

CIBERSEGURIDAD PRÁCTICA

Nombre Asignatura Ciberseguridad:
Módulo Asociado: Unit 5: Security
Profesor: Walter Llop Masia
Curso: 2021/2022
Autor: José M^a Sánchez Carnero



Índice/Index

1.- Características, servicios y recursos de la empresa	3
2.- Amenazas existentes	4
3.- Soluciones de seguridad	6
4.- Plan de gestión de riesgos	23
5.- Políticas de seguridad implementadas	27
6.- Planes de recuperación de desastres	43
7.- Bibliografía	44



1.- Características ,servicios y recursos de la empresa

La empresa KMP es una compañía pequeña que realiza trabajos como third party para otras compañías, encargándose del desarrollo de juegos de una gama bastante alta y gran volumen mediático pese a su tamaño.

Sus juegos no envuelven un carácter competitivo pero cuentan con un multijugador de máximo 4 personas por lo que no se requiere un estado excelente e impecable de los servidores, pero aun así se vela por conseguir tal calidad. La empresa quiere velar por sus usuarios y su privacidad en medida de lo posible para poder garantizar la mejor experiencia posible.

KMP Cuenta con un grupo de 10 programadores, y 15 artistas y diseñadores, incluyendo a los lead y el director y manager son 30 integrantes en total.

Entre los activos de la empresa se encuentran 30 ordenadores, conectados vía ethernet a un router. El equipo de artistas cuenta con tabletas gráficas en sus ordenadores para el desempeño de su trabajo . También tienen montado un pequeño servidor para hospedar su página web. Sin embargo tienen contratado el servicio de un servidor externo para hospedar las partidas online.



2.- Amenazas existentes

Threat Actors :

Perfiles de usuario o grupos de usuarios maliciosos que pueden suponer una amenaza para la compañía.

Script kiddies o Newbies

Estos son usuarios inexperimentados, por lo general nunca utilizan código propio ya que carecen de los conocimientos y experiencia requeridos para realizar sus propios ataques. Su falta de experiencia a la vez puede llegar a ser muy dañina siendo impredecibles si consiguen tener éxito en un ataque. Tienen un gran volumen de usuarios por lo que es común recibir un ataque de este estilo. Tomar las medidas de seguridad básicas suelen mantenerlos a raya.

Ciberdelincuentes

Estos usuarios son más experimentados y tienen mayores conocimientos. Estos son protagonistas de ataques más serios, como robos de información, accesos a redes privadas, estafas, piratería, fraudes, publicaciones y ventas de datos privados o ilegales. Los ciberdelincuentes suelen trabajar solos o en pequeños grupos y tienen intereses económicos en su mayor parte por lo que pueden ser una potencial amenaza.

Hacktivistas

Son grupos de personas experimentadas que se mueven por ideales tanto políticos como ideológicos. Las formas de ataque más utilizadas por estos son robo de información y sabotajes virtuales como ataques DoS y DDoS, modificaciones de sitios web y redirecciones. Estos grupos podrían llegar a suponer una amenaza dependiendo de las relaciones de tu empresa con el resto, pudiendo llegar a situar a la empresa en el punto de mira, también la actitud del equipo de la empresa en redes sociales y prensa podría llamar la atención de los hacktivistas.

Gobiernos

Grupos gubernamentales con un presupuesto enorme y personal cualificado. El objetivo principal de los gobiernos es la información por lo que no son una potencial amenaza, aunque las relaciones de la empresa puede llegar a captar la atención de estos.

Ciberterroristas

Estos grupos se mueven por motivos políticos o religiosos, pueden llegar a ser realmente dañinos a nivel humano. Al igual que con los gobiernos y los hacktivistas, no es común estar en el punto de mira de este grupo, pero las relaciones externas pueden llevarte a ser un objetivo pero esto sería extremadamente difícil.

Threat Vectors :

Estas son las formas de ataque perpetradas por los threat actors para conseguir sus objetivos.

Malware

Es la forma de denominar al software malicioso, siendo creado para dañar, extorsionar o extraer información del equipo del usuario sin que este tenga conocimiento de ello. Es común que estos sean ejecutados sin conocimiento previo de los usuarios, de ahí su peligrosidad.



El malware es una de las herramientas más comunes utilizadas por los threat actors para atacar por lo que es un punto crucial a tener en cuenta a la hora de defenderse, estos tienen una amplia variedad entre los que encontramos gusanos, troyanos, bombas lógicas..

Ransomware

Es un tipo de malware que bloquea el ordenador de la víctima, el atacante suele amenazar con el bloqueo permanente del acceso al dispositivo si no se le paga una suma de dinero por el desbloqueo del dispositivo. Este tipo de malware es bastante común y suele descargarse pasando desapercibido por el usuario junto a otros elementos infectados.

Hardware externo

La conexión de hardware externo tales como dispositivos USB en un equipo de tu red local puede ser potencialmente peligroso , ya que estos pueden contener malware sin que el usuario de este dispositivo externo necesariamente lo sepa, llevando a la posible infección de la red local.

E-Mail

Uno de los ataques más comunes y efectivos, el envío masivo de correos es muy habitual en técnicas de phishing , donde la víctima es redirigida a una página web que, aunque luzca como la página original, es un fake, buscando que el usuario introduzca los datos “*Usuario*” y “*Contraseña*” para extraerlos, a continuación suelen dar un mensaje de error en el acceso y redirigiendo a la página original para no levantar sospechas del usuario. Los E-mail además pueden traer archivos adjuntos que estén infectados con malware.

Esto es una amenaza potencialmente grande para la empresa ya que implica el factor humano y cierto conocimiento sobre estas técnicas por parte del usuario para evitarlo.

