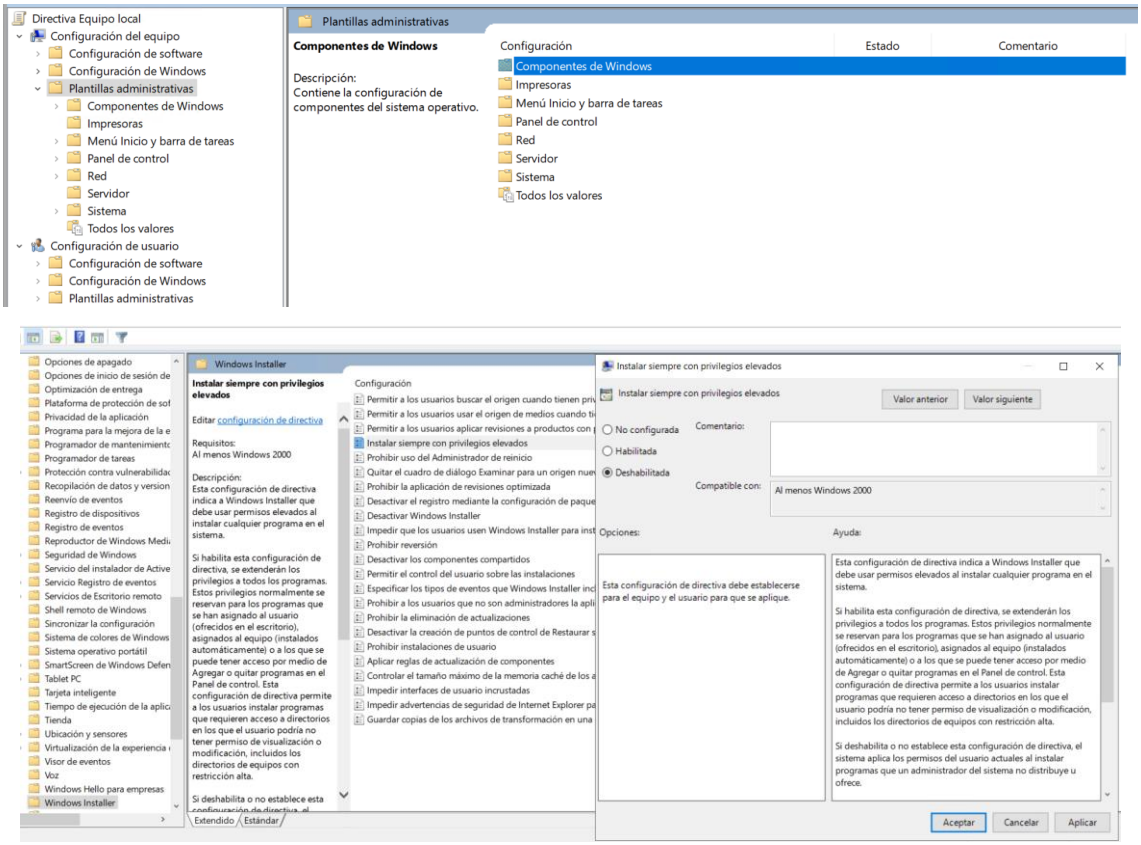


Figura 3.85 Configuración manual del segundo problema de categoría I

Así también se procedió a solventar cuatro configuraciones con problemas de la categoría II, estos problemas se detallan a continuación y su respectivo proceso para solventar el problema.

Primer problema de categoría II: Límite de inactividad de la máquina

Como primer problema se detalla en base a la Figura 3.86, en donde se visualiza los detalles del problema, la regla que se empleó para realizar la comparación, también se observa el impacto que tiene en el sistema al no solventarse el problema.

V-205633 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver.

Rule ID:	xccdf_mil.disa.stig_rule_SV-205633r569188_rule
Test Type:	Automated
Result:	Fail
Version:	WN19-SO-000120
Identities:	V-92961 SV-103049 CCI-000056 (NIST SP 800-53: AC-11 b; NIST SP 800-53A: AC-11.1 (iii); NIST SP 800-53 Rev 4: AC-11 b; NIST SP 800-53 Rev 5: AC-11 b) CCI-000057 (NIST SP 800-53: AC-11 a; NIST SP 800-53A: AC-11.1 (ii); NIST SP 800-53 Rev 4: AC-11 a; NIST SP 800-53 Rev 5: AC-11 a) CCI-000060 (NIST SP 800-53: AC-11 (1); NIST SP 800-53A: AC-11 (1).1; NIST SP 800-53 Rev 4: AC-11 (1); NIST SP 800-53 Rev 5: AC-11 (1))
Description:	Unattended systems are susceptible to unauthorized use and should be locked when unattended. The screen saver should be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012 false
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Machine inactivity limit" to "900" seconds or less, excluding "0" which is effectively disabled.
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2019 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2019 Identifier: 2907
Definitions:	Definition ID: oval:mil.disa.stig.windows2019:def:205633 Result: false Title: WN19-SO-000120 - Windows Server 2019 machine inactivity limit must be set to 15 minutes or less, locking the system with the screen saver. Description: Unattended systems are susceptible to unauthorized use and should be locked when unattended. The screen saver should be set at a maximum of 15 minutes and be password protected. This protects critical and sensitive data from exposure to unauthorized personnel with physical access to the computer. Satisfies: SRG-OS-000028-GPOS-00009, SRG-OS-000029-GPOS-00010, SRG-OS-000031-GPOS-00012 Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false (The machine inactivity limit is set to 15 minutes or less)
Tests:	Test ID: oval:mil.disa.stig.windows:tst:25344400 (registry_test) Result: false Title: The machine inactivity limit is set to 15 minutes or less Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). State Operator: All item-state comparisons must be true. Object ID: oval:mil.disa.stig.windows:obj:25344400 (registry_object) Object Requirements: ○ hive must be equal (case insensitive) to 'HKEY_LOCAL_MACHINE' ○ key must be equal (case insensitive) to 'Software\Microsoft\Windows\CurrentVersion\Policies\System'

Figura 3.86 Detalles del primer problema de categoría II

Para abordar esta cuestión, se llevaron a cabo una serie de pasos, comenzando por la configuración de la computadora. En primer lugar, se accedió a la Configuración de Windows. A continuación, se accedió a la sección de Configuración de seguridad, donde se optó por las Directivas locales. En la nueva ventana, se eligieron las Opciones de seguridad y se procedió a ajustar el parámetro "Inicio de sesión interactivo: límite de inactividad de la máquina" a un valor igual o inferior a "900" segundos. Esto se evidencia en la Figura 3.87.

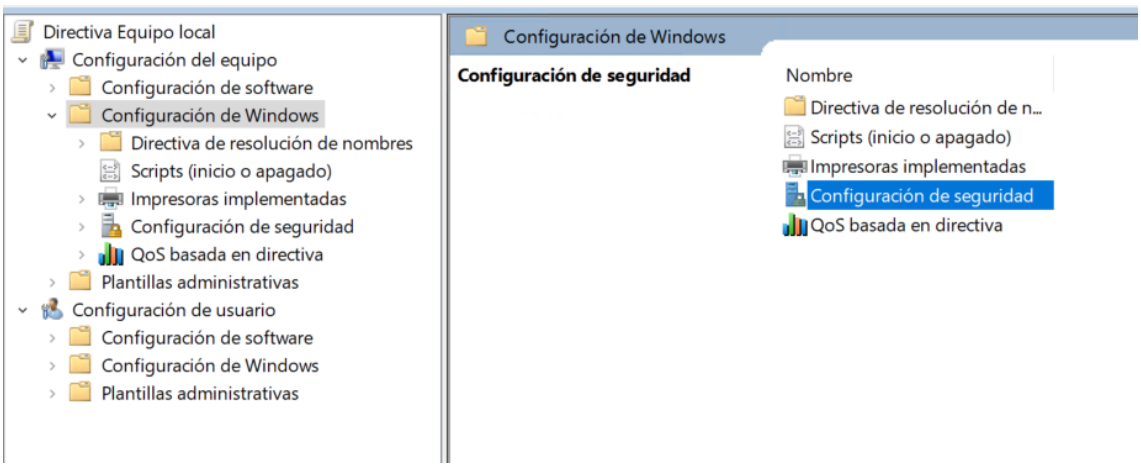


Figura 3.87 Configuración de *Windows* y Configuración de seguridad

En la nueva ventana, se eligieron las Opciones de seguridad y se procedió a ajustar el parámetro "Inicio de sesión interactivo: límite de inactividad de la máquina" a un valor igual o inferior a "900" segundos. Esto se evidencia en la Figura 3.88.

