Universidad Zaragoza
1542

Trabajo Fin de Grado

FORTIFICACIÓN DEL ENTORNO DE WINDOWS EN EL DESPLIEGUE DE LOS PUESTOS DE MANDO TÁCTICOS

Noelia Sosa Almario

Director académico: Lacramioara Dranca

Director militar: Cristina Díaz García

Centro Universitario de la Defensa

Academia General Militar 2022

Agradecimientos

Me gustaría agradecer, en primer lugar, a la teniente Cristina Díaz, mi tutora militar, la cual me ha aportado grandes conocimientos, no solo referente a este TFG, si no referente al mundo de la securización, el cual, me ha empezado a parecer fascinante a partir de este trabajo de investigación. Su ayuda ha sido determinante a la hora de desarrollar el presente TFG, y sin sus conocimientos habría sido imposible. En segundo lugar, he de agradecer a mi tutora académica, la cual me ha ayudado en este arduo trabajo y me ha dirigido por el camino que debía seguir. Su presencia en el TFG es de vital importancia, ya que sin ella no habría llegado a los estudios que hoy se presentan en el presente trabajo, y tampoco habría tenido el buen aspecto con el que cuenta hoy en día. Por último, agradecer a la CIA de Transmisiones de la BRILEG su apoyo incondicional en todos los requerimientos necesarios que solicitaba, y por sus leales servicios prestados en mi ayuda. Sin ellos no se habría terminado este TFG.

Por lo tanto, he de decir que estoy totalmente agradecida y que este trabajo no solo lo he hecho yo, si no que, de una forma indirecta, he sido ayudada por las personas o miembros anteriormente citadas. Muchas Gracias.

Resumen

El creciente desarrollo tecnológico que vive la sociedad cada día obliga a todo tipo de empresas u organizaciones a reforzar sus sistemas de información de cara a poder blindarlos para que resulten impenetrables a los delincuentes informáticos. El ejército, en este caso, recoge muchos documentos e información de alto secreto, la cual en manos enemigas podría suponer una desventaja para España. Se puede decir que es de vital importancia mantener esa documentación en buenas manos para poder trabajar sobre la sorpresa.

Para poder mantener el Ejército actualizado, se ha diseñado un plan de ataque cuyo objetivo es convertir las Brigadas en Brigadas Experimentales (BRIEX) de cara a que formen parte del ejército denominado Fuerza 2035. Como se puede entender, estar al día en todos los métodos operativos es el camino para la victoria. La BRILEG (Brigada de la Legión) es, por tanto, una Brigada Experimental, en la que se están llevando a cabo cambios con el fin de llegar a los objetivos de la Fuerza 2035.

Siguiendo la dinámica de poder mejorar el ámbito de las Transmisiones en CIA de Transmisiones de la BRILEG, se observó la posibilidad de poder implementar una posible mejora en el hardening del entorno de Windows en el despliegue de los PCTAC (Puesto de mando táctico) así como poder implementar un nuevo método para agilizar la configuración del entorno de Windows.

Este proyecto trata de cubrir dos objetivos, reducir tiempo y mejorar el hardening, con el fin de aumentar la efectividad de la BRILEG. Para poder llevar a cabo estos dos objetivos, este trabajo se basa en métodos experimentales y teóricos sobre los sistemas operativos de Windows, con la creación de dos máquinas virtuales (una con Windows Server 2016 y otra con Windows 10) para replicar el nodo de la BRILEG en ellas. Una vez creadas, se procede a realizar las configuraciones de seguridad sobre las máquinas virtuales para crear un entorno más seguro y blindarlo de cara a los ladrones informáticos. No sólo se securiza el entorno de Windows, sino que también se propone la creación de un manual para reducir el tiempo de configuración del entorno de Windows. Posteriormente, se realizan las comprobaciones necesarias sobre las configuraciones realizadas y se efectúan entrevistas para conocer la utilidad a los usuarios sobre el nuevo método. Estos resultados, como posteriormente se observa, salen verdaderamente favorables, y por lo tanto corresponden con los objetivos buscados.

Palabras clave

PCTAC

Windows Server 2016 y Windows 10

Hardening

Directiva de grupo

Política de contraseñas

AppLocker

Dominio de Windows

Active Directory

Firewall de Windows

Script

Política de seguridad

Carpetas Compartidas

BRIEX

Abstract

The growing technological development that society experiences every day forces all types of companies or organizations to reinforce their information systems in order to be able to shield them so that they are impenetrable to computer criminals. The army, in this case, collects many top-secret documents and information, which in enemy hands could be a disadvantage for Spain. It can be said that it is of vital importance to keep this documentation in good hands in order to work on the surprise.

In order to keep the Army updated, an attack plan has been designed whose objective is to convert the Brigades into Experimental Brigades (BRIEX) so that they form part of the army called Force 2035. As can be understood, being up to date with all the methods operations is the path to victory. The BRILEG (Legion Brigade) is, therefore, an Experimental Brigade, in which changes are being carried out in order to reach the objectives of Force 2035.

Following the dynamics of being able to improve the field of Transmissions in the CIA of Transmissions of the BRILEG, the possibility of being able to implement a possible improvement in the hardening of the Windows environment in the deployment of the PCTAC (Tactical Command Post) as well as to be able to implement a new method to streamline the configuration of the Windows environment.

This project tries to cover two objectives, reduce time and improve hardening, in order to increase the effectiveness of the BRILEG. In order to carry out these two objectives, this work is based on experimental and theoretical methods on Windows operating systems, with the creation of two virtual machines (one with Windows Server 2016 and the other with Windows 10) to replicate the node of the BRILEG in them. Once created, we proceed to carry out the security configurations on the virtual machines to create a more secure environment and shield it from computer thieves. Not only is the Windows environment secured, but it is also proposed to create a manual to reduce the time for setting up the Windows environment. Subsequently, the necessary checks are carried out on the configurations made and interviews are carried out to find out the usefulness to the users of the new method. These results, as later observed, are truly favorable, and therefore correspond to the objectives sought.

Keywords

PCTAC

Windows Server 2016 and Windows 10

Hardening

Group policy

Password policy

AppLocker

Window’s Domain

Active Directory

Window’s Firewall

Script

Security policy

Password policy

Shared Folders

BRIEX

ÍNDICE DE CONTENIDO

Contenido

TABLA DE FIGURAS

ÍNDICE DE TABLAS

Abreviaturas, siglas y acrónimos

- BRIEX: Brigada Experimental
- BRILEG: Brigada de la Legión
- CCN: Centro criptológico nacional
- CEMA: Ciber electromagnéticas
- CIA: Compañía
- CIATRANS: Compañía de Transmisiones
- CIS: Centros Integrados de Servicios
- CSV: Código de verificación de documentos
- CT: Centro Táctico
- DLL: Dynamic-link library
- DNS: Domain name service
- ENS: Esquema nacional de seguridad
- ET: Ejército de Tierra
- GPO: Group Policy Object
- LLAA: Lecciones Aprendidas
- PC: Puesto de Mando
- PC: Puesto de mando
- PCTAC: Puesto de Mando Táctico
- RRC: Red radio de combate
- S.O: Sistema operativo
- TCP: Protocolo de control de transmisión
- TFG: Trabajo de Fin de Grado
- TIC: Tecnologías de la Información y la comunicación
- TTPs: Tácticas Técnicas y Procedimientos
- UDP: Protocolo de datagramas de usuario

- VHF: Very high frecuency
- ZO: Zona de Operaciones

1. Introducción

1.1. Fuerza 2035

La Fuerza 2035 tiene mucha importancia en la evolución del ejército, debido a que la sociedad evoluciona cada día y es responsabilidad del ejército y de los militares estar actualizados para poder dar frente a las nuevas amenazas que van surgiendo. Debido a que estar desactualizado representa un peligro para toda la nación, el Ejército propone cambiar los medios, así como los procedimientos de actuación. Tener presente que la obligación de un militar es poder afrontar al enemigo con medios que puedan igualar sus fuerzas es crucial. Para poder llevarlo a cabo, se implantaron nuevas formas de proceder en los ejercicios y maniobras dentro de las Brigadas, denominándolas Brigadas experimentales (BRIEX)[1]. Hoy en día, la BRILEG[2] (lugar donde se ha realizado el trabajo) es Brigada Experimental y la propuesta de este trabajo de fin de grado va ligada de la mano a poder servir a la BRIEX.

Una de las principales responsabilidades que tiene el ET (Ejército de Tierra) es la de mantener unas fuerzas terrestres instruidas, preparadas y eficaces para el combate, no solo de hoy, sino también del futuro. Para cumplir este propósito, se ha tenido que iniciar el proceso de cambio hacia el denominado concepto Fuerza 2035. En la siguiente figura se puede observar la imagen representativa de la Fuerza 2035. (Tierra, 2019)

Figura 1.Símbolo Fuerza 2035. (Tierra, 2019)

La Fuerza 2035 se basa en un prototipo de unidad a alcanzar en el año 2035, por todas las unidades que componen el ET español. Con este proyecto se buscan unidades y fuerzas operativas, flexibles y cohesionadas, con medios tecnológicos avanzados y personal altamente formado. (Tierra, 2019)

La razón de ser de este tipo de unidad viene motivada por el ambiente híbrido en el que despliegan hoy en día nuestras fuerzas españolas en ZO (Zona de Operaciones). Hoy en día, no se estila el concepto de guerra convencional, sino que ha evolucionado a un estado híbrido, en el que se mezclan TTPs (Tácticas Técnicas y Procedimientos) para alcanzar el éxito de la misión, ante el conflicto entre un ejército convencional y fuerzas irregulares.

[1] La Brigada Experimental o BRIEX es una Brigada que tiene la responsabilidad de ejecutar actividades de experimentación necesarias para extraer conclusiones que posteriormente puedan ser volcadas en los desarrollos conceptuales de la Fuerza 2035

[2] BRILEG significa Brigada de la Legión

Para alcanzar esa unidad, tipo Brigada, cohesionada, flexible y autosuficiente se han marcado tres fases:

- Fase de estudio conceptual: en esta fase, se identifican y se somete a debate las necesidades operativas, las estructuras orgánicas y funcionales, los materiales y la tecnología necesaria para llevar a cabo este proyecto de nuevas brigadas. Todo ello mediante cooperaciones cívico-militares entre el personal militar y distintas universidades y laboratorios.
- Fase de experimentación: en esta fase, se ponen a prueba esas estructuras teóricas para llevarlas a la práctica, mediante ejercicios y simulaciones.
- Fase de implantación y consolidación: la última fase reside en la toma de resultados y aplicación en las unidades reales de todas aquellas conclusiones y LLAA (Lecciones Aprendidas) que supongan una mejora para las FFAA (Fuerzas Armadas) del ET.

Hoy en día, el ET se encuentra en la segunda fase, habiendo designado a la BRILEG como punta de lanza para afrontar la puesta a punto del nuevo concepto de brigada polivalente y autosuficiente. (Terrestre, 2019) (Tierra, 2019)

1.2 BRILEG

Este proyecto se ha llevado a cabo en la Brigada 'Rey Alfonso XIII' II de la Legión, también conocida como BRILEG. Se trata de una de las seis Brigadas encuadradas en la División 'Castillejos', unidad perteneciente a la Fuerza Terrestre del Ejército de Tierra. La Legión Española se sitúa por tanto en las ciudades de Melilla, Ceuta, Ronda y Almería, siendo ésta última, Almería, el lugar en el que se han efectuado las seis semanas de investigación y experimentación de este trabajo.

Una vez que se instauró la Fuerza 2035, la BRILEG se ha convertido en punta de lanza del proyecto del Ejército de Tierra, convirtiéndose en BRIEX, y de esta forma implantando todas las posibles mejoras y realizando cambios en su estructuración, así como en su forma de proceder en el trabajo, con el fin de sacar resultados y encaminar al resto de Brigadas con las conclusiones sacadas de la BRILEG.

Con respecto al Proyecto de Fin de Grado que se llevó a cabo en esta unidad, se ha basado en una investigación sobre el posible hardening[3] que se puede integrar en la unidad, con el objeto de establecer ciertas políticas de seguridad y blindarlo de cara al programa maligno. Se centrará en la fortificación del entorno de Windows[4], ámbito de vital importancia durante el despliegue de los PCTAC[5] (Terrestre, 2019)De igual forma se pretende adoptar métodos con los que poder

[3] Hardening: Es un endurecimiento informático o fortificación, con el fin de reducir y evitar las amenazas

[4] Windows es el sistema operativo con el que se trabaja en este TFG. Se trata de un software el cual acepta funciones básicas. Se puede distinguir entre Windows de versión de escritorio, de uso en tareas diarias en oficinas y Windows Server es utilizado para efectuar servicios.

[5] PCTAC: Puestos de Mando Tácticos: Puestos donde el comandante encargado del ejercicio ejerce el mando y control de la unidad.

1.3. Motivación y Justificación del problema

Este trabajo ha sido motivado por diferentes razones, las cuales se van a explicar a continuación.

Cada ejército debe lidiar día a día con la lucha de no quedarse obsoleto, y es por ello por lo que, como solución, el gobierno destina parte del capital para poder dedicarlo a la adquisición de medios, mejoras de las infraestructuras, aumento de personal, investigaciones sobre nuevas formas de proceder ante las amenazas, etc. Sin embargo, es erróneo creer que la responsabilidad de que las FFAA no queden obsoletas recae única y exclusivamente sobre el Gobierno o JEME[6]. Los militares que conforman las FFAA tienen el deber y responsabilidad de buscar solución a cualquier obstáculo que se interponga en el cumplimiento de su misión, que es poder estar preparado para dar frente a cualquier amenaza que haya. Es por ello que la motivación reside en poder mejorar cualquier infraestructura que se considere posible desarrollar.

Partiendo de la base anterior, durante la estancia en la BRILEG, se buscaron ámbitos en los que poder mejorar la eficiencia de la Compañía de Transmisiones, de cara al despliegue de Puestos de Mando Tácticos de Brigada, y se observó que para el extendido de los medios se necesita cierta rapidez, sobre todo en el área de Sistemas de Información, y más concretamente en la configuración de los entornos de Windows. Esta configuración se hace de forma manual y llega a ser bastante laboriosa. Por lo tanto, se busca dar solución al problema del tiempo, por una parte.

Tener blindado todos nuestros dispositivos con el fin de mantener protegida nuestra información, es esencial de cara a poder superar al enemigo. Poder contar con un entorno securizado otorga cierta ventaja con respecto al adversario de cara a crear una planificación. El Ejército, es una de las instituciones que más información clasificada trabaja, la cual es de gran importancia para el enemigo. Por esta razón, se deben reflejar el mayor número de los 12 principios de seguridad (UNIR, 2022) de SW[7] (Software) en la configuración y despliegue de los centros de transmisiones[8], tanto en periodo de maniobras en territorio nacional, como en misiones en ZO (Zona de Operaciones). Por ello, resulta de vital importancia poder tener fortificado un entorno donde tener de manera segura todos aquellos documentos e información que podría querer adquirir el enemigo.

[6] JEME: Jefe de Estado Mayor del Ejército

[7] 1) Defensa en profundidad, 2) simplicidad en el diseño, 3) mínimo privilegio, 4) separación de privilegio, 5) separación de dominios, 6) separación de código, ejecutables y datos de configuración y programa, 7) entorno de producción o ejecución inseguro, 8) registro de eventos de seguridad, 9) fallar de forma segura, 10) diseño de SW resistente, 11) la seguridad por oscuridad es un error, 12) seguridad por defecto.

[8] Centro en el que despliega la CIA de Transmisiones junto con sus medios

1.4. Estructura de la memoria

Este trabajo se estructura es varios apartados, los cuales se van a explicar a continuación.

El primer punto que se va a explicar es la Introducción. En ella se dará a entender la importancia que tiene la Fuerza 2035 en este proyecto, junto con una breve exposición de la Brigada donde se han desempeñado las prácticas. Posteriormente se dará a conocer la motivación con la que se ha creado este proyecto.

En segundo lugar, tenemos los objetivos, metodología y tareas a realizar que se han llevado a cabo durante la realización de este proyecto, que determinan la meta que se quiere alcanzar y cómo se pretende llegar a ella (por medio de las tareas).

El tercer punto explica el contexto y el estado del arte que engloba el presente trabajo. En relación con el estado del arte están las aclaraciones respecto al despliegue de los puestos de mando tácticos, Windows Server, en concreto Windows Server 2016, conceptos básicos de seguridad y los pasos del proceso de hardening.

En el cuarto punto se encuentra el desarrollo del proyecto, en el que se explican los pasos que se han seguido para poder llegar a los resultados pertinentes, junto con breves aclaraciones de las opciones escogidas. Por último, se lleva el trabajo al ámbito real, replicándolo en un nodo[9].

En último lugar se tienen las conclusiones y las líneas futuras que se deben de coger para poder evolucionar en el proyecto.

[9] Lugar físico donde residen los servicios que proporciona el área de Sistemas de Información.

2. Objetivos y Metodología

2.1. Objetivos y alcance

Este proyecto presenta varios objetivos a alcanzar de acuerdo con las características que debería de tener un centro de Transmisiones en una Brigada y de acuerdo con el fin del Ejército, que es dar frente a las amenazas.

Como se ha dicho anteriormente, la motivación de este proyecto es poder lograr que el Ejército pueda evolucionar y desarrollarse para que en ningún momento se pueda decir que está obsoleto. Animado por esto, se buscan los objetivos con los que se podría lograr.

El primer objetivo que se busca es la reducción de tiempo dentro de la configuración del entorno de Windows durante el despliegue de los PCTAC. Alcanzar este objetivo es fundamental, ya que una disminución temporal supone en la mayoría de los ámbitos, poner a nuestro Ejército en superioridad con respecto al resto.

El segundo objetivo que se busca es la seguridad, es decir, efectuar el hardening del entorno de Windows. Esta segunda finalidad es igual de importante que la primera, en la cual una reducción de tiempo puede significar tener ventaja sobre el adversario, lo que es determinante en muchas ocasiones para poder alcanzar los objetivos. La protección de la información es crucial hoy en día, debido a los peligros informáticos que existen los cuales van mejorando sus técnicas de hurto en cada momento. Es importante tener cierta seguridad en nuestros equipos, pero sobre todo si se trata de equipos militares, los cuales contienen informes de alto secreto, muy precisado por el enemigo, el cual, si llegara a sus manos se dejaría de contar con ventaja al haber perdido la sorpresa.

El cumplimiento de estos objetivos nos asegura la superioridad con respecto al enemigo y, por tanto, poder realizar nuestros cometidos sin ningún tipo de impedimento. Es importante que el proceso de hardening esté realizado acorde a los avances que sufre la sociedad, para poder dar frente a las amenazas que vayan surgiendo con respecto a los avances que sufre la sociedad y sobre todo para poder seguir teniendo los mismos resultados que se buscan.

2.1.2 Alcance

Para poder conseguir los dos objetivos anteriores, se llevan a cabo una serie de tareas a realizar, y para ello se ha hecho una investigación y observación sobre las necesidades que se deben cubrir dentro de la BRILEG, en concreto de la CIA de Transmisiones, y posteriormente una recopilación de información y documentación.

El primer objetivo que se debe cumplir es el hardening del entorno de Windows de la BRILEG. Éste se conseguirá por medio de la investigación sobre máquinas virtuales[10] de la implantación de ciertas medidas de seguridad. Es por lo tanto el primer paso, la instalación de VMware para posteriormente creación de las máquinas virtuales que serán el entorno de pruebas del S.O[11]

[10] Máquina virtual: ordenadores de software que proporcionan la misma funcionalidad que los ordenadores físicos.

[11] S.O: Sistema Operativo. conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software.

que se utiliza en los PCTAC. Se crearán dos, unas con Windows Server 2016, y otra con Windows 10. Posteriormente, gracias al Server se creará un dominio[12] en el que se unirá la máquina con Windows 10, emulando un cliente. Este proceso de hardening incluye la configuración de diferentes aspectos de seguridad, tales como la implementación de una política de contraseñas, configuración del Firewall de Windows con seguridad avanzada, configuración del AppLocker y añadir cierto hardening en las directivas de grupo como especificar cuando debe acceder un usuario al sistema o cual dispositivo. Después se efectúan las pruebas pertinentes para comprobar que dicho hardening cumple con los requisitos establecidos, para posteriormente replicar el proceso en el nodo real de la BRILEG.

El segundo objetivo, la reducción del tiempo, se logra por medio de dos procedimientos. El primero de ellos se realiza por medio de la utilización de un Script[13]. El segundo procedimiento será la creación de un manual explicando detalladamente todo el proceso de instalación de VMware, creación de las máquinas virtuales y todo el desarrollo de hardening previamente explicado, junto con la utilización del Script.

Todas estas actividades expuestas se pueden contemplar de forma cronológica en el **ANEXO 1** cual representa una tabla que ordena las tareas según se han planificado temporalmente.

2.2. Metodología

Para poder poner solución a los problemas planteados anteriormente y alcanzar los dos objetivos propuestos se han utilizado diferentes métodos.

En primer lugar, se realiza una revisión bibliográfica para poder contar con toda la información existente sobre Windows, hardening y máquinas virtuales. Posteriormente se realiza el desarrollo experimental de las diferentes tareas anteriormente planteadas. Al finalizar la instalación y configuración se efectúan análisis de la pertinente configuración del entorno de Windows (para corroborar su grado de seguridad), entrevistas a los usuarios habituales sobre sus opiniones respecto al nuevo método y mediciones temporales para conocer cuánto tiempo se ahorra con el proyecto expuesto.

[12] Red de identificación asociada a un grupo de dispositivos

[13] Script: secuencia de comandos, que se utiliza para hacer referencia a un tipo de programa, que habitualmente suele ser simple. Estos comandos son leídos y son interpretados de manera que al descifrarlos se ejecutan los programas que contiene.

3. Contexto y Estado del Arte

Para poder entender la necesidad de fortificar el entorno de Windows, debemos de conocer el contexto que existe detrás, al igual que su evolución. El empleo de forma masiva de las tecnologías de la información y las telecomunicaciones (TIC), en la sociedad, ha creado un nuevo espacio denominado ciberespacio, en el cual proliferan los conflictos y agresiones y se atacará a la seguridad y prosperidad nacional por medio de ciber amenazas. Es por ello por lo que para mantener nuestra privacidad y no ser víctimas de ataques debemos de contar con un mecanismo de defensa informático, como el que este proyecto quiere exponer.

3.1. Contexto

Como se ha dicho anteriormente, las TIC evolucionan cada día, y es por ello, que es de vital importancia que el ejército esté constantemente contrarrestando estas nuevas formas de ataques por parte de las ciber amenazas. No solo se quiere un método con el que se pueda blindar los medios de los que dispone el ejército, si no también poder aplicarlo de forma rápida, fácil y eficiente. La transformación de la BRILEG que está experimentando para lograr convertirse en la fuerza que se espera en 2035, tiene bastante en cuenta los medios CIS[14] en este cambio. Es por ello, que se está construyendo una arquitectura que satisfaga las necesidades operativas en el escenario 2035 y sirva de referencia para la orientación de posteriores. (Tierra, 2019)

Dentro del objetivo que tiene la Fuerza 2035, la misión que desempeña en este ámbito pretende conseguir que las capacidades CIS, ciberguerra y guerra electrónica de Cuerpo de Ejército y División puedan permitir la sincronización de la maniobra y de los efectos de las unidades subordinadas en un entorno electromagnético degradado ante un oponente tecnológicamente avanzado. En un escenario de enfrentamiento de alta intensidad es donde los requerimientos CIS y CEMA (actividades Ciber-Electromagnéticas) de la Fuerza 35 son más exigentes, pues una de las claves del éxito está precisamente en la superioridad de la información y en disponer de un ciclo de la decisión más rápido que el del adversario.

La Arquitectura CIS en los niveles Cuerpo de Ejército y División debe permitir establecer la extensión del sistema de mando y control táctico desplegado, sirviendo por un lado a la integración con la I3D[15] del nivel estratégico, y por otro permitiendo la integración de las unidades en su zona de acción estableciendo una infraestructura integral CIS, táctica, móvil y que alcance hasta el nodo combatiente/sensor. (Ejército, 2020)

Los elementos que se identifican para ello deben dar respuesta al marco de referencia en el que a los condicionantes de dispersión, movilidad y redundancia en un ambiente electromagnético hostil se añade el amplio despliegue. Es por ello por lo que este proyecto debe de dar solución a la lentitud del área de Sistemas de Información a la hora de estar totalmente preparada, basándose en un nuevo método para poder agilizar una de las tareas que se requieren para llevar a cabo el correcto despliegue y extensión de los medios.

[14] CIS: Sistemas de Información y telecomunicaciones

[15] La I3D es una red privada con el objetivo de proporcionar servicios concretos para la defensa y seguridad nacional

3.2. Estado del Arte

A continuación, se va a desarrollar el estado del arte de los diferentes componentes clave para poder entender de manera correcta este Trabajo de Fin de Grado.

3.2.1. Despliegue de los PCTAC de Brigada

Poder saber, entender y comprender cómo despliegan los Puestos de Mando Tácticos de Brigada es imprescindible, ya que, sobre esta información se ha basado este proyecto, con el propósito de poder agilizar esta acción.

Con carácter general el CT (Centro Táctico) despliega acompañando a los elementos de Infraestructura y Seguridad del PC (Puesto de Mando) y también mantiene una estructura y prioridad de despliegue de Sistemas y servicios en función de la situación en la que se encuentre ya sea en movimiento, despliegue y repliegue. (Ejército, 2020)

Previamente al despliegue, se lleva a cabo un movimiento táctico a la zona donde se deseen asentar los medios y dar servicio. Durante este movimiento a la zona donde se quiera asentar la unidad, se dan una serie de acciones concurrentes al despliegue de medios y servicios. Esta serie de acciones son totalmente necesarias para poder llevar a cabo de manera eficaz el completo despliegue, como son, los tendidos de líneas entre CT y PC, activación de toda la energía eléctrica y enmascaramiento de todos los medios e instalaciones.

Una vez que se ha tenido en cuenta lo anteriormente citado, llega el movimiento hacia la zona donde se debe mantener el Puesto de Mando Táctico de Brigada. Durante todo este movimiento se tienen activados los servicios de RRC[16].

Para el despliegue del Centro de Transmisiones, hay que tener en cuenta ciertos factores. En un primer lugar, antes de proceder directamente con el despliegue, es necesario haber podido contar con un buen planeamiento, en el que se valoran factores tales como terreno, seguridad y enlace. Se debe sabe que cada área despliega sus medios independientemente del resto de áreas hasta el momento en el que hay que integrarlos entre sí, y por ello, se determina una lista en la que se priorizan los medios que deben ser los primero en establecerse, no sólo por su importancia si no también de acuerdo con su poca o alta complejidad. En primer lugar, se debe mantener el enlace de RRC durante el movimiento y durante todo el. Después, se debe establecer el enlace de RRC para los servicios de BMS entre PCTAC y Unidades Subordinadas. La siguiente fase viene con la conexión por medio de enlace. Por último, se instauran los servicios de radioenlaces entre los PCTAC para poder complementar o reanudar los servicios. (Terrestre, 2019)

Durante el despliegue de los Centros de Transmisiones de Puesto de Mando Táctico (CTPCTAC) es de vital importancia asegurar ciertas características como rapidez, seguridad, agilidad y eficiencia. Es por ello por lo que es imprescindible estar actualizado para poder contar con las mejores propiedades. (Terrestre, 2019)

Los centros de Transmisiones se componen de una rigurosa organización dividida en distintas áreas:

[16] RRC: Red Radio de combate. Comunicación por medio de Radio militar

- Área de explotación: En el área de explotación se incluyen los elementos de mando del centro y los medios CIS no radiantes, especialmente aquellos desde los que se entregan servicios a los usuarios. Sería aquí donde se encuadre la sección de Sistemas de Información, que es donde se enmarca este trabajo.

- Área herciana: En el área herciana se instalarán los medios radiantes del CTPC y los medios radiantes no pertenecientes al CTPC.

- Área de energía: En esta área se encuentran los medios de energía que abastecen de energía eléctrica a los distintos equipos de telecomunicaciones y medios de vida del CT, lo que permite:

    - Aprovechar mejor los medios mediante su alternancia en la producción de energía eléctrica.

    - Concentrar los puntos productores de ruido electromagnético.

    - Minimizar las interferencias que crean sobre los equipos de telecomunicaciones del CT.

    - Centralizar su mantenimiento y suministro.

    - Facilitar el enmascaramiento acústico del resto de áreas del CT.

Todas estas áreas se planifican y se estudian previamente al despliegue de acuerdo con una serie de factores como son el terreno, seguridad y, el más importante, el enlace con el PCAR (Puesto de Mando de Apoyo a Retaguardia). Tener una rápida capacidad de despliegue y repliegue es esencial ya que como se debe recordar, estas unidades se instruyen para poder dar frente al enemigo y trabajar bajo fuego y tensión. Es por ello por lo que se debe de dar especial primordialidad a todo aquello que el enemigo pueda utilizar para delatar la posición del CT. Todas estas áreas se representan de forma visual en el **ANEXO 2**, el cual es un ejemplo de la disposición de dichas áreas en el despliegue de los PCTAC.

Durante el despliegue cada área empieza a desarrollar su maniobra de forma individual hasta el momento de integrarlos los unos con los otros. Dentro de cada área se da una secuencia de acontecimientos para poder llegar a dar los servicios y medios CIS lo más rápido posible de tal forma que se pueda empezar a tener enlace con el órgano superior, que es con el que se tiene que contactar. Aun así, el servicio mínimo que se debe de tener nada más desplegar el centro de Transmisiones es el de RRC, el cual se basa en obtener servicios de Voz VHF y Voz y Datos de HF.

A la hora de replegar se sigue la secuencia inversa del despliegue, con el fin de mantener la capacidad de transmisiones y el flujo de información, de igual forma que un rápido repliegue de los medios. Al igual que en el despliegue el primer medio que se debe de tener activo es el de RRC, este servicio quedará activado durante el repliegue. (Terrestre, 2019)

Una vez que se ha expuesto brevemente la complejidad con la que trabajan los centros de Transmisiones es posible entender qué necesitan para poder mejorar su rendimiento o facilitar su maniobra. Por ello se cree conveniente incidir en el problema Tiempo, es decir, mejorar la rapidez en el despliegue, y en el problema Seguridad, esto es, poner barreras infranqueables de cara a que el enemigo no pueda obtener nuestra información y, por ende, sabotear nuestro objetivo.

En la siguiente imagen se puede observar un centro de Transmisiones camuflado.

Figura 2.Centro de Transmisiones. Imagen propia

3.2.2. Windows Server

Windows Server es el S.O utilizado en la BRILEG, y sobre el que se ha realizado este proyecto, y es, por lo tanto, de vital importancia poder conocer sus características y posibles funciones. Windows inició su vida con la intención de facilitar el empleo del ordenador, aunque como ya vemos, se ha convertido, hasta el día de hoy, en el sistema operativo más íntegro y completo. Windows es el pilar en donde se apoyan muchas aplicaciones a la hora de trabajar.

Windows Server es un sistema operativo cuya primera versión fue lanzada por la empresa Microsoft en el año 1993. Se trata de un sistema multiproceso y multiusuario el cual utilizan, hoy en día, millones de empresas debido a las ventajas y características que ofrece. (Stanek, 2017).Se trata de una organización con el objetivo de crear unas bases de aplicaciones conectadas, redes y servicios de web. Los servicios de red que se pueden disfrutar gracias a Windows Server son los siguientes:

-Uno de sus principales objetivos es compartir recursos de la máquina en sí

-Pueden soportar a varios clientes a la vez

-Permiten la gestión centralizada de una red

-Consienten la gestión centralizada de los usuarios

-Acostumbra a consentir la gestión centralizada de permisos y privilegios

-Disponen de herramientas para detectar posibles deficiencias de servicio

A continuación, se explican una serie de características que se pueden encontrar en Windows Server y las cuales tienen gran importancia en el trabajo, como son: Active Directory, AppLocker, controlador de dominio, directiva de grupo. (UNIR, 2021)

3.2.2.1 Active Directory

Active Directory permite administrar de una forma centralizada tareas de control de acceso y recursos para el resto de los clientes o usuarios que componen la red. Este directorio contiene toda la información sobre el entorno y dispositivos que hay, así como de sus directivas[17]. (Stanek, 2017)

Active Directory se encuentra estructurado de una forma bastante simple, se pueden diferenciar tres niveles, que son: dominios, árboles y bosques. Cuando se hace referencia a un dominio, se entiende que es un conjunto de usuarios que guardan relación entre sí, dispositivos y otros objetos, e incluso las unidades organizativas, es decir, empresas u organizaciones. Los dominios, al combinarse, forman un árbol, y éstos a su vez al combinarse forman un bosque. Es conveniente detallar que los dispositivos que se encuentren en bosques distintos no podrán tener relación alguna a no ser que los administradores creen una relación de confianza. (Windows, 2021). A continuación, se puede observar la siguiente imagen, haciendo referencia a como se estructura Active Directory.

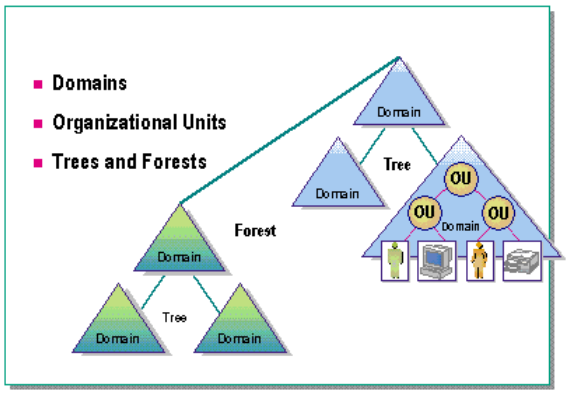


Figura 3. Estructura de un controlador de dominio. (Windows, 2021)

El hecho de utilizar Active Directory implica que dispondremos de ciertos beneficios, es por ello el motivo de su uso. Estos beneficios podrían resumirse en que hacen más simple la ejecución de las tareas de los administradores y de los usuarios, al mismo tiempo que implementa mejoras dentro de las organizaciones a través de las directivas de grupo de AD. Cada usuario que se haya registrado y autenticado dentro de un dominio en concreto podrá posteriormente hacer uso de los recursos dentro de dicho dominio siempre y cuando estén autorizados. Cabe destacar también que los documentos se almacenan en un repositorio centralizado, los cuales se pueden distribuir entre los usuarios para poder facilitar el trabajo grupal. (Jimeno, 2011)

El servicio más importante dentro del Active Directory es el Active Directory Domain Services (ADDS), el cual está integrado dentro del SO del Windows Server. Estos servidores que realizan el ADDS, son también denominados controladores de dominio o DC. Las modificaciones que se efectúen en el directorio del controlador de Dominio, como son modificaciones de contraseñas o usuarios, se actualizan directamente para poderse copiar y renovar en el resto de los controladores de dominio. En el caso de dispositivos que utilicen Windows (en vez de Windows Server), pueden pertenecer a un dominio y, por lo tanto, formar

[17] Directiva: Reglas que se configuran en el dispositivo para proteger sus recursos o de la red.

parte del Active Directory, pero, sin embargo, no ejecutarán ADDS [18]. (UNIR, 2021)

3.2.2.2. Controlador de Dominio

Son bastantes los servicios de los que podemos beneficiarnos de Windows Server, y algunos de ellos se exponen aquí:

- Servidor de DHCP: También conocido como 'Dynamic Host Configuration Protocol' se trata de un protocolo cliente/Servidor que proporciona de forma automática un host de Protocolo de Internet (IP) adjuntando su dirección IP[19], máscara de red[20] y puerta de enlace predeterminada[21] (CCN, 2018)

- Servidor de DNS: También conocido como 'Domain Name Service', se trata de un servicio de internet cuya función es traducir los nombres de los dominios en direcciones IP

- Controlador de dominio: Sirve para crear y controlar todas las configuraciones de los dispositivos que se encuentran integrados dentro de un mismo dominio. De todas las características importantes que nos ofrece Windows Server, podemos destacar Active Directory, la cual es la herramienta principal que se utiliza en este proyecto, junto con el servicio de Controlador de Dominio.

Como antes se ha mencionado ya, un controlador de dominio es una parte esencial del Active Directory, y, en otras palabras, se podría definir como el lugar donde se agrupan una gran variedad de componentes, los cuales están registrados en una base de datos. El controlador de dominio es por tanto el servidor que lleva a cabo las funciones de Dominio del Active Directory. (CCN, 2018)

Algunos de los beneficios que aporta la utilización de un controlador de dominio son:

-Tan solo se da permiso de acceso a aquellos que lo necesitan y están autorizados

-Consigue eludir las vulneraciones de datos de tipo "error del operador"[22]

-Puede bloquear un intento de acceso que no esté autorizado

3.2.2.3. Applocker

AppLocker es una herramienta avanzada cuya finalidad es el control de ejecución de

---

[18] AD DS se basa en varios protocolos y estándares establecidos, incluidos LDAP (protocolo ligero de acceso a directorios), Kerberos y DNS (sistema de nombres de dominio).