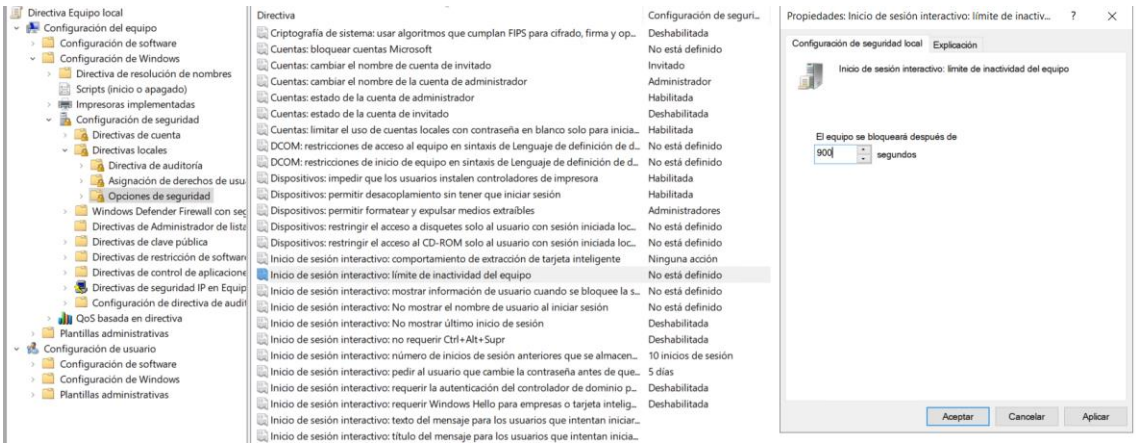


Figura 3.88 Configuración manual del primer problema de categoría II

Segundo problema de categoría II: Administración remota de Windows

Para el segundo problema se escogió acceso remoto sin cifrar, ya que al estar sin cifrar puede comprometer información confidencial. Esta configuración se visualiza en la Figura 3.89, donde se detalla el problema.

V-205817 - Windows Server 2019 Windows Remote Management (WinRM) service must not allow unencrypted traffic.

Rule ID:	xccdf_mil.disa.stig_rule_SV-205817r877382_rule
Test Type:	Automated
Result:	Fail
Version:	WN19-CC-000510
Identities:	SV-103587 V-93501 CCI-002890 (NIST SP 800-53 Rev 4: MA-4 (6); NIST SP 800-53 Rev 5: MA-4 (6)) CCI-003123 (NIST SP 800-53 Rev 4: MA-4 (6); NIST SP 800-53 Rev 5: MA-4 (6))
Description:	Unencrypted remote access to a system can allow sensitive information to be compromised. Windows remote management connections must be encrypted to prevent this. Satisfies: SRG-OS-000393-GPOS-00173, SRG-OS-000394-GPOS-00174 false
Fix Text:	Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> "Allow unencrypted traffic" to "Disabled".
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2019 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2019 Identifier: 2907
Definitions:	Definition ID: oval:mil.disa.stig.windows:def:2092 Result: false Title: WN19-CC-000510 Description: Windows Server 2019 Windows Remote Management (WinRM) service must not allow unencrypted traffic. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('WinRM Service: Allow unencrypted traffic' is set to 'Disabled')
Tests:	Test ID: oval:mil.disa.stig.windows:tst:112700 (registry_test) Result: false Title: 'WinRM Service: Allow unencrypted traffic' is set to 'Disabled' Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.stig.windows:obj:112700 (registry_object) Object Requirements: ○ hive must be equal to 'HKEY_LOCAL_MACHINE' ○ key must be equal to 'Software\Policies\Microsoft\Windows\WinRM\Service' ○ name must be equal to 'AllowUnencryptedTraffic'

Figura 3.89 Detalles del segundo problema de categoría II

Para la respectiva solución se accede a la Configuración del dispositivo, posteriormente se seleccionó la alternativa de Plantillas administrativas. En la ventana subsiguiente, se optó por la categoría de Componentes de *Windows*, visualizada en la Figura 3.90 seguida por la elección de Administración remota de *Windows* (WinRM), en la cual se seleccionó el Servicio WinRM. Finalmente, se ubicó la opción "Permitir tráfico sin cifrar" y se desactivó. Este cambio se evidencia en la Figura 3.91.

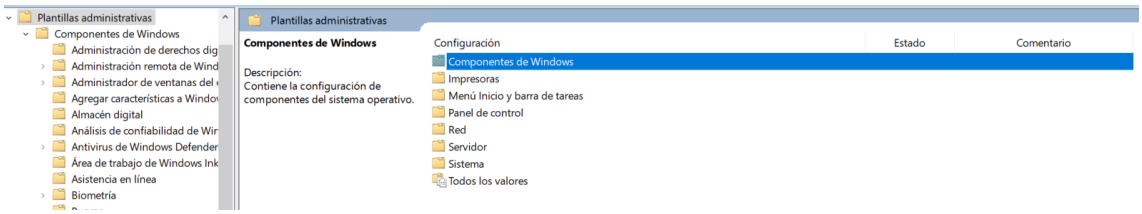


Figura 3.90 Plantillas administrativas y componentes de *Windows*

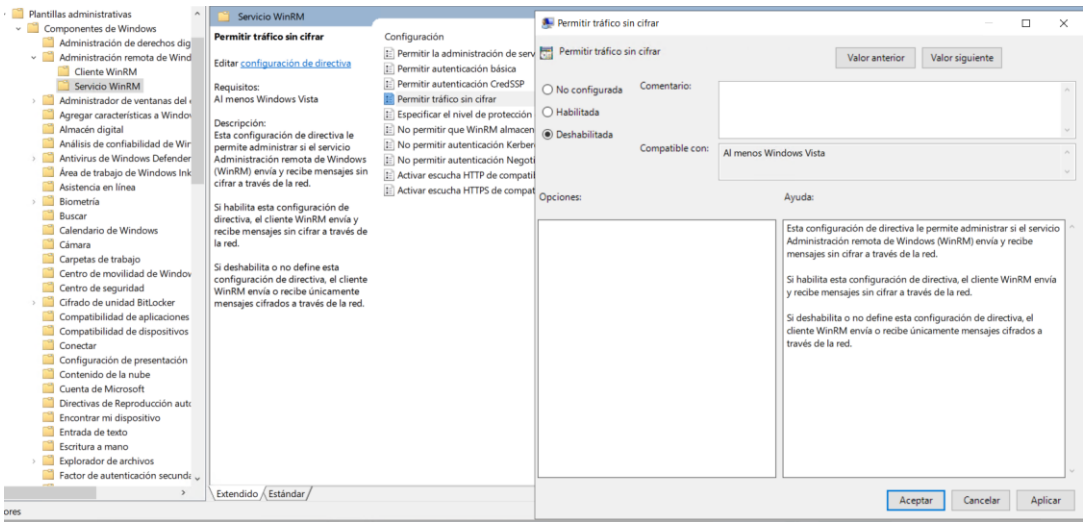


Figura 3.91 Configuración manual del segundo problema de categoría II

Tercer problema de categoría II: Solicitud de autentificación cuando el sistema sale del modo de suspensión

Para el tercer problema se escogió la solicitud de autentificación cuando el sistema está en modo suspensión ya que un sistema que no requiere autenticación al salir del modo de suspensión puede proporcionar acceso a usuarios no autorizados. En la Figura 3.92 se detalla el problema de la configuración.

V-205867 - Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (on battery).

Rule ID:	xccdf_mil.disa.stig_rule_SV-205867r569188_rule
Test Type:	Automated
Result:	Fail
Version:	WN19-CC-000180
Identities:	V-93253 SV-103341 CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b)
Description:	A system that does not require authentication when resuming from sleep may provide access to unauthorized users. Authentication must always be required when accessing a system. This setting ensures users are prompted for a password when the system wakes from sleep (on battery). false
Fix Text:	Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Power Management >> Sleep Settings >> "Require a password when a computer wakes (on battery)" to "Enabled".
Severity:	medium

Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2019 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2019 Identifier: 2907
Definitions:	Definition ID: oval:mil.disa.stig.windows:def:2061 Result: false Title: WN19-CC-000180 Description: Windows Server 2019 users must be prompted to authenticate when the system wakes from sleep (on battery). Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (All child checks must be true.) ▪ false ('Require a password when a computer wakes (on battery)' is set to 'Enabled')
Tests:	Test ID: oval:mil.disa.stig.windows:tst:109400 (registry_test) Result: false Title: 'Require a password when a computer wakes (on battery)' is set to 'Enabled' Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.stig.windows:obj:109400 (registry_object) Object Requirements: ○ hive must be equal to 'HKEY_LOCAL_MACHINE' ○ key must be equal to 'Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f7d2daa51f51' ○ name must be equal to 'DCSettingIndex' State ID: oval:mil.disa.stig.windows:ste:109400 (registry_state) State Requirements: ○ check_existence = 'at_least_one_exists', type must be equal to 'reg_dword' ○ for check = 'all', value, the following must be true: ▪ value must be equal to '1' Additional Information: Check existence requirement not met.

Figura 3.92 Detalles del tercer problema de categoría II

Para abordar la solución correspondiente, se procedió a seguir el siguiente conjunto de pasos: en primer lugar, se accedió a la Configuración del equipo. Dentro de esta área, se optó por Plantillas administrativas. Posteriormente, se eligió la opción de Sistemas. Una vez en la nueva ventana, se hizo clic en la selección de Administración de energía. Dentro de este apartado, se seleccionó la Configuración de suspensión, visualizadas en la Figura 3.93 seguido por la elección de Requerir una contraseña cuando una computadora se activa. En la cual se procedió a habilitarlo. Esta configuración se visualiza en la Figura 3.94.

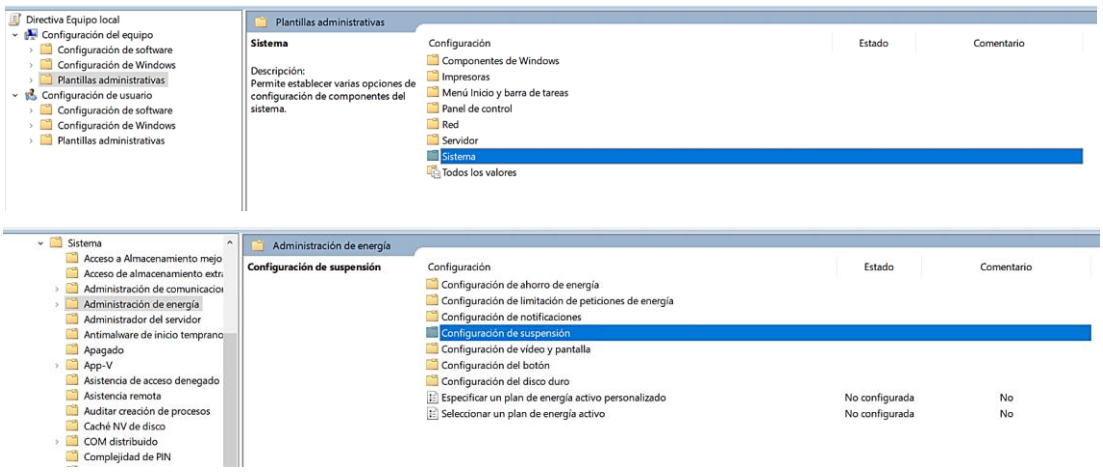


Figura 3.93 Plantillas administrativas y administración de energía

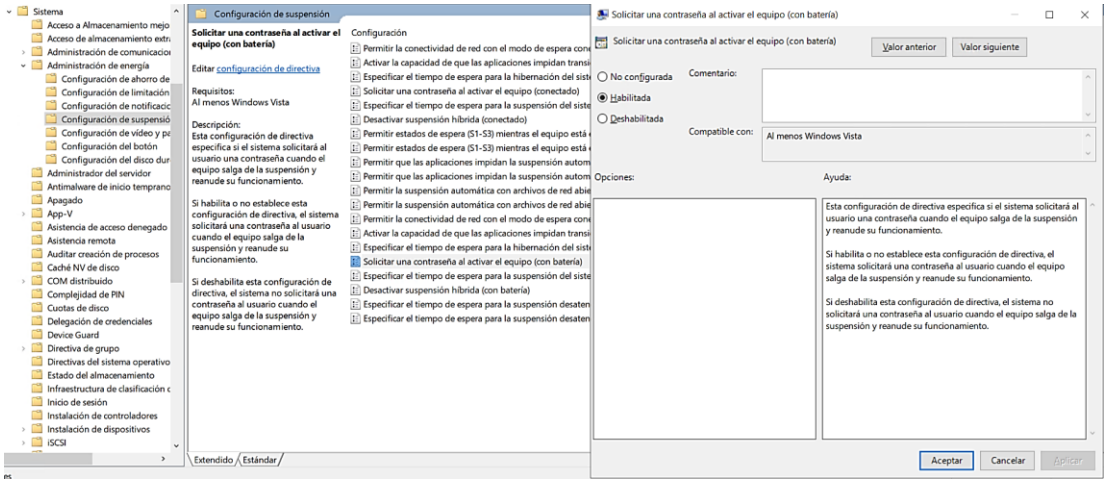


Figura 3.94 Configuración manual del tercer problema de categoría II

Por último, se procedió a configurar la opción de eliminación de tarjeta inteligente, ya que al estar desatendido es susceptible al uso de personal no autorizado; mediante el bloqueo se evita el acceso al sistema cuando la tarjeta inteligente sea retirado. Este problema se visualiza en la Figura 3.95.

V-205912 - Windows Server 2019 Smart Card removal option must be configured to Force Logoff or Lock Workstation.

Rule ID:	xccdf_mil.disa.stig_rule_SV-205912r569188_rule
Test Type:	Automated
Result:	Fail
Version:	WN19-SO-000150
Identities:	V-93287 SV-103375 CCI-000366 (NIST SP 800-53: CM-6 b; NIST SP 800-53A: CM-6.1 (iv); NIST SP 800-53 Rev 4: CM-6 b; NIST SP 800-53 Rev 5: CM-6 b)
Description:	Unattended systems are susceptible to unauthorized use and must be locked. Configuring a system to lock when a smart card is removed will ensure the system is inaccessible when unattended. false
Fix Text:	Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Smart card removal behavior" to "Lock Workstation" or "Force Logoff".
Severity:	medium
Weight:	10.0
Reference:	Title: DPMS Target Microsoft Windows Server 2019 Publisher: DISA Type: DPMS Target Subject: Microsoft Windows Server 2019 Identifier: 2907
Definitions:	Definition ID: oval:mil.disa.stig.windows:def:2140 Result: false Title: WN19-SO-000150 Description: Windows Server 2019 Smart Card removal option must be configured to Force Logoff or Lock Workstation. Class: compliance Tests: ○ false (All child checks must be true.) ▪ false (One or more child checks must be true.) ▪ false ('Interactive logon: Smart card removal behavior' is set to 'Lock Workstation') ▪ false ('Interactive logon: Smart card removal behavior' is set to 'Force Logoff')

Tests:	Test ID: oval:mil.disa.stig.windows:tst:119700 (registry_test) Result: false Title: 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.stig.windows:obj:119700 (registry_object) Object Requirements: ○ hive must be equal to 'HKEY_LOCAL_MACHINE' ○ key must be equal to 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon' ○ name must be equal to 'scremoveoption' State ID: oval:mil.disa.stig.windows:ste:119700 (registry_state) State Requirements: ○ check_existence = 'at_least_one_exists', type must be equal to 'reg_sz' ○ check_existence = 'at_least_one_exists', value must be equal to '1' Collected Item/State Result: ○ hive equals 'HKEY_LOCAL_MACHINE' [false] ○ key equals 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon' ○ name equals 'scremoveoption' ○ last_write_time equals '133363085870000000' ○ type equals 'reg_sz' ○ value equals '0' ○ windows_view equals '64_bit' Additional Information: Check requirement not met. value --- Test ID: oval:mil.disa.stig.windows:tst:119701 (registry_test) Result: false Title: 'Interactive logon: Smart card removal behavior' is set to 'Force Logoff' Check Existence: One or more collected items must exist. Check: All collected items must match the given state(s). Object ID: oval:mil.disa.stig.windows:obj:119700 (registry_object) Object Requirements: ○ hive must be equal to 'HKEY_LOCAL_MACHINE' ○ key must be equal to 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon' ○ name must be equal to 'scremoveoption' State ID: oval:mil.disa.stig.windows:ste:119701 (registry_state) State Requirements: ○ check_existence = 'at_least_one_exists', type must be equal to 'reg_sz' ○ check_existence = 'at_least_one_exists', value must be equal to '2' Collected Item/State Result: ○ hive equals 'HKEY_LOCAL_MACHINE' [false] ○ key equals 'Software\Microsoft\Windows NT\CurrentVersion\Winlogon' ○ name equals 'scremoveoption' ○ last_write_time equals '133363085870000000'

Figura 3.95 Detalles del cuarto problema de categoría II

Para encontrar la solución correspondiente, se procedió con los siguientes pasos: en primer lugar, se accedió a la sección de Configuración de la computadora; posteriormente, se ingresó a la Configuración de *Windows*. Dentro de esta sección, se eligió la opción de Configuración de seguridad y, a continuación, se accedió a las Políticas locales. Este proceso se evidencia en la Figura 3.96.

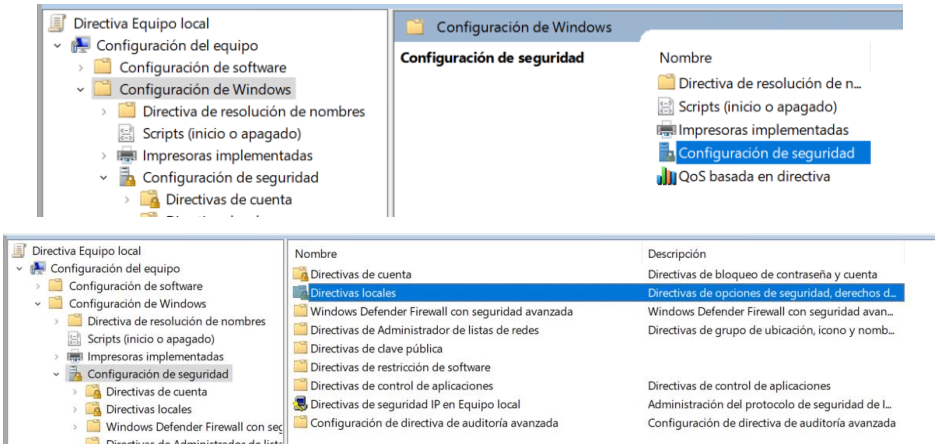


Figura 3.96 Configuración de *Windows* y directivas locales

Dentro de las Políticas locales, se abrió una nueva ventana en la que se seleccionaron las Opciones de seguridad. Finalmente, se optó por la alternativa "Inicio de sesión interactivo: comportamiento de eliminación de tarjeta inteligente" y se eligió entre las opciones "Bloquear estación de trabajo" o "Forzar cierre de sesión". Esta configuración se evidencia en la Figura 3.97.