[19] Etiqueta numérica que identifica a un dispositivo en la red

[20] Distingue dentro de la dirección IP los bits que corresponden a red y a host

[21] Punto de enlace entre dos redes

[22] Error de operador: Estos tipos de errores son cometidos por el mismo operador del sistema, como son la falta de agudeza visual, descuidos, cansancio…

aplicaciones y scripts, y también archivos de Windows Installer[23], DLL[24], instaladores de aplicaciones, etc. Esta herramienta se utiliza en el presente proyecto para poder mejorar la seguridad. (CCN, 2018)

Esta herramienta es bastante manejable y sencilla, de cara a que los administradores del equipo puedan especificar exactamente qué se puede ejecutar en el entorno de escritorio. Gracias a esta herramienta, se puede:

- Evitar que el software provisto sin licencia pueda llegar a ser ejecutado si no está en una lista blanca de software permitido.

- Evitar y tener la posibilidad de denegar la ejecución de aplicaciones que no están dentro de la lista de permitidas y que igualmente puedan llevar programa maligno.

- Denegar que los usuarios de dicho entorno lleven a cabo aplicaciones que usen un gran ancho de banda innecesario o que alteren a dicho entorno de escritorio y que se agrande el costo de soporte y mantenimiento

- Consentir que se lleve a cabo la instalación de aplicaciones con sus posteriores actualizaciones permitidas por los usuarios y que tan solo los administradores puedan instalar y ejecutar dichas aplicaciones. (CCN, 2018)

3.2.2.4. Firewall de Windows de seguridad avanzada

El firewall de Windows defiende a los dispositivos ante una amenaza como la de ser invadido desde el exterior de forma e intención maliciosa. Este firewall se puede configurar de diversas formas dependiendo la utilidad que se le quiera otorgar. Se puede definir entonces dos tipos de interfaces, una más básica y otra más avanzada. (UNIR, 2021)

- Interfaz básica: Compuesta por tres tipos de perfiles (de dominio, privado y público) ha sido la que más mejoras ha experimentado a lo largo de su vida. El perfil de dominio es una agrupación de normas que se llevan a cabo cuando el dispositivo se encuentra dentro de un dominio corporativo. El perfil privado es utilizado cuando el dispositivo se encuentra dentro de una red privada, como es el caso de redes domésticas, o trabajo. Por último, se tiene el perfil público, el cual es recomendable utilizar cuando el dispositivo que va a conectarse no se encuentra en ambientes seguros, como lo son las redes públicas.

- Interfaz avanzada: Con esta otra opción se pueden editar las opciones que se encuentran dentro del Firewall de Windows y de esta forma se pueden modificar y configurar otras características, como aplicar restricciones de usuario o grupo y especificar las comunicaciones que se desean destilar.

El firewall de Windows con seguridad avanzado define unas reglas de filtrado para poder definir el tránsito de red entrante y saliente del servidor que debe ser permitido o denegado. (CCN, 2017)

[23] Aplicación en el S.O. de Windows para instalar software

[24] Archivos con código ejecutable que se cargan por medio de un programa del S.O.

El Firewall de Windows con seguridad avanzada nos puede ofrecer tres opciones de configuración, las cuales las detallaremos a continuación. Estas características se pueden diferenciar en tres tipos, de manera que, para cada conexión de red, sólo se empleará uno de estos perfiles:

- Dominio: Se pone en funcionamiento cuando el servidor no dispone de conectividad con un controlador de dominio por medio de la interfaz de red

- Privado: Se pone en funcionamiento cuando el servidor no dispone de conectividad con un controlador de dominio y la red a la que está conectado se ha categorizado como privada por el administrador.

- Público: Se pone en funcionamiento cuando el servidor no dispone de conectividad con un controlador de dominio y la red a la que está conectado no ha sido previamente categorizada por el administrador. (CCN, 2018)

3.2.2.5. Directiva de grupo

En este apartado se va a desarrollar el concepto de directiva de grupo o GPO (Group Policy Object), ya que, en el desarrollo del proyecto se exponen ciertas configuraciones que guardan relación con la directiva de grupo. Las directivas de grupo engloban a un conjunto de reglas, las cuales tienen la función de controlar el entorno de trabajo de todas las cuentas de usuario y dispositivos. En resumidas cuentas, facilita la gestión centralizada y configuración de los S.O, aplicaciones y las configuraciones de los usuarios dentro del entorno de Active Directory. Proporciona control sobre lo que pueden y no pueden hacer los usuarios. Con el diseño de una directiva de grupo se consigue que cada servidor pueda recibir las configuraciones de seguridad por medio de las directivas propuestas en los tres niveles jerárquicos siguientes (Windows, 2021):

-Nivel de Dominio: Para poder cumplir con los requerimientos comunes de seguridad, como son las directivas de cuenta y contraseña

-Nivel de Referencia: Para poder cumplir con los requerimientos de seguridad más específicos del servidor que son generales a todos los servidores miembros del dominio.

-Nivel de Rol: Para poder cumplir los requisitos de seguridad de los característicos del servidor

En la siguiente imagen se observa de forma visual los distintos tipos de niveles en las directivas de grupo

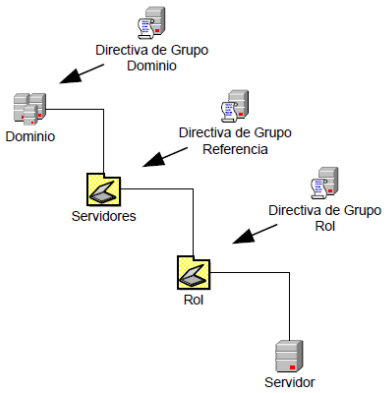


Figura 4.Ilustración de los distintos tipos de niveles en la directiva de grupo. (CCN, 2018)

3.2.2.6. Carpetas Compartidas

Las carpetas compartidas en Windows Server se crean con la finalidad de que sean un punto para el acceso a información tanto de usuarios como de administradores. Esta información se pone a su disposición y cada uno de los usuarios, dependiendo de los permisos que tengan, puede hacer un uso u otro con esa documentación. Esta característica dentro de Windows Server es uno de los elementos básicos para poder trabajar en colaboración, ya que se consigue un aumento de productividad inmediato debido a que los miembros de la red trabajan con la misma documentación, y que ésta se almacena como si se tratase del propio disco duro. (Microsoft.Shared Folders, s.f.)

3.2.2.7. PowerShell

PowerShell es otra de las herramientas que nos ofrece Windows, y la cual, tiene un papel importante en este proyecto, sobre todo a la hora de crear los usuarios. Se trata de una consola en la que se pueden utilizar comandos para automatizar diversas tareas. Es por tanto una solución de automatización de tareas multiplataforma formada por un Shell[25] de comandos, lenguaje scripting y un marco de administración de configuración. (UNIR, 2021)

3.2.3. Conceptos básicos de seguridad

La securización de un sistema implica la aplicación de principios y uso de conceptos de seguridad. Es por ello necesario dedicar unos apartados explicando todas estas ideas. En este apartado se abordarán los principios de diseño de seguridad, los cuales constituyen la base fundamental para poder utilizar de forma segura un dispositivo y no ser vulnerables frente a los ciberataques. A continuación, se detallan las principales técnicas de diseño de seguridad para tener en cuenta en este proyecto. (UNIR, 2022)

3.2.3.1. Principio de defensa en profundidad

Uno de los principios más importantes de una estrategia defensiva efectiva es la «Defensa en Profundidad», que se define en la guía CCN-STIC-400 (CCN, 2017) como: «Estrategia de protección consistente en introducir múltiples capas de seguridad, que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto».

Este principio propone un enfoque defensivo, que implanta protecciones o mecanismos de seguridad en todos los niveles del sistema o capas del modelo Open Systems Interconnection (OSI). Las medidas de seguridad a implementar en cada capa pueden variar en función del entorno de operación del sistema, sin embargo, el principio base o general permanece inalterable. (UNIR, 2021)

El principio fundamental detrás de este concepto es el de dificultar las acciones del atacante a través de las diferentes medidas de seguridad aplicadas a cada una de las capas de forma que los diferentes sensores que tenga nuestro sistema detecten las actividades maliciosas. Cuando una capa se vea comprometida, las medidas de detección, de reacción y de recuperación nos permitirán reaccionar, disminuyendo la probabilidad de que otras capas se vean

[25] Un Shell es la interfaz que sirve de intermediario para traducir comandos del usuario

comprometidas, evitando así, que la seguridad del servicio en su conjunto se vea burlada, disminuyendo por tanto el riesgo. (UNIR, 2022)

A continuación, se muestra una tabla con las distintas capas OSI, las amenazas a las que se enfrenta y los controles que efectúa.

Capa	Nombre	Amenaza	Controles
7	Aplicación	Intrusión Malware	Cortafuegos de aplicaciones, Antivirus
6	Presentación	Fuga de información Divulgación de contenido	Cifrado de datos sensibles
5	Sesión	Divulgación de datos Robo de credenciales Spoofing[26]	Control de autenticación y acceso
4	Transporte	Pérdida de paquetes Apertura de puertos	Monitorización de puertos
3	Red	Suplantación de identidad Spoofing	Cortafuegos Monitoreo del tráfico de red
2	Enlace	Ataques inalámbricos	Firewall, Filtrado de MAC
1	Físico	Accidente natural Robo	Virtualización Sistemas detección intrusión física

[26] Spoofing: Usurpar la identidad electrónica y así cometer delitos

0	Normativa	Ataque a la confidencialidad	Política de la seguridad Concienciación de la seguridad

Tabla 1.Principio de Defensa en Profundidad (UNIR, 2021)

3.2.3.2. Principio del mínimo privilegio

Por otro lado, se tiene el principio del mínimo privilegio, el cual consiste en conceder, tanto a usuarios, como procesos o dispositivos, el conjunto de privilegios mínimo más restrictivo con el que pueden desempeñar sus tareas autorizadas. Su finalidad se basa en limitar el agravio que puede resultar de un accidente, error o uso no autorizado. Además, reduce la cantidad de acciones potenciales entre los procesos predilectos o programas, y de esta forma, se minimiza la posibilidad de que puedan producirse empleos maliciosos de privilegios, no deseados o inadecuados. (Rambla, 2009)

Uno de los motivos esenciales por los que es indispensable que un individuo o grupo cuente con los mínimos privilegios posibles es debido a que, si se lleva a cabo un ataque informático en un proceso del sistema, éste debería de efectuarse con los mismos privilegios que tuviera un usuario en ese mismo proceso en el que se ha producido la intrusión maliciosa.

Este principio, exige que el diseñador efectúe un listado de los individuos de software con los recursos que utiliza y las labores que tiene que desempeñar dentro del sistema, detallando los privilegios mínimos necesarios que necesita cada entidad. (UNIR, 2022)

3.2.3.3. ENS y Dimensión segura

La finalidad del ENS es precisamente crear las condiciones necesarias para generar confianza «en el uso de los medios electrónicos a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos que permita a los ciudadanos y a las administraciones públicas el ejercicio de derechos y el cumplimiento de deberes a través de estos medios». (UNIR, 2022). Para cumplir con el ENS, en este trabajo se han utilizado las guías CCN-STIC, las cuales corresponden a normas o guías para poder tener un grado apto de ciberseguridad en los dispositivos u organizaciones. En este TFG se han utilizado las guías CCN-STIC 570A (Implementación de Seguridad sobre Microsoft Windows Server 2016) y CCN-STIC 599B19 (Configuración segura de Windows 10). Estas guías aseguran que los principios y dimensiones de seguridad (posteriormente citados) del ENS que se tienen que cumplir en este trabajo se abarcan sin ningún problema.

Los principios del ENS son los siguientes:

-Seguridad integral

-Gestión de riesgos

-Prevención, reacción y recuperación

-Líneas de defensa

-Reevaluación periódica

-Función diferenciada

El ENS trata las siguientes dimensiones de la seguridad (definiciones extraídas de la Guía CCN-STIC 800):

-Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

-Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

-Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

-Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

-Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Con base a estas dimensiones se calculan los impactos que tendrían los incidentes de seguridad sobre los sistemas afectados por el ENS y con ello se determinaría su categorización (básico/medio/alto).

De todos estos principios anteriormente citados este trabajo considera esenciales abarcar seguridad integral, líneas de defensa y reevaluación periódica, en cuanto a las dimensiones de seguridad, se considera importante abarcar todas, pero en especial las de confidencialidad, integridad y autenticidad, debido a la importancia que adquiere mantener seguros los documentos que maneja el E.T.

3.2.3.4. Política de contraseñas

Para garantizar un alto nivel de seguridad para las cuentas de usuario en el dominio de Active Directory, un administrador debe configurar e implementar una política de contraseña de dominio. La política de contraseñas debe proporcionar suficiente complejidad, longitud de contraseña y la frecuencia de cambio de contraseñas de cuentas de usuario y servicio como se verá a continuación. Por lo tanto, puede dificultar que un atacante utilice la fuerza bruta o capture las contraseñas de los usuarios cuando se envían a través de una red.

El formato más general para poder llevar a cabo la autenticación de usuarios es el empleo de contraseñas. El usuario debe recordar un ‘secreto’, que teóricamente, solo sabría él y el sistema. Para poder acreditar su persona, se necesitaría un nombre de usuario (identificación) y una clave o contraseña (acreditación). El dispositivo al que se intentaría conectar comprobaría la validez de las credenciales dadas y en caso de ser correctas, el usuario podría acceder al sistema. (Royer, 2004)

Desgraciadamente hay una gran cantidad de ataques a los sistemas de validación de usuarios basadas en contraseñas, cuyo objetivo es acceder no solo al sistema sino también a los mismos usuarios, ya que estos suelen considerarse el objetivo más fácil al que se puede llegar. Algunos de los ataques más comunes son:

-Ataques de diccionario o fuerza bruta: Este tipo de ataque se produce cuando el agresor trata de adivinar las credenciales apoyándose en datos que son públicos o sencillamente va probando con contraseñas de uso común, hasta poder tener las credenciales verdaderas.

-Keyloggers: Dispositivo hardware o módulo de software encargado de capturar cada una de las pulsaciones que se producen en un teclado.

-Phising: Este ataque se basa en hacerse pasar por un sitio verdadero para que el usuario introduzca sus credenciales.

Reutilización de contraseñas: Muchos usuarios utilizan la misma contraseña para distintos servicios distintos, y por ende, las credenciales que se almacenan en cualquiera de estos servicios queda expuesta.

En este trabajo se le da verdadera importancia a la política de contraseñas, ya que confiere seguridad a cualquier dispositivo que se le aplique, y al trabajar con material de alta relevancia es conveniente utilizarlas. Posteriormente se verá cómo se puede configurar. (Royer, 2004)

3.2.3.5 Script y CSV

Siguiendo con los conceptos básicos de seguridad, se procede a explicar qué es un Script y un archivo CSV, ya que se utilizan en este proyecto. Como se recuerda, el Script, es el término que se usa en programación para referirse a fragmentos de código que son utilizados para crear herramientas. Ese código es interpretado y ejecutado por el navegador, que en el caso de este proyecto se realizará por parte del PowerShell, en el cual se ejecutará el Script para poder crear a los usuarios de forma automática. (CCN, 2018)

Por otra parte, un archivo CSV, no es más que un archivo de texto, el cual contiene tablas de filas y columnas, rellenadas por caracteres separados por comas. Suele utilizarse el programa Excel para confeccionar un archivo CSV debido a que Excel identifica automáticamente los separadores y forma una tabla directamente. Este archivo CSV se utiliza cuando se tiene una gran cantidad de datos a emplear. Su principal uso es el de mover datos entre los programas. Estos archivos son fáciles de crear y se componen de un esquema bastante sencillo. En este proyecto se utiliza el archivo CSV para establecer los datos de los 15 usuarios a crear.

En este trabajo, estos dos conceptos se ponen en funcionamiento a la hora de crear de forma automática los usuarios, fin para el que se van a emplear.

3.3 Hardening

Se procede a explicar brevemente en qué consiste o de qué trata el proceso de Hardening. El Hardening, o también denominado como ‘endurecimiento informático’, es el nombre que se le da a todo proceso que tiene como objetivo principal conseguir reducir y evitar las vulnerabilidades, amenazas y peligros posibles que puedan surgir en un sistema. Para poder reforzar las zonas más vulnerables que puede tener un sistema, hay que reconocer las diferentes amenazas que puede haber (de esta forma se podrá enfocar el problema para poder dar una solución). Las posibles amenazas a las que nos enfrentamos serán:

-Cliente: Las modificaciones que puede realizar un usuario, en muchos casos son sin intención, como consecuencia del desconocimiento, aun así, pueden causar grandes males en la seguridad del equipo.

-Programas maliciosos: Programas cuyo objetivo consiste en querer perjudicar ya sea al equipo, usuario, empresa u obtener cierta información.

-Exploits: Se trata de fallas en el sistema de programación que suponen ‘puertas traseras’ que el pirata informático aprovecha para poder acceder al sistema y robar información.

-Intrusos: Usuarios sin autorización que han accedido al sistema.

-Acciones externas: Huracanes, terremotos, riada… que llegan a afectar a nuestro sistema.

Es importante el entendimiento de este apartado, ya que en él se asienta el trabajo presente, en un proceso de hardening informático. (CISET. Hardening, s.f.)

4. DESARROLLO: ANÁLISIS Y RESULTADOS

En este apartado se explicará el desarrollo que se ha hecho en este proyecto para poder llegar a los resultados que se buscaban. En primer lugar, se analizará la situación con respecto a la seguridad en la que se encontraba la BRILEG, y los puntos en los que se quiere mejorar su fortificación, incluyendo un estudio sobre los tiempos que tarda un administrado en configurar un entorno dentro de Windows. En segundo lugar, se desarrollará todo el proceso que se ha tenido que hacer en la creación de las máquinas virtuales para proponer las mejoras que se desean implantar. El tercer punto se centrará en la realización de pruebas y resultados para comprobar que con los métodos propuestos se agiliza la creación de un entorno de Windows. Por último, se hablará de la replicación al nodo de la BRILEG

4.1. Hardening a implantar en la BRILEG

Como se ha dicho anteriormente, la estancia de las seis semanas en la BRILEG se centró en la investigación de un método para mejorar la situación de la CIA de Transmisiones.

Por medio de la observación y la investigación de los integrantes de la BRILEG se dio a conocer su forma de trabajar. Actualmente, en los ejercicios de la BRILEG que requieren de la creación y configuración de un dominio se han detectado algunas carencias de seguridad en el despliegue de medios. La razón principal de este hecho viene promovida por la premura en el tiempo de ciertos despliegues y la inexistencia de dos maniobras o ejercicios idénticos. Normalmente, la creación de usuarios la realizan de forma manual. Esto genera mucha demora entre los administradores de los dominios. Además, dada la premura de ciertas actividades, tienen que priorizar en el funcionamiento del sistema y medios al propio hardening.

Para agilizar el proceso de configuración del dominio de Windows, se suelen guardar backups[27] de dicha configuración y realizar los cambios necesarios en los ejercicios venideros, pero se siguen arrastrando algunas carencias en la seguridad del sistema de ejercicio a ejercicio. El bien más preciado con el que juegan los administradores de BRILEG es el tiempo. Por esta razón, este trabajo pretende aportar, de manera constructiva, una metodología que les ayude a agilizar ese proceso de hardening y se implante en los backups.

A partir de las observaciones anteriores se ha desarrollado un método con el que poder agilizar y securizar la CIA de transmisiones durante el despliegue de los puestos de mando tácticos. A continuación, se muestra una tabla resumen de las medidas que se propone implantar según la Guía de seguridad de las TIC CCN STIC 599A (CCN, 2017) en BRILEG y la aplicación en el trabajo.

En naranja, se muestran aquellos aspectos que, aunque se encuentren implementados, se pretende mejorar la aplicación de los mismos gracias a la metodología que se diseña en el presente TFG.

En rojo, se muestran aquellos aspectos que no se encuentran implementados y pretende seguir complementando la seguridad de los medios en base a los 12 principios de seguridad mencionados con anterioridad y en base a la Guía de seguridad de las TIC. (CCN, 2017)

[27] Backup: Se trata de la expresión para referirse a un duplicado de información para poder recuperar los datos ante cualquier pérdida

La GPO existente en la CIA de Transmisiones de la BRILEG se compone de todos los aspectos que se desarrollan a continuación de color naranja, sin las mejoras que este trabajo desea implantar.

Medida	Implementación
Firewall	
Carpetas compartidas	
Script	
Directivas de grupo	
Política de contraseñas	
AppLocker	

Tabla 2.Medidas que se proponen implementar y grado de implementación actual

Con respecto al hardening se han llevado a cabo los siguientes pasos:

-Directivas de grupo: Se lleva a cabo el impedimento del acceso al panel de control, así como el bloqueo al cambio del fondo de pantalla. Con respecto a los usuarios, se les restringe el acceso a determinadas horas y en determinados dispositivos. En la BRILEG, actualmente solo se implanta el bloqueo al panel de control.

-Política de contraseñas, con el objetivo de implantar unos requisitos de contraseñas y fortificarla de cara a los intrusos.

-Configuración del Firewall de seguridad avanzada, con el objeto de establecer reglas de entrada, de salida y de la seguridad de la conexión. En el Firewall con seguridad avanzada, el proyecto plantea la creación de una nueva regla, la cual controle todas las conexiones de cualquier programa al dispositivo, y que permita dicha conexión si es segura, de igual manera esta se aplicaría a cualquier tipo de red y dominio. En la BRILEG solo se plantea el control de las conexiones por puerto TCP y UDP, conexiones que dentro del despliegue de los PCTAC se prevén que sean seguras.

-Configuración de AppLocker, con el objeto de poder tener el control de la ejecución de aplicaciones y scripts.

-Carpetas Compartidas: Se asignan carpetas compartidas exclusivamente a ciertos usuarios. La implementación que este proyecto aporta se basa en configurar y habilitar el acceso encriptado de archivos con el fin de garantizar que la información viaja de forma segura y confidencial, encriptado que no presentaba la BRILEG.

-Script: Para agilizar la configuración del entorno de Windows se propone implementar el uso de Script, para crear los usuarios automáticamente.

4.2. Desarrollo del proceso

Como se explicó anteriormente, en este apartado se expondrán los pasos a seguir para poder fortificar el entorno de Windows. Esta configuración del hardening del entorno de Windows, antes de plasmarlo directamente en el nodo de la BRILEG, se lleva a cabo en un entorno virtual de pruebas formado por máquinas virtuales. Se ha elegido trabajar con máquinas virtuales en este trabajo debido a que ofrecen una serie de ventajas, como son el aumento del tiempo de respuesta junto con los tiempos y plazos de productividad, los cuales se incrementan, los recursos que utiliza suelen ser mucho más rápidos, con su empleo se reduce el coste de la infraestructura, en concreto el físico y con su utilización, se reduce también el tiempo ejecutado externo al servicio. Otra de las ventajas se basa en que las máquinas virtuales proporcionan un entorno seguro, es decir, un espacio de ejecución aislado, donde poder ejecutar aplicaciones. La idea es que la máquina virtual provea un entorno seguro de ejecución para realizar las configuraciones de seguridad antes de plasmarlas en el nodo de la BRILEG. (VMware, s.f.). Estas máquinas virtuales tendrán como sistemas operativos Windows Server 2016 (el servidor) y Windows 10 (emulador de cliente).

4.2.1. Instalación VMware

Previamente a los siguientes pasos habrá que instalar el software de VMware Workstation Pro[28], sin embargo, se puede instalar cualquier otra de las versiones que VMware ofrece a los usuarios. Previamente a la instalación de la aplicación hay que tener en cuenta una serie de características las cuales debe tener el dispositivo con el que vamos a trabajar:

- Procesador de arquitectura de 64 bits mínimo
- Comprobar que se puede instalar en SO Windows y Linux
- La memoria RAM que se requiere debe de ser de 1 GB, aunque se recomienda que sea de 2 GB
- El disco duro debe contar al menos con 1GB de espacio libre para cada máquina virtual que se vaya a instalar

Durante el proceso de instalación, habrá que aceptar los términos de licencia, indicar la ubicación deseada para la instalación (en este caso se eligió que las herramientas de consola de VMware Workstatios se añadieran en la ruta del sistema. La instalación seguirá pidiendo que elijamos más opciones, las cuales serán marcadas si lo desea el usuario, ya que no implican que su elección o no impida el funcionamiento del programa. Por último, habrá que añadir el código de licencia obtenido y finalizar con la instalación. (VMware, 2017)

[28] VMware Workstation Pro: Estándar para la ejecución de varios sistemas operativos como máquinas virtuales en un mismo PC.

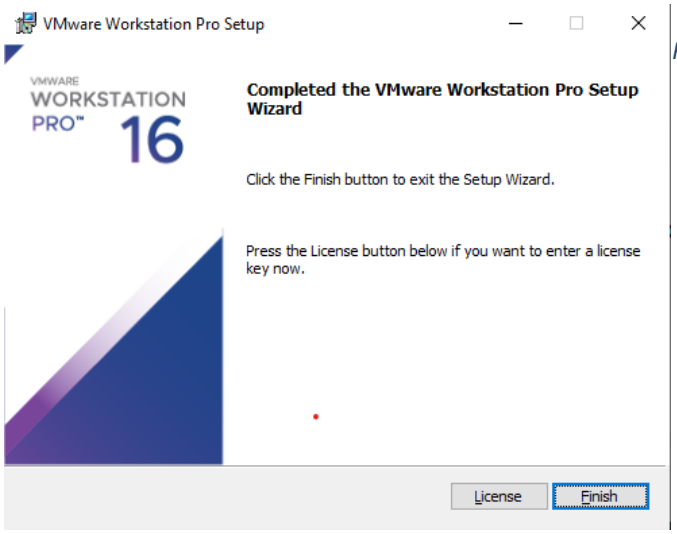


Figura 5. Instalación VMware

Una vez que la aplicación está ya instalada se procede a la creación de máquinas virtuales.

4.2.2. Creación máquinas Virtuales

Se van a crear en total dos máquinas virtuales, la primera será el controlador de dominio, y se instalará sobre Windows Server 2016, y otra máquina virtual que simula ser una máquina local, con Windows 10. El Dominio que se va a crear se llamará DOMINIO.ES. (VMware, 2017). Lo anteriormente dicho se puede observar en la siguiente figura, en la que las dos máquinas virtuales con sus respectivos S.O se encuentran dentro del dominio: DOMINIO.ES.

Figura 6.Estructura del dominio creado: DOMINIO.ES

Para llevarlo a cabo se tendrá que elegir la opción de '**Create a New Virtual Machine'.** A partir de aquí seleccionaremos las opciones que convengan a cada usuario. Cuando nos pida la imagen ISO[29] que se va a instalar en nuestra máquina virtual la elegimos mediante la opción que dice '**Installer disc image file'**. Es importante tener descargada la imagen ISO de nuestra máquina virtual previamente a la creación de esta. Finalizamos la creación de la máquina virtual. Una vez el proceso haya terminado, se nos mostrará en el panel izquierdo de la parte superior en la pantalla de inicio de la aplicación de VMware Workstation Pro, la máquina virtual creada. (Windows, 2021).

[29] Archivo ISO: Permiten almacenar carpetas de archivos, como archivos de sistema y de instalación de sistemas operativos

Para poder cumplir adecuadamente con la organización de las diversas tareas que se pueden ejecutar en el servidor, hay que tener en cuenta que existen dos grupos fundamentales:

- Roles: son empleados para definir una funcionalidad específica de un servidor, como pueda ser un servidor: Web, DNS, DHCP, etc.

- Características: son componentes autónomos de los roles pero que pueden servir de apoyo a algunos de los roles instalados.

El siguiente paso que se tiene que llevar a cabo será instalar el Active Directory junto con las características necesarias del mismo para poder llevar a cabo este proyecto.

Al iniciar Windows Server se muestra el panel que resume los servicios que se ejecutan en el servidor, y en la parte superior existen unos atajos para realizar unas acciones de forma rápida dentro del servidor. Entre estas acciones rápidas se encuentra la acción de “Agregar roles y características” con la que se configura el Active Directory (Microsoft, 2022)

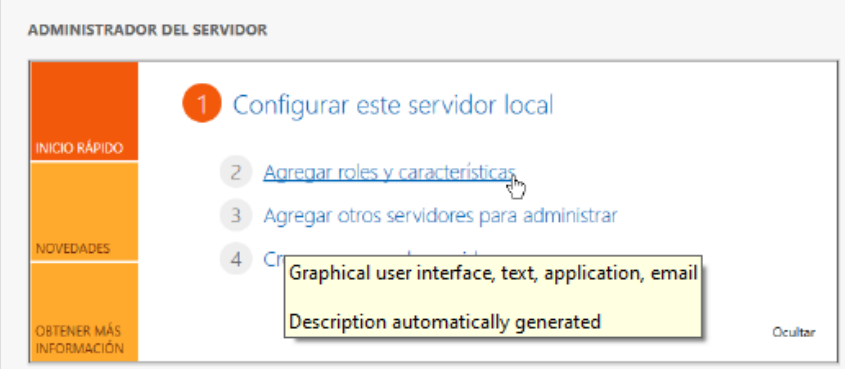


Figura 7.Administrador del servidor

Al seleccionar la acción se ejecuta un asistente para la configuración del servidor. Siguiendo las pantallas del asistente se selecciona “agregar el servicio de Active Directory” en el servidor que se ejecuta en la máquina. La instalación es sencilla, ya que en todas las pantallas hay que aceptar la configuración por defecto, excepto en la pantalla en la que se selecciona el rol de servidor donde se selecciona el servicio de dominio de Directorio Activo. (Microsoft, 2022)

La creación de las máquinas virtuales, así como la instalación del Active Directory se desarrollan ampliamente en el **ANEXO 3** y **ANEXO 4.**

4.2.3. Creación del dominio

Una vez que se ha llevado a cabo la instalación del Directorio Activo con sus roles y características, es necesario continuar con los siguientes pasos, los cuales nos ayudarán a poder realizar la configuración del Controlador del Dominio. Para poder ejecutarlo se dirigirá al Administrador del servidor y se procederá a la configuración. Habrá que pulsar la opción llamada: ‘Promover este servidor a Controlador de Dominio’. El siguiente punto para desempeñar será seleccionar la opción denominada: ‘Añadir un nuevo bosque’, y posteriormente se introducirá en el apartado de ‘Nombre de dominio raíz’, el nombre de nuestro dominio. (Microsoft, 2022)

Los siguientes pasos corresponderán con las elecciones correspondientes a las opciones del controlador del dominio. Se dejarán las opciones que ya están marcadas por defecto y se añadirán las casillas:

- Servicio de Sistema de Nombres de dominio (DNS)

- Catálogo Global (GC): Las funciones que realiza esta propiedad son la posibilidad de inicio de sesión y por otro lado las consultas de Microsoft Active Directory.

Será muy necesario que se recuerde en todo momento la contraseña de restauración de los servicios de directorios, debido a que, si en algún momento es necesario realizar una restauración, ésta será completamente imprescindible para poder llevar a cabo lo anteriormente mencionado.

Para poder finalizar con la creación de un dominio habrá que continuar con la realización de unos pasos más. Se requerirá que se indique un nombre de dominio de NetBios. Posteriormente se indicarán las rutas de acceso por las que se podrá acceder, y que se dejarán marcadas las que ya hay por defecto. Se revisarán todas las opciones que hemos configurado para poder tener la opción de modificar alguna antes de que se cree el dominio. Una vez que se ha terminado de verificar que todo está tal y como se requiere, pulsaremos en siguiente y se llevará a cabo una comprobación de que se cumplen cada uno de los prerrequisitos que requiere el sistema para que se pueda llevar a cabo la instalación. Señalamos, para finalizar, la opción de finalizar y posteriormente la máquina se reiniciará. Una vez que haya terminado la instalación de nuestro dominio, si se accede al Administrador del Servidor, se podrá observar que nuestro DNS se ha instalado de forma correcta y que tan solo faltaría proceder con la configuración de este. (Microsoft, 2022). Todos los pasos referentes a la creación del dominio se desarrollan más ampliamente en el **ANEXO 5**.

4.2.4. Creación de usuarios por medio del Script

En este apartado se llevará a cabo la creación masiva de usuarios pertenecientes a un grupo en concreto. Saber crear usuarios y a su vez poder asignarlos en un grupo es esencial de cara al perfecto funcionamiento de cualquier empresa o realización de trabajo y de cara al ahorro de tiempo. La creación de los usuarios se va a realizar a través de un Script que va a coger los datos de sus cuentas por medio de un archivo CSV, es decir, la lista de todos los nombres de usuarios y departamento en el que se encuentran se guarda en formato CSV (Excel) para posteriormente ejecutar un Script en PowerShell. Se crearán 15 usuarios y 3 grupos, dentro de los cuales habrá 5 usuarios en cada uno. Todos ellos se crearán con la finalidad de crear un entorno de prueba. La creación automática de usuarios se hace por medio de un archivo Script y los detalles de su configuración paso a paso se puede encontrar en **ANEXO 6**.

En primer lugar, se crea el archivo CSV, que no es más que un archivo de texto el cual contiene caracteres separados por comas. Este archivo se crea de forma manual en nuestro PC (no en la máquina virtual). Se utiliza el documento Excel para conformar estas columnas, en las que aparecen ‘Name’ (nombre de usuario), ‘Password’ (contraseña que tiene el usuario para acceder al sistema) y ‘Department’ (no es más que el grupo al que pertenece dentro de los tres que se crean). El archivo CSV y el Script se introducen en la máquina virtual como se observa en el **ANEXO 7**, que explica los pasos a seguir para introducir documentos desde el PC a la máquina virtual. Posteriormente se procede a crear los tres grupos que están previstos, manualmente dentro de la máquina virtual. Para finalizar se abre el PowerShell dentro de la máquina virtual, en el que introduciremos el Script para crear la creación automática de usuarios. Por medio del PowerShell se ejecuta el Script el cual abre el archivo CSV, por medio de la ruta en la que se encuentra, y lee cada línea de manera que va cogiendo los datos de cada usuario uno a uno y ejecuta los comandos “New-ADUser” y “Add- ADGroupMember” para crear los usuarios con los datos del archivo *CSV* y asociar el área que corresponde al usuario.

Este Script (Educaticaa, 2022) lleva dentro la ruta donde se accede al archivo CSV, para que

el PowerShell pueda utilizar esa información para la creación automática de usuarios. En la figura 9 se muestra el archivo Script, el cual, en el apartado de '#CSV path', vemos como referencia el lugar donde se encuentra el archivo CSV.

Figura 8.Archivo CSV

```
Name, Password, Department
Usuario01, Usuario.01, Grupo01
Usuario02, Usuario.02, Grupo01
Usuario03, Usuario.03, Grupo01
Usuario04, Usuario.04, Grupo01
Usuario05, Usuario.05, Grupo01
```

En la anterior imagen se muestra el archivo CSV donde se introducen los parámetros necesarios para que se creen los usuarios.

Para permitir la creación de más usuarios en un futuro con el mismo formato, al ejecutar el script se introduce la ruta del archivo CSV. Así, se evita el uso de un único archivo CSV y que el script sea más versátil. La creación de usuarios por medio de un archivo Script y los detalles de su configuración paso a paso se puede encontrar en **ANEXO 6**.

```
#Import modules
Import-Module ActiveDirectory

#CSV path
#$filepath = "C:\Users\Administrador\Desktop\usuarios01-50.csv"
$filepath = Read-Host -Prompt "Introduce el path del archivo CSV"

#Import CSV
$users = Import-Csv $filepath

#Read info of each user
ForEach ($user in $users){

    $name = $user.'Name'
    $password = $user.'Password'
    $department = $user.'Department'

    $secPassword = ConvertTo-SecureString $password -AsPlainText -Force

    #New-ADUser cmd
    New-ADUser -Name $name -AccountPassword $secPassword -Description $department -Enabled $True

    #Add-ADGroupMember cmd
    Add-ADGroupMember -Identity $department -Members $name
```

Figura 9.Script. (Educaticaa, 2022)

4.2.5. Carpeta compartida

En esta parte se configurarán las carpetas compartidas. La idea de este apartado se basa en que los usuarios correspondientes a un grupo utilicen la misma carpeta, de tal forma que tan solo cinco clientes correspondientes a un mismo grupo tienen permiso sobre una misma carpeta (en la BRILEG se configuran más de cinco clientes por cada grupo). Estas carpetas serán visibles tan solo a los usuarios que se quiera dar el permiso, de esta forma se restringe, aún más, el acceso a la información, ya que solo se puede tener acceso a los documentos que le competan, es decir se mantiene la confidencialidad y disponibilidad de estas según los principios de seguridad. En el caso de que un intruso informático pueda acceder al dispositivo, no sólo tendrá que sortear barreras como la política de contraseñas, firewall de seguridad avanzada, etc. si no que no le será posible acceder al contenido total de la información. Esta clase de propiedad es casi siempre una tarea prácticamente ordinaria y esencial en todas las organizaciones. Los pasos para desarrollar la configuración de Windows Server se pueden encontrar en el **ANEXO 8**, en el cual se explica cómo se crean las carpetas compartidas (Microsoft.Shared Folders, s.f.).

4.2.6. Directiva de grupo

A continuación, se va a definir una directiva de grupo que bloquee el acceso al panel de control e impida el cambio de fondo de pantalla a los trabajadores, incluyendo las restricciones a los usuarios a establecer conexión a ciertas horas y en ciertos dispositivos. (Active Directory Microsoft, s.f.).

Son dos los motivos por los que se bloquea el acceso al panel de control y a cambiar el fondo de pantalla. El primero de todos es evitar que otro usuario ajeno al sistema pueda acceder a esa ventana, y así estar seguro de que, en el caso de compartir el dispositivo con otro usuario, las aportaciones que se hayan hecho van a seguir intactas. El segundo motivo nace de que la mayoría de los usuarios que van a trabajar en los dispositivos no tienen amplios conocimientos, por lo tanto, para evitar que puedan desordenar inintencionadamente la configuración de red, personalización, privacidad, etc.

Otra de las opciones y medidas de seguridad que se aplican a los diferentes usuarios es el establecimiento de un rango de hora que controlará cuando se pueden y no conectar. Es importante definir un horario de inicio de sesión, por diversos motivos:

- Control de usuario.
- Control de los recursos del servidor.
- Realización del seguimiento de los accesos que no están autorizados.
- Gestionar tareas administrativas y de mantenimiento sobre el servidor.

Otra medida que se efectúa es limitar en qué dispositivo/s puede iniciar sesión un usuario en concreto. De esta forma, minimizamos, a su vez, las posibles incidencias maliciosas. Los motivos por los que, por otra parte, se implementan restricciones de horario a los usuarios, así como limitar accesos de inicio de sesión en otros dispositivos no autorizados, son debido a poder blindar aún más el PC frente al programa maligno. Cualquier intrusión en horario o PC no autorizado será una clara señal de intento de invasión. (Microsoft, 2022) (Active Directory Microsoft, s.f.) (GPOTechExpert TIPS., s.f.) (SYSADMIN, 2016). En el **ANEXO 9** se puede encontrar el desarrollo completo de la configuración de lo anteriormente citado.

4.2.7. Política de contraseñas

Como se ha explicado anteriormente es determinante en un centro de Transmisiones poder tener una política de contraseñas.

Desde el menú de Active Directory (configuración de contraseñas) se pueden cambiar los requisitos de las contraseñas del dominio. Se elige un nombre para la regla (“PASS”) y su número de precedencia [30]. Configuramos la longitud mínima de 10 caracteres[31] y un historial de

[30] Este número de precedencia determina la prioridad de la política de contraseñas. Si un objeto tiene asignadas varias políticas, se aplicará la política con el valor más bajo.

[31] Se recomienda que la longitud mínima de las contraseñas se establezca en 8 símbolos, un número menor implica poder sufrir robo de credenciales

10 contraseñas[32]. Desde el menú Añadir se puede seleccionar los grupos de usuarios a los que se quiere aplicar esta política, como los grupos que anteriormente se crearon. (Microsoft.Contraseñas, s.f.) (Windows, 2021).

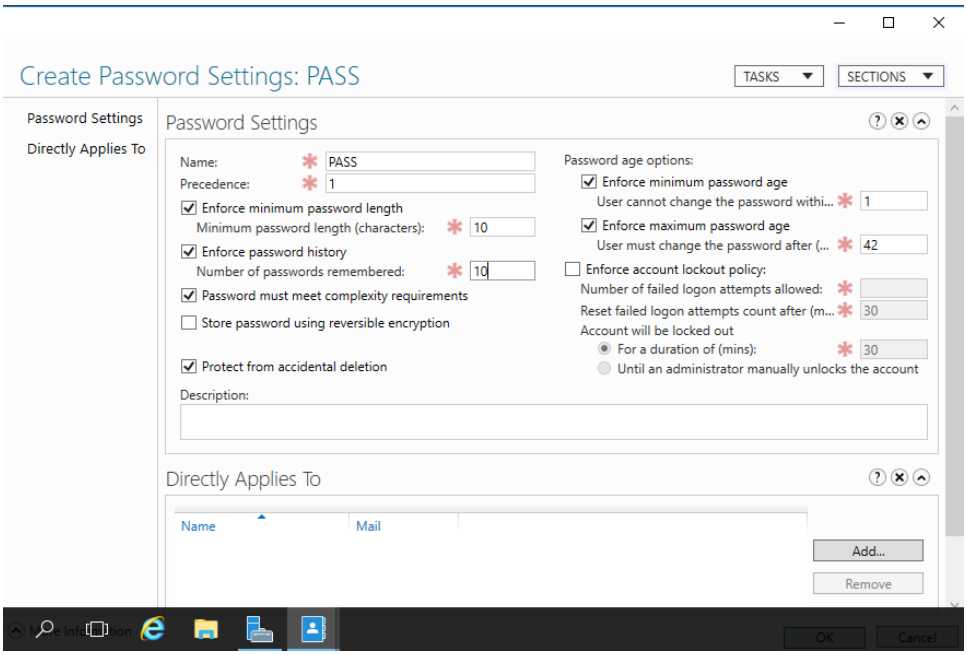


Figura 10.Política de contraseñas

En la anterior imagen se puede observar la pantalla principal donde configurar todos los campos necesarios para establecer una política de contraseñas.

La elección de estas características se basa en estudios publicados por INCIBE (INCIBE, s.f.) (Instituto Nacional de Ciberseguridad). La longitud mínima será de 8 caracteres como recomienda INCIBE, sin embargo, en el presente trabajo pondré 10 caracteres para poder aumentar la robustez y complejidad de la contraseña. Demandar el historial de las contraseñas determina la cantidad de contraseñas recientes únicas que tienen que vincularse con una cuenta de usuario previamente a que se pueda volver a utilizar una contraseña antigua. Se deben habilitar los requisitos de complejidad establecidos. Se deshabilita la opción de almacenamiento de contraseñas con cifrado reversible, ya que habilitarla significaría que las contraseñas cifradas se pueden descifrar. Se establece una vigencia mínima y máxima de la contraseña, para obligar al usuario a renovarla cada cierto tiempo. Se establece un número de intentos de sesión incorrectos permitidos, para evitar la intrusión por prueba y error de delincuentes, adjuntando también un bloqueo temporal de la cuenta una vez llegada a ese límite. Y, por último, se selecciona la casilla que permite que la cuente se desbloquee tan solo cuando el administrador lo haga de forma manual. (INCIBE.CERT, s.f.)

4.2.8. Firewall de Windows de seguridad avanzada

A continuación, se lleva a cabo la configuración del Firewall de seguridad avanzada de Windows. El desarrollo de dicha explicación se puede encontrar en el **ANEXO 12**, en el que

[32] El historial de contraseñas determina el número de contraseñas antiguas que se han almacenado en Active Directory, evitando que el cliente utilice una contraseña antigua.

aparece de forma más detallada. Se ha decidido configurar el Firewall de seguridad avanzada ya que permite proteger al dispositivo de dos formas distintas. La primera mediante el filtrado de tráfico de red controlado y la segunda, por medio de que admita IPsec[33]. La interfaz de este Firewall es mucho más extensa y adaptable que el Firewall de Windows Defender, el cual no concentra las características suficientes para ayudar a defender el tránsito de red. (CCN, 2018)

En este apartado se crea una nueva regla entrada dentro de este Firewall. Las reglas de entrada se definen por controlar el tránsito de red entrante a un programa o servicio que se especifique y, por lo tanto, bloquear las conexiones entrantes que no coincidan con una regla. Se tendrá que acceder a la consola de administración denominada 'Administrador de servidor', para posteriormente entrar dentro de la pestaña 'Configuración' y elegir la opción de 'Firewall de Windows con seguridad avanzada'. Se van a desplegar un glosario de las opciones de configuración que se pueden hacer. Dentro de estas, se elige la que se denomina 'Programa'.

Como se ha dicho antes esta nueva regla será del tipo 'Programa', en la que incluirá a todos los programas del dispositivo, y cuya finalidad se basará en que se permitirá la conexión con dicho programa si la nueva regla creada determina que sea seguro.

Posteriormente se permitirá a los usuarios que se han creado, que se incluyan dentro de la regla hecha con la finalidad de que todos se rijan con las mismas normas de seguridad y se pueda tener control sobre los programas que entran y salen del dispositivo. En el apartado en el que se pueden autorizar las conexiones con otros dispositivos, no se autorizará a ninguno, ya que no se contempla conexiones con otras computadoras según el uso que se le da en la BRILEG. En el caso de que el ejercicio cambie, se podrá modificar esta regla. Por último, esta regla se aplicará tanto cuando el dispositivo se conecte a un dominio corporativo, como a una red privada o a una red pública, y de esta forma se abarca todos los tipos de conexión. (Firewall, 2022)

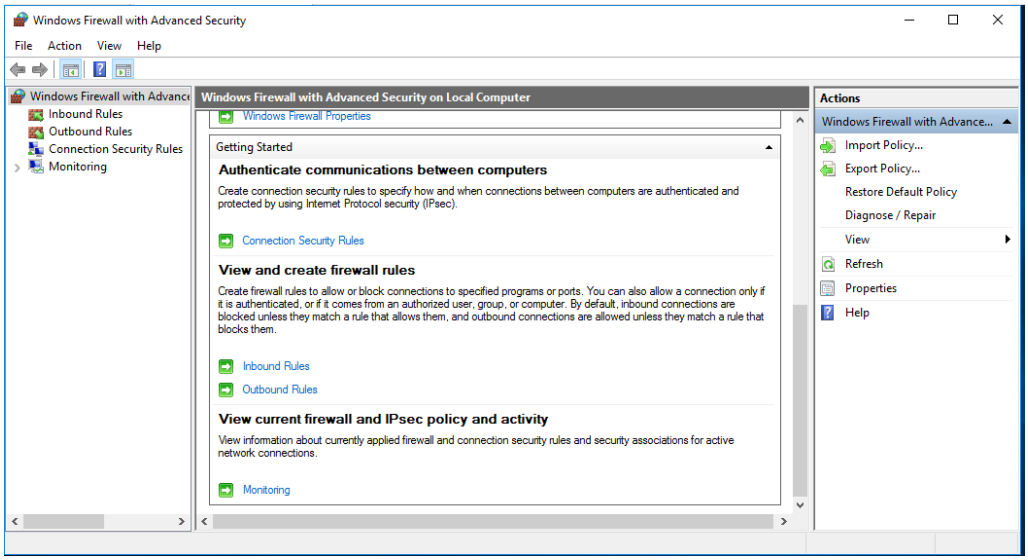


Figura 11.Nueva regla del Firewall

[33] IPsec asegura que se requiera autenticación desde cualquier dispositivo que intente comunicarse con nuestro PC.

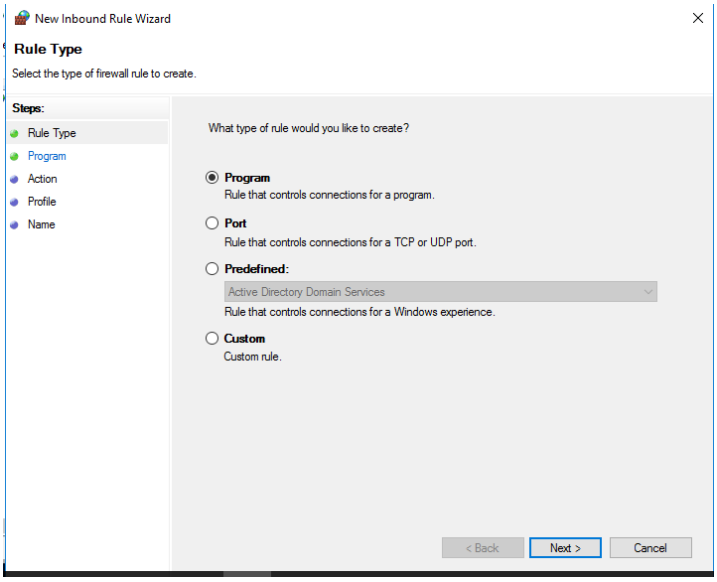


Figura 12.Apartados de creación de nueva regla

En estas dos imágenes se muestra, en la primera, la interfaz donde se accede para poder crear una nueva regla dentro del firewall de Windows de seguridad avanzada, y en la segunda, se ha accedido a la creación de la regla y se puede observar todos los diferentes apartados en los que configurar la norma.

4.2.9. AppLocker

En este apartado se explica el procedimiento llevado a cabo para configurar AppLocker. Dicha configuración, así como la creación de una nueva regla se puede observar en el **ANEXO 11**, donde se desarrolla de forma detallada.

AppLocker se utiliza en este trabajo debido a las funcionalidades que puede aportar al mismo. AppLocker posibilita el cumplimiento de ciertas medidas del ENS. Con AppLocker se puede tener un mayor control de lo que sucede dentro de puesto de trabajo, sobre todo, un mayor control sobre la ejecución de software. Con él, se puede evitar que se ejecute programa maligno o simplemente software no deseable por medio del control de una ruta de fichero o carpeta (se pueden controlar también por medio de firma de ficheros o publicador, pero en este trabajo es el anteriormente citado). Permite o bloquea rutas específicas de ficheros o carpetas. Por añadidura, los controles de ficheros pueden llegar extenderse a librerías de vínculos dinámicos del tipo '.dll'. Es por ello, que para tener control de estas librerías se debe habilitar el uso de las características avanzadas de AppLocker y habilitar las reglas DLL (paso que se muestra en el anexo).

En este trabajo se lleva a cabo la configuración de una nueva regla de AppLocker en la que se imposibilita la ejecución de aplicaciones provenientes de una carpeta, la cual es la carpeta en la que van a parar las descargas de programas. A esta nueva regla se anclarán todos los usuarios creados. (CCN AppLocker, 2015)

Como resultado de dicha configuración se obtiene la siguiente imagen, en la que se establece la nueva regla creada. En la última línea es donde se establece la regla en la que AppLocker deniega la ejecución de las aplicaciones provenientes de la carpeta seleccionada.

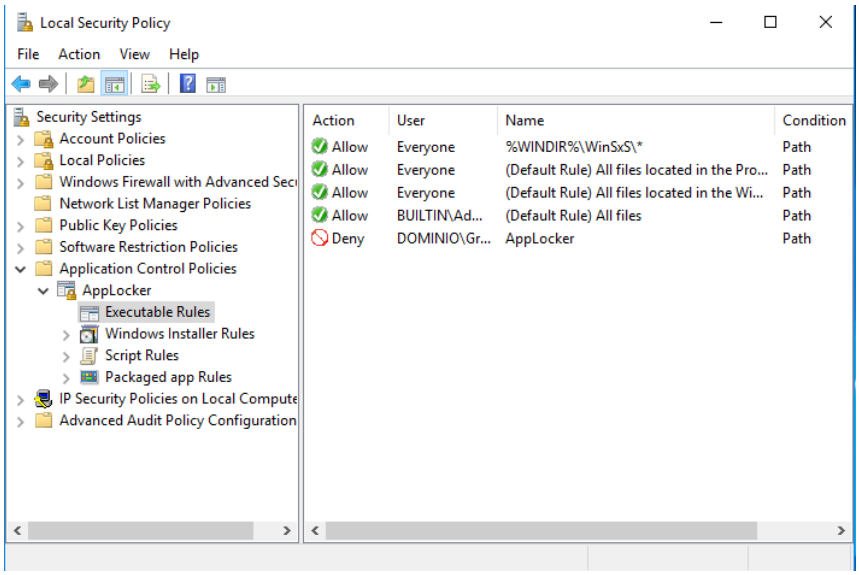


Figura 13. Resultado

4.2.10. Máquina local

Como cabe recordar, en este trabajo se van a crear dos máquinas virtuales, una con Windows 2016, en la que se procede a establecer la configuración de hardening informático y posteriormente la creación de una máquina virtual con Windows 10 emulando a un cliente que se enlaza con el dominio creado en el servidor. Se recuerda que en un primer momento se trabaja en un entorno virtual o de prueba para emular el nodo de la BRILEG para posteriormente proceder a su replicación si las pruebas sobre el entorno de prueba van acorde a los objetivos. En el **ANEXO 13** se puede encontrar los pasos a seguir para poder enlazar una máquina local (Windows 2010) a un servidor (Windows Server 2016). La finalidad de este paso es poner en funcionamiento las configuraciones hechas y poder ver si existe algún fallo o mejora. (Windows, 2022)

4.2.11. Pruebas y comprobaciones de la configuración

En este apartado se dan a conocer los resultados de las pruebas sobre la configuración de hardening hecha. El primer punto que se estudia es la comprobación del acceso a las carpetas compartidas. Como se explicó anteriormente, se han creado ciertos usuarios los cuales tienen determinados permisos para poder acceder a las caretas compartidas correspondientes o ciertas autorizaciones de cara al uso de la sesión que tiene permitido cada usuario. Dentro de la máquina virtual de Windows 10, se abre sesión con un usuario cualquiera de los que se han creado para hacer las comprobaciones pertinentes. Lo que se pretende a continuación es, mediante las configuraciones realizadas no se le ha dotado de acceso a ciertas carpetas y mediante la siguiente prueba se comprueba que realmente la configuración funciona y el sistema impide acceso a dicha carpeta. Dentro de la sesión de ese usuario elegido se intenta acceder a las carpetas compartidas a las que no tienen acceso y acceder en un rango de horas en el que no tiene ningún permiso. Si las configuraciones son correctas, un usuario con determinados permisos solo debe acceder a las carpetas a las que se le ha dado acceso y de igual forma, acceder a rangos de hora correctos. Como vemos en la siguiente imagen, se ha intentado acceder a una carpeta a la que no tenía acceso y no ha sido posible. El dispositivo lo detecta y envía un mensaje de que es imposible dicho acceso. (Lockhart, 2007)

Figura 14.Comprobación Carpeta Compartida

En la figura anterior se puede observar cómo, un usuario que no tiene acceso a la carpeta denominada Grupo01, intenta acceder a ella, pero, sin embargo, al no contar con los permisos pertinentes se le niega la entrada.

El siguiente punto que se comprobará será el intento de acceso al panel de control o el intento de cambiar el fonde de escritorio. Para ello abrimos sesión con un usuario aleatorio (ya que todos tienen incorporados esta norma), y dentro de su sesión se tratará de cambiar el panel de control o modificar el fonde de escritorio. Como se verá, es imposible, y aparecerán mensajes de error, como los que se enseñan a continuación.

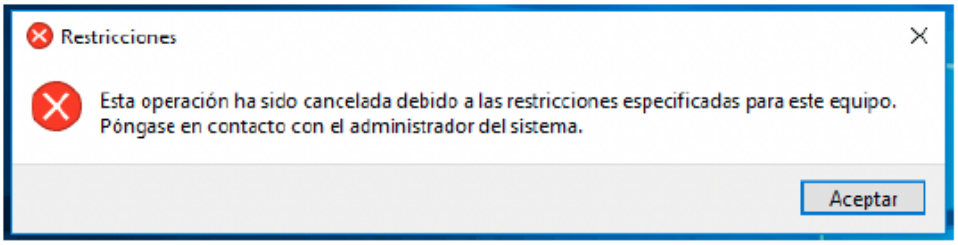


Figura 15.Acceso denegado a panel de control

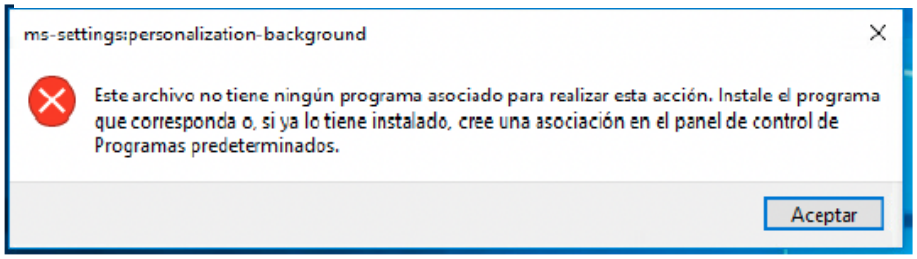
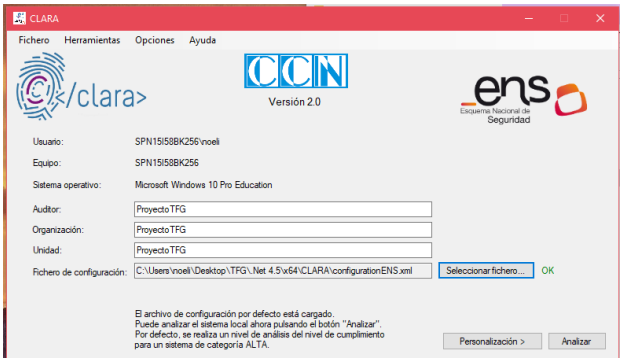


Figura 16.Acceso denegado a fondo de escritorio

El siguiente punto será la comprobación del cambio de contraseñas. Se elige un usuario cualquiera con el que iniciar sesión. Al iniciar sesión por primera vez en un usuario del grupo, se nos pide realizar un cambio de contraseña. Si tratamos de introducir una contraseña que no cumple los requisitos de longitud, nos aparece un mensaje de error. Cuando elegimos una contraseña con más de 10 caracteres, el sistema la acepta.

Por último, se hará uso de CLARA[34]. (CLARA, s.f.). Esta herramienta realiza un análisis del equipo para poder comprobar que se cumple total o parcialmente las reglas de seguridad proporcionadas por el ENS. Este análisis se basará en su plenitud en las características que constituyen dicho dispositivo a analizar, teniendo como referencia las plantillas de seguridad, según las guías de uso de CCN-STIC.

Figura 17.Aplicación CLARA



Una vez que se ha instalado la aplicación de CLARA, podremos comenzar a ejecutar el análisis de la configuración de seguridad hecha en la máquina servidor. El funcionamiento de esta herramienta es bastante sencillo. Se tiene que definir el nivel de análisis con el que se quiere trabajar. Dichos niveles pueden distinguirse como: bajo, medio o alto. La elección de estos niveles estará determinada, en este caso, por el tipo de ejercicio que vaya a desarrollar la BRILEG, como son, por ejemplo, ejercicios de instrucción y adiestramiento o maniobras. Para comenzar el estudio se ejecuta el análisis, y posteriormente se pueden consultar los resultados. Los distintos informes que genera la aplicación de CLARA, se pueden diferenciar en dos tipos:

-Informe ejecutivo: Este informe coge las conclusiones obtenidas del análisis basado en las normas de la ENS

-Informe técnico: Este informe coge los resultados de cada una de las variables que se han evaluado para que puedan cumplir el ENS en el nivel correspondiente.

Estos informes valoran los parámetros que se han analizado conforme a un porcentaje, en el que el 100% es que está todo correcto y el 0% indicaría que existe una gran falla de seguridad.

En relación con el análisis realizado con la aplicación CLARA dentro del nivel ALTO en las máquinas virtuales creadas podemos concluir que:

-Por la parte del informe ejecutivo, la configuración hecha de seguridad tiene un 'Cumplimiento del Sistema' de un 86,23%. Este porcentaje es el resultado de la media de distintos parámetros, de los cuales destacan los siguientes con sus respectivos porcentajes: Proceso de gestión de derechos de acceso con 70%, configuración de seguridad con 88,89%, protección de equipos informáticos con 100%, mecanismos de autenticación con 77,92% y protección de frente a código dañino con 83,56%. Estos han sido algunos de los parámetros utilizados en el

[34] CLARA: Herramienta para analizar las características de seguridad técnicas definidas a través del Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

estudio.

-Por la parte del informe técnico, la configuración de seguridad realizada obtiene un cumplimiento del valor de criticidad de un 82,46%. Este porcentaje es resultado de la media obtenida del análisis de otros parámetros, algunos de los cuales, junto con sus porcentajes, se citan a continuación: Gestión de cambios con 100%, registro de actividad de los usuarios con 88,89%, directivas del sistema de ficheros con 100%, directivas de servicios del sistema con 88,32%, protección de la autenticidad y de la integridad con 92,03% y acceso local con 79%.

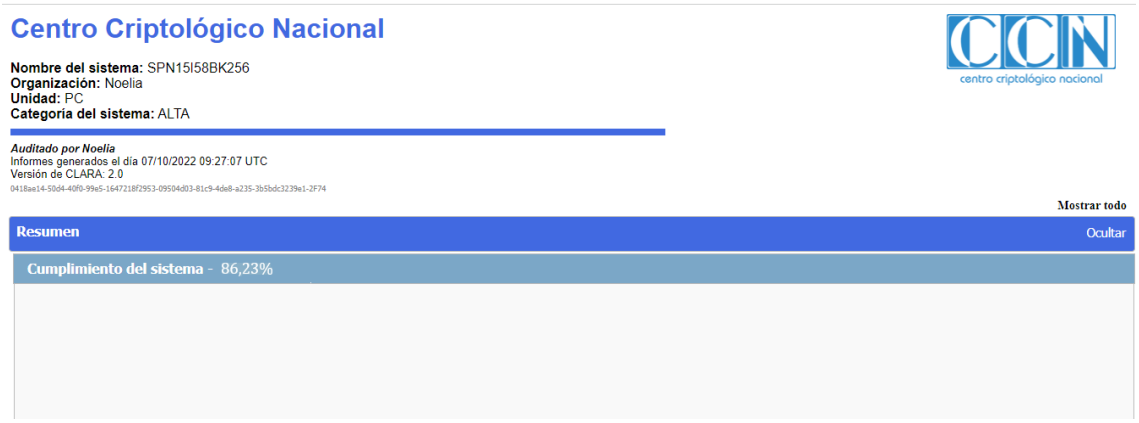


figura 18.Informe técnico

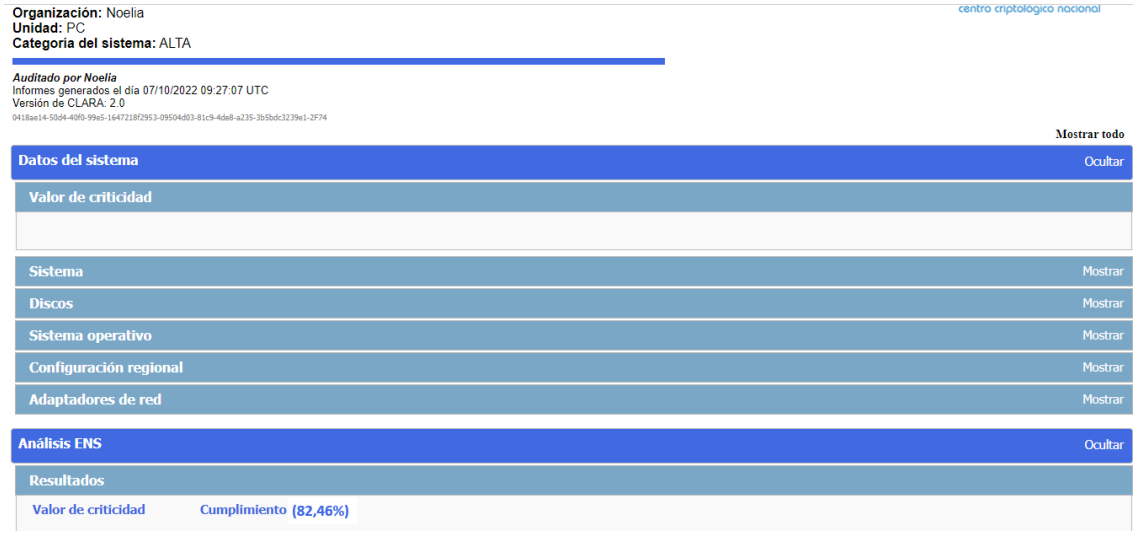


Figura 19.Informe ejecutivo

En estas dos imágenes podemos observar los resultados de los informes ejecutivo y técnico (se ven al final de las imágenes). Estos resultados concluyen que la configuración del hardening propuesto cumple con los objetivos que se buscaban. Estos dos informes tienen las mayores puntuaciones en los apartados referentes a 'proceso de gestión de derechos de acceso', 'registro de actividad de los usuarios', 'protección de los registros de actividad', 'gestión de cambios' y 'protección de equipos informáticos'. Sin embargo, obtiene bajos porcentajes dentro de los apartados de 'protección frente a código dañino' y 'bloqueo de puesto de trabajo'. Cabe decir que, aunque estos dos últimos apartados sean los de más bajo valor de porcentaje, sí cumplen con los valores que se pretende alcanzar.

4.2.12. Líneas futuras

A lo largo del proyecto se han planteado una serie de mejoras que no han podido llegar a ser ejecutadas por falta de tiempo y medios disponibles. A continuación, se citan dichas mejoras:

-Configuración de la UAC[35], la cuál es un control de seguridad cuya función a la que está destinado es avisar y, si es el caso, impedir que se procedan a efectuar cambios no autorizados en el dispositivo.

-Directivas de clave pública: Estas directivas se usan para poder controlar el cifrado del sistema de archivos, protección de datos y el cifrado del bitlocker[36]. También incluye rutas de acceso de certificado y configuración de servicios.

-Directivas de restricción de software: Estas directivas tienen la misión de identificar el software y mantener controlada su capacidad de ejecución situado en el dispositivo local, unidad organizativa, dominio o sitio.

-Restringir la instalación de controladores de impresora por parte de los usuarios: Con esta directiva se determina que usuario tiene los permisos para poder instalar un controlador de impresora

-Forzar la protección con claves de alta seguridad para las claves de usuario almacenadas en el dispositivo. (Windows, 2021)

4.3. Replicación al nodo de BRILEG

Una vez que se ha observado el correcto funcionamiento sobre las máquinas virtuales, se lleva a cabo la configuración propuesta del presente TFG en el nodo de la BRILEG.

Figura 20.Replicación nodo BRILEG

En la anterior figura se puede observar un nodo de la BRILEG, lo que es un servidor. El nodo se configura con el hardening propuesto en la máquina virtual server, es decir, esta configuración se instala en el servidor del nodo de la BRILEG, en el que se anclarán los usuarios con sus distintos PC dentro del dominio creado y conforme a las normas y reglas

[35] UAC: El control de cuentas de usuario evita que programas tipo programa maligno puedan instalarse automáticamente

[36] BitLocker: Es una aplicación de cifrado que permite proteger el disco duro de un posible robo

establecidas en el hardening, el cual está plasmado en el manual conformado desde el anexo 3 al 13 y que ha servido de guía para su implementación en dicho nodo. Una vez que se ha llevado a cabo la replicación pertinente y se observa que los resultados son favorables se llevan a cabo ciertos informes para determinar si por medio de este hardening, la BRILEG ahorra tiempo de cara a la configuración de los entornos de Windows durante el despliegue de los PCTAC. De igual forma se realizan entrevistas a dichos usuarios que se encargan de establecer la configuración para conocer su perspectiva sobre esta nueva forma de proceder, con el propósito de saber si el estudio ha incidido de forma positiva o negativa en los militares de la BRILEG.

Tabla 3.Cálculo de tiempos

	Usuario1	Usuario2	Usuario3	Usuario4	Usuario5	Usuario6	Usuario7	Usuario8	Usuario9	Usuario10
Implementa TFG	0º10’27’’	0º11’31’’	0º9’02’’	0º11’24’’	0º10’39’’	0º10’11’’	0º11’04’’	0º10’28’’	0º9’49’’	0º10’42’’
Sin implementar TFG	0º15’56’’	0º18’27’’	0º16’40’’	0º14’21’’	0º16’23’’	0º13’02’’	0º15’32’’	0º13’31’’	0º13’23’’	0º14’18’’

Esta tabla contiene 10 columnas que representan a 10 militares encargados de la configuración de Windows, y dos filas, las cuales representa el tiempo tardado en configurar el entorno de Windows sin y con el hardening propuesto.

En esta tabla se puede observar que se ha escogido una muestra de 10 militares encargados de la configuración de Windows durante los despliegues de los PCTAC, los cuales, en primer lugar, han configurado el entorno de Windows sin aplicar el nuevo método, y en segundo lugar han aplicado el nuevo método propuesto. En los dos casos se ha cronometrado el tiempo que se tarda en realizar por completo una configuración entera.

Como se observa representa una mejora, aunque sea de 0º3’45’’ de media.

Empleo y nombre	Comentario
Cabo 1º Juárez	Implementaré este método, porque, aunque sea de dos minutos la diferencia, es mejor que el anterior método utilizado
Sgto. Cristóbal	Con respecto a nuestro método, éste implementa más securización
Sdo. García	Me resulta más sencillo seguir este manual, ya que nosotros no tenemos ninguno
Cabo. Ramos	Prefiero seguir este método al que ya teníamos, implementa más seguridad y con el manual se hace más fácil

Tabla 4.Comentarios después de la utilización del método

Referente a la descripción de esta tabla se observa que existen dos columnas, la primera representa el nombre y el empleo de los cuatro militares entrevistados y la segunda los comentarios hechos por los mismos.

Esta tabla representa las impresiones que han tenido 4 militares encargados de la configuración de Windows en el despliegue de los PCTAC. Como se observa estas opiniones resultan ser todas positivas y los comentarios con respecto a la nueva propuesta han resultado tener un aspecto favorable y de mejora con respecto al anterior método.

5. CONCLUSIONES Y LÍNEAS FUTURAS

A continuación, se exponen brevemente las conclusiones de este proyecto junto con las líneas futuras surgidas a lo largo del mismo

5.1 Conclusiones

El fundamento de este proyecto se basa en poder mejorar las características en el ámbito de las transmisiones, en concreto dentro del marco de la BRIEX y el enfoque se ha centrado en el ahorro de tiempo de cara al despliegue de los PCTAC y mejorar la seguridad de los entornos de Windows dentro de éstos, en concreto en la BRILEG. Para poder conseguir dichos objetivos se lleva a cabo, por un lado, la configuración del entorno de Windows del nodo de la BRILEG. Este hardening se fundamenta en la configuración de directivas de grupo, firewall de Windows de seguridad avanzada, política de contraseñas, creación de carpetas compartidas y AppLocker. Por otro lado, para poder ahorrar tiempo, se crea un manual con todas estas configuraciones y se implementa el uso de Script (para automatizar la creación de usuarios). Posteriormente se realizan pruebas para comprobar la funcionalidad de estas. En vista a los resultados obtenidos, los análisis de CLARA muestran que la configuración propuesta cumple con los estándares de hardening que se buscan, y las pruebas sobre el nodo de la BRILEG demuestran que funcionan de forma correcta. Los resultados muestran que se mejora la seguridad con respecto a la anterior configuración del nodo de la BRILEG y que se ahorra tiempo. Es por tanto conveniente decir que los objetivos se han cubierto satisfactoriamente, y es por ello por lo que a la BRILEG se le ha proporcionado una copia de este manual para poder llevarlo a cabo en los ejercicios que vayan a efectuar. Se insta a la BRILEG, a implementar este nuevo método en sus tropas.

Bibliografía

Active Directory Domain Services, 2022. *Novedades sobre la instalación y eliminación de Active Directory Domain Services.* [En línea] Available at: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/deploy/what-s-new-in-active-directory-domain-services-installation-and-removal

Active Directory Microsoft, s.f. *Cuentas con privilegios y grupos de Active Directory.* [En línea] Available at: https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory

AppLocker, s.f. *Cómo funciona AppLocker.* [En línea] Available at: https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-defender-application-control/applocker/how-applocker-works-techref

CCN AppLocker, 2015. *Implementación de AppLocker.* [En línea] Available at: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/1159-ccn-stic-869-implementacion-de-applocker-en-el-esquema-nacional-de-seguridad/file.html

CCN, 2013. *Guía de Seguridad de la STIC. Manual de Seguridad de las Tecnologías de la Información y Comunicaciones.* s.l.:s.n.

CCN, 2018. *Implementación de Seguridad sobre Microsoft Windows Server 2016.* s.l.:s.n.