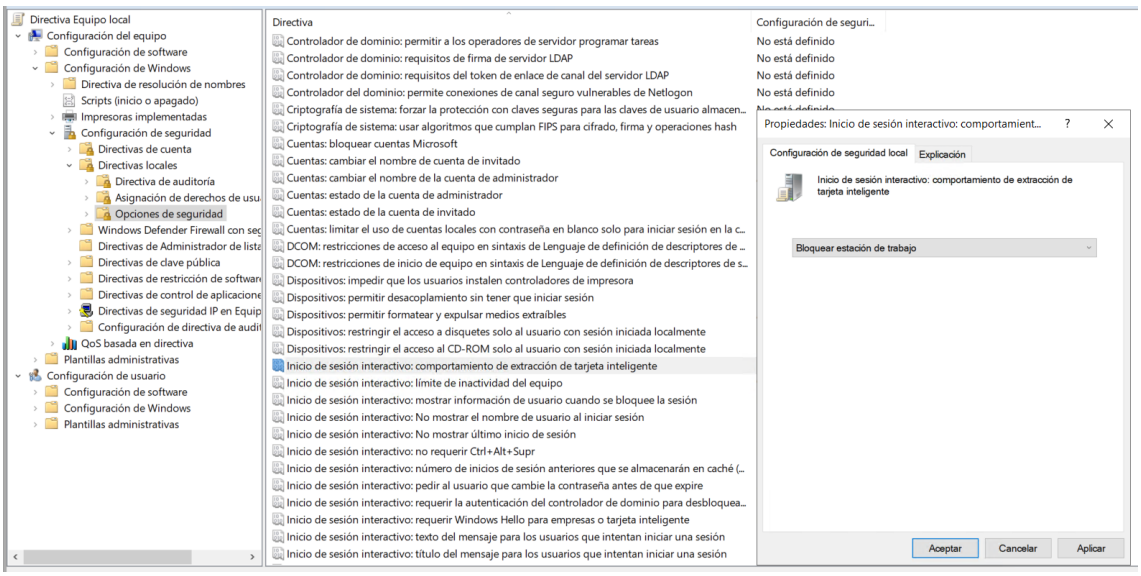


Figura 3.97 Configuración manual del cuarto problema de categoría II

Tercer reporte de vulnerabilidades

Una vez que se finalizó las configuraciones manuales para solventar problemas que afectan al sistema se procedió a realizar un tercer escaneo con la finalidad de visualizar los cambios realizados para lo cual se obtuvo los siguientes resultados:

Porcentaje del sistema asegurado: En la Figura 3.98 se visualiza el porcentaje del sistema asegurado la cual corresponde al 63.84 %. En esta se evidencia que el porcentaje de seguridad del servidor ha aumentado luego de realizar las configuraciones.

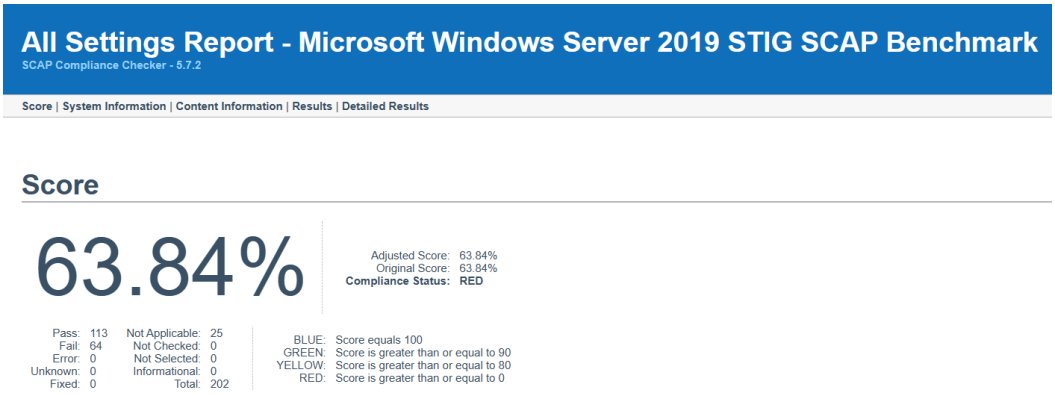


Figura 3.98 Tercer reporte del porcentaje del servidor asegurado

Configuraciones de categoría I: En la Figura 3.99 se observa los problemas que existe en la categoría I, lo cual corresponde a un solo error. Al momento de realizar las configuraciones se evidencia que los errores fueron solventados. Dando como resultado configuraciones en color azul.

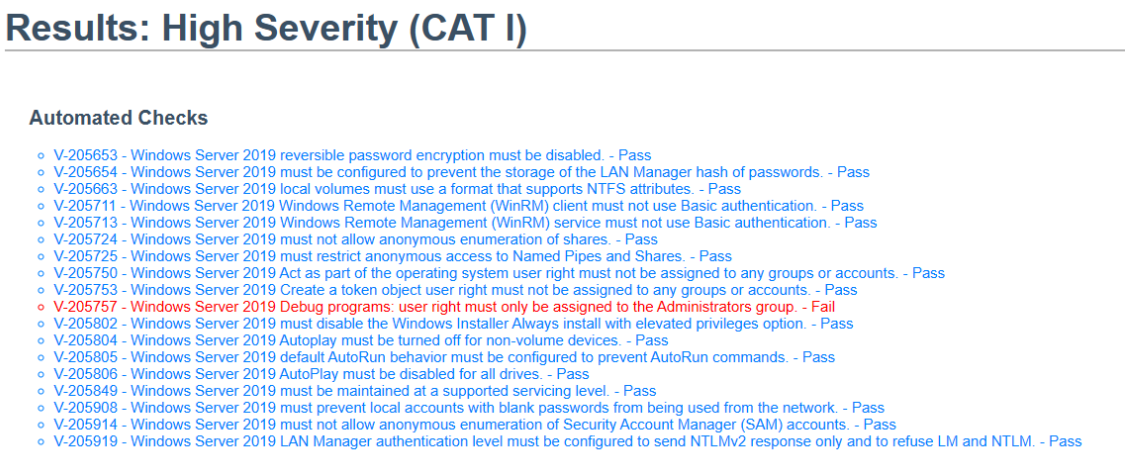


Figura 3.99 Configuraciones de gravedad I

Configuraciones de categoría II: En la Figura 3.100 se visualiza las configuraciones que se han logrado solventar, así como también los que falta por solventar.

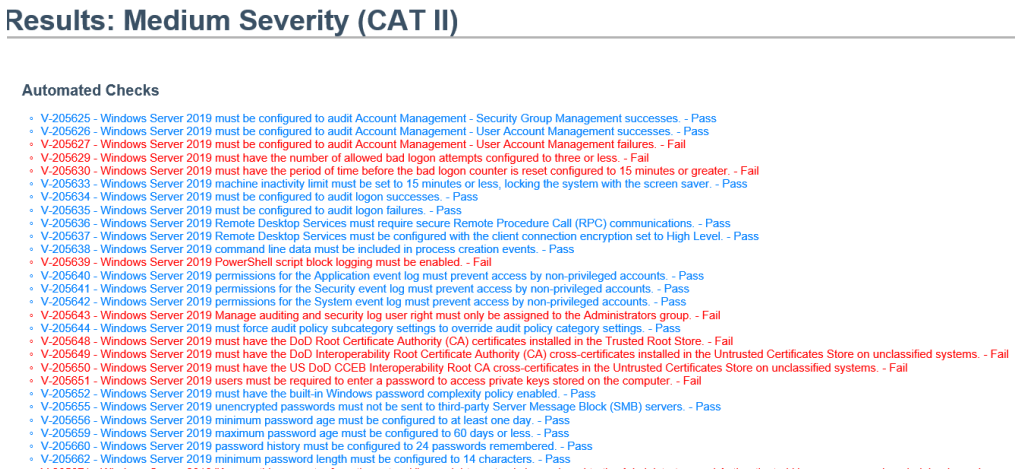


Figura 3.100 Configuraciones de gravedad II

Configuraciones de categoría III: En este caso no se visualiza cambios debido a que no se realizó ninguna configuración, por lo tanto, la configuración es la misma que en el reporte dos, ver Figura 3.76.

Prueba final del funcionamiento del servidor y gestor de correo electrónico

Con el fin de verificar el correcto funcionamiento del servidor de correo se procedió a realizar las respectivas pruebas, para lo cual se procedió a enviar nuevos mensajes entre los tres usuarios.