CISET. Hardening, s.f. *CISET. Hardening.* [En línea] Available at: https://www.ciset.es/publicaciones/blog/746-hardening

CLARA, s.f. *Guía para la utilización de CLARA.* [En línea] Available at: https://loreto.ccn-cert.cni.es/index.php/s/UFYYHR2n0YyFu7O

Educaticaa, 2022. *Script para crear usuarios.* [En línea] Available at: https://www.educatica.es/informatica/sistemas-operativos/windows/scripts-windows/script-para-crear-usuarios/

Ejército, E. M. d., 2020. *Conceptos de Transformación FUERZA 2035,* s.l.: s.n.

Firewall Rules, s.f. *sys.firewall_rules.* [En línea] Available at: https://learn.microsoft.com/es-es/sql/relational-databases/system-catalog-views/sys-firewall-rules-azure-sql-database?view=azuresqldb-current

Firewall, 2022. *Firewall de Windows Defender con seguridad avanzada.* [En línea] Available at: https://opdhsblobprod04-secondary.blob.core.windows.net/contents/4960c3bad9654704b3e1888df466a99c/86b9d278d60c331c738bcfa0df90aa6c?skoid=2d004ef0-5468-4cd8-a5b7-14c04c6415bc&sktid=975f013f-7f24-47e8-a7d3-abc4752bf346&skt=2022-11-08T05%3A55%3A00Z&ske=2022-

Firewall, s.f. *Configure the Windows Firewall to alow SQL Server Access.* [En línea] Available at: https://learn.microsoft.com/es-es/sql/sql-server/install/configure-the-windows-firewall-to-allow-sql-server-access?view=sql-server-ver16

GPOTechExpert TIPS., s.f. *Impedir acceso a panel de control.* [En línea] Available at: https://techexpert.tips/es/windows-es/gpo-impedir-el-acceso-al-panel-de-control/

Holmes, L., 2019. *Powershell Cokkbook: Complete Guide to Scripting.* s.l.:s.n.

INCIBE.CERT, s.f. *INCIBE. Política de contraseñas. CERT.* [En línea] Available at: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

INCIBE, s.f. *INCIBE.* [En línea] Available at: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

Jimeno, M. T. M. C. H. E. C. M. Á., 2011. *Destripa la Red.* Madrid: EJEMP Multimedia.

Lockhart, A., 2007. *Seguridad de redes, los mejores trucos.* Madrid: EJEMP Multimedia.

Microsoft.Administrar AppLocker, s.f. *Administrar AppLocker.* [En línea] Available at: https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-defender-application-control/applocker/administer-applocker

Microsoft.AppLocker, s.f. *¿Qué es AppLocker?.* [En línea] Available at: https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-defender-application-control/applocker/what-is-applocker

Microsoft.Contraseñas, s.f. *Directiva de contraseñas.* [En línea] Available at: https://learn.microsoft.com/es-es/sql/relational-databases/security/password-policy?view=sql-server-ver16

Microsoft.Diseño AppLocker, s.f. *Guía de siseño de AppLocker.* [En línea] Available at: https://learn.microsoft.com/es-es/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-design-guide

Microsoft.Shared Folders, s.f. *Configure and manage shared folders.* [En línea] Available at: https://learn.microsoft.com/en-us/training/modules/configure-manage-shared-folders/

Microsoft, 2022. *Directiva de Grupo.* [En línea] Available at: https://learn.microsoft.com/es-es/azure/active-directory-domain-services/manage-group-policy

Profesional, M., 2018. *Introducción a los sistemas operativos en red.* [En línea] Available at: https://www.macmillaneducation.es/wp-content/uploads/2018/10/sistemas_red_advantage_multimedia.ppt#:~:text=Permiten%20la%20gesti%C3%B3n%20centralizada%20de,detectar%20posibles%20deficiencias%20de%20servicio.

Rambla, J. L. G. A. J. M., 2009. *Esquema Nacional de Seguridad con Microsoft.* s.l.:Microsoft Ibérica S.R.L..

Reglas de Firewall, s.f. *Procedimientos almacenados de reglas de Firewall.* [En línea]

Available at: https://learn.microsoft.com/es-es/sql/relational-databases/system-stored-procedures/firewall-rules-stored-procedures-azure-sql-database?view=azure-sqldw-latest

Royer, J. M., 2004. *Seguridad en la informática de la empresa- Riesgos, amenazas. Prevención y soluciones.* Barcelona: ENI.

Stanek, W., 2017. *Windows Server 2016, Guía del administrador.* Madrid: EJEMP Multimedia.

SYSADMIN, 2016. *GPO: Establecer fondo de escritorio.* [En línea] Available at: https://www.sysadmit.com/2016/05/gpo-establecer-fondo-escritorio.html

Terrestre, F., 2019. *NOP 300 Puestos de mando de BRILEG,* s.l.: s.n.

Tierra, E. d., 2019. Revista Fuerza 2035.

UNIR, 2021. Sistema Windows. En: *Seguridad en Sistemas Operativos.* s.l.:s.n.

UNIR, 2022. El esquema nacional de seguridad. En: *Aspectos legales y regulatorios.* s.l.:s.n.

VMware, 2017. *Guía del usuario de VMware Tools.* [En línea] Available at: https://docs.vmware.com/es/VMware-Tools/10.1.0/vmware-tools-user-guide.pdf

VMware, s.f. *VMware.* [En línea] Available at: https://www.vmware.com/es/topics/glossary/content/virtual-machine.html

Windows, 2021. *Seguridad en Windows.* [En línea] Available at: https://learn.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/security-options

Windows, 2022. *Unir un equipo a un dominio.* [En línea] Available at: https://learn.microsoft.com/es-es/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain

Windows, 2022. *Unir un equipo a un dominio.* [En línea] Available at: https://docs.microsoft.com/es-es/windows-server/identity/ad-fs/deployment/joina-

ANEXOS

ANEXO 1. EDT

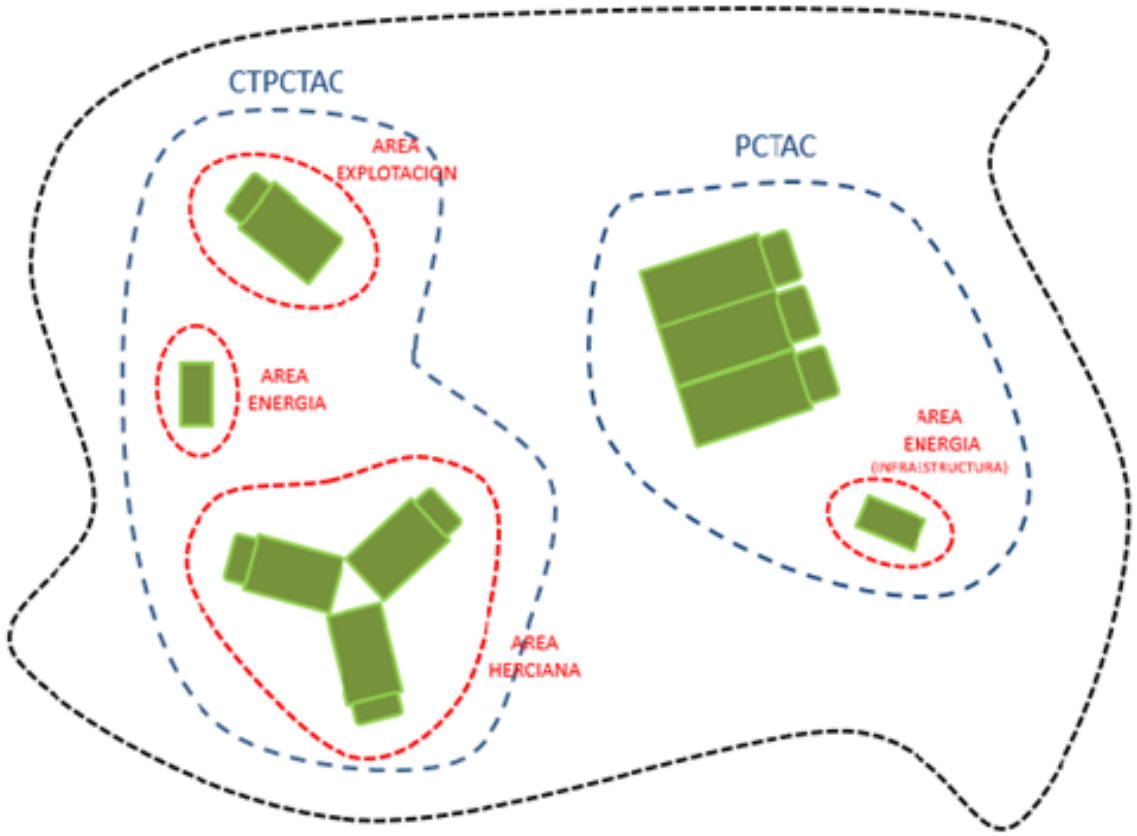
A continuación, se expone una tabla que relaciona las tareas que se han llevado a cabo con las semanas de estancia en la BRILEG, para indicar cuando se efectuaron dichas tareas temporalmente

	Semanas y actividades	**1**	**2**	**3**	**4**	**5**	**6**
Compilación Información	Investigación y observación de la BRILEG	X	X				
	Recopilación de información	X	X				
Instalación Entorno De prueba	Instalación VMware			X	X		
	Creación máquina virtual			X	X		
	Instalar Active Directory			X	X		
	Crear Dominio			X	X		
	Usuarios y Grupos			X	X		
	Carpetas Compartidas			X	X		
	Directiva de grupo			X	X		
	Política de contraseñas			X	X		

	Configuración de AppLocker			X	X		
	Firewall con seguridad avanzada			X	X		
Pruebas Y Replicación Del nodo	Enlazar con máquina local					X	X
	Replicación en el nodo de la BRILEG					X	X
	Pruebas					X	X

Tabla 5.EDT

ANEXO 2. ÁREAS DE TRANSMISIONES DURANTE SU DESPLIEGUE



En esta imagen se puede observar la disposición que adquiere la CIA de Transmisiones una vez que ha completado el despliegue, con sus distintas áreas, y con las distancias que se deben establecer con las zonas de radiación. Por un lado, tenemos el CTPCTAC en donde se establecen las áreas que irradian (herciana), junto a un área de energía y el área de explotación (donde se explotan los servicios). Por otro lado, está el área PCTAC, en donde se establecen los mandos para dirigir la maniobra, junto con un área de energía.

ANEXO.3 Creación máquina virtual

Para crear la máquina virtual de Windows 2016, se debe de tener su imagen y VMware instalado. En la siguiente imagen vemos como se elige la imagen ISO W2016

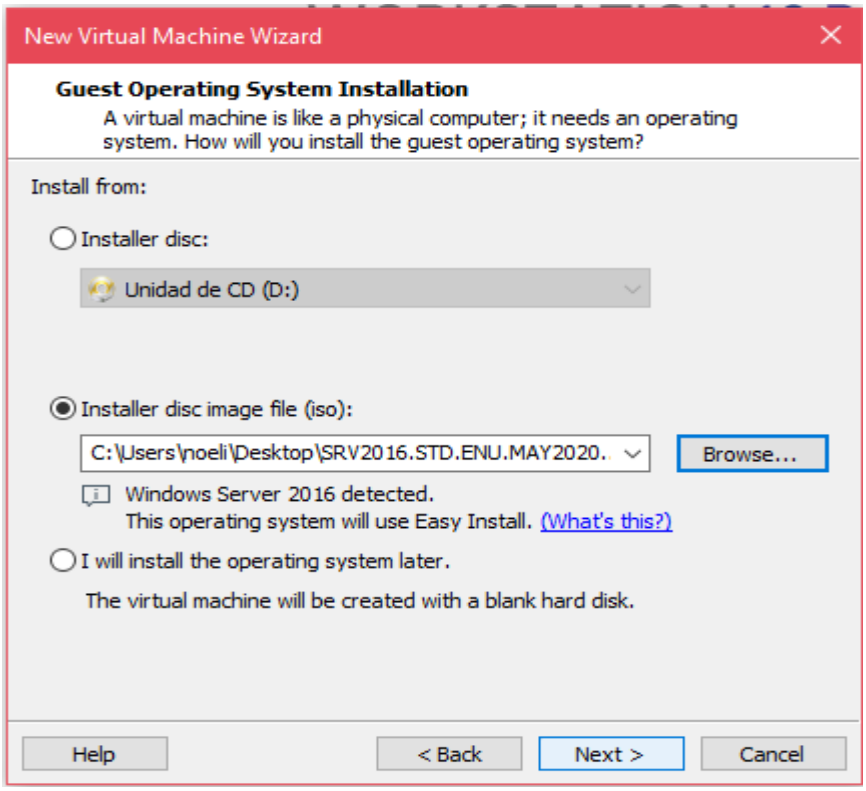


Figura 21.Elección de la imagen ISO

En la siguiente imagen vemos que piden licencias, sin embargo, podemos seguir con la creación de máquinas virtuales sin la licencia que piden y por tanto pulsamos 'next' directamente.

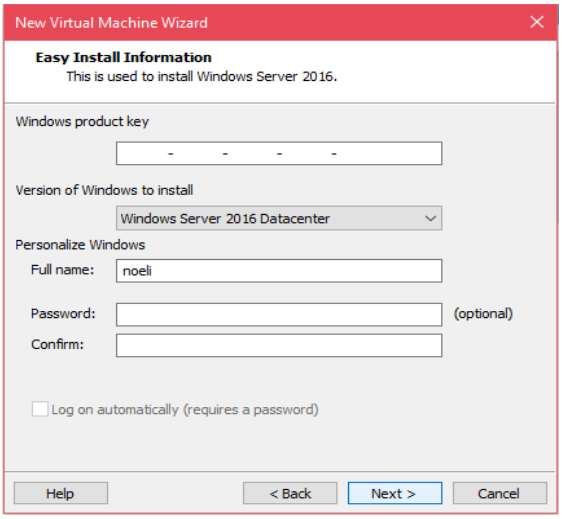


Figura 22.Claves de licencia

En las siguientes imágenes a continuación, se elige el nombre de la máquina virtual, así como su localización (figura 24) y cuánto tamaño del disco del PC se compartirá con la máquina virtual, así como la elección de guardar el disco virtual como un archivo múltiple o único y por último la opción de customizar el hardware (figura 23). Las elecciones que se deben seguir son las propuestas en las capturas de pantalla, es decir, elegir un nombre para la máquina virtual y un lugar donde almacenarla como en la figura 24, un tamaño de disco máximo dedicado a la máquina virtual de 60 GB como en la figura 23 y la finalización de la creación de la máquina como en la figura 25, donde muestra una lista de los pasos hechos para verificarlos. Una vez que se ha comprobado los distintos tipos de configuración, se elige la opción 'next'.

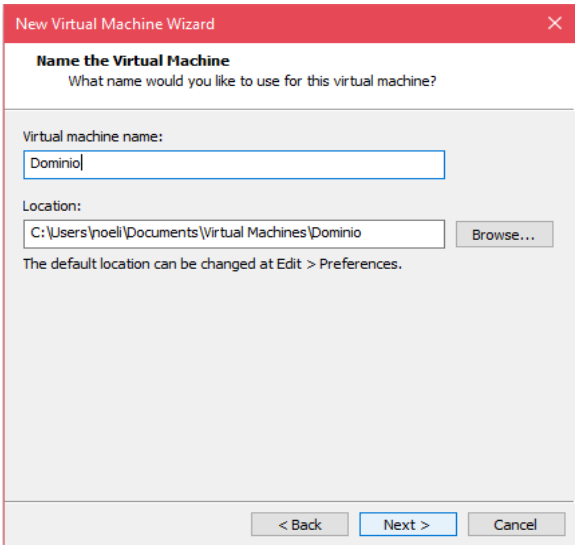


Figura 24.Elección nombre M.V.

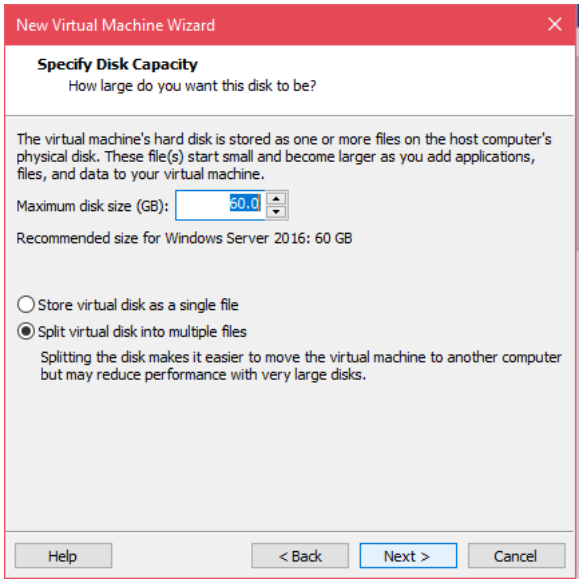


Figura 23.Especificación de la capacidad del disco

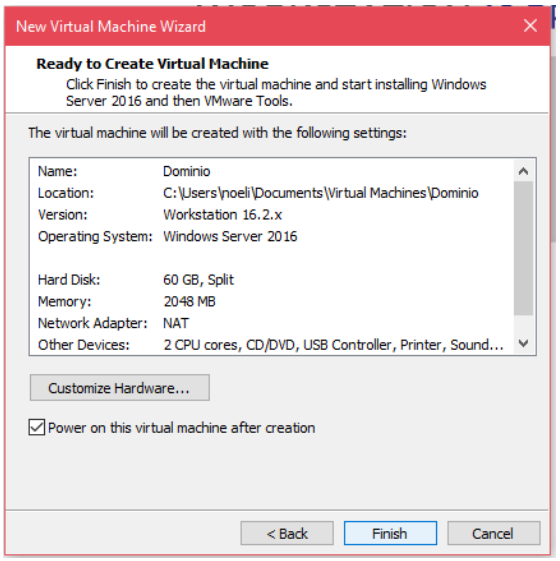


Figura 25.Finalización de la creación

Una vez que se han seguido estos pasos, finalizamos la creación de la máquina virtual, y posteriormente seleccionamos el S.O que queremos para la instalación. En nuestro caso será de tipo STD., de Windows Server 2016, como aparece en la figura siguiente.

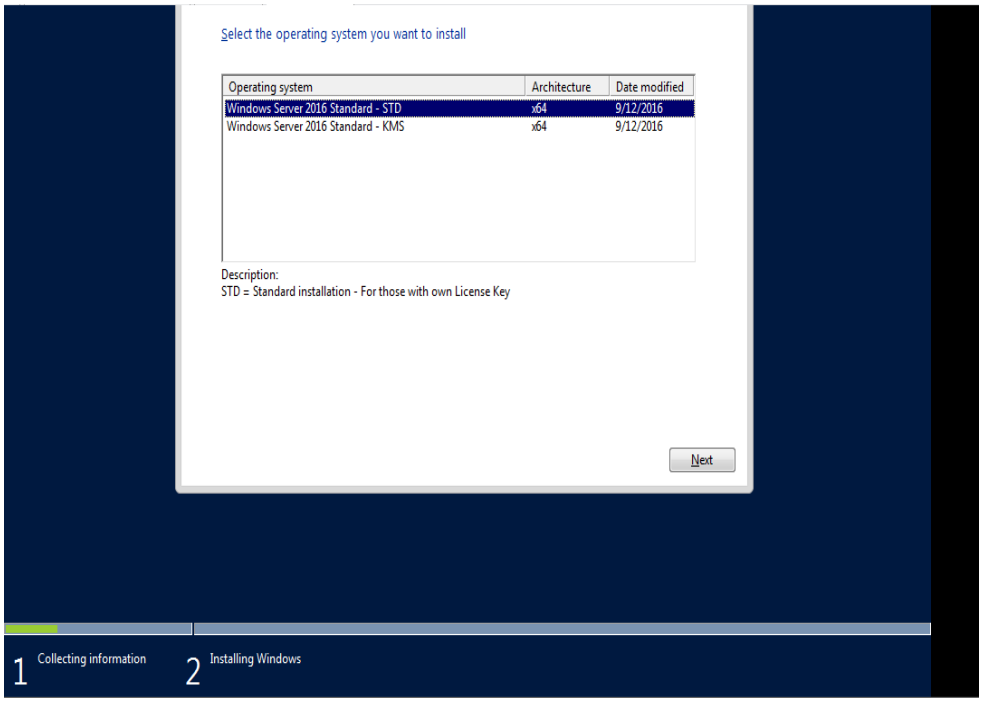


Figura 26.Elección del S.O.

ANEXO.4 Instalación Active Directory y configuración DNS

Una vez que se ha creado la máquina virtual con W2016, se abrirá directamente el Active Directory y será el momento de instalar los roles y configurar el DNS. Al iniciar Windows Server se muestra el panel que resume los servicios que se ejecutan en el servidor, y en la parte superior existen unos atajos para realizar unas acciones de forma rápida dentro del servidor. Entre estas acciones rápidas se encuentra la acción de “Agregar roles y características” con la que se configura el Directorio Activo. La imagen siguiente muestra la pantalla para configurar el Active Directory.

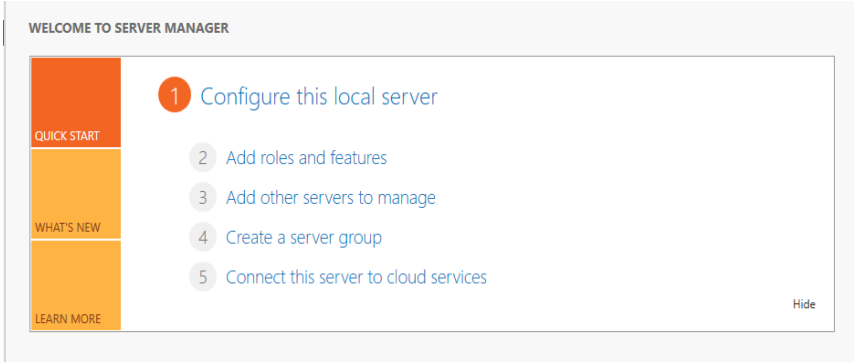


Figura 27.Active Directory

Al seleccionar la acción de ‘Add roles and features’ se ejecuta un asistente para la configuración del servidor. Siguiendo las pantallas del asistente se selecciona “agregar el servicio de *Active Directory*” en el servidor que se ejecuta en la máquina. La instalación es sencilla, ya que en todas las pantallas hay que aceptar la configuración por defecto, excepto en la pantalla en la que se selecciona el rol de servidor donde se elige el servicio de dominio de Active Directory. En la siguiente imagen se observa la primera tarea para añadir los roles y configuraciones, las explicaciones previas de la aplicación.

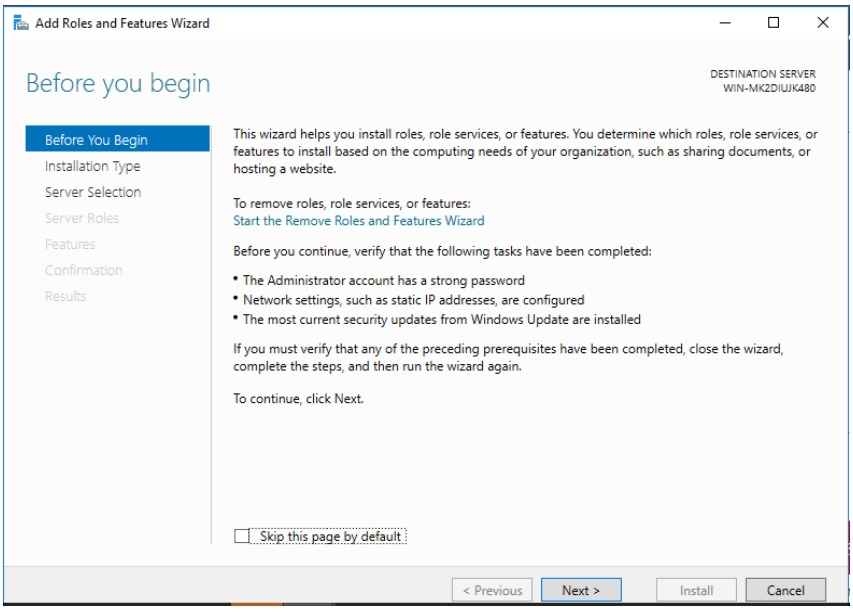


Figura 28.Explicaciones previas

En la siguiente imagen se observa que en el apartado de ‘server selection’ se marca nuestro servidor.

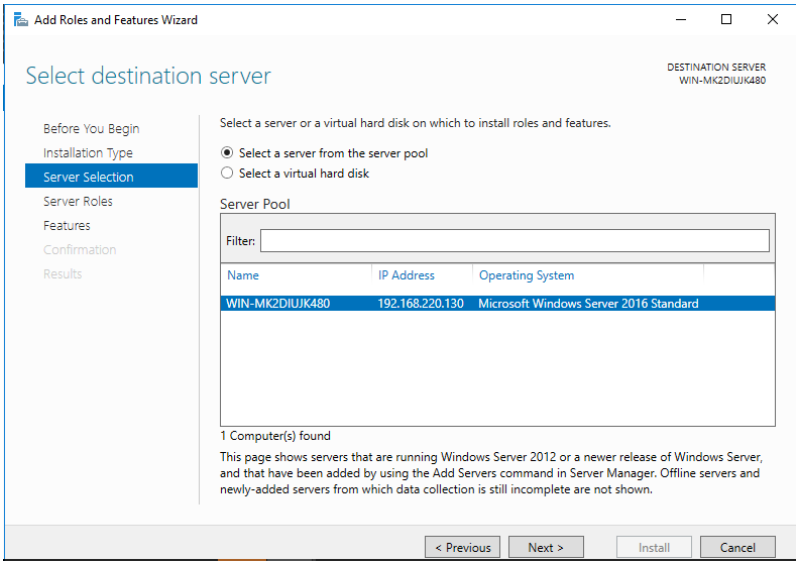


Figura 29.Selección servidor de destino

Posteriormente se activan los roles de ‘Servicios de Dominio del Directorio Activo’ como se muestra en la siguiente imagen. Pulsamos ‘siguiente’ y en la siguiente pantalla revisamos las configuraciones y incluimos las características como en la figura 31.

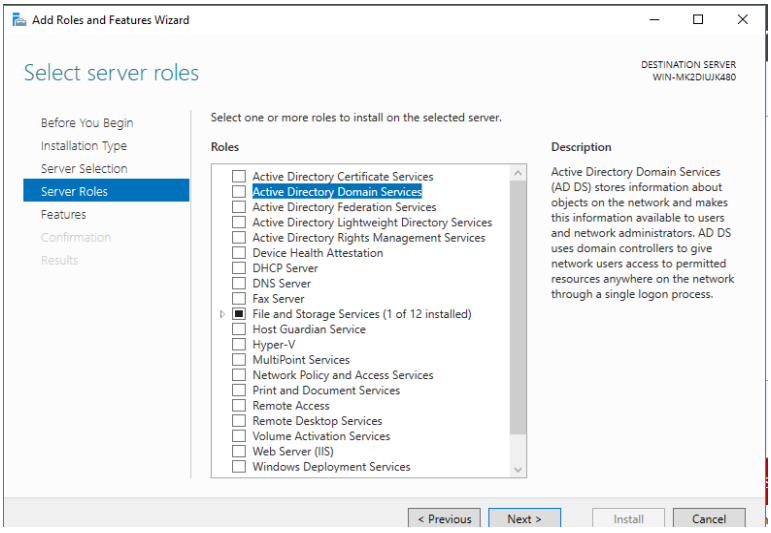


Figura 30.Active Directory Domain Service

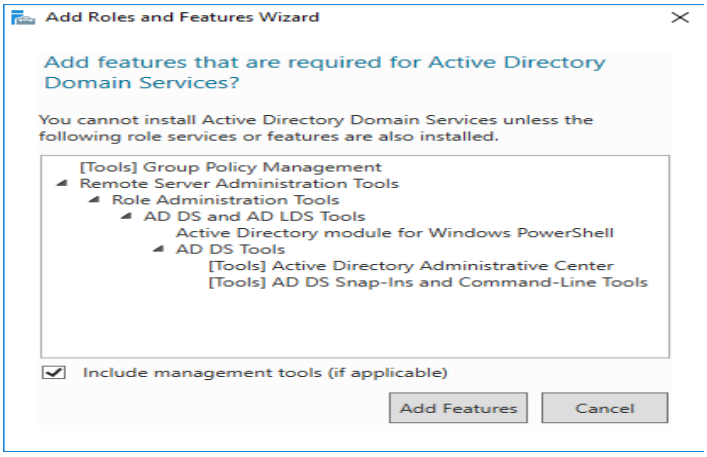


Figura 31.Incluir las características

En la siguiente imagen aparecen los componentes que se deben instalar en nuestro servidor. Dejamos los que vienen por defecto y añadimos 'Group Policy Management' como se muestra.

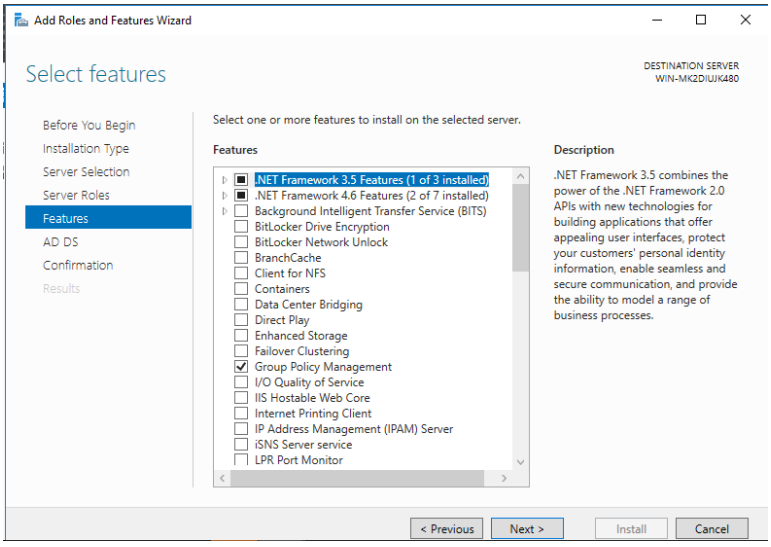
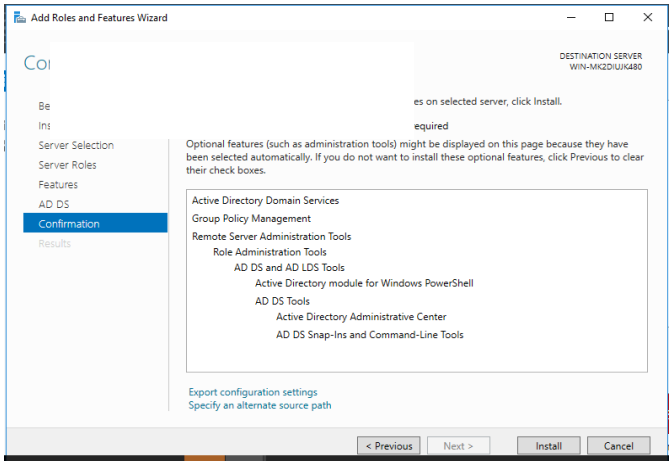


Figura 32.Componentes del Servidor

En la siguiente imagen se muestran los roles que se van a instalar. Una vez revisadas estas características se pulsará 'instalar' y el proceso habrá finalizado.

Figura 33.Confirmar instalación



ANEXO 5. Controlador de Dominio

Una vez que se ha llevado a cabo la instalación del Active Directory, se debe configurar el controlador de dominio. El primer paso será promover nuestro servidor a controlador de dominio como se muestra en la siguiente imagen la cual muestra donde se accede para promover el servidor a controlador de dominio.

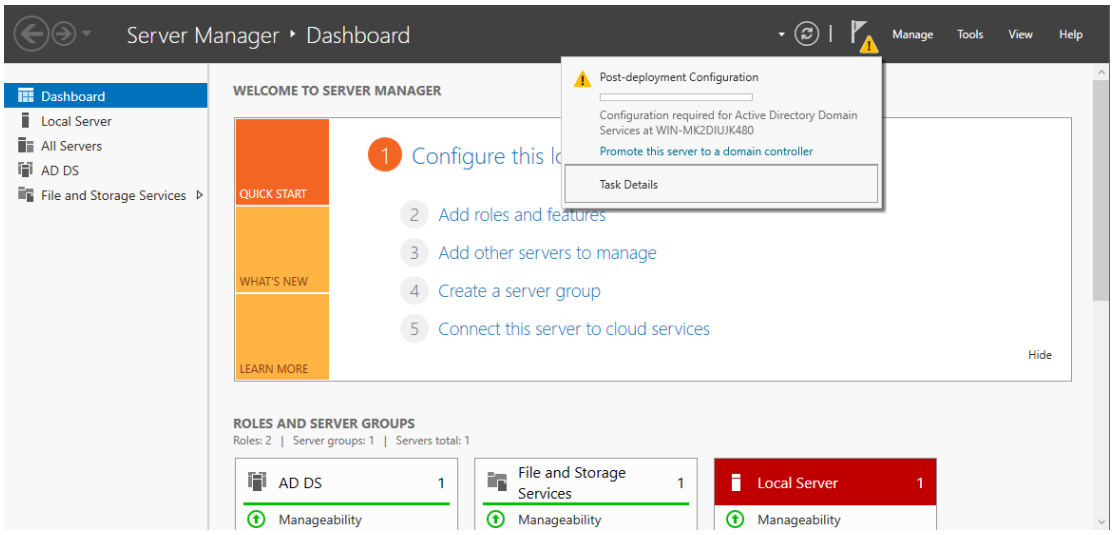


Figura 34.Promover a controlador de dominio

Una vez que se ha promovido a controlador de dominio, se abrirá un desplegable de configuraciones, el cual habrá que modelar. El siguiente paso será añadir un nuevo bosque junto con el nombre del dominio raíz, como se muestra en la imagen siguiente.

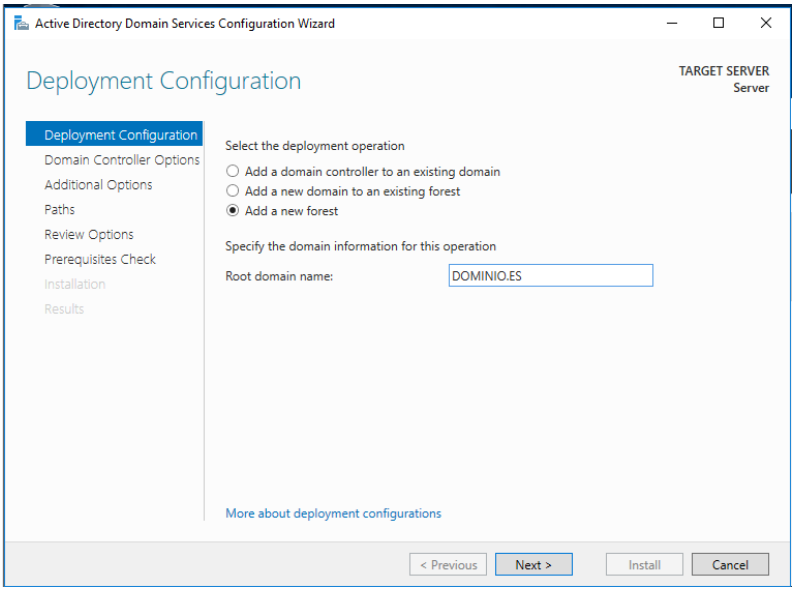


Figura 35.Nombre del dominio

El siguiente paso corresponde a las opciones del controlador de dominio. Se dejan marcadas las que vienen por defecto y se añaden las contraseñas de restauración de los servicios de

directorio como se muestra en la siguiente imagen.

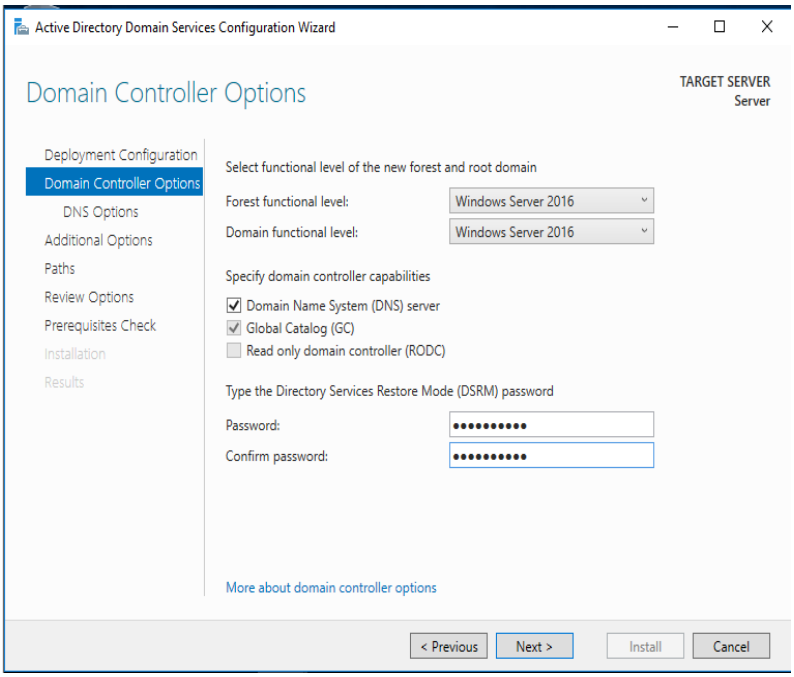


Figura 36.Opciones del controlador

Posteriormente se elige un nombre de dominio de NetBios en la siguiente pantalla a configurar como se muestra en la siguiente imagen.

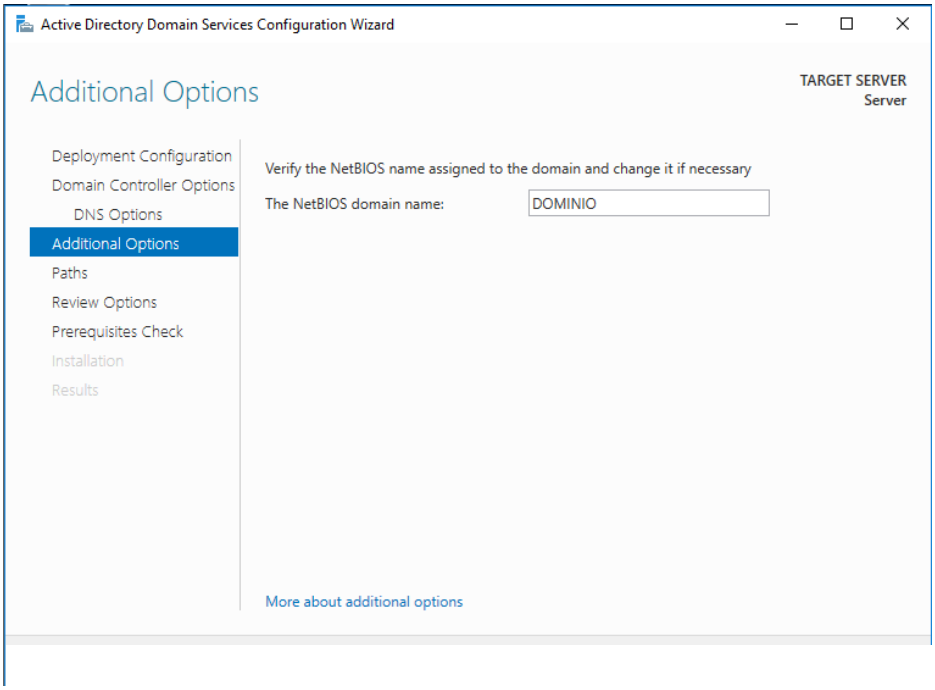


Figura 37.Nombre de NetBios

El siguiente paso será indicar las rutas de acceso, las cuales se dejarán las que vienen determinadas por defecto y que se muestran en la siguiente imagen.

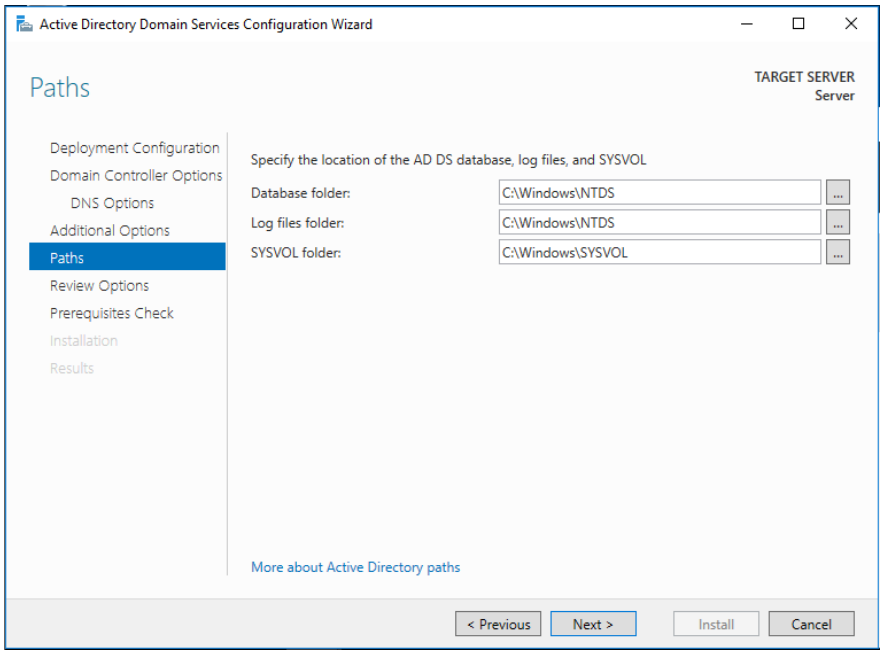


Figura 38.Rutas de acceso

Una vez seleccionadas las rutas de acceso, pulsamos 'next'. La siguiente pantalla que nos aparecerá será para revisar que las opciones que hemos configurado, como aparece en la siguiente imagen. Una vez comprobado pulsamos 'next', y se llevará a cabo la comprobación de que la máquina virtual cumple con los prerrequisitos establecidos para que pueda llevar a cabo la instalación.

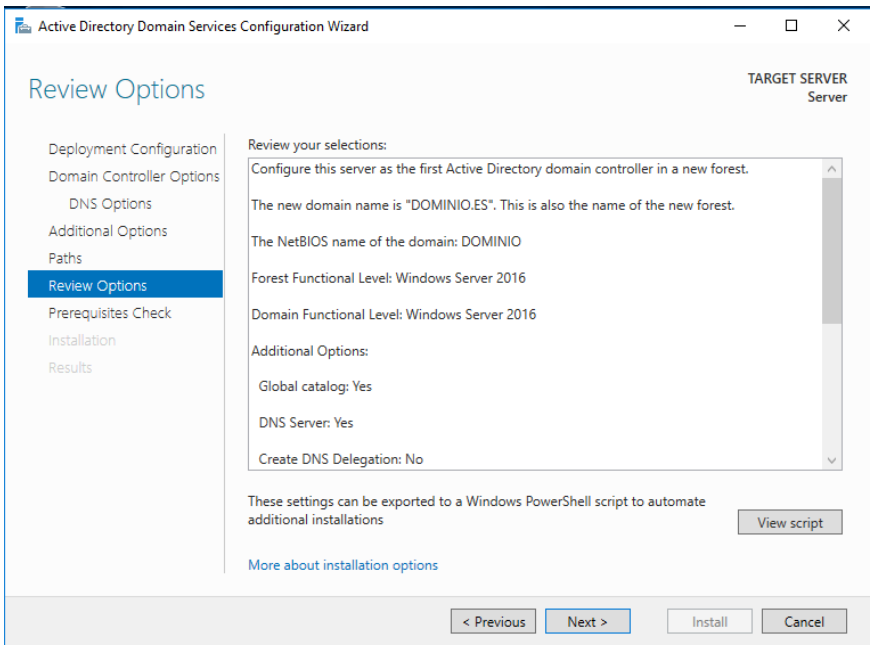


Figura 39.Revisión opciones

La siguiente imagen muestra un análisis del cumplimiento de los prerrequisitos, el cual, ha sido exitoso.

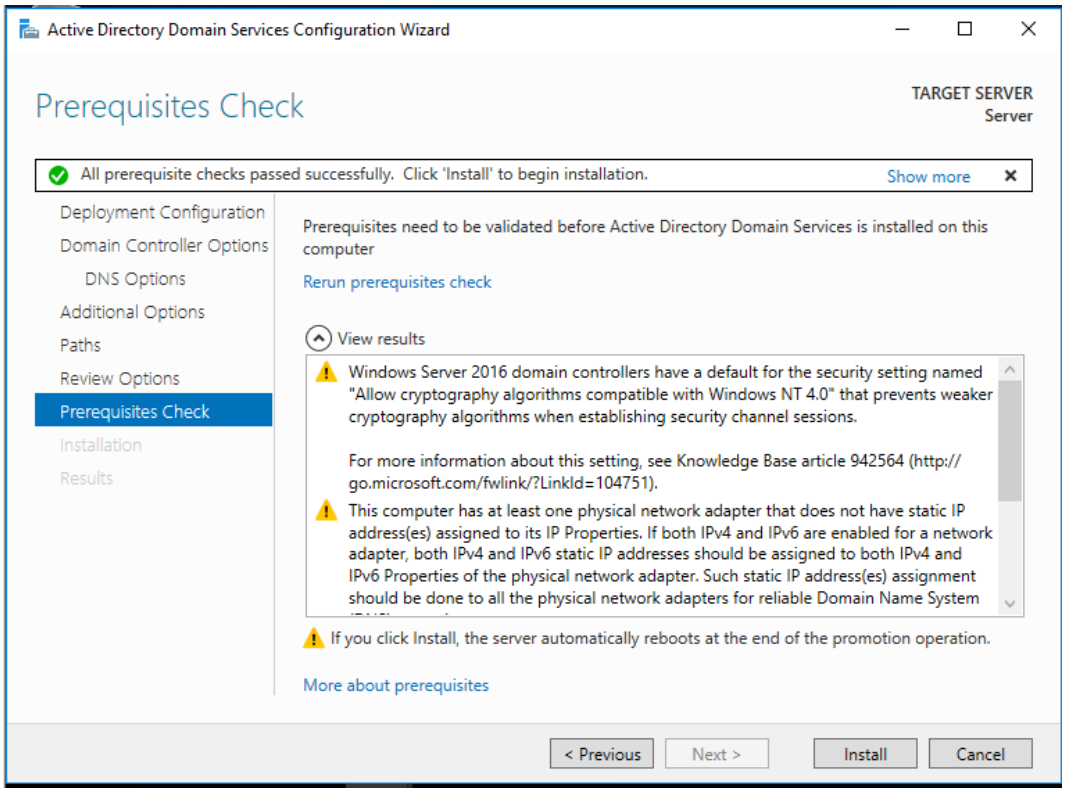


Figura 40.Pre-requisitos

Pulsaremos 'instalar' en la anterior imagen y la máquina se reiniciará. Una vez haya finalizado el proceso de instalación, si se accede al administrador del servidor, aparecerá que nuestro DNS se ha instalado correctamente. La siguiente imagen representa lo que se debe observar cuando se ha instalado correctamente Active Directory.

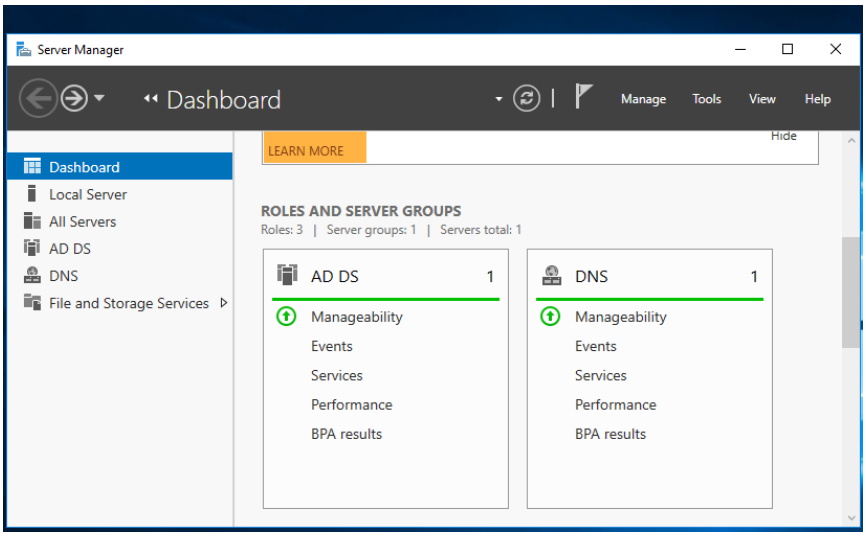


Figura 41.DNS instalado

ANEXO 6. Creación de Usuarios y Grupos

En esta parte se crearán los usuarios y los grupos. En primer lugar, crearemos los tres grupos que tenemos propuestos: Grupo01, Grupo02 y Grupo03. Para ello, habrá que ir, dentro de las herramientas de Active Directory, a la sección de usuarios y equipos de Active Directory, como se observa en la siguiente imagen.

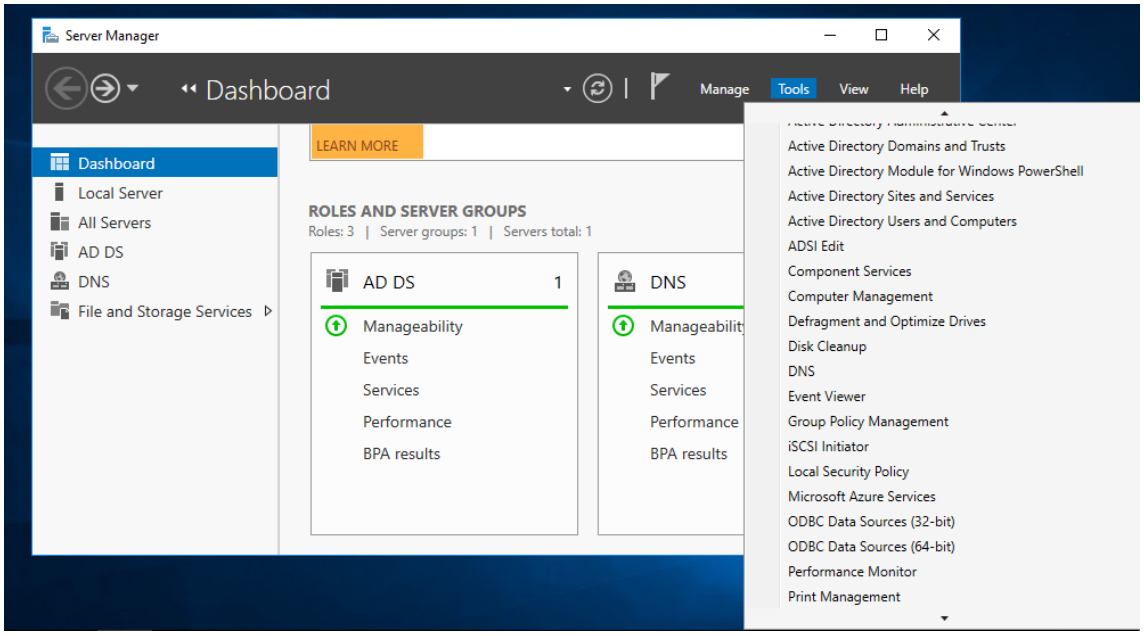


Figura 42.Usuarios y equipos de Active Directory

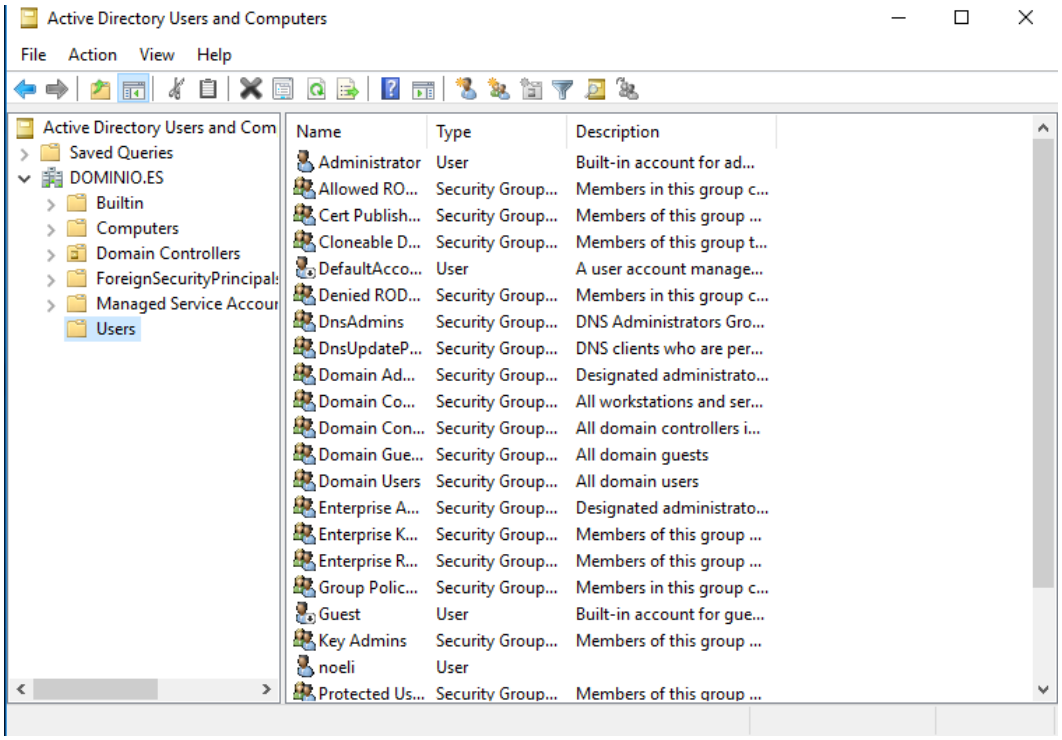


Figura 43.Usuarios y equipos de Active Directory

Como vemos en la anterior imagen, una vez que accedemos a la interfaz de Usuarios y Equipos de Active Directory, para crear los distintos grupos, habrá que clicar, en primer lugar, en la carpeta Users, y, en segundo lugar, en la barra superior, en el icono de creación de grupos. Como se ve en la siguiente imagen, se van creando los grupos manualmente.

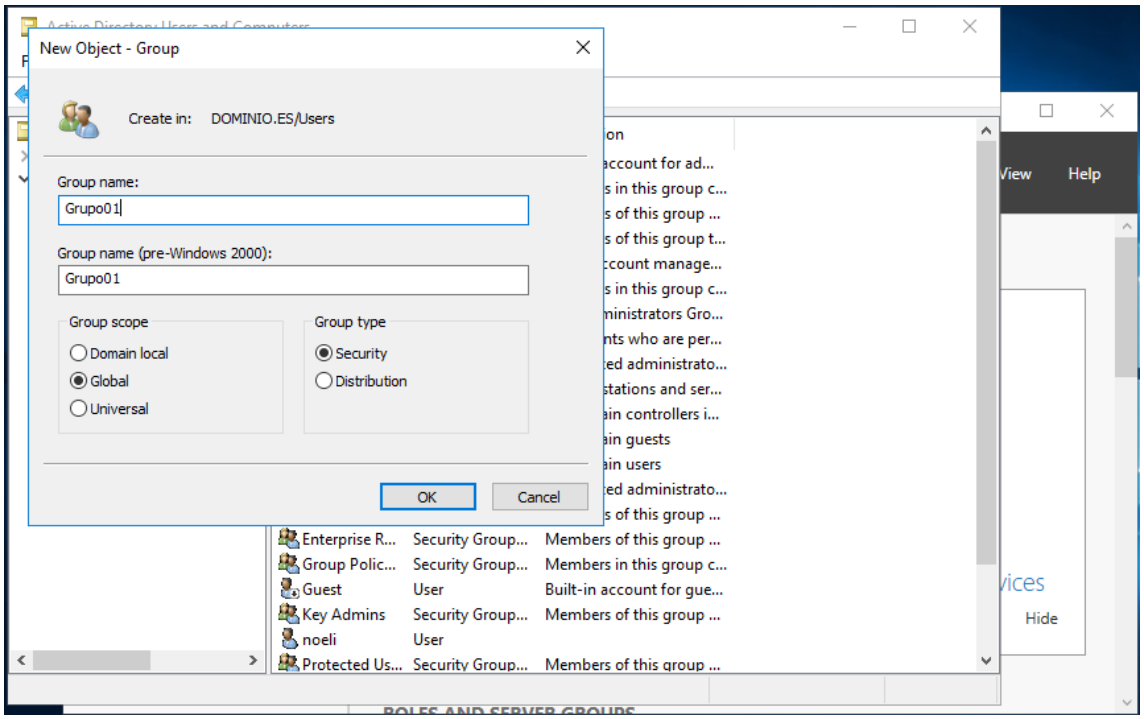


Figura 44.Creación de Grupo01

Repetimos el proceso con el resto de los grupos que faltan. Una vez que están los grupos creados, se crea el archivo CSV. Este archivo CSV es cualquier archivo de texto en el cual los caracteres están separados por comas, realizando una especie de tabla con columnas y filas. Para su realización se elegirá un Excel en el cual aparecerán las columnas necesarias para este proyecto, que posteriormente lo convertiremos a archivo CSV. En la siguiente imagen se muestra el archivo CSV, con las tres columnas que corresponden a nombre, contraseña y departamento (grupo al que pertenecen). Este archivo se crea en nuestro PC para posteriormente introducirlo en la máquina virtual como se ve en el ANEXO 7.

```
Name, Password, Department
Usuario01, Usuario.01, Grupo01
Usuario02, Usuario.02, Grupo01
Usuario03, Usuario.03, Grupo01
Usuario04, Usuario.04, Grupo01
Usuario05, Usuario.05, Grupo01
```

Figura 45.Archivo CSV

Con la ayuda del ANEXO 7 se podrán compartir archivos hechos dentro del PC con la máquina virtual. Una vez que hemos exportado el archivo CSV y el Script, que utilizaremos en el PowerShell, se tendrá que ejecutar para que se creen los usuarios en los grupos pertinentes.

```powershell
#Import modules
Import-Module ActiveDirectory

#CSV path
#$filepath = "C:\Users\Administrador\Desktop\usuarios01-50.csv"
$filepath = Read-Host -Prompt "Introduce el path del archivo CSV"

#Import CSV
$users = Import-Csv $filepath

#Read info of each user
ForEach ($user in $users){

    $name = $user.'Name'
    $password = $user.'Password'
    $department = $user.'Department'

    $secPassword = ConvertTo-SecureString $password -AsPlainText -Force

    #New-ADUser cmd
    New-ADUser -Name $name -AccountPassword $secPassword -Description $department -Enabled $True

    #Add-ADGroupMember cmd
    Add-ADGroupMember -Identity $department -Members $name
```

Figura 46.Script propuesto del libro "PowerShell Cookbook"

En la anterior imagen está el archivo script que se exporta desde nuestro PC a la máquina virtual y el cual contiene la ruta hacia el archivo CSV.

En la siguiente imagen se ve cómo se ha procedido a introducir el archivo Script (con la ruta que hace referencia al archivo CSV para que PowerShell lo pueda ejecutar), el cual contiene las instrucciones que PowerShell debe realizar para poder crear automáticamente los usuarios.

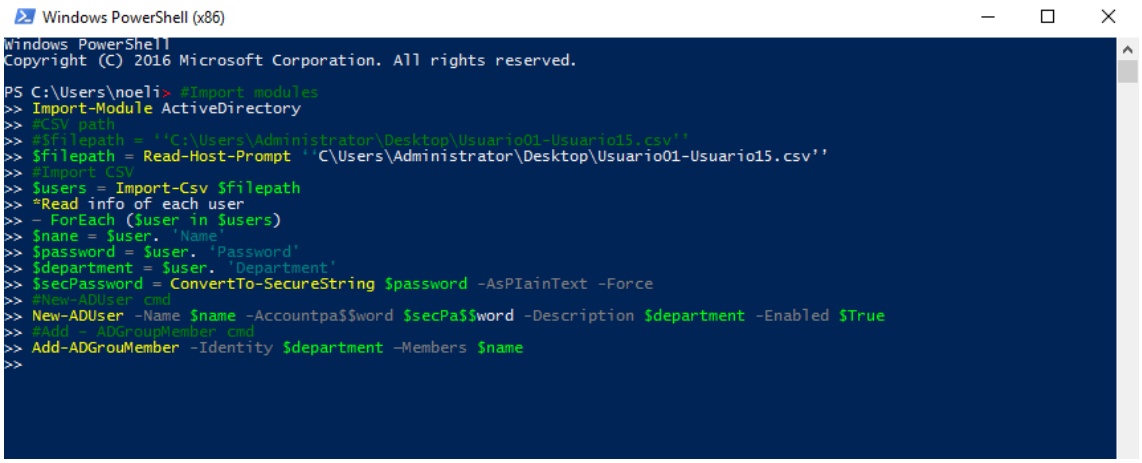


Figura 47.PowerShell con el Script

En la siguiente imagen se puede apreciar el resultado de ejecutar el PowerShell, es decir, la creación de los usuarios que se pretendían.

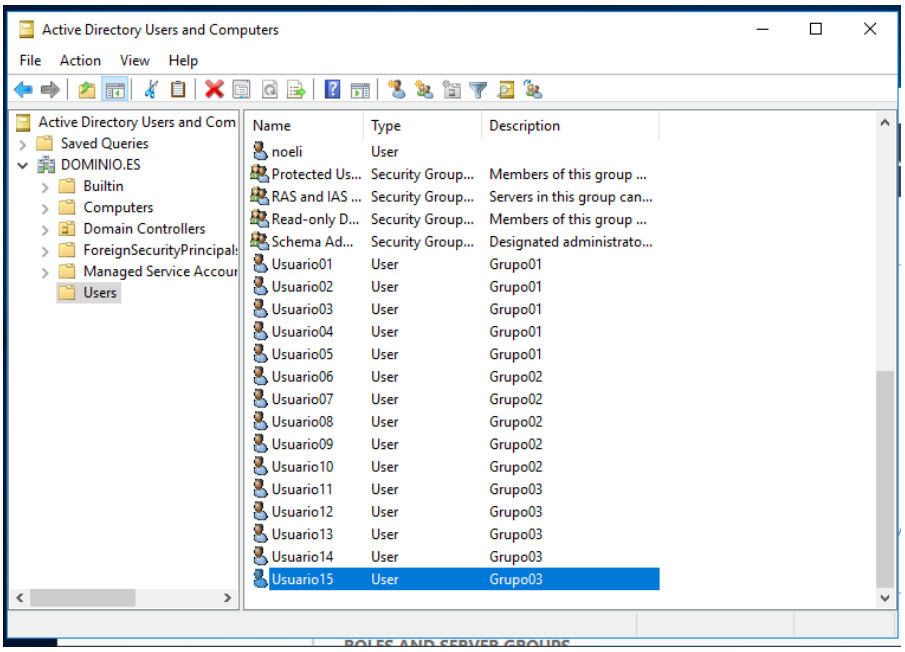


Figura 48.Creación de usuarios

ANEXO 7 Compartir archivos de PC a Máquina virtual

Para poder compartir archivos del PC con la máquina virtual, se deben de seguir estos pasos. En la imagen siguiente se muestra el primer paso que se debería hacer. En pestaña de 'VM', se accede a ''Reinstall VM tools''. Una vez que está instalada, se accede a la misma ventana ('VM'), pero esta vez se elige la opción de ''settings'', como se observa también en la misma imagen.

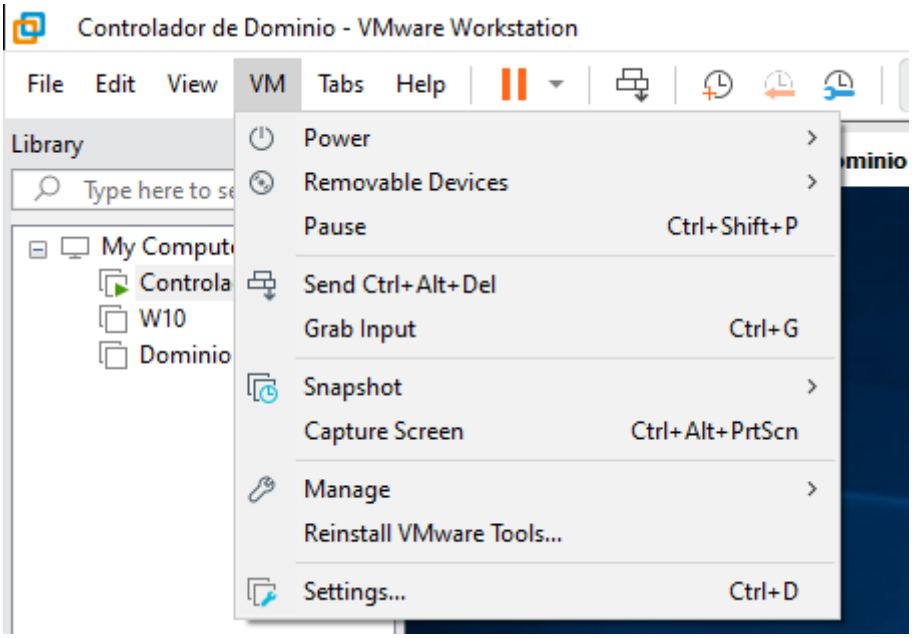


Figura 49.VMware Tools

Dentro de la pestaña de ''settings'' se elige la opción de carpetas compartidas ('Shared Folders') y se añade la ruta de la carpeta dentro del PC que se desea compartir con la máquina virtual, como se observa en la siguiente imagen.

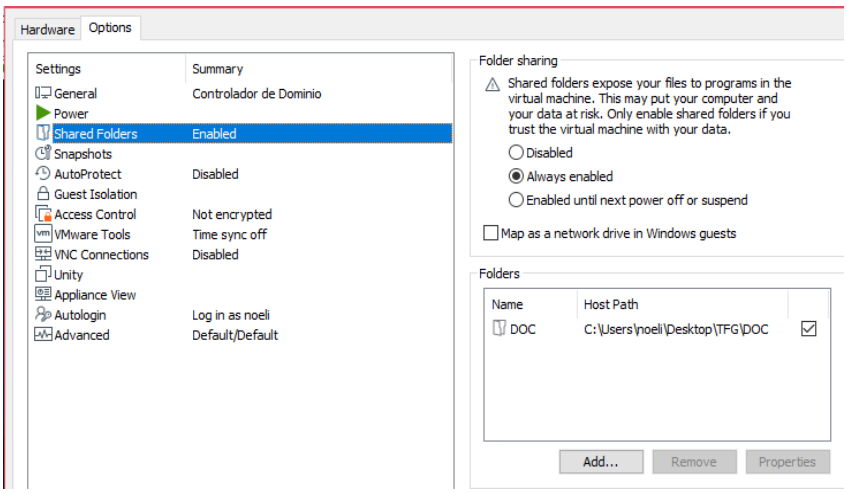


Figura 50.Compartir archivos

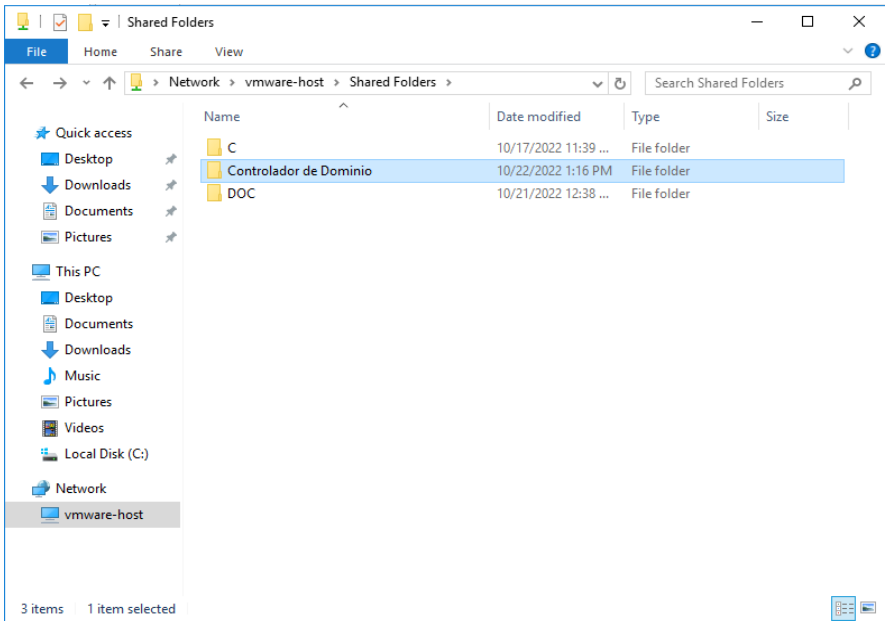


Figura 51.Carpetas compartidas

En la anterior imagen se ve donde se debe acceder dentro de la máquina virtual para poder tener acceso a todos los archivos compartidos desde el PC hacia la máquina virtual.

ANEXO.8 Carpetas compartidas

En primer lugar, se deben crear y compartir las tres carpetas: Grupo01, Grupo02 y Grupo03, para ello se debe acceder y elegir las opciones como se encuentran en la siguiente figura, las cuales se encuentran dentro de 'this PC', 'Local Disk', 'File Sharing'. Es aquí donde se añaden los grupos con los que se desea compartir una determinada carpeta.

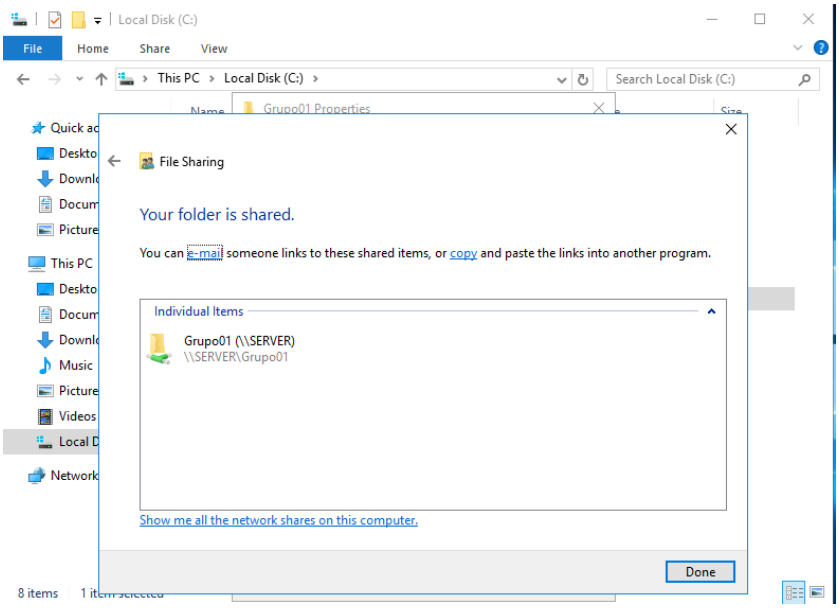


Figura 52.Creación carpetas

Dentro de los usuarios con los que se va a compartir las carpetas, se eligen los pertinentes dentro de un grupo. Es decir, la carpeta de Grupo01 solo se debe compartir con los usuarios que se incluyen dentro de ese grupo. En la siguiente imagen se observa cómo se incluyen usuarios dentro de un grupo y se les incluyen permisos, y por lo tanto se deben de elegir esas opciones para configurar este apartado.

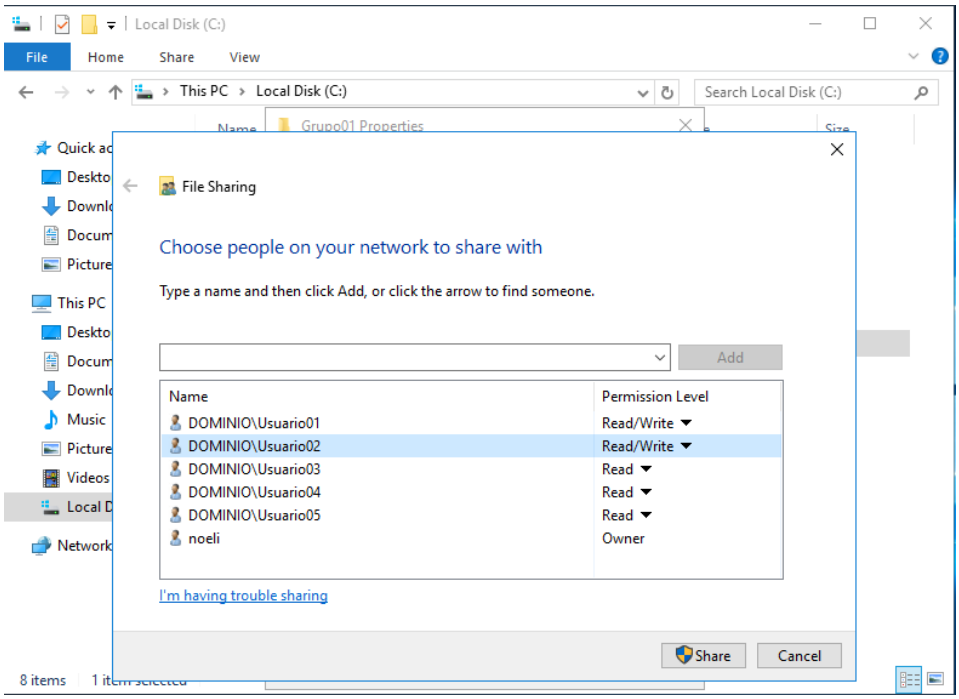


Figura 53.Elección de permisos

El siguiente paso será acceder al módulo de la sección ‘Rol de servicios de archivos y almacenamiento’. Para poder llevarlo a cabo se accede al ‘’Administrador del Servidor’’ y dentro de él, a la ventana de ‘’Servicios de archivos y almacenamiento’’. Se clica en ‘’Volúmenes’’ para luego pinchar en ‘’Iniciar el asistente para agregar roles y características’’, dentro de recursos compartidos. En la siguiente imagen se observa donde se debe acceder para poder configurar los servicios de archivo y almacenamiento.