Primero se envió desde el usuario JUAN JANETA hacia el usuario MARIA SIMBA, en la Figura 3.101 se evidencia el envío y recepción del mensaje. Donde el mensaje enviado fue “saludos estimada María prueba final”

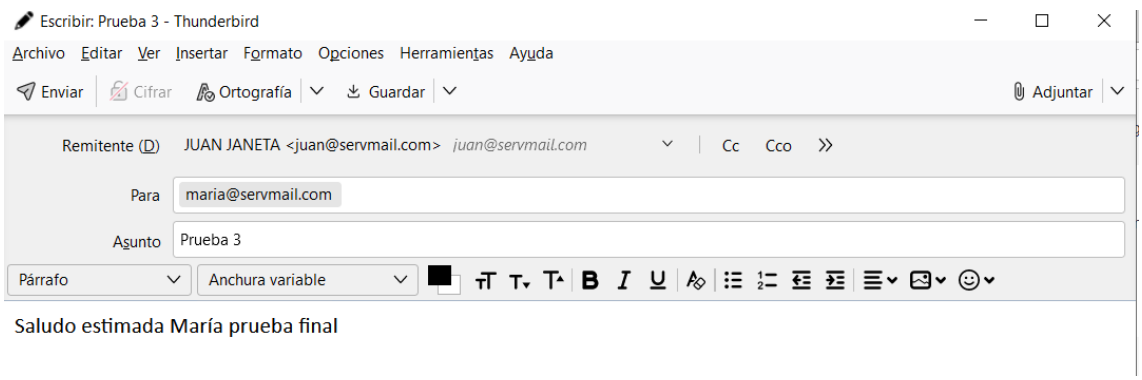


Figura 3.101 Mensaje enviado del usuario Juan hacia el usuario María

En la Figura 3.102 se evidencia que en la bandeja de entrada del usuario María se encuentra un mensaje enviado del usuario Juan con el asunto de Prueba 3.

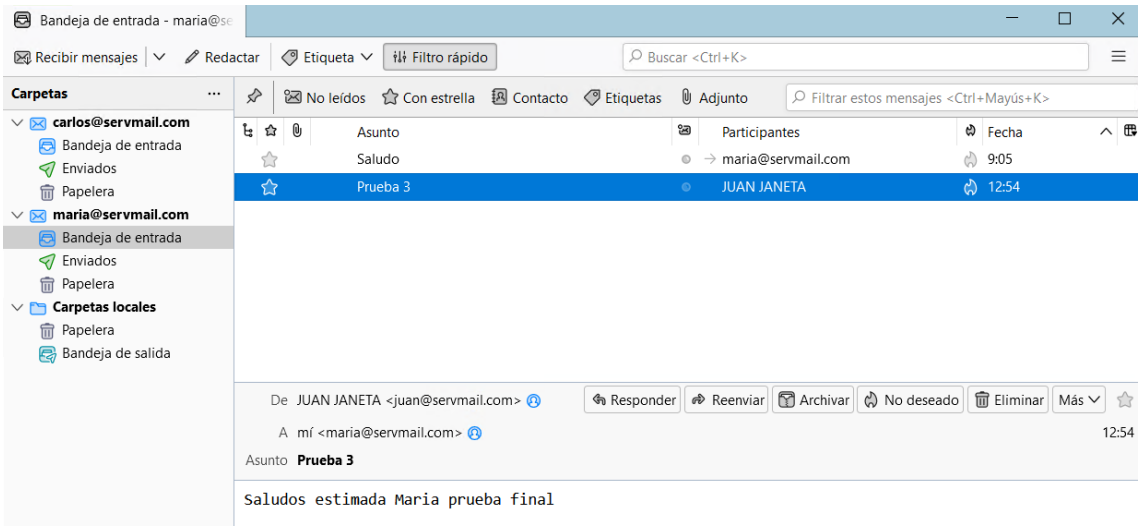


Figura 3.102 Recepción del mensaje enviado por Juan

De la misma manera se procedió a enviar un mensaje al usuario CARLOS RAMIREZ desde el usuario JUAN JANETA con el mensaje “Saludos estimado Carlos prueba final”, la cual se evidencia en la Figura 3.103.

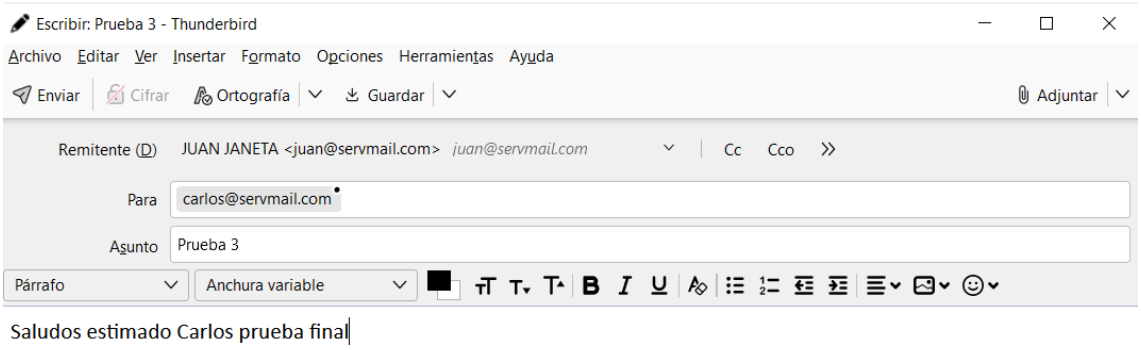


Figura 3.103 Mensaje enviado del usuario Juan hacia Carlos

Al ingresar a la cuenta del usuario Carlos se puede visualizar en la Figura 3.104 que evidentemente llego el mensaje enviado por Juan con el asunto de Prueba 3.

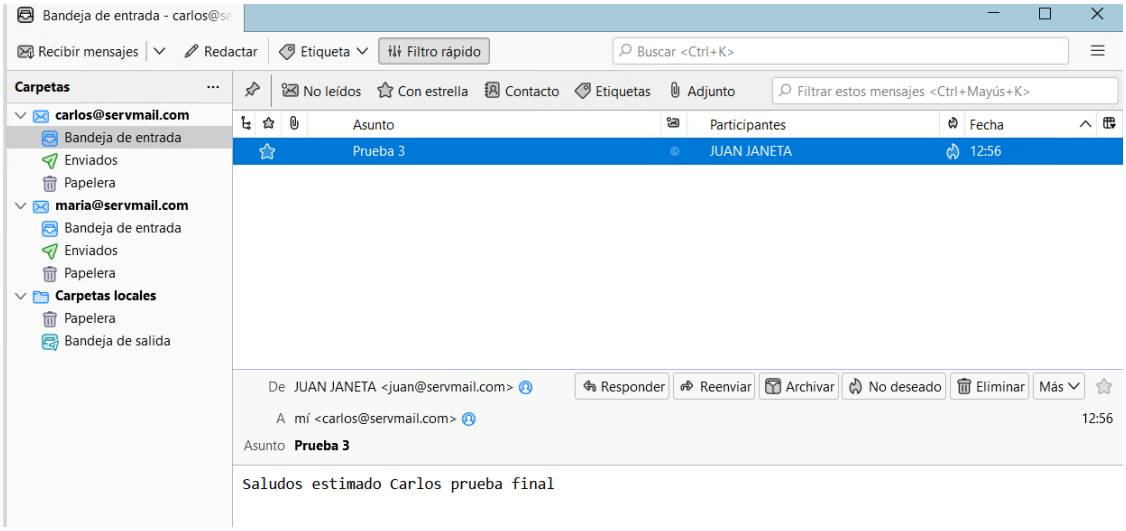


Figura 3.104 Recepción del mensaje enviado por Juan

Finalmente, para la última prueba se procedió a enviar un mensaje desde el usuario MARIA SIMBA Y CARLOS RAMIREZ hacia el usuario JUAN JANETA, mencionando un saludo con la prueba final la cual se visualiza en la Figura 3.105.