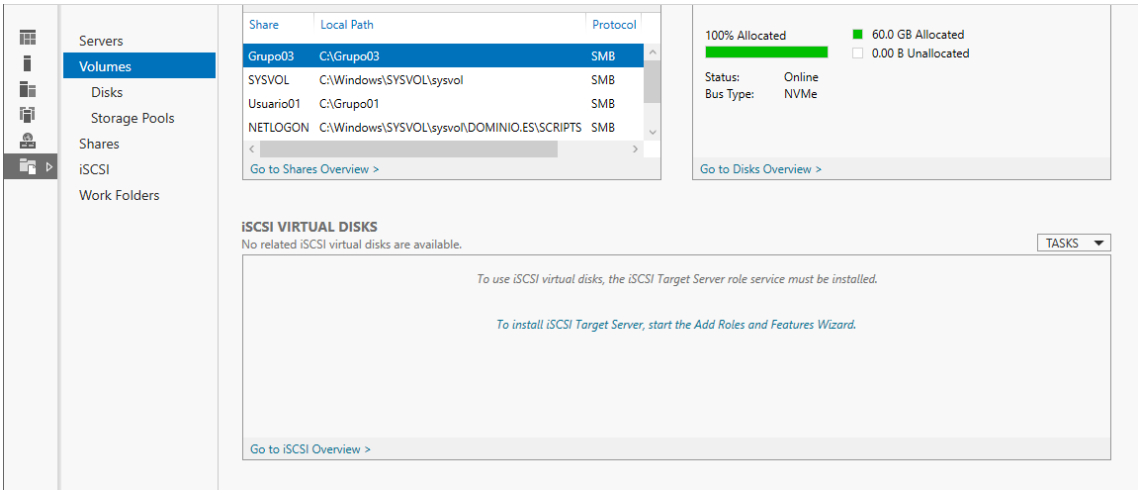


Figura 54.Servicios de archivo y almacenamiento

Se procede a abrirse el asistente con la pestaña: ‘’Servidor de archivos y almacenamiento’’ y se dejan las opciones que vienen por defecto y se añade ’’Servicios de iSCI’’, ya marcado en la siguiente imagen que se muestra. Se pincha en siguiente, como se observa en la imagen para finalizar por último con su instalación.

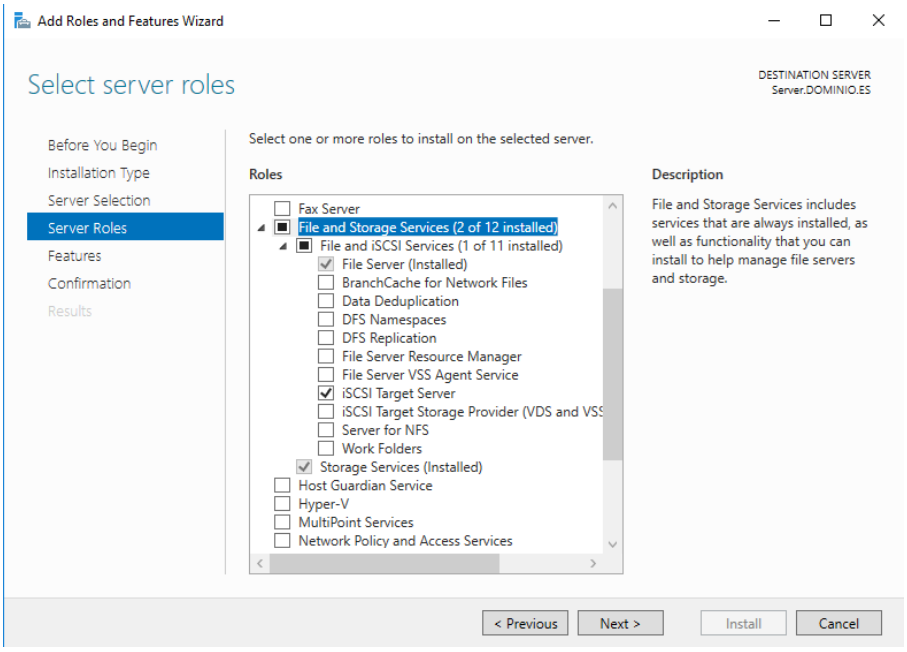


Figura 55.Almacenamiento y servicios y archivos

Se procede a la instalación, como se ve en la siguiente imagen, en la que aparecen las configuraciones hechas para que sean revisadas, y una vez verificadas, se elige la opción de 'install'.

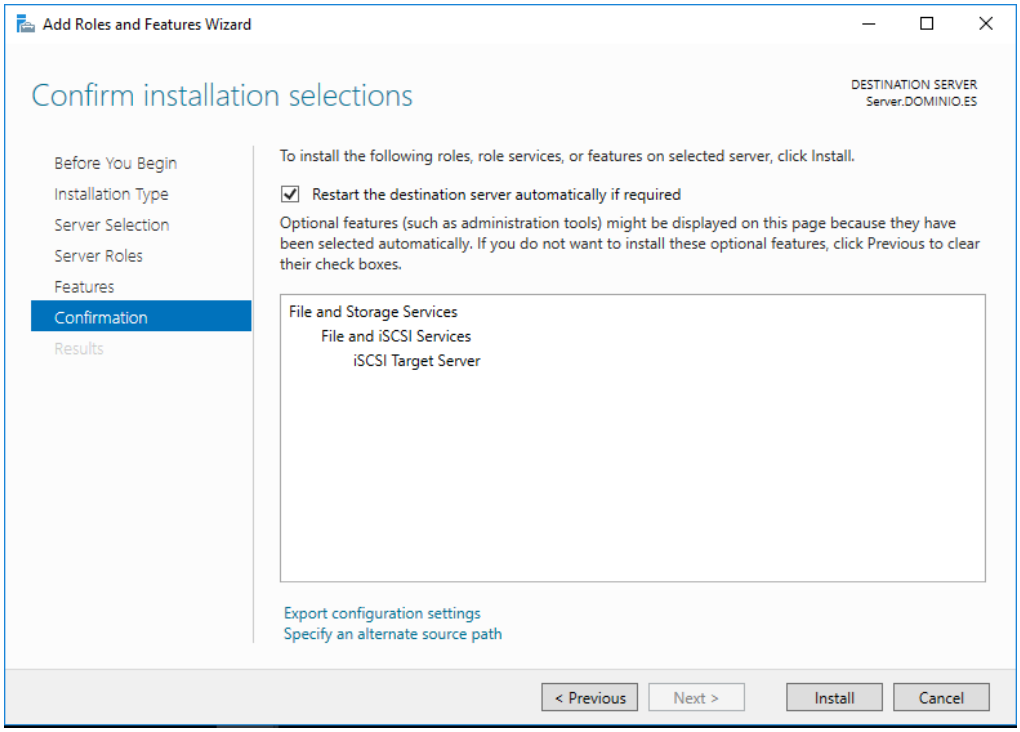


Figura 56.Instalación

Una vez haya terminado la instalación, se vuelve a ''Administrador del Servidor'', 'Volúmenes' ''Tareas'' y ''Nuevo recurso compartido'', como se observa en la siguiente imagen.

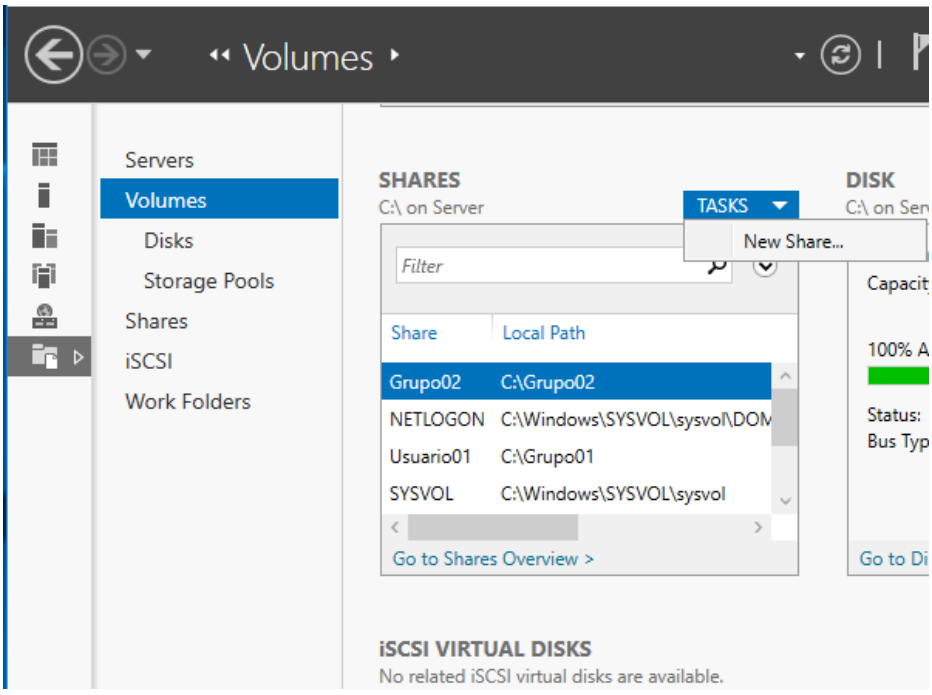


Figura 57.Nueva compartición

La siguiente ventana que aparecerá será el requerimiento del tipo de recurso compartido. En este caso se elige SMB-Quick, como se ve en la siguiente imagen, ya que es un protocolo estándar, usado por la mayoría de las versiones de Windows.

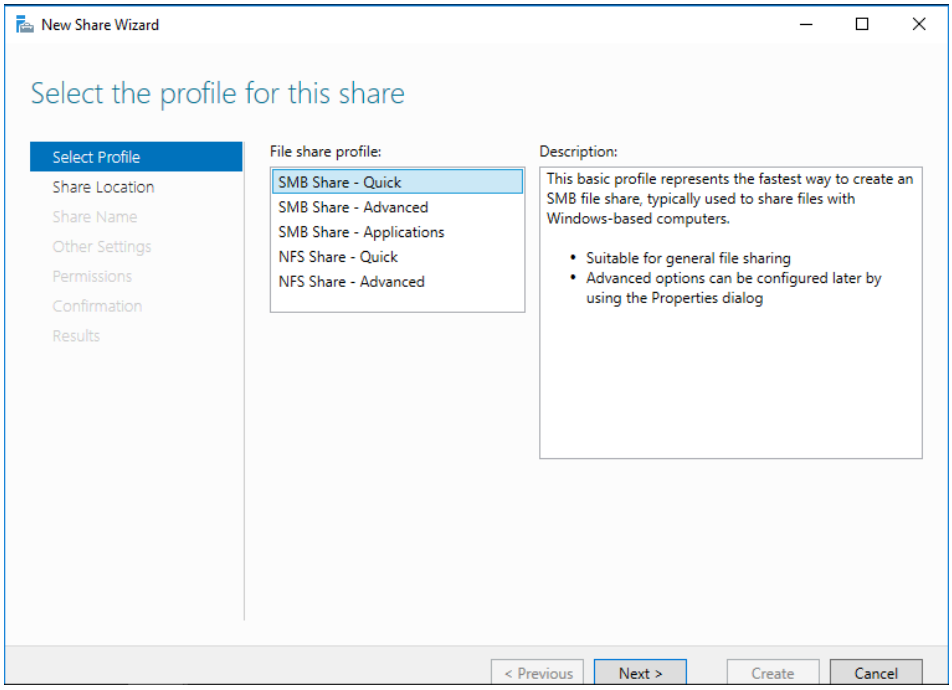


Figura 58.Tipos de recursos compartidos

Lo seleccionamos y pulsamos en siguiente. La siguiente pantalla que está en la siguiente imagen solicita que se establezca una ruta en la que se encuentre la carpeta compartida, es decir, la ruta en la que se haya creado la carpeta compartida.

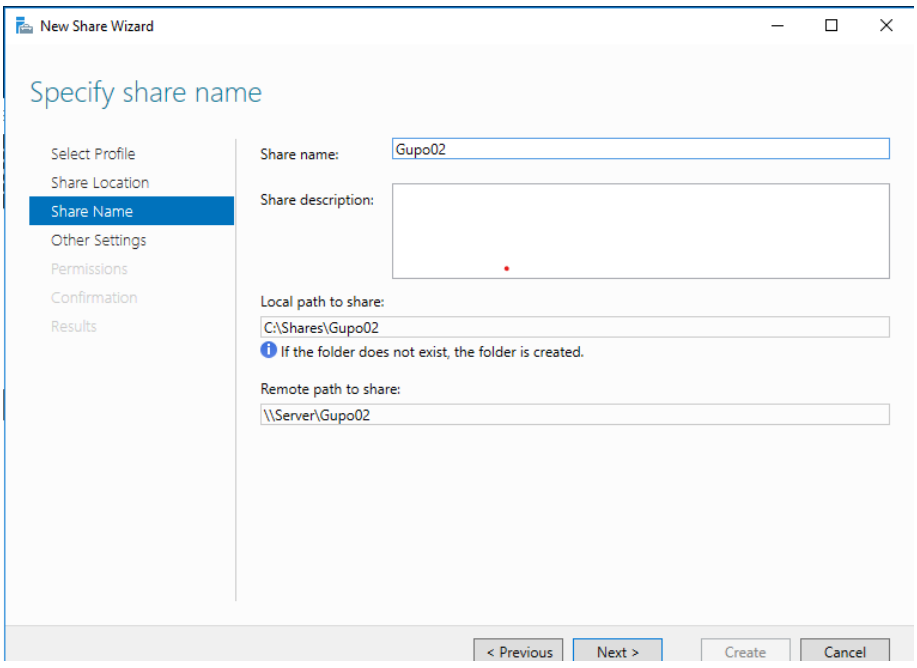


Figura 59.Ruta carpeta compartida

La siguiente pantalla que aparecerá corresponde a configuraciones de las carpetas compartidas. En esta opción elegimos:

-Habilitar enumeración basada en el acceso: Para que el recurso se muestre únicamente a los usuarios autorizados.

-Cifrar acceso de datos: Para que el acceso del archivo remoto se cifre evitando que pueda ser manipulado.

Las elecciones anteriores se reflejan en la siguiente imagen y posteriormente elegimos ‘next’.

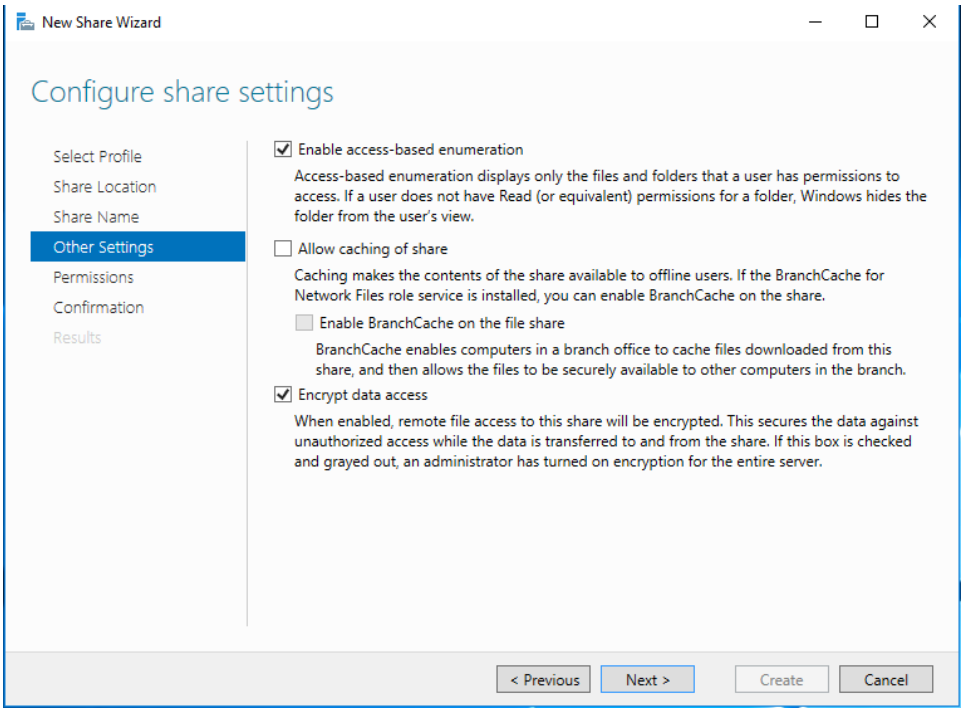


Figura 60.Parámetros de configuración del recurso compartido

Ahora se puede llevar a cabo la modificación de los permisos que se consideren convenientes, accediendo mediante ‘’personalizar permisos’’ como se observa en la siguiente imagen. No se realizará ninguno y se dirigirá directamente a ‘next’

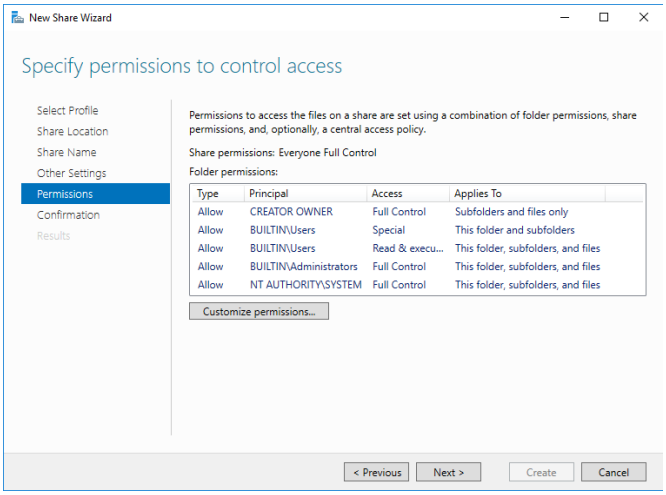


Figura 61.Configuración de permisos de recurso compartido

La siguiente ventana es un resumen para verificar que todos los pasos son correctos. Se elige la opción de ‘’crear’’ y ya aparece ese recurso en la interfaz de recursos compartidos, como se observa en la siguiente imagen

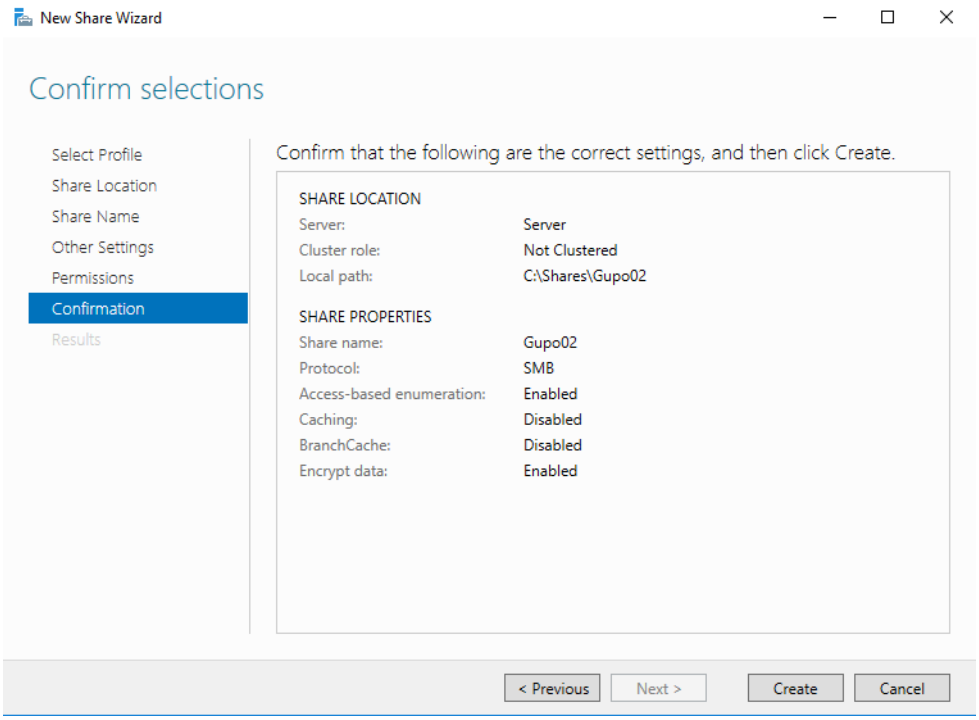


Figura 62.Resumen recurso compartido

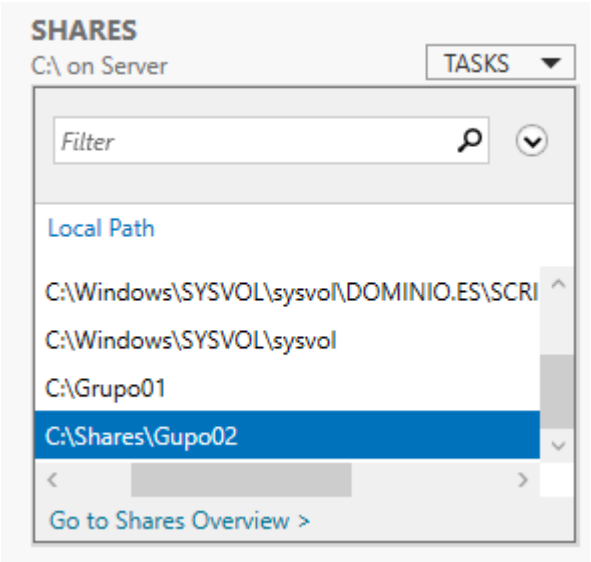


Figura 63.Recurso compartido

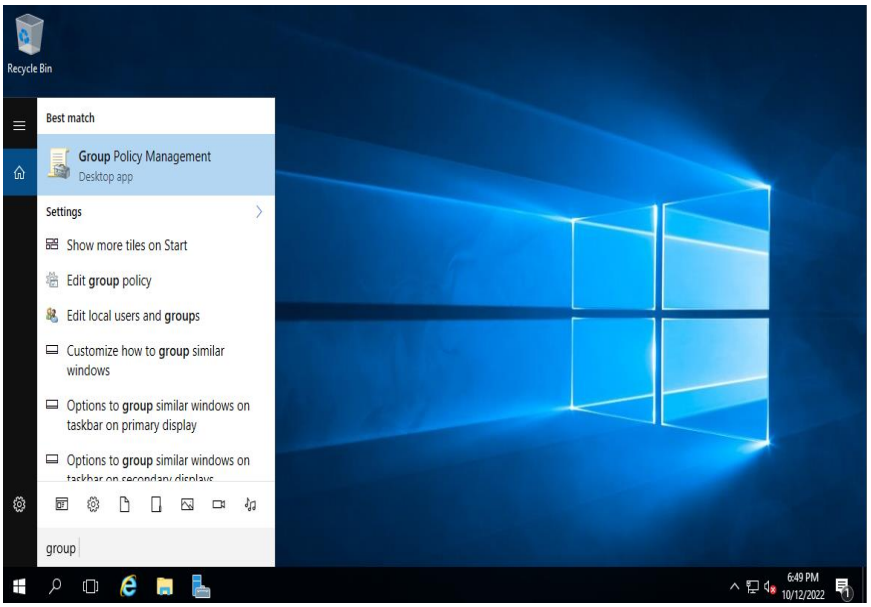
La anterior imagen representa el resultado de todo el procedimiento creado cuando se accede a una carpeta compartida. Ya se podría disponer de las carpetas compartidas.

ANEXO 9. Directiva de Grupo

En este anexo se va a definir una directiva de grupo que bloquee el acceso al panel de control e impida el cambio de fondo de pantalla a los trabajadores.

9.1 PANEL DE CONTROL

En primer lugar, se accede a la Consola de administración (como aparece en la figura 64) de directivas de grupo desde el menú de Windows. Se selecciona el bosque y el dominio creados, y se crea una nueva política de grupo eligiendo la opción de ‘’Objetos y directivas de grupo’’ (como se muestra en la figura 65). Se ha nombrado como ‘’Panel de control-Fondo de pantalla’’, como se observa en la siguiente imagen.



Fígura 64.Políticas de grupo

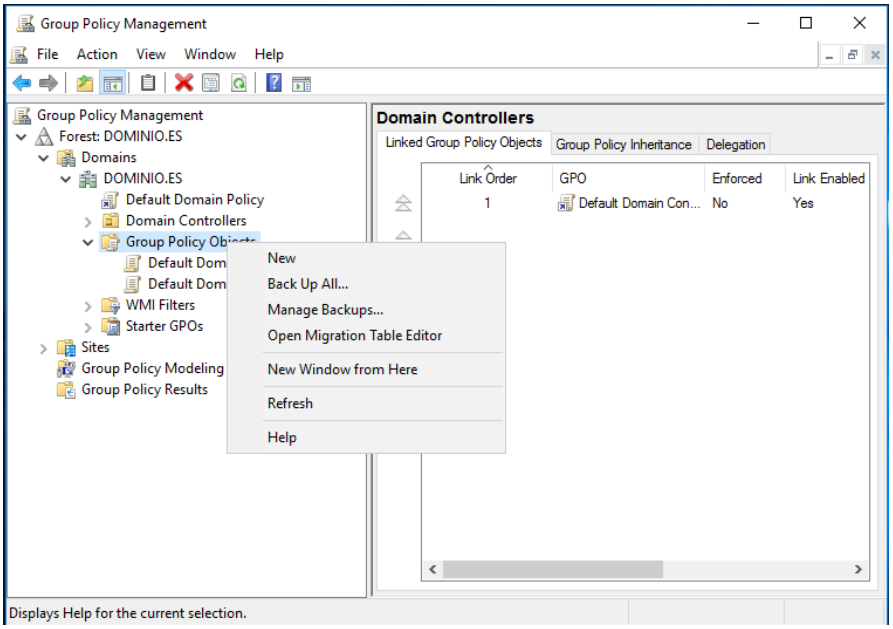


Figura 65.Nueva política

De la imagen anterior se elegirá la opción de ‘’nueva’’, para crear una nueva política de grupo. La siguiente imagen que se muestra trata sobre definir el nombre de esta nueva política, como se observa en la siguiente imagen, cuyo nombre es ‘Panel de control/Fondo de pantalla’.

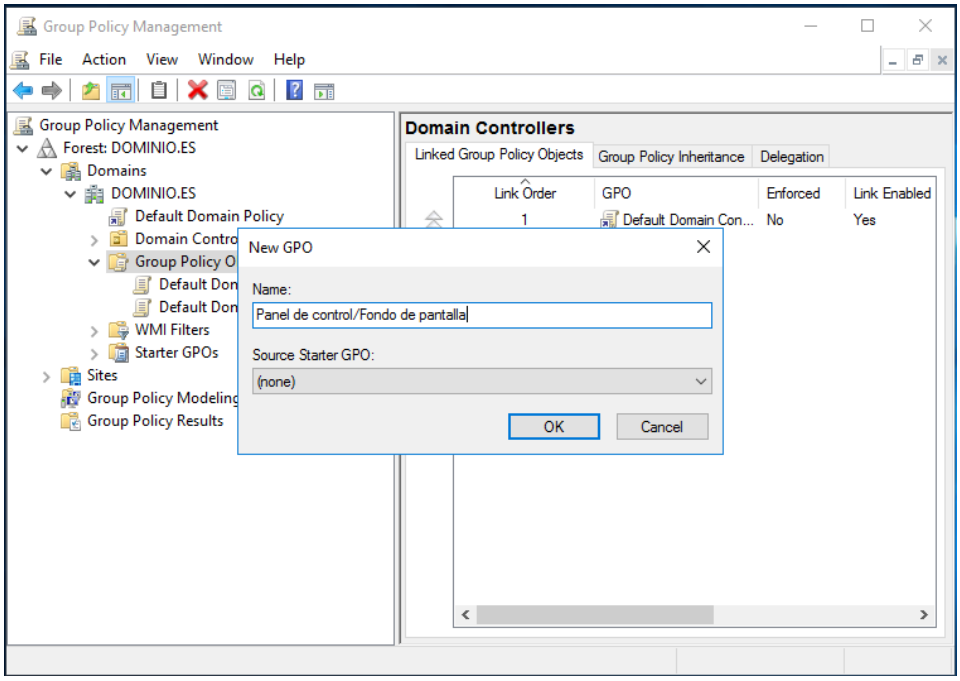


Figura 66.Nombre de la política

Una vez creada, se elige la opción de ‘’Editar’’ haciendo ‘’click’’ derecho sobre ella., y se busca la directiva que se desea añadir dentro de ‘’Configuración de Usuarios’’ y ‘’Policies’’. Desde el panel de control se eligen las opciones que conciernen a este desarrollo, es decir, ‘’Prohibit Access to Control Panel and PC Settings’’ y ‘’Prevent changing desktop backgrounf’’, como se observa en las siguientes dos imágenes. Mientras que en la primera imagen a continuación se muestra donde se accede para poder tener la opción de ‘Edit’ y posteriormente, en la siguiente imagen, se observa la opción que se debe elegir.

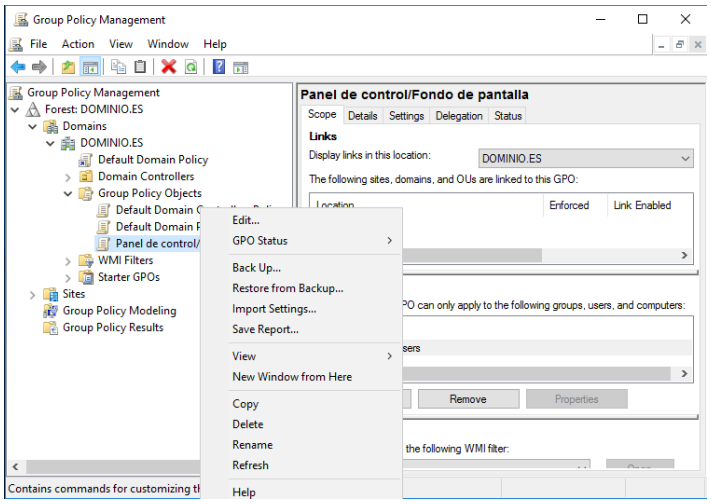


Figura 67.Opción de editar

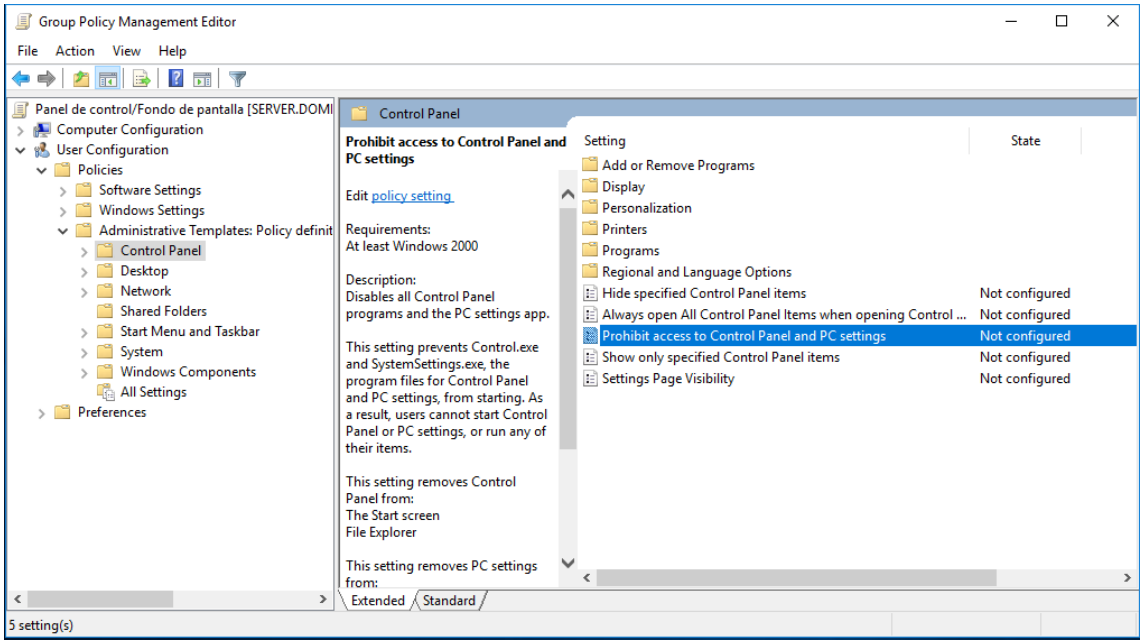


Figura 68.Acceso a panel de control

En cada una de las opciones correspondientes al impedimento de acceso del panel de control y cambio del fondo de escritorio se debe marcar la opción de ‘’Habilitada’’ para después elegir la opción de ‘’Aplicar’’. La siguiente imagen representa la pantalla una vez que se aplican las configuraciones, representa un panel en el que poder modificar las opciones escogidas.

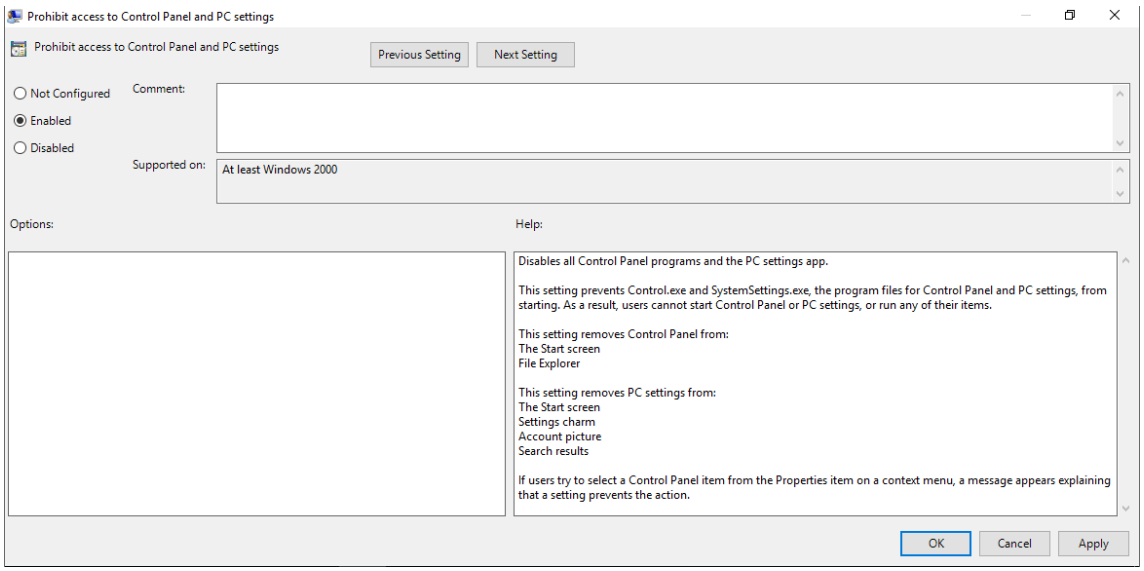


Figura 69.Prohibir acceso a panel de control

9.2 FONDO DE ESCRITORIO

Para prohibir cambiar el fondo de escritorio se habrá que redirigir hasta ‘’Personalización’’, como se muestran en las siguientes dos imágenes, en las que la primera representa el acceso a ‘personalización’ por medio de la pestaña de ‘Group Policy Management Editor’, ‘User configuration’.