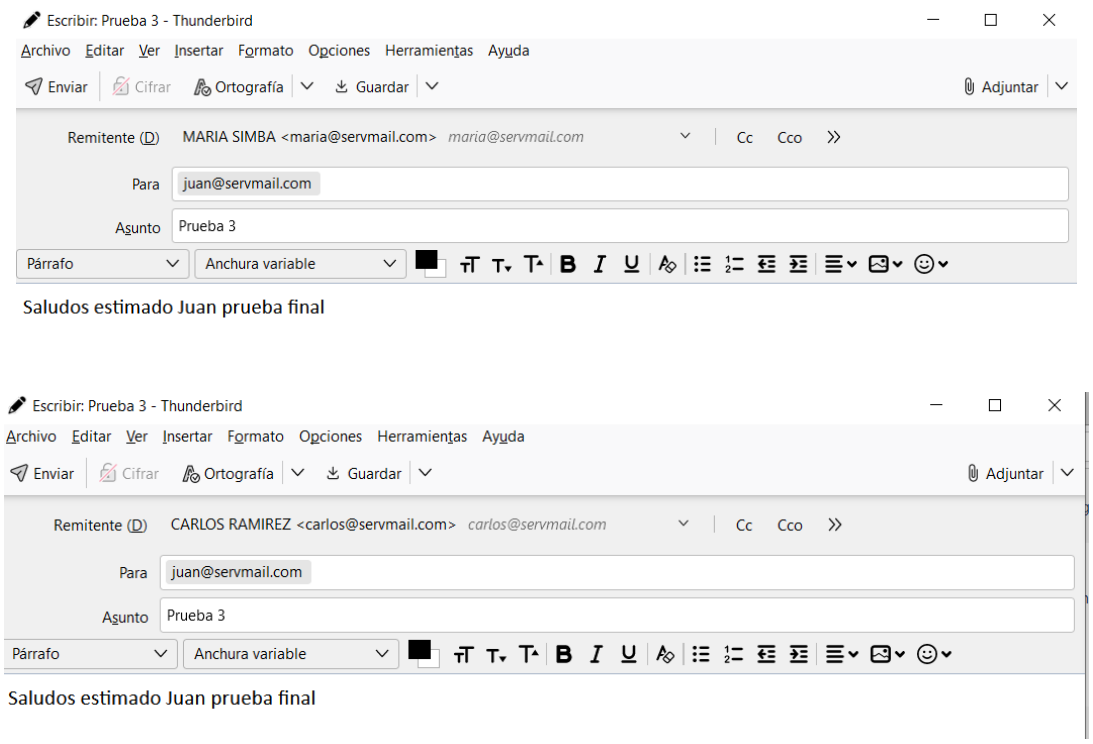


Figura 3.105 Envío de mensajes de María y Carlos hacia el usuario Juan

Así también se evidencia en la Figura 3.106 que el mensaje enviado por los dos usuarios ingresó de manera exitosa a la bandeja de entrada del usuario Juan, constatando el correcto funcionamiento del servidor después de realizar las configuraciones de forma manual.

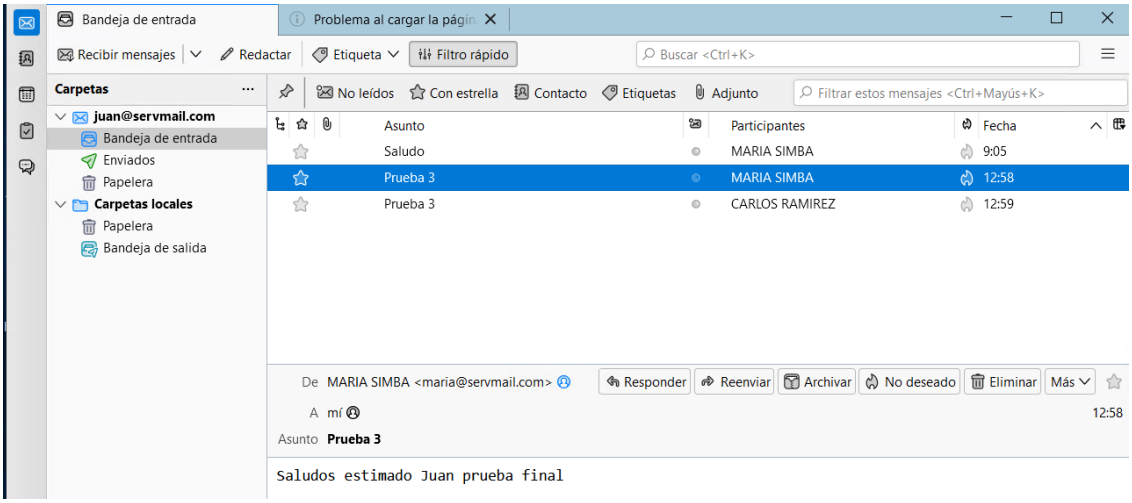


Figura 3.106 Recepción de los mensajes del usuario María y Carlos

3.4 Verificación del *hardening* en el servidor, en base en los elementos de la triada CIA

Verificación de los problemas solventados en base a la triada CIA

En base en el último reporte se procede a verificar las configuraciones que se han solventado tomando en cuenta la triada CIA, para ello se presenta el reporte en la Tabla 3.6. En la cual se detalla cada una de las configuraciones con su respectivo parámetro.

Tabla 3.6 Configuraciones solventadas de la categoría I con triada CIA

POLÍTICAS IMPLEMENADAS EN CATEGORIA I			
Políticas críticas implementadas	**Impacto sobre elementos triada CIA**		
	Confiabilidad	**Integridad**	**Disponibilidad**
El cliente de administración remota de Windows (WinRM)		X	
Enumeración anónima de recursos compartidos		X	X
Desactivación de dispositivos sin volumen		X	
Ejecución automática de comandos	X	X	
Desactivación reproducción automática		X	
El nivel de autenticación de LAN *Manager*	X	X	X
Deshabilitar la autenticación básica		X	
Windows Installer eleva los privilegios al instalar programas.		X	

En la Tabla 3.7 se presenta las configuraciones solventadas con su respectivo parámetro basado en la triada CIA.

Tabla 3.7 Configuraciones solventadas en la categoría II con triada CIA

POLÍTICAS IMPLEMENADAS EN CATEGORIA II			
Políticas criticas implementadas	**Impacto sobre elementos triada CIA**		
	Confiabilidad	**Integridad**	**Disponibilidad**
Servicios de escritorio remoto.	X	X	
Servicios de escritorio remoto con el cifrado de conexión del cliente en alto nivel	X	X	
Línea de comandos con ilusión de creación de eventos.		X	
Configuración de subcategoría de la política de auditoría.	X	X	X
Configuración de antigüedad de contraseñas.			X
Configuración de historial de contraseñas	X	X	
La longitud mínima de la contraseña la cual deber ser robusta y con un valor de 8 caracteres.	X	X	
Visualización de presentaciones de diapositivas en la pantalla de bloqueo.		X	
La interfaz de usuario (IU) no debe mostrarse en la pantalla de inicio de sesión.		X	
Defender *SmartScreen* debe estar habilitado	X	X	
Desactivación de indexación de archivos cifrados	X	X	

Administración remota de *Windows* no debe usar la autenticación Digest.		X	
Las cuentas de administrador no deben enumerarse durante la elevación	X	X	
Control de cuentas de usuario	X	X	
El tamaño del registro de eventos de la aplicación.	X		X
El tamaño del registro de eventos de seguridad.	X		X
Opciones de instalación para los usuarios para usuarios		X	
No se debe guardar contraseñas en *Remote Desktop Client*.	X	X	
Siempre deben solicitar al cliente las contraseñas al conectarse.		X	
Políticas criticas implementadas	**Impacto sobre elementos triada CIA**		
	Confiabilidad	**Integridad**	**Disponibilidad**
Las credenciales RunAS no deben ser almacenado por WinRM		X	
El modo de aprobación del Control de cuentas de usuario	X	X	
El Control de cuentas de usuario debe rechazar automáticamente las solicitudes de elevación de usuarios estándar.		X	

El cliente de administración remota no debe permitir el tráfico sin cifrar	X	X	X
Las comunicaciones con firma digital (siempre) deben estar configuradas como Habilitadas.	X	X	
Las comunicaciones con firma digital (si el cliente está de acuerdo) deben estar configuradas como Habilitadas.	X	X	
Los inicios de sesión no seguros en un servidor SMB deben estar deshabilitados.		X	
La telemetría debe configurarse en Seguridad o Básico	X	X	X
Evitar que se descarguen archivos adjuntos de fuentes RSS.		X	
Los servicios que emplean el sistema local para llevar a cabo la negociación durante el proceso de autenticación NTLM, deben utilizar la identidad de la máquina en vez de autenticarse de manera anónima.	X	X	
Se debe evitar que NTLM vuelva a una sesión nula.		X	

Se debe evitar la autenticación PKU2U mediante identidades en línea.		X	
Es necesario establecer la configuración de seguridad de la sesión para los clientes que utilizan NTLM SSP de manera que se exija la implementación de seguridad de sesión NTLMv2 y un nivel de cifrado de 128 bits.	X	X	
Es necesario establecer la configuración de seguridad de la sesión en servidores que utilizan NTLM SSP de manera que se exija la implementación de seguridad de sesión NTLMv2, así como el empleo de cifrado de 128 bits.	X	X	X
Políticas criticas implementadas	**Impacto sobre elementos triada CIA**		
	Confiabilidad	**Integridad**	**Disponibilidad**
Concesión inadecuada de derechos de usuario.		X	
El protector de pantalla debe configurarse en un máximo de 15 minutos y estar protegido con contraseña.	X	X	
Auditoría de los registros de actividad del sistema ayuda a identificar errores de configuración, solucionar problemas de interrupciones.		X	X

Guías para implementar un servidor de correo en *Windows server* endurecido

Prácticas y recomendaciones para implementar *Windows Server* endurecido

La implementación de un servidor de correo basado en *Windows Server* endurecido es fundamental para garantizar tanto la seguridad como la resistencia de un sistema. Para ello existen varias prácticas para lograrlo:

- Definir los roles y funciones del servidor para limitar la superficie del ataque. Esto se lo realiza directamente ingresando a la configuración de directivas locales, configuración de equipo, niveles de permisos de cuentas.
- Es importante separar los roles y servicios en servidores distintos para minimizar el impacto en caso de una brecha. Con esto se evita que los servicios queden fuera de funcionamiento en caso de haber algún problema en un servidor específico.
- Considerar las últimas actualizaciones de seguridad más recientes para proteger el sistema. En *Windows Server* existen parches de seguridad, los cuales están en constante actualización. Estas se deben aplicar de forma seguida.
- Una manera de minimizar los riegos en el servidor es tener instalado solo los componentes y características necesarios. Ya que aplicaciones que no están en funcionamiento utilizan recursos del *hardware* lo que reduce la eficiencia del servidor.
- Es importante emplear contraseñas seguras para las cuentas locales y no predeterminadas. Mediante esta medida se logra limitar el impacto de ingreso no autorizado al servidor.
- Habilitar el *Firewall* de *Windows* para regular el tráfico. Así también se evita que personas extrañas empleen un puerto abierto para realizar sus actividades maliciosas.

- Es una buena medida restringir el acceso a recursos mediante permisos de archivo y carpeta. Ya que la información sé que se maneja dentro del servidor es confidencial de la empresa.
- Una manera de asegurar el ingreso del personal de TI al servidor es mediante una autenticación fuerte, como autenticación de múltiples factores (MFA).
- Limitar el número de cuentas con privilegios de administrador, para tareas no administrativas otorgar cuentas de usuario estándar.
- Una buena medida para evitar *hackeos* en el servidor es mediante la auditoría de eventos, con esto se puede efectuar un seguimiento de actividades dudosas. Para que en futuro se tenga un informe detallado de algún problema que se presente.
- Una forma de supervisar un sistema es mediate el uso de herramientas de monitoreo como puede ser herramientas de escaneo que ayudan a visualizar o detectar posibles intrusos o problemas dentro del servidor.
- En importante cifrar los datos en reposo utilizando *BitLocker* u otras soluciones de cifrado. Ya que en caso de sustracción la información no sea presentada en texto plano.
- Establecer copias de seguridad regularmente y realizar pruebas de recuperación.
- Desactivar servicios y protocolos innecesarios para reducir la superficie de ataque.
- Configurar los servicios con la mínima cantidad de privilegios necesarios.
- Limitar el acceso físico al servidor y al centro de datos.
- Implementar medidas de seguridad física, como controles de acceso y cámaras.
- Proporcionar formación en seguridad cibernética a tu equipo y asegurar las buenas prácticas.

Prácticas y recomendaciones para implementar un servidor de correo electrónico

Configurar un servidor de correo electrónico seguro es fundamental para proteger la confidencialidad, integridad y disponibilidad de los datos de los usuarios.

- Mantener tanto el sistema operativo como el *software* del servidor actualizados con las últimas correcciones de seguridad.
- Configurar correctamente un *firewall* para permitir solo conexiones necesarias.
- Limitar los puertos abiertos a los servicios principales, como el puerto 25 (SMTP) y el puerto 587 (SMTP con autenticación).
- Implementar una autenticación segura para el acceso al servidor de correo electrónico, mediante contraseñas robustas que deben contener mínimo 8 caracteres combinadas con mayúsculas y minúsculas.
- Establecer políticas de contraseñas fuertes para las cuentas de correo electrónico.
- Configurar sistemas de filtrado de spam y antivirus para minimizar la cantidad de correos electrónicos maliciosos.
- Implementar estrategias de copias de seguridad periódicas para asegurar los datos del correo electrónico estén respaldados y puedan recuperarse.
- Configurar sistemas de monitoreo para supervisar la seguridad y el rendimiento del servidor de correo electrónico.
- Limitar el acceso al servidor solo a usuarios autorizados. Aplicando el principio de "menos privilegios" para evitar accesos innecesarios.
- Verificar que el servidor esté ubicado en un lugar seguro y que solo personal autorizado tenga acceso físico al mismo.
- Proporcionar a los usuarios información sobre la seguridad del correo electrónico, cómo la detección de correos electrónicos de *phishing* y cómo proteger las cuentas.

4 CONCLUSIONES

- En el presente proyecto de titulación se ha demostrado que al momento de instalar un sistema operativo de servidor tal como lo es *Windows Server 2019,* al ser analizado mediante una herramienta de escaneo de vulnerabilidades se ve reflejado que el sistema contiene varias configuraciones con problemas de seguridad. Estas configuraciones comprometen la información del sistema y del usuario. Estos problemas pueden se representados como puertas traseras para que personas no autorizadas ingresen al sistema y realicen actividades ilícitas.
- Con respecto al servidor de correo, se evidenció que al levantar el servicio no se reflejó ningún inconveniente, así como también al crear los usuarios no se tuvo problemas ni en la cuenta ni en las contraseñas por ende los usuarios se crearon con credenciales sencillas. Al igual que en el sistema operativo *Windows* 10 se conectó sin inconvenientes al servidor, además al desactivar los *firewalls* las pruebas de recepción y envío de mensajes se dio sin inconvenientes.
- Al implementar las políticas de seguridad al sistema operativo de servidor se pudo evidenciar que la mayoría de las configuraciones con problemas fueron solventados, permitiendo que el sistema tenga un nivel de seguridad elevado con respecto al primer sistema sin políticas. Mediante esta aplicación se evidenció que al momento de abrir un programa se presentaban notificaciones con mensajes de requerir ejecución como administrador. Así como también en varias configuraciones se presentó mensajes que solo el administrador puede realizar esas configuraciones.
- Al contar con un servidor que ha sido configurado con políticas de seguridad rigurosas, se observaron mejoras significativas al poner en funcionamiento el servidor de correo electrónico. Esto se debió a que, para desactivar los firewalls, se requería la autorización del administrador. Para abordar este desafío, se desarrollaron reglas de control de acceso tanto entrantes como salientes, con el fin de autorizar la conexión de un cliente con el servidor. Sin la implementación de estas reglas, la comunicación entre ambas entidades se tornaba prácticamente imposible.

- Los resultados generados por la herramienta de escaneo reflejaron de manera notable los niveles de aseguramiento del sistema. Inicialmente, el porcentaje se situaba por debajo del 50%, pero al implementar las políticas, este incrementó. En consecuencia, se puede concluir que las políticas aplicadas al sistema resultaron efectivas, aunque no se resolvieron todos los problemas, sí se abordaron los más críticos.
- Al configurar manualmente el sistema, se lograron resultados favorables, ya que el porcentaje de seguridad del sistema aumentó en un 3.7%. A partir de esto, podemos concluir que las configuraciones manuales son efectivas para mejorar la seguridad del servidor.
- En relación a la seguridad en el proyecto desarrollado, se puede concluir que se ha logrado mejorar significativamente la protección de la información siguiendo los principios fundamentales de la triada CIA. Para garantizar la integridad de los datos, se implementaron medidas como la restricción de acceso mediante contraseñas robustas y la limitación de configuraciones exclusivas para el administrador. Asimismo, se fortaleció la confidencialidad mediante la encriptación de la información. Por último, se aseguró la disponibilidad del servidor a través de auditorías periódicas, con el propósito de prevenir problemas tanto a nivel de hardware como de software.
- Finalmente, a partir de este proyecto, se llega a la conclusión de que comprender los aspectos de seguridad es de vital importancia en la era actual, donde la tecnología avanza a un ritmo exponencial, con consecuencias tanto positivas como negativas. Numerosas empresas se enfrentan a ataques maliciosos dirigidos a sus servidores, lo que pone en riesgo la integridad de la información. Por lo tanto, la realización de prácticas orientadas a la seguridad, tanto en servidores como en ordenadores, nos capacita para abordar posibles problemas que puedan surgir en nuestros equipos, evitando así la exposición de información confidencial a terceros.

5 RECOMENDACIONES

- Es importante asignar los recursos necesarios para levantar una máquina virtual para la implementación de un servidor de correo ya que al no asignarle los recursos suficientes al momento de correr la máquina virtual esta tendrá problemas para la ejecución del sistema operativo de servidor. Además, se debe tomar en cuenta las características de la máquina principal ya que de él depende como funcione las máquinas virtualizas.
- Para el correcto funcionamiento del servidor DHCP es importante definir una dirección ip estática mientras que para la comunicación entre las máquinas virtuales se debe seleccionar un conmutador de red virtual, dicho conmutador debe establecerse para las dos máquinas virtuales ya que mediante este conmutador el servidor DHCP asignará una dirección IP válida para el cliente. Posteriormente se empleará para la comunicación entre los gestores de correo electrónico de ambos sistemas operativos.
- Para aplicar las políticas de seguridad es recomendable emplear la versión 5 de *Power Shell* ya que versiones superiores requieren de paquetes adicionales para ejecutar comandos, además se debe redirigir los archivos a la carpeta donde está ubicado cada programa lo cual hace muy complicado correr los comandos. La versión 5 ya viene preinstalada en el sistema operativo de servidor por lo cual solo se requerirá ingresar los comandos a ejecutar.
- Para comunicar el servidor y el cliente se recomienda crea reglas que permitan el ingreso de solicitud, mas no se debe desactivar los *firewalls* ya que al deshabilitarlo se estará abriendo varias puertas para el ingreso de personas que podrían tomar el control total de sistema. Mediante las reglas ya sea de entrada y salida solo se abrirá el puerto que emplee esa aplicación en este caso el servidor de correo electrónico.
- Como recomendación en base al proyecto empleado, al crear las cuentas de usuario se debe tener en cuenta varias características con el fin de evitar futuros *hackeos*. Para evitar dichos inconvenientes se debe emplear usuarios con credenciales fuertes, tanto en el nombre del usuario como

en las contraseñas, el nombre de usuario se debe ingresar mínimo un nombre y un apellido si es posible combinarlos con mayúsculas, minúsculas y números. Para el caso de las contraseñas se debe emplear contraseñas robustas que combinen caracteres, números, letras y con una longitud mínima de 8.