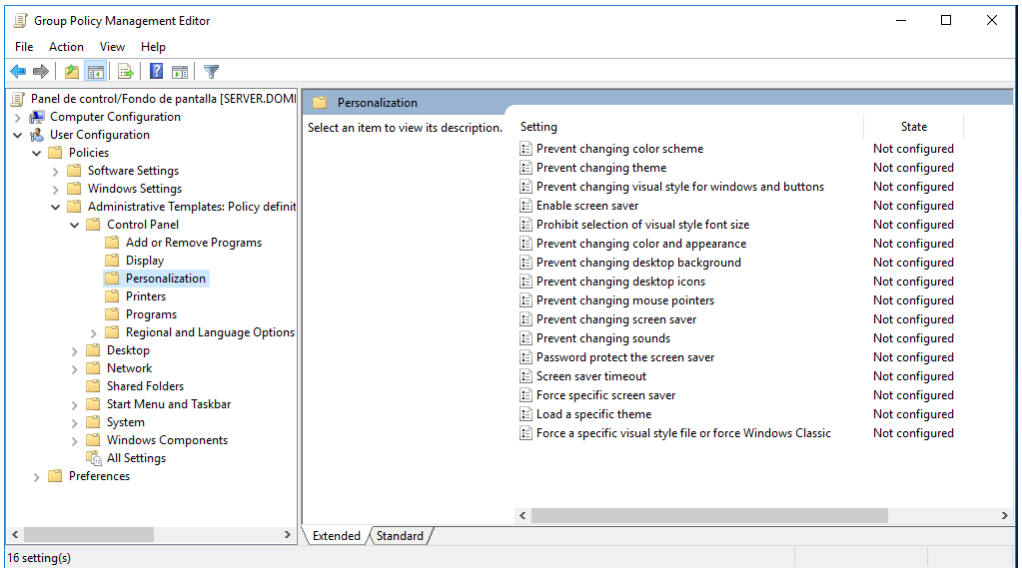


Figura 70.Personalización

Una ve que se accede a ‘Personalización’, se puede elegir qué parámetro configurar, en el que se elegirá ‘Prevent Chnaging Desktop Background’. Una vez que accedamos a configurar dicha opción, aparece esta pantalla plasmada en la siguiente imagen, en la que se procede a cambiar las configuraciones.

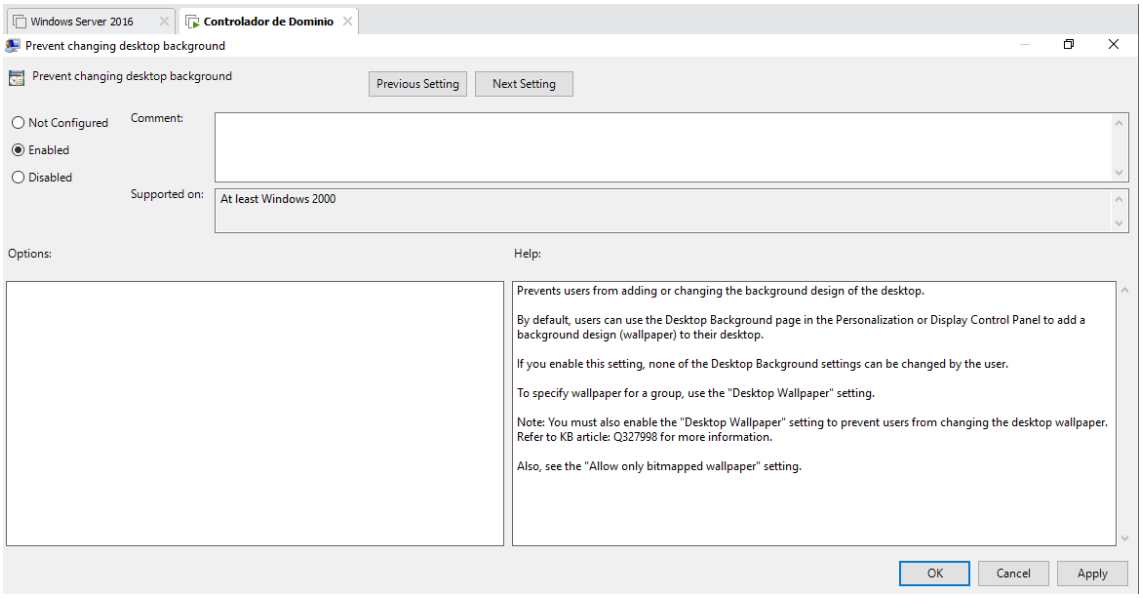


Figura 71.Prohibir cambiar el fondo de escritorio

Para poder aplicar esta política a los tres grupos anteriormente creados, desde la pestaña

''Delegación'', se pueden agregar los tres grupos, seleccionando en Propiedades la opción ''Aplicar directiva'', como se observa en la siguiente imagen. En la primera se accede a la pantalla donde poder insertar los tres grupos y la segunda es la imagen que enseña los tres grupos ya agregados a esta directiva.

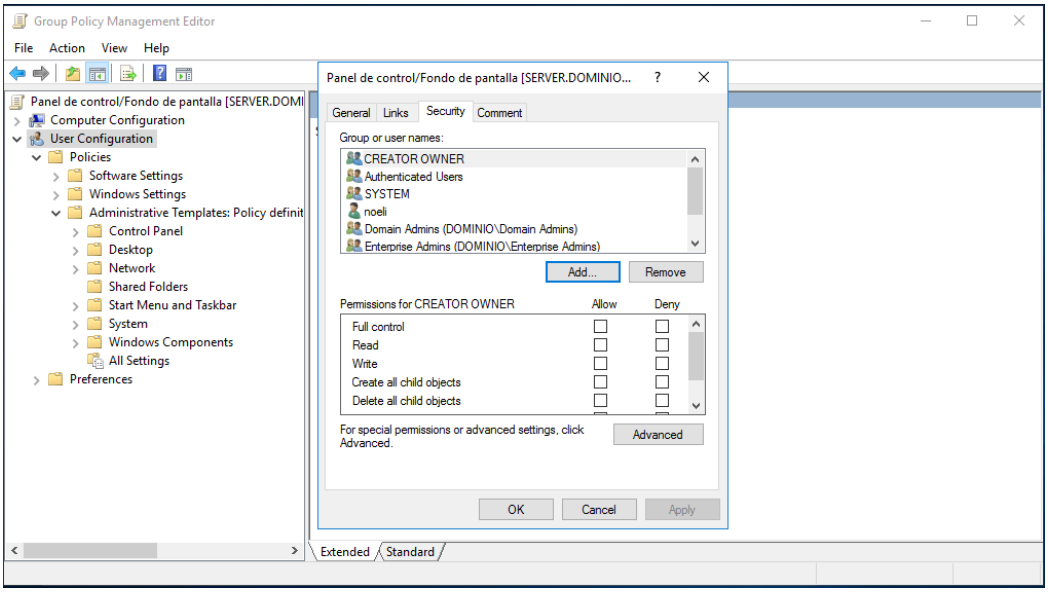


Figura 72.Agregar política

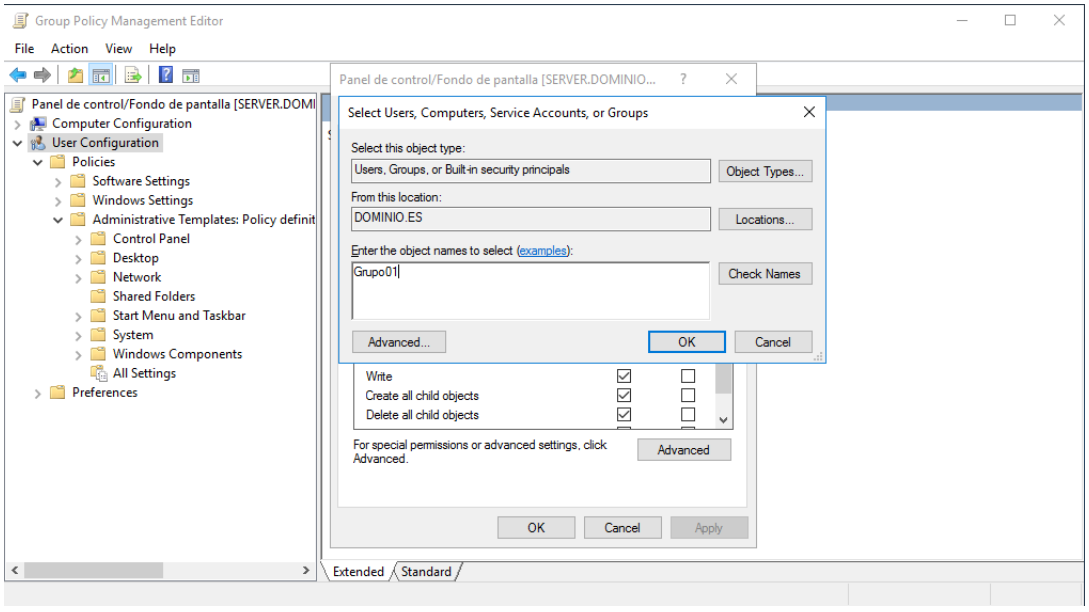


Figura 73.Agregar grupos

Posteriormente se modifican las propiedades de los usuarios de cara a la hora de acceso en sus respectivas sesiones, así como la autorización de acceso en otros dispositivos, como se muestra en la anterior imagen.

9.3. DIRECTIVAS DE USUARIO

En la primera imagen se muestra la ventana donde se configuran las horas de acceso de los usuarios y en la segunda el permiso de los usuarios a poder acceder en otros dispositivos. Dentro de las dos también se muestra el recorrido que se debe de hacer para poder acceder y configurar dichos parámetros. Para poder acceder a estas configuraciones, es necesario entrar dentro de las propiedades de los usuarios. Para la primera imagen es tan simple como pinchar en el apartado 'Logon Hours' como se muestra, y en la segunda imagen, se accede a esa configuración mediante el acceso por medio de 'Log On to'. Dentro de ellas se configuran los parámetros.

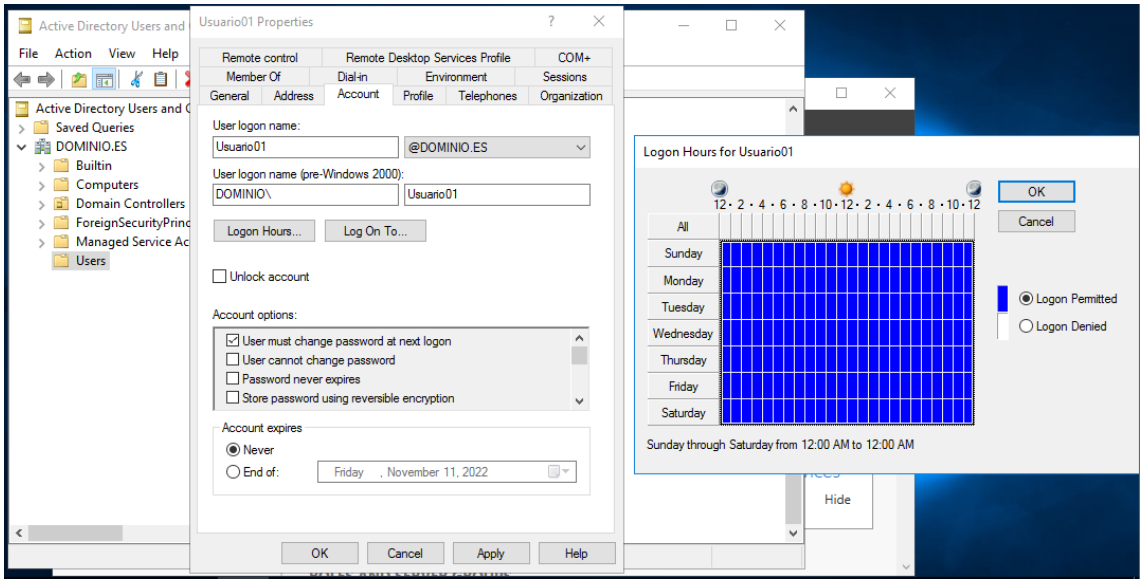


Figura 74.Acceso por horarios

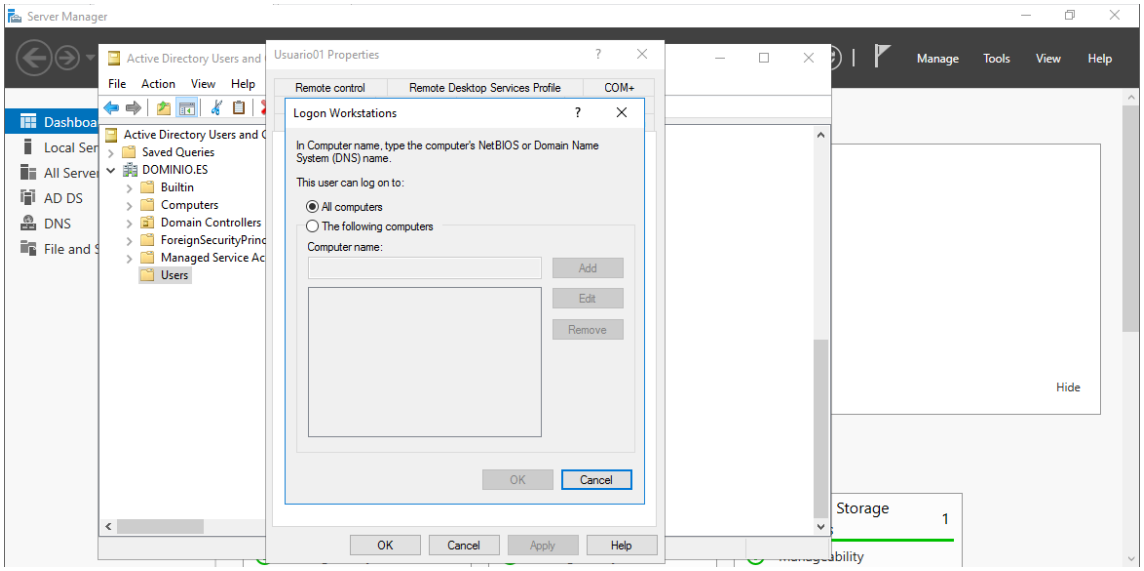


Figura 75.Acceso a otros dispositivos

Con estos dos controles se tienen vigilados las entradas de los usuarios a los dispositivos y el

rango de horas en el que pueden acceder al sistema.

ANEXO 10. Política de contraseñas

Para poder establecer una política de contraseñas, se debe de acceder al Centro de Administración de ‘’Active Directory’’. Posteriormente, se selecciona el dominio creado, ‘’Sistema’’, ‘’Password Seting container’’ y ‘’Nueva’’, ‘’Password Setting’’, como se observa en las siguientes dos imagénes. La primera imagen muestra la primera pantalla donde se accede, y de todo el desplegable de ‘Tools’ se pincha en ‘Active Directory Administration Centre’.

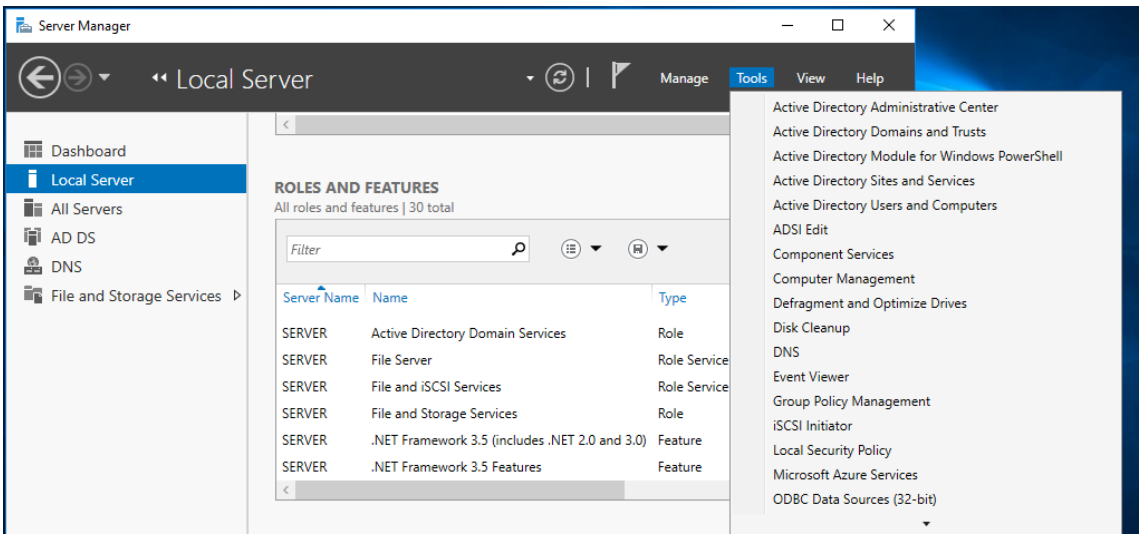


Figura 76.Centro Administrativo de A.D.

En la imagen siguiente, el recorrido que se ha de seguir es el siguiente, como se observa, ‘System’, ‘’Password Seting container’.

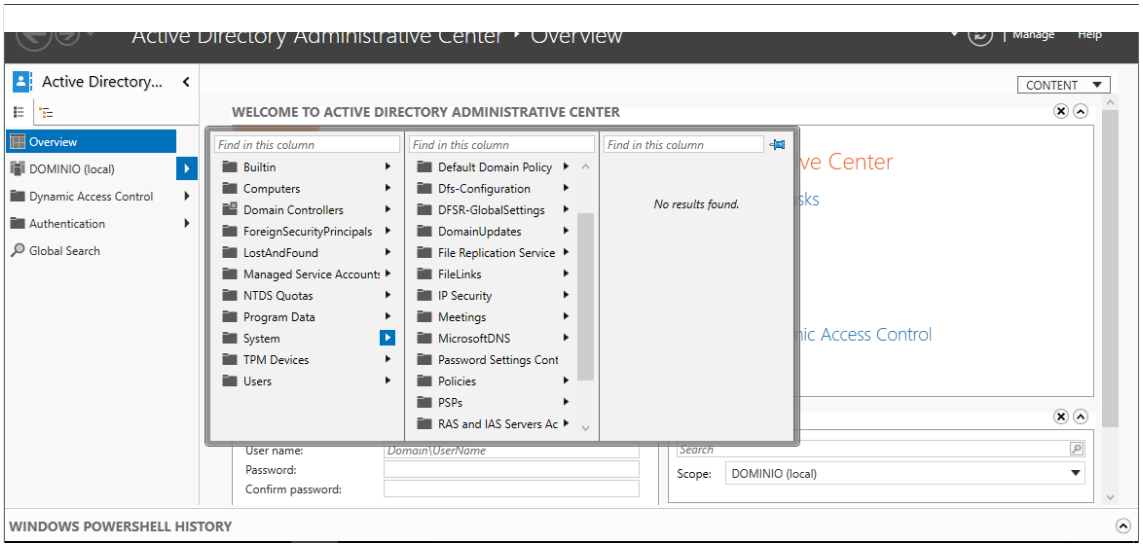


Figura 77.Sistema

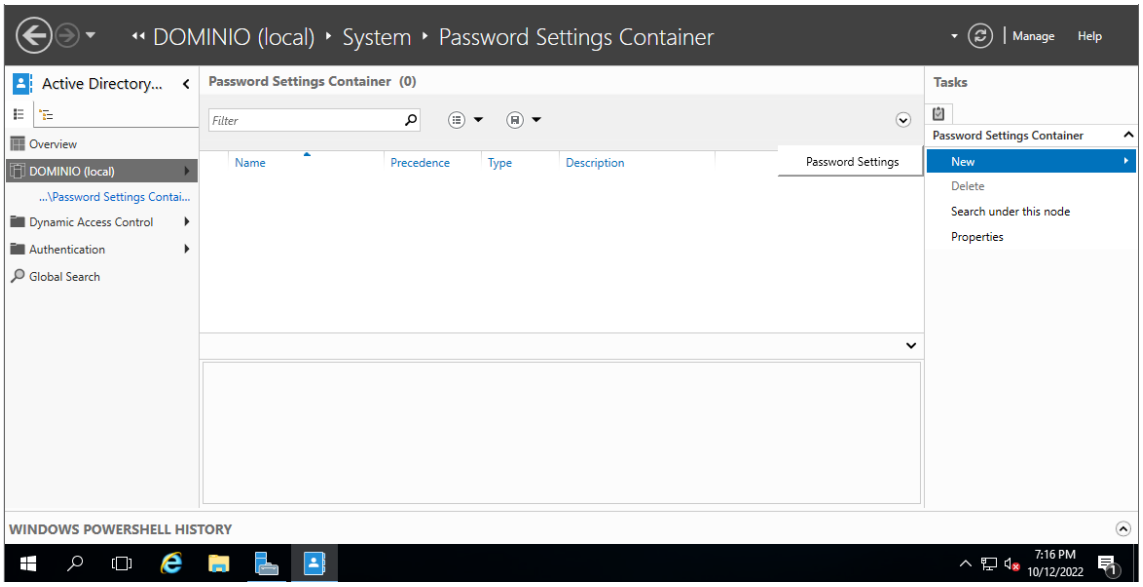


Figura 78.Nueva política de contraseñas

En la anterior imagen se observa la pantalla posteriormente de elegir 'Password container', en la que se elige crear una nueva regla de contraseñas, con las opciones que se observan elegidas. Una vez que se accede a crear una nueva política de contraseñas, se va al siguiente menú referenciado en la siguiente imagen.

Desde este menú (siguiente imagen) se pueden cambiar los requisitos de las contraseñas del dominio. Se elige un nombre para la regla ("PASS") y su número de precedencia que marca su prioridad. Configuramos la longitud mínima de 10 caracteres y un historial de 10 contraseñas. Desde el menú Añadir se puede seleccionar los grupos de usuarios a los que se quiere que aplique esta política. Se muestran los dos últimos pasos en las dos siguientes imágenes.

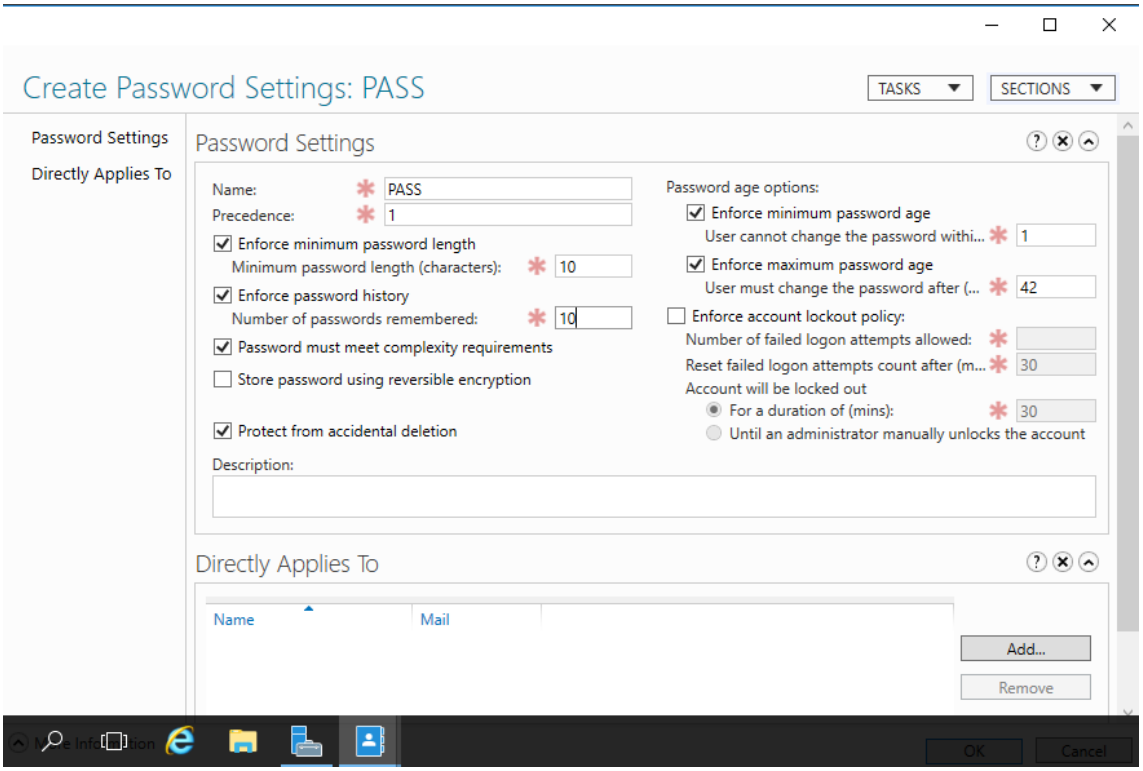


Figura 79.Política de contraseña

Una vez creada la nueva política de contraseñas, se configura el apartado de 'Directly Applies To', en el que se introducen los tres grupos como se muestra en la siguiente figura.

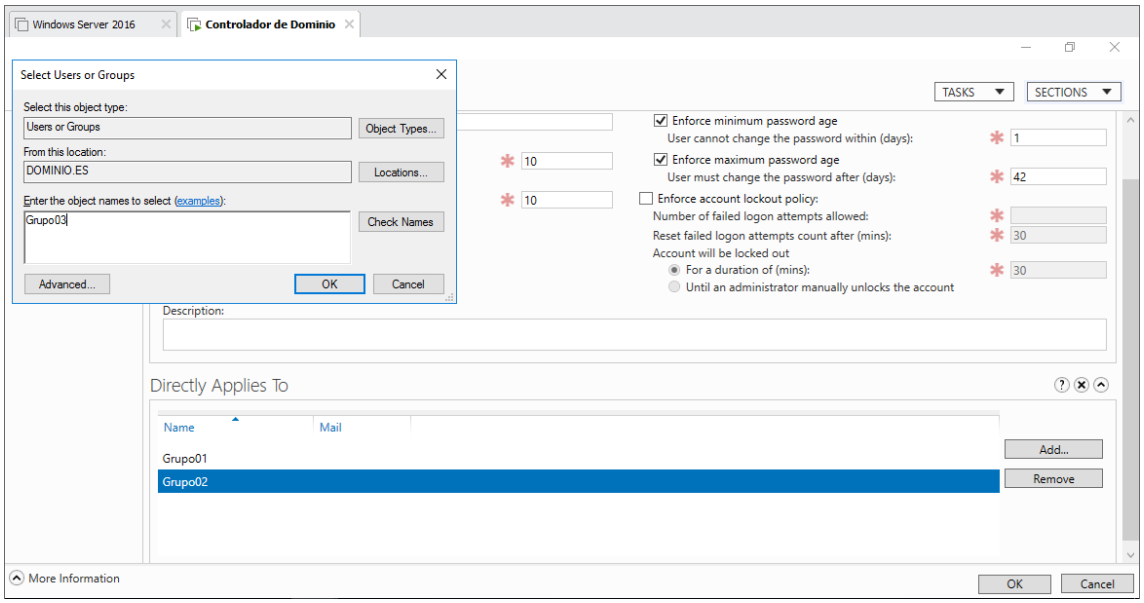


Figura 80.Añadir grupos a la política de contraseñas

ANEXO 11 Configuración AppLocker

En el siguiente anexo se va a proceder a la configuración de AppLocker. Para ello, en primer lugar, se debe habilitar la colección de reglas DLL. Se selecciona la tecla de Windows + R y se ejecuta el comando ‘’secpol.msc’’ para poder acceder a las Directivas de Seguridad Local. Posteriormente se selecciona las Directivas de Control de Aplicaciones y AppLocker. La siguiente imagen muestra el primer paso de introducir ‘secpol.msc’ en el ejecutable ‘Run’.

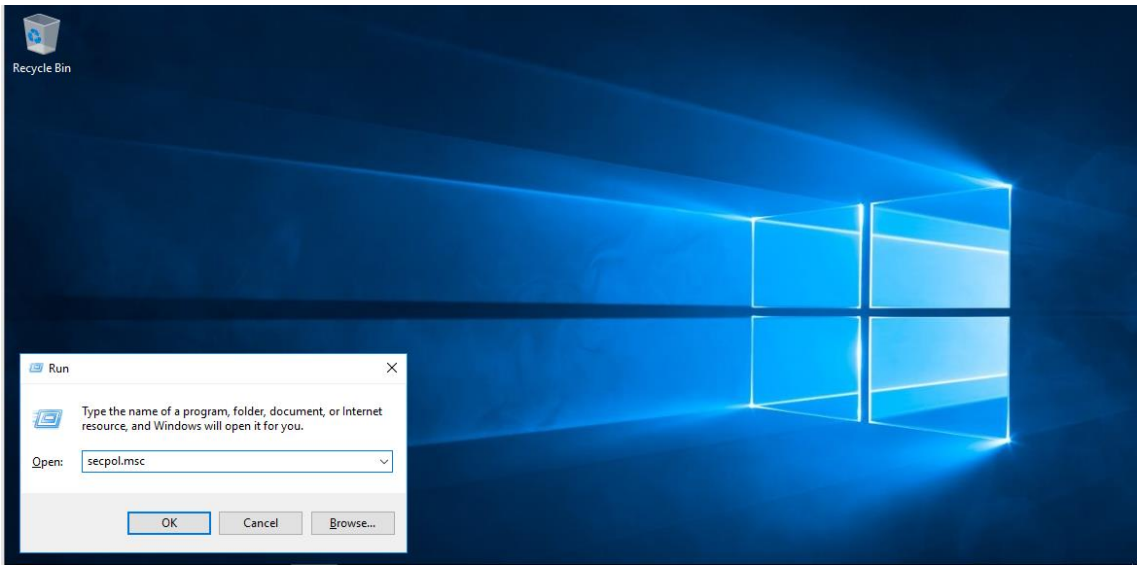


Figura 81.secpol.msc

En la siguiente imagen se observa los distintos apartados en los que se tiene que acceder para poder activar las reglas DLL. Estos son ‘Local Security Policy’, ‘Security Settings’, ‘Application Control Policies’, ‘AppLocker’ y ppsteriormente entrar en la configuración de sus propiedades para habilitar dichas reglas.

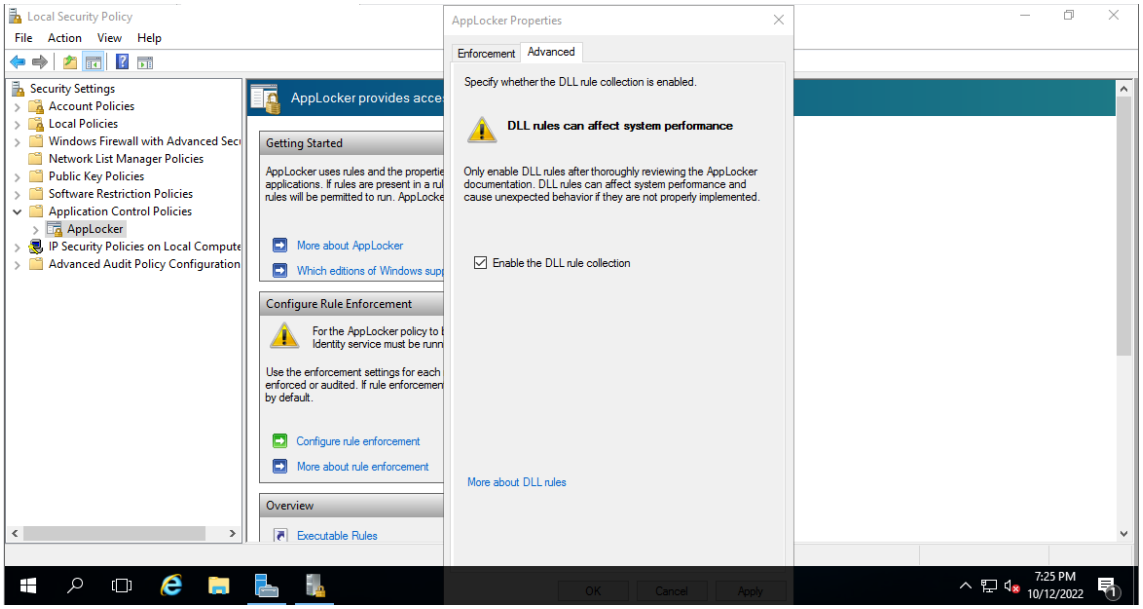


Figura 82.Reglas DLL

En la imagen siguiente se muestran los pasos a seguir para empezar a crear la nueva regla de AppLocker, que son acceder a ‘Executable rules’.’action’, ‘Create new Rule’.

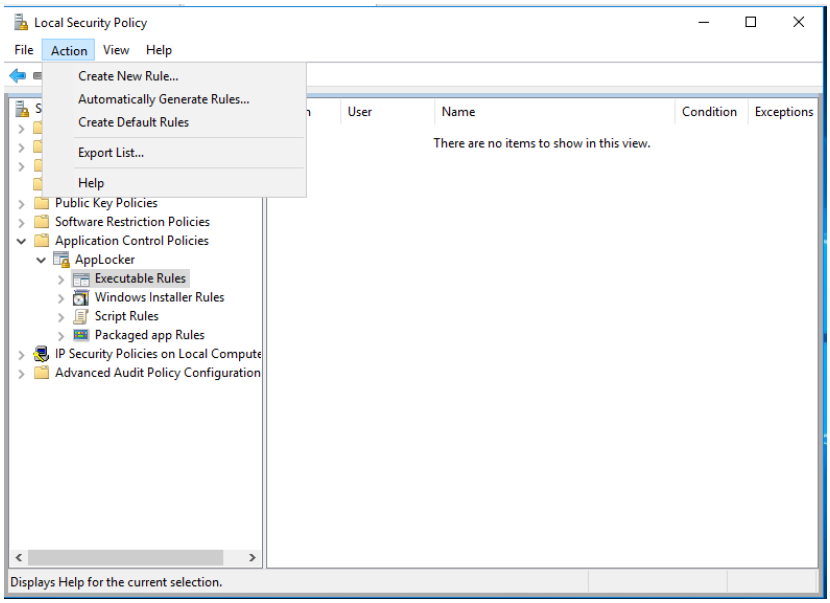


Figura 83.Crear una nueva regla

Al elegir crear una nueva política, en primer lugar, se desplegará una pantalla con opciones preparadas para ayudar a la configuración de esta regla. El primer paso, como se muestra en la siguiente imagen hay que elegir los grupos que permitimos que estén bajo esta política. Se incluyen todos los grupos creados, como la imagen siguiente muestra. La acción que se sigue es la de ‘deny’, en la que se niega que los archivos afectados con esta regla se ejecuten.

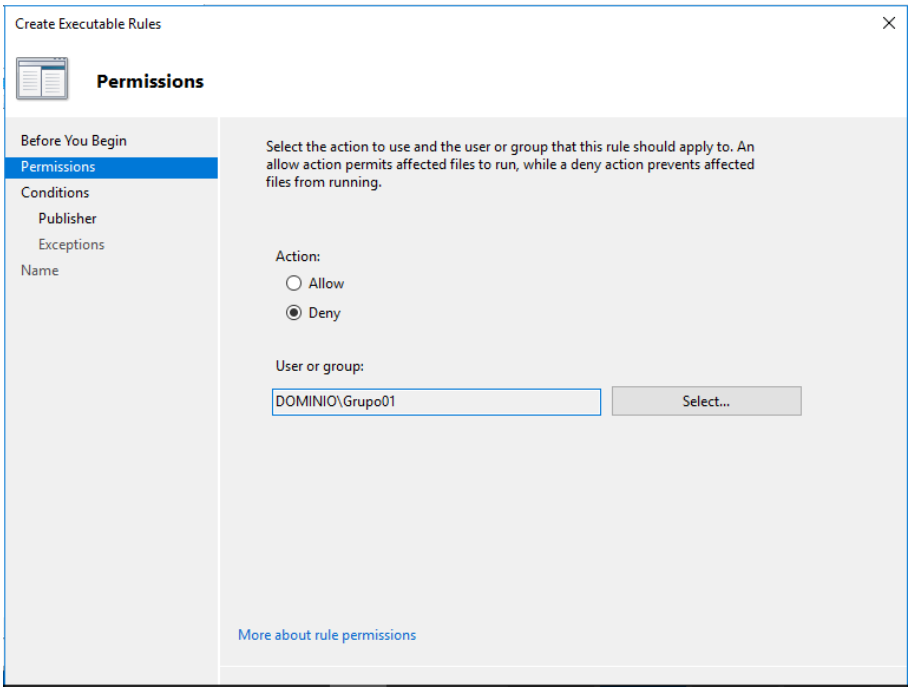


Figura 84.Permisos

En la siguiente ventana, se elegirá que esta regla se cree para una específica ruta de archivos

y carpetas, y por ello se elegirá la carpeta de la máquina donde se puedan depositar aplicaciones de origen malicioso. En la siguiente imagen se muestra la elección de regla de tipo camino o 'path' y en la siguiente la ruta seleccionada en donde se deniegan la ejecución de los programas entrantes.