6 REFERENCIAS BIBLIOGRÁFICAS

[1] I. R. Torres, «Sistemas operativos para servidores», *Profesional Review*, 20 de julio de 2022. https://www.profesionalreview.com/2022/07/20/sistemas-operativos-para-servidores/ (accedido 10 de julio de 2023).

[2] R. Borja, «¿Qué es un sistema operativo de servidores y cómo elegirlo? | Comunidad FS», *Knowledge*, 30 de mayo de 2022. https://community.fs.com:7003/es/blog/server-operating-system-explained.html (accedido 10 de julio de 2023).

[3] D. Vasquez, «¿Qué es un sistema operativo de servidores y cómo elegirlo?», *Sistemas Operativos para servidores*, 27 de abril de 2018. https://ucloudglobal.com/blog/sistema-operativo-de-servidores/ (accedido 10 de julio de 2023).

[4] A. Cordova, «Servidor Windows 2000 | wiki de microsoft | Fandom», *Servidor Windows 2000*, 22 de mayo de 2019. https://microsoft.fandom.com/wiki/Windows_2000_Server (accedido 12 de julio de 2023).

[5] F. Garcia, «Historia de Windows Server 2003», *Windows Server 2003*, 14 de mayo de 2019. https://www.trucoswindows.com/historia/windows-server-2003 (accedido 12 de julio de 2023).

[6] I. Herdandez, «Windows Server 2008 Service Pack 2 y Windows Vista Service Pack 2, versión independiente en 5 idiomas, imagen ISO de DVD (KB948465)», *Microsoft Download Center*. https://www.microsoft.com/es-es/download/details.aspx?id=24212 (accedido 12 de julio de 2023).

[7] B. Valdés, «Sistema operativo Windows Server 2012», *Windows Server 2012*, 13 de enero de 2015. https://www.administracionderedes.com/sistemas-operativos/sistema-operativo-windows-server-2012/ (accedido 12 de julio de 2023).

[8] M. Vargas, «Servidores Dedicados Windows Server 2016 - Características y Versiones», *INTERNET YA*, 9 de abril de 2018. https://www.internetya.co/servidores-windows-server-2016-caracteristicas-y-versiones/ (accedido 12 de julio de 2023).

[9] R. Bolaños, «Windows Server 2019 Essentials, Standard, Datacenter: Full Comparison», *Windows Server 2019*, 11 de diciembre de 2022. https://www.nakivo.com/blog/windows-server-2019-essentials-standard-datacenter-full-comparison/ (accedido 12 de julio de 2023).

[10] J. Ramirez, «Windows Server 2022: cómo es el nuevo sistema operativo de servidores - Imagar Solutions Company», *Windows Server 2022, Como es el nuevo Sistema Operativo*, 1 de febrero de 2022. https://www.imagar.com/blog-desarrollo-web/windows-server-2022-como-es-el-nuevo-sistema-operativo-de-servidores/ (accedido 12 de julio de 2023).

[11] J. Almendar, «Hardening informático ¿Qué es?», *Hardening*, o4 de 2022. https://www.ciset.es/publicaciones/blog/746-hardening (accedido 12 de julio de 2023).

[12] G. Smartekh, «¿QUÉ ES HARDENING?», *TIPS TECNOLÓGICOS, DE CONFIGURACIÓN Y NEGOCIO QUE COMPLEMENTAN TU SEGURIDAD*,

3 de mayo de 2012. https://blog.smartekh.com/que-es-hardening (accedido 12 de julio de 2023).
[13] B. Santander, «Integridad», *Banco Santander*, 17 de julio de 2018. https://www.bancosantander.es/glosario/integridad-seguridad-online (accedido 12 de julio de 2023).
[14] T. Naeem, «¿Qué es la integridad de datos en una base de datos? ¿Por qué lo necesitas?», *Astera*, 31 de octubre de 2020. https://www.astera.com/es/tipo/blog/integridad-de-datos-en-una-base-de-datos/ (accedido 12 de julio de 2023).
[15] D. Sing, «Disponibilidad de la información: ¿Por qué es importante contar con opciones seguras?», *¿Por qué es importante contar con opciones seguras?*, 17 de agosto de 2021. https://www.docusign.mx/blog/disponibilidad-de-la-informacion (accedido 12 de julio de 2023).
[16] P. Muñoz, «¿Qué Es La Disponibilidad En Seguridad Informática? | Servicios Informáticos Para Empresas», *Disponibilidad Informatica*, 20 de octubre de 2022. https://salesystems.es/que-es-disponibilidad-seguridad-informatica/ (accedido 12 de julio de 2023).
[17] D. Walkowski, «¿Qué es la tríada de la CIA? | Computer Weekly», *ComputerWeekly.es*, 31 de julio de 2019. https://www.computerweekly.com/es/opinion/Que-es-la-triada-de-la-CIA (accedido 12 de julio de 2023).
[18] J. Burgos, «Confidencialidad en seguridad informática, ¿en qué consiste?», *UNIR*, 31 de marzo de 2021. https://www.unir.net/ingenieria/revista/confidencialidad-seguridad-informatica/ (accedido 12 de julio de 2023).
[19] C. Kariuki, «Protocolo de automatización de contenido de seguridad (SCAP) explicado en 5 minutos o menos», *Geekflare*, 4 de enero de 2023. https://geekflare.com/es/security-content-automation-protocol/ (accedido 12 de julio de 2023).
[20] G. Mendez, «Los Ciberdelincuentes: Quiénes Son, Qué Hacen Y Por Qué Lo Hacen - Acktib», *Ciberdelincuentes*, 24 de febrero de 2021. https://acktib.com/blog-los-ciberdelincuentes-quienes-son-que-hacen-y-por-que-lo-hacen/ (accedido 12 de julio de 2023).
[21] «Security Content Automation Protocol (SCAP) – DoD Cyber Exchange». https://public.cyber.mil/stigs/scap/ (accedido 14 de agosto de 2023).
[22] F. Flores, «OpenSCAP», *¿Qué es SCAP?*, 23 de septiembre de 2021. https://flealf.com/doku.php?id=linux:openscap (accedido 12 de julio de 2023).
[23] K. Tech, «¿Qué es Nessus? | KeepCoding Bootcamps», 23 de septiembre de 2022. https://keepcoding.io/blog/que-es-nessus/ (accedido 12 de julio de 2023).
[24] R. Vera, «Qué es OpenVAS, para qué sirve y características», *OpenWebinars.net*, 11 de noviembre de 2020. https://openwebinars.net/blog/que-es-openvas/ (accedido 12 de julio de 2023).
[25] J. Gates, «¿Qué son los CIS Benchmarks y cómo usarlos?», *CalCom*, 6 de enero de 2023. https://www.calcomsoftware.com/que-son-los-cis-benchmarks-y-como-usarlos/ (accedido 6 de septiembre de 2023).

[26] J. Gates, «¿Qué son los puntos de referencia de CIS? | IBM», *CIS PUNTOS DE REFERENCIA*, O6 de 2023. https://www.ibm.com/mx-es/topics/cis-benchmarks (accedido 26 de julio de 2023).
[27] D. Kosutic, «¿Qué es norma ISO 27001?», *What is the ISO 27001*, 15 de octubre de 2022. https://advisera.com/27001academy/es/que-es-iso-27001/ (accedido 31 de julio de 2023).
[28] C. Villamizar, «¿Qué es NIST Cibersecurity Framework?», *GlobalSuite Solutions*, 22 de octubre de 2020. https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/ (accedido 31 de julio de 2023).
[29] J. A. Gomez, «Marco de Ciberseguridad Del NIST: Qué es y Cómo Implementarlo», *NIST*, 30 de marzo de 2023. https://www.deltaprotect.com/blog/marco-ciberseguridad-nist (accedido 31 de julio de 2023).
[30] F. Gonzalez, «hMailServer, servidor de correo para Windows», *Servidor Correo Electronico*, 10 de marzo de 2020. https://www.batiburrillo.net/hmailserver-servidor-de-correo-para-windows/ (accedido 7 de agosto de 2023).
[31] N. S, «Download - hMailServer - Free open source email server for Microsoft Windows», *Download HmailServer*. https://www.hmailserver.com/download (accedido 7 de agosto de 2023).
[32] S. Perich, «▷ Mozilla Thunderbird ¿qué es y para qué sirve?», *Soplos Linux*, 24 de marzo de 2020. https://soploslinux.com/mozilla-thunderbird-que-es-y-para-que-sirve/ (accedido 7 de agosto de 2023).