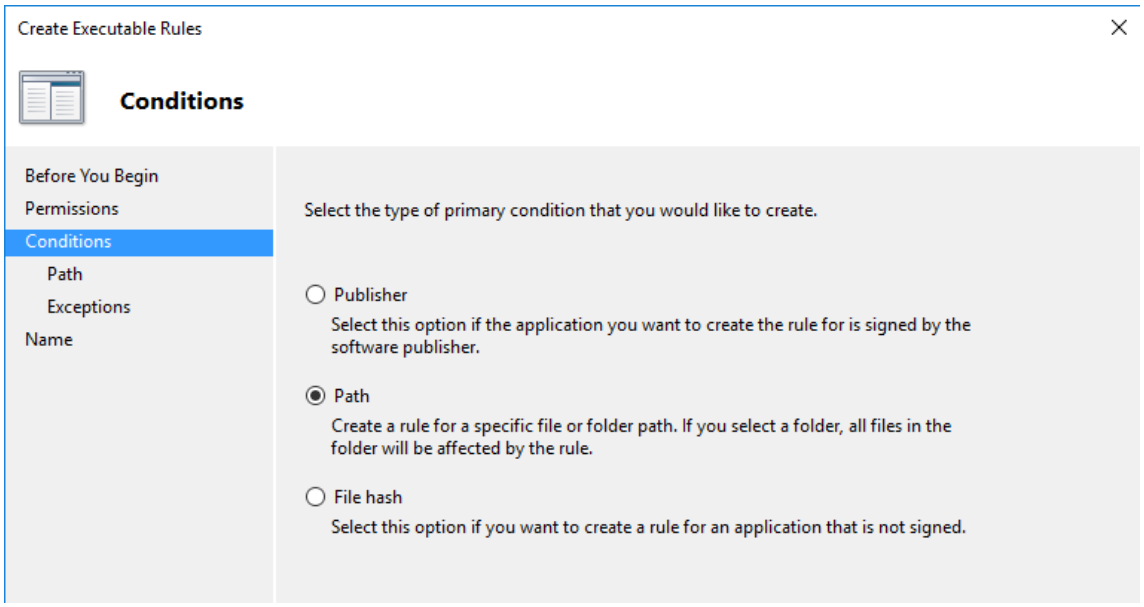


Figura 85.Condiciones de la regla

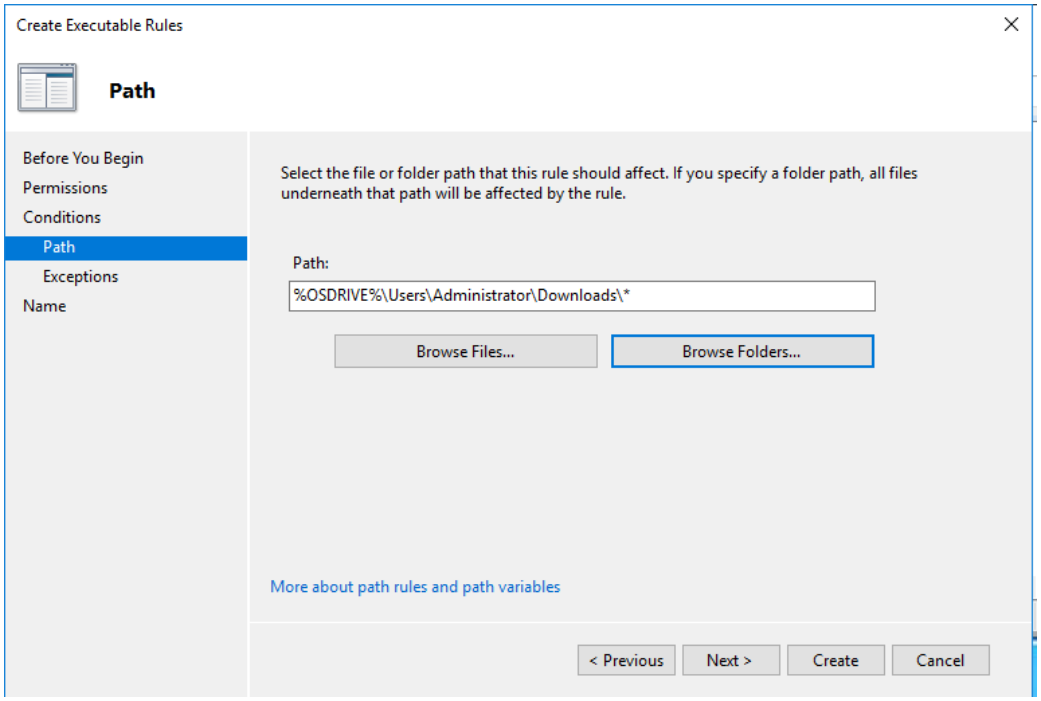


Figura 86 Elección de la ruta.

En las excepciones no se elige ninguna. Posteriormente se le da un nombre a la nueva regla creada. Dentro de las reglas ejecutables de AppLocker se podrá observar la creación, como se muestra en la siguiente imagen, la cual, una vez creada, permite tener modificaciones accediendo a cada una de estas líneas de reglas.

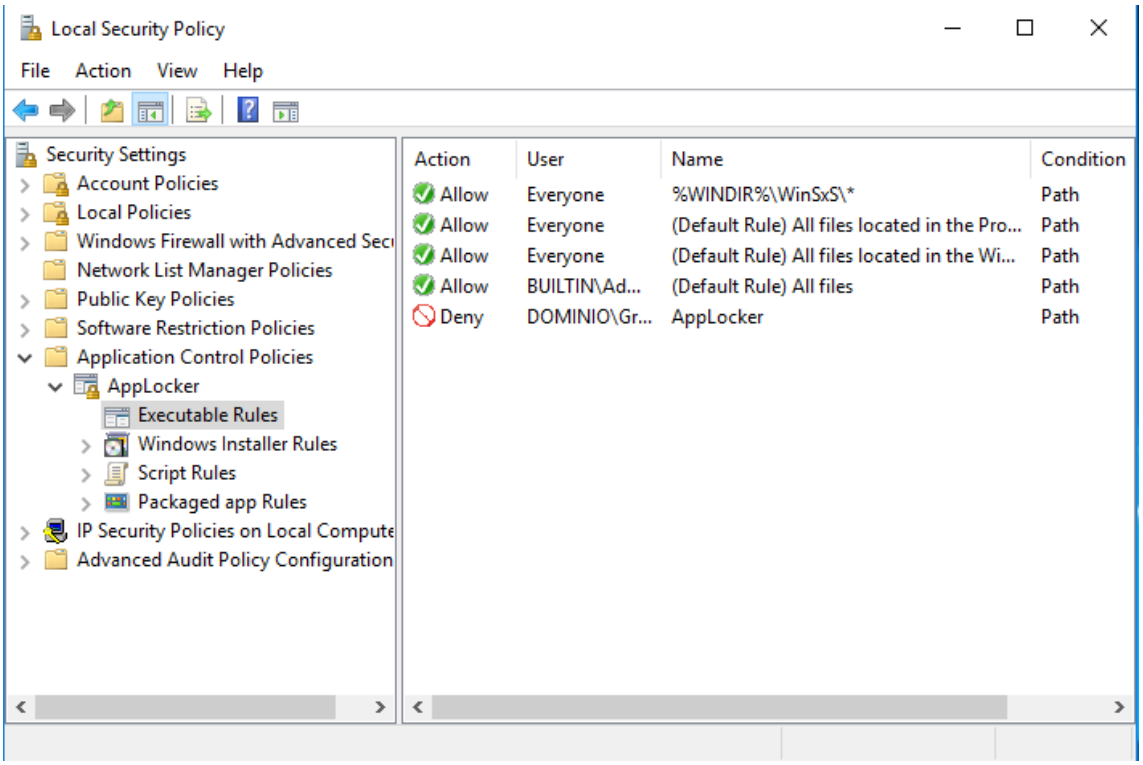


Figura 87.Regla AppLocker

ANEXO 12 Configuración del Firewall de Windows con seguridad avanzada

En este anexo se llevará a cabo la configuración de una nueva regla dentro del Firewall de Windows con seguridad avanzada. La siguiente imagen muestra los pasos a seguir para poder entrar dentro de los parámetros modificables de Windows de Seguridad avanzada. Desde el buscador de Windows se accede a “Windows Firewall with Advanced Security” donde se muestra un resumen de las reglas activas y la gestión de estas. El administrador de las reglas del Firewall permite la creación de nuevas reglas a través de un asistente paso a paso. A continuación, se muestra el proceso de creación de la regla. En primer lugar, hay que seleccionar la opción “*New Rule*” para iniciar el asistente de creación de una nueva regla.

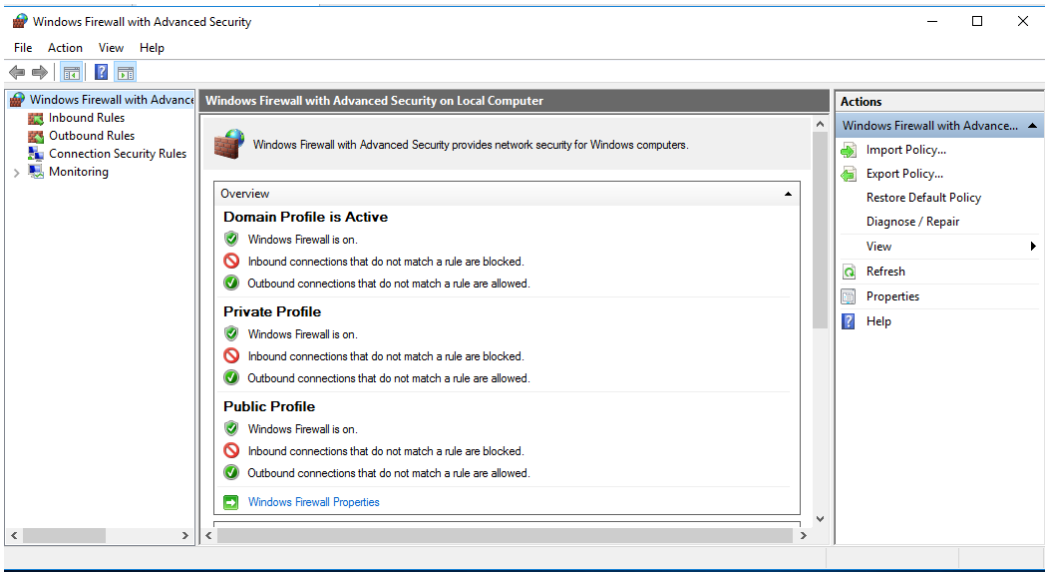


Figura 88.Firewall con seguridad avanzada

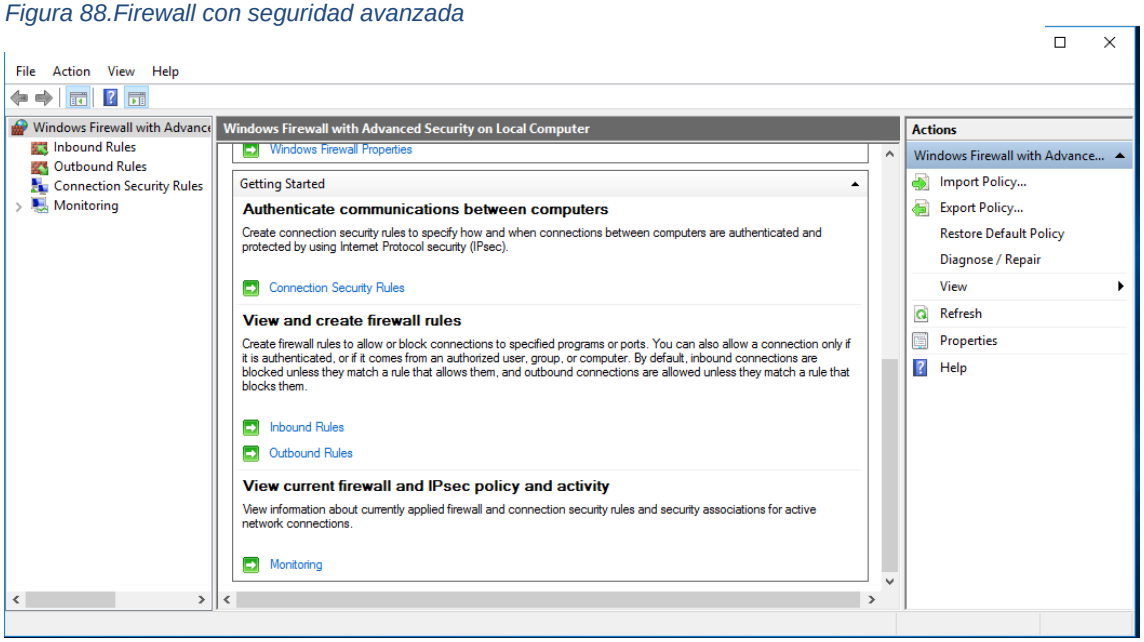


Figura 89.Crear una nueva regla

La anterior imagen muestra la interfaz de entrada del Firewall con seguridad avanzada, junto con las opciones que tiene, de las cuales, para poder crear la nueva regla, se deberá elegir la opción de ‘’inbound rules’’ dentro de ‘view and create firewall rules’. Una vez que se accede a la creación de una nueva regla, aparecerán una serie de opciones.

Como veremos en la siguiente imagen, esta regla se creará para controlar los programas que toman conexión con el dispositivo, y por lo tanto se marca la opción de ‘promgram’

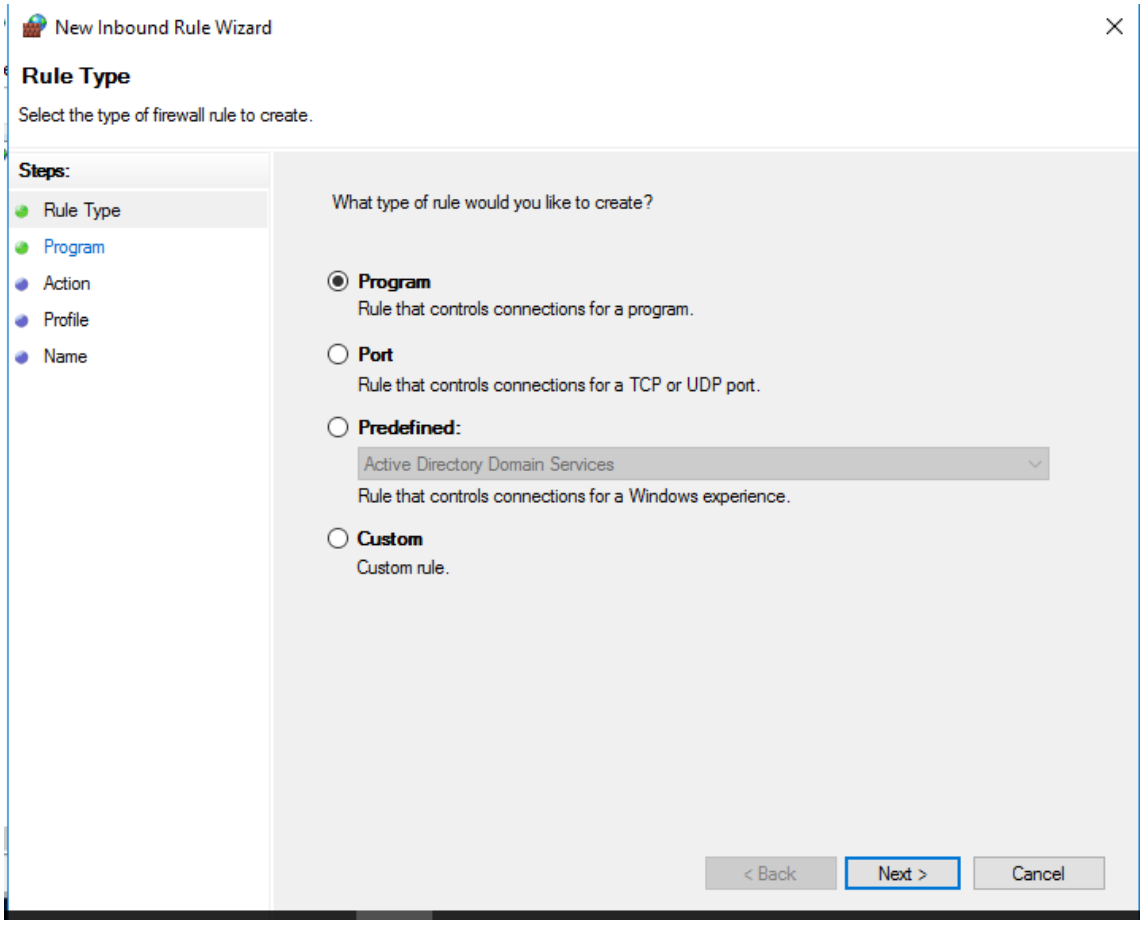


Figura 90.Tipo de regla

El siguiente paso será aclarar qué programas esta regla abarcará, de la cual se señalarán que ‘’todos los programas’’, como se ve en la siguiente imagen., en la que se especifica que esta regla se aplica a todas las conexiones en el dispositivo que coincidan con otras propiedades de la regla.

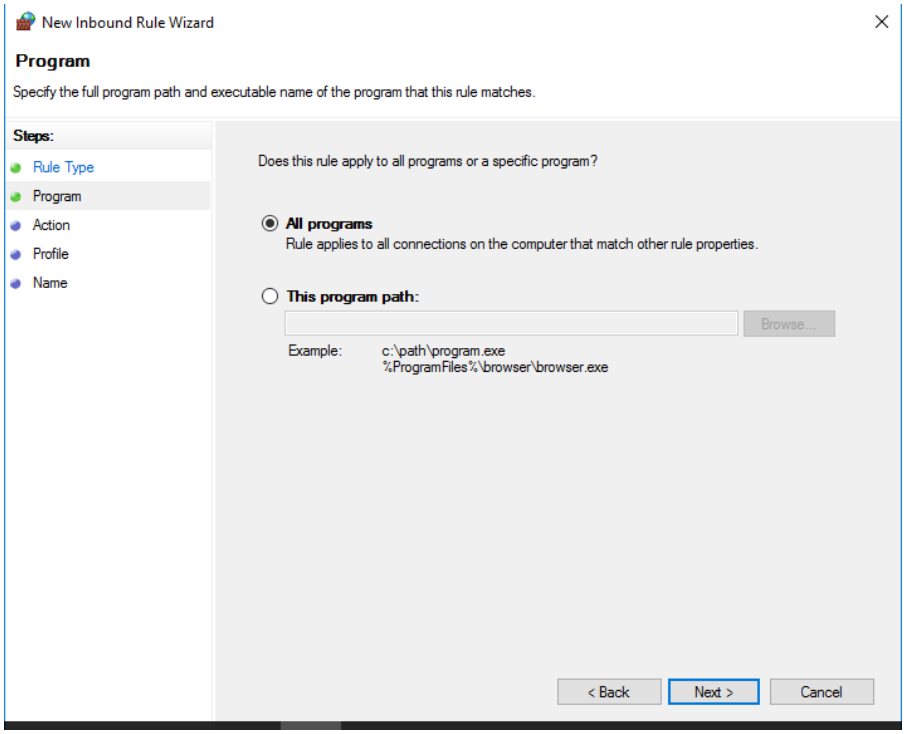


Figura 91.Programas que abarca la regla

En el apartado de ‘’acciones’’, se elegirá la opción que define que la conexión tan solo se establecerá si se considera previamente que puede ser una conexión segura, como se observa en la siguiente imagen, en la que especifica que solo se permiten conexiones que han sido autenticadas por medio de la utilización de Ipsec, y que los conectores están securizados por medio de las reglas establecidas en Ipsec y las reglas establecidas en el nodo de seguridad de conexión.

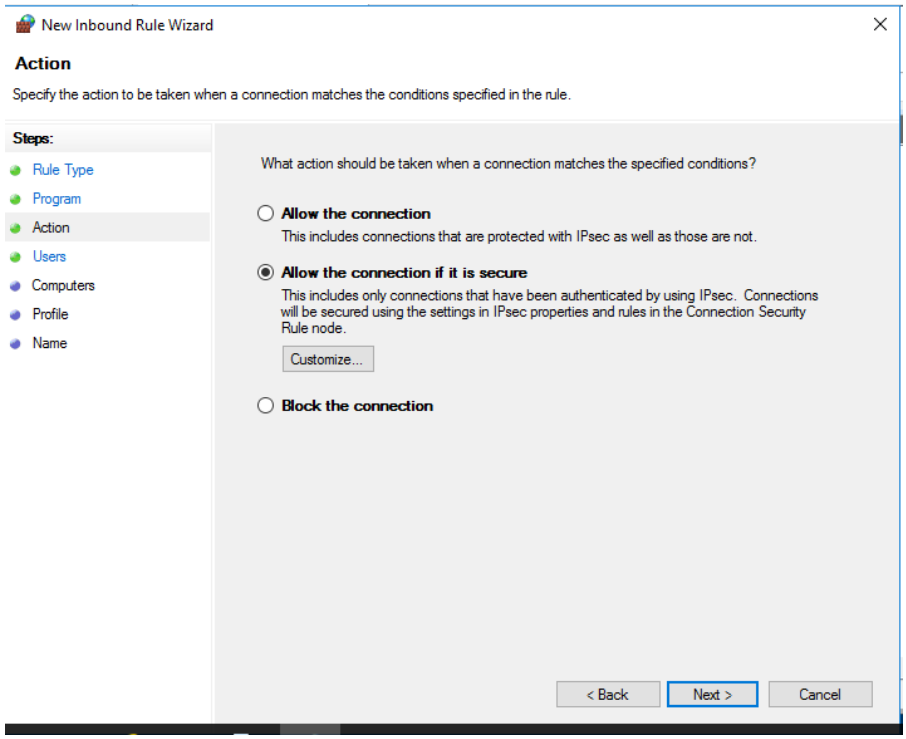


Figura 92.Conexión solo si es segura

En el siguiente apartado se autorizan las conexiones solo de usuarios autorizados, los cuales corresponden a los que forman parte de los tres grupos, como se observa en la siguiente imagen.

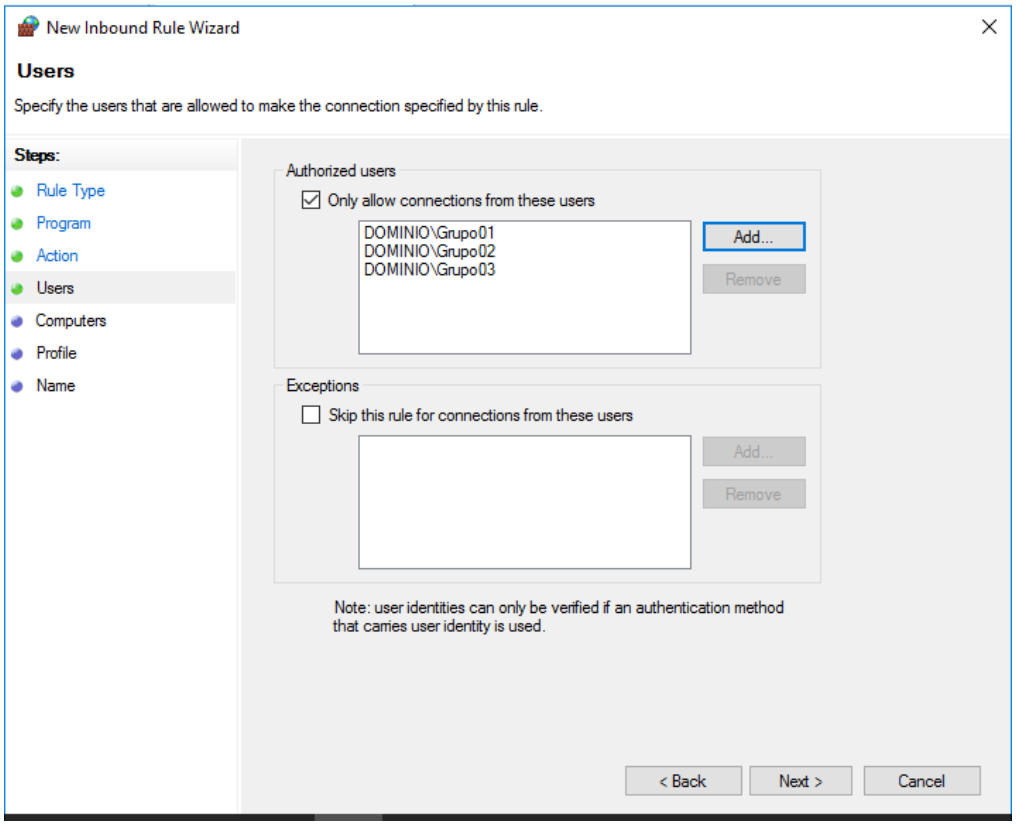


Figura 93.Permisos de conexión

En el apartado de ordenadores no se permitirá la conexión con otro dispositivo externo. Posteriormente se define los ámbitos en los que esta regla se aplica, los cuales serán todos, como se observa en la siguiente imagen. Esto significa que esta regla se aplicará tanto dentro del dominio como en una red pública o privada.

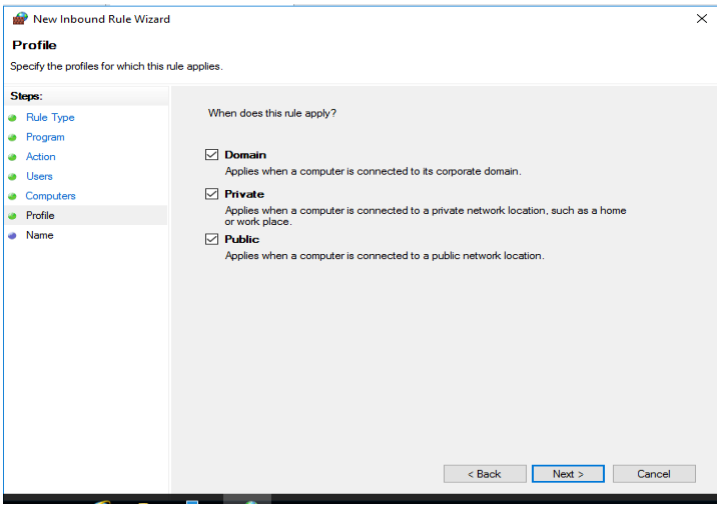


Figura 94.Aplicaciones de la regla

Posteriormente se le dará un nombre y se termina de crear como se ve en la siguiente imagen. Se podrá observar la nueva regla creada dentro del apartado ‘’inbound rules’’. Todos estos pasos se observan en las siguientes imágenes, en las que nos encontramos la elección de nombre de la regla y el resultado de la creación de esta.

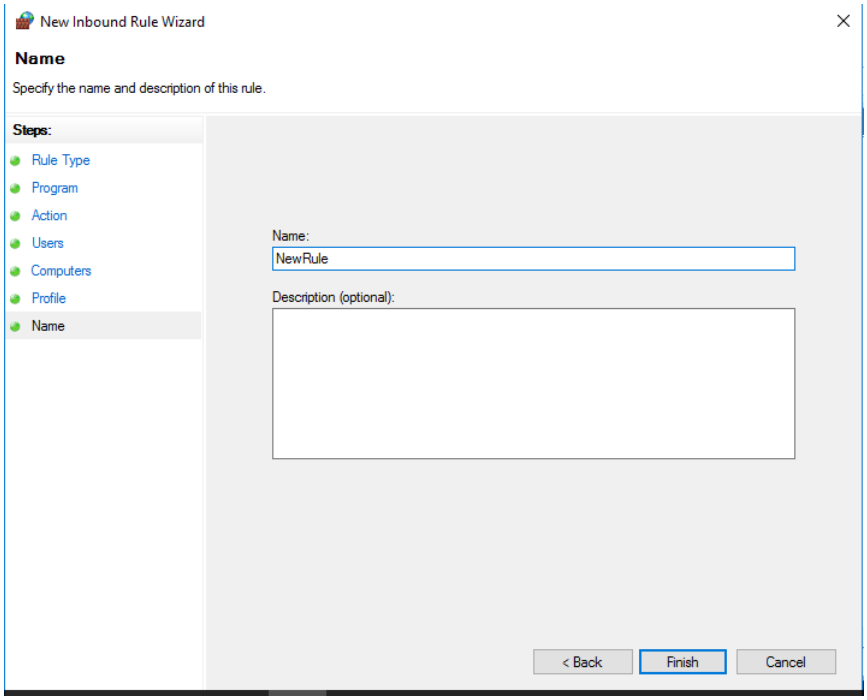


Figura 95.Nombre de la regla

Como se ve en la siguiente imagen, está la nueva norma desplegada en su totalidad con todas las configuraciones hechas dispuestas en cada una de las líneas.

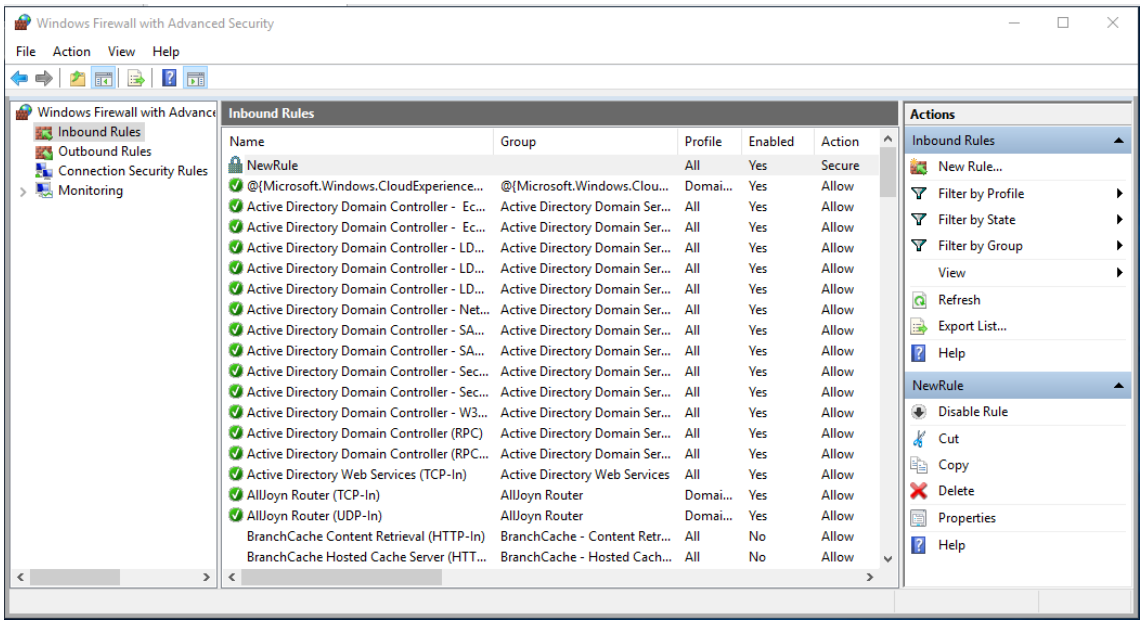
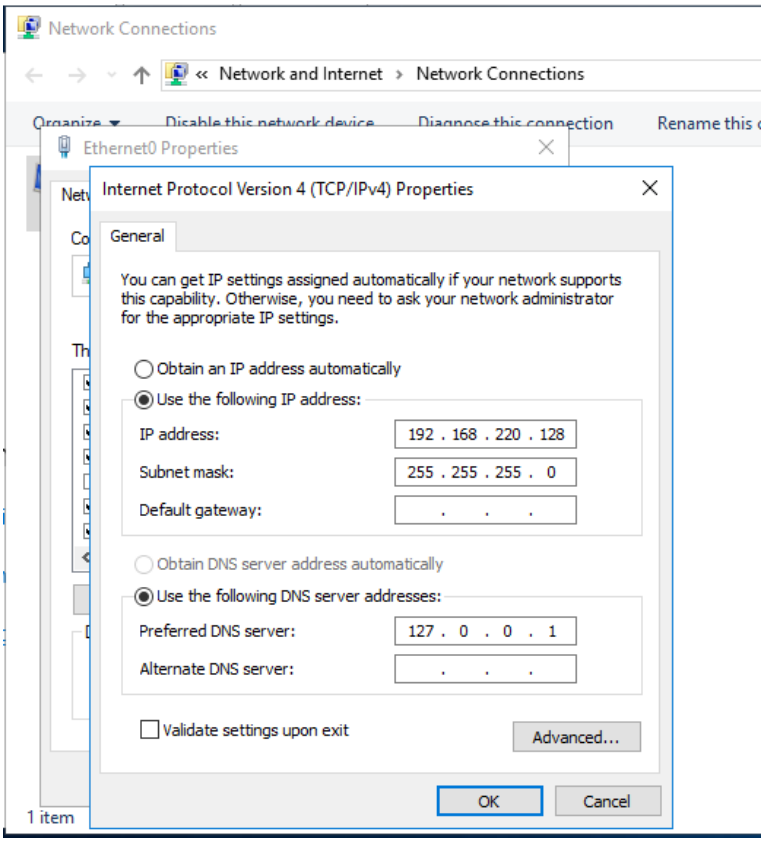


Figura 96.Regla creada

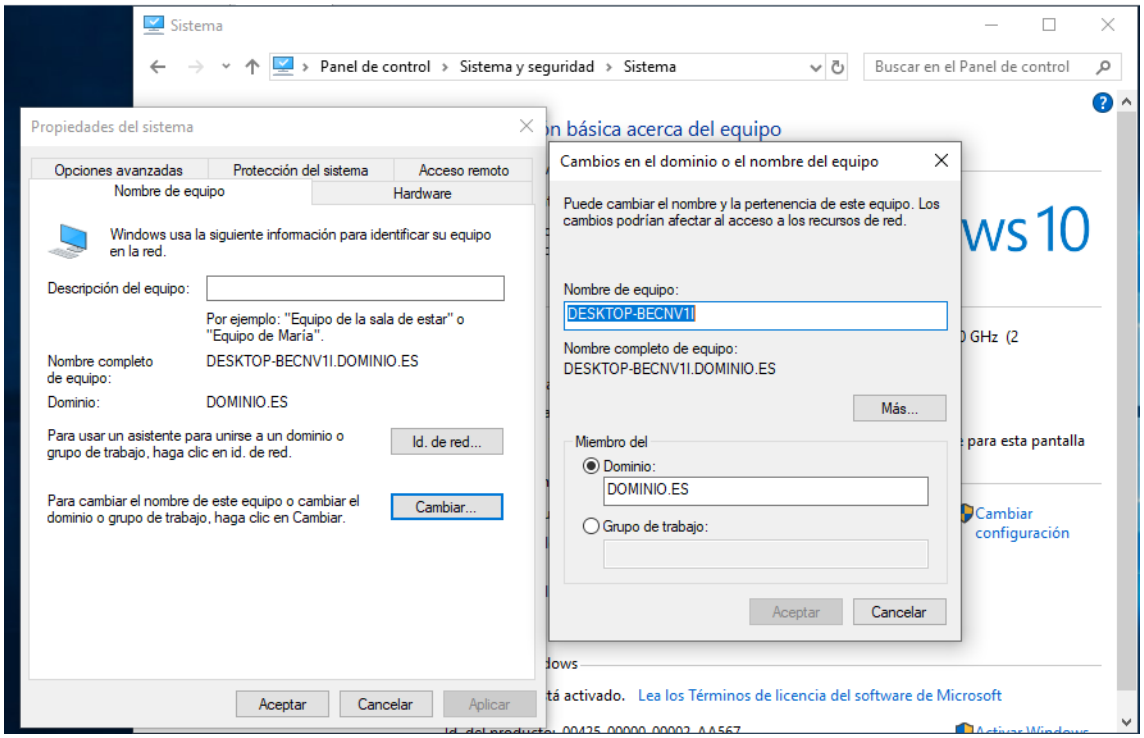
ANEXO 13 Enlace a máquina local

En este anexo se procederá a explicar cómo enlazar la máquina con Windows 10 con el servidor de 2016. En primer lugar, se crea la máquina de Windows 10, siguiendo los mismos pasos que en el anexo de 'creación de máquina virtual' con el único cambio que el sistema operativo que se debe de poner será el de Windows 10. Para enlazar una máquina al dominio creado, en primer lugar, se debe acceder al Centro de redes y recursos compartidos del Panel de Control. Desde ahí, seleccionando la conexión Ethernet0, se puede configurar la dirección IP del servidor DNS al que se quiere conectar; en este caso, la dirección de la máquina donde está desplegado el servidor. La imagen siguiente representa los pasos que se deben seguir, desde acceder al panel de 'Network and internert', 'network connections', 'ethernet0 properties' hasta la configuración su dirección IP, máscara y DNS server.



Fígura 97.Dirección IP del servidor

Esta Dirección IP del servidor de Windows 2016, será la que habrá que establecer como dirección IP del DNS en la máquina de Windows 10. Una vez configurado, el siguiente paso es acceder a la pantalla de Sistema dentro del Panel de control de la máquina virtual de Windows 10. Seleccionando "Cambiar configuración", se accede a la ventana de Propiedades del Sistema. Ahí se puede cambiar el dominio al que pertenece el equipo. Se solicitará al usuario que ingrese las credenciales de un usuario perteneciente al dominio. Tras reiniciar el equipo, se podrá acceder al dominio desde la opción Otros Usuarios en la pantalla de inicio de sesión. La siguiente imagen representa la conexión al dominio de Windows 10 por medio de los pasos antes dichos.



Fígura 98.Vincular a la máquina local al dominio

Con estos pasos hechos, ya está vinculada la máquina virtual de Windows 10 la dominio creado de Windows 2016.