Web

Los ataques a tu servidor web son un riesgo a asumir a la hora de crear un sitio web, y son un punto a tener en cuenta. Entre ellos encontramos XSS (Cross-Site Scripting) introducción de código js para obtener información (cookies..), SQL injection (ataques a bases de datos de tu página web con la utilización de queries), fuzzing, DDoS (Distributed Denial of Service) y ataques por fuerza bruta entre otros.



3.- Soluciones de seguridad

VPN (Virtual Private Network)

Una VPN oculta tu dirección IP al navegar por la red, redirigiéndote por una ruta específica hasta el host de tu VPN, un túnel seguro donde tu tráfico de paquetes será cifrado. Esto significa que tu identidad será ocultada, protegiéndote del acceso externo, haciendo que sea más difícil seguir tus movimientos en la red y el robo de información.

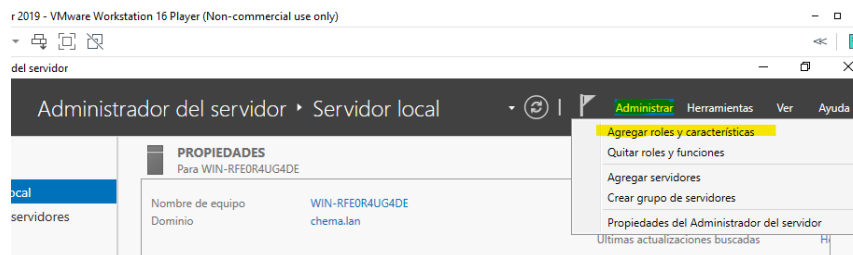
Al ser una red privada tus actividades online serán escondidas en las redes públicas, para leer los datos que viajan por una VPN necesitas una llave de cifrado única haciendo que el acceso a tu información sea prácticamente imposible sin una. El host de tu VPN oculta tu localización, dándote posible acceso a páginas que pueden estar ocultas por región.

En nuestro caso nuestros trabajadores pueden trabajar de forma remota contra nuestro servidor, para garantizar una conexión segura entre un ordenador externo a nuestra red local será necesario el uso de una VPN para así reducir riesgos.

Implementación de VPN

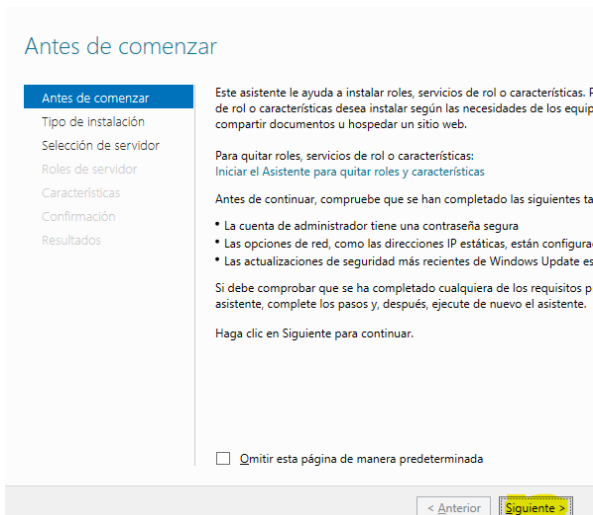
Para la implementación de VPN en windows server debemos seguir los siguientes pasos:

- Abrimos el administrador de Windows Server y clicamos en administrar. Tal y como se muestra en la imagen aparecerá un desplegable y seleccionaremos la opción “agregar roles y características”



- Se nos mostrará una ventana del asistente para agregar roles con diferentes pasos. El primero de todos será la ventana de antes de comenzar donde presionaremos siguiente.

Asistente para agregar roles y características





- Seleccionar tipo de instalación usaremos la opción de instalación basada en características o en roles y presionaremos siguiente.

Asistente para agregar roles y características

Seleccionar tipo de instalación

SERVIDOR DE DESTINO
WIN-RFE0R4UG4DE.chema.lan

Antes de comenzar

- Tipo de instalación**
- Selección de servidor
- Roles de servidor
- Características
- Confirmación
- Resultados

Seleccione el tipo de instalación. Puede instalar roles y características en un equipo físico, en una máquina virtual o en un disco duro virtual (VHD) sin conexión.

☒ **Instalación basada en características o en roles**
Para configurar un solo servidor, agregue roles, servicios de rol y características.

☐ **Instalación de Servicios de Escritorio remoto**
Instale los servicios de rol necesarios para que la Infraestructura de escritorio virtual (VDI) cree una implementación de escritorio basada en máquinas o en sesiones.

< Anterior **Siguiente >** Instalar Cancelar

- Seleccionar servidor de destino tendremos que seleccionar nuestro servidor donde queremos aplicar la VPN y darle a siguiente

Asistente para agregar roles y características

Seleccionar servidor de destino

Antes de comenzar

- Tipo de instalación
- Selección de servidor**
- Roles de servidor
- Características
- Confirmación
- Resultados

Seleccione un servidor o un disco duro virtual en el que se instalarán roles y

☒ **Seleccionar un servidor del grupo de servidores**

☐ Seleccionar un disco duro virtual

Grupo de servidores

Filtro:

Nombre	Dirección IP	Sistema operativo
WIN-RFE0R4UG4DE.che...	192.168.1.200	Microsoft Windows Server 2012

1 equipo(s) encontrado(s)

Esta página muestra los servidores que ejecutan Windows Server 2012 o una versión posterior de Windows Server, y que se agregaron mediante el comando Agregar servidor. No se muestran los servidores sin conexión ni los servidores recién recopilación de datos aún está incompleta.

< Anterior **Siguiente >**



- En los roles del servidor seleccionamos la opción de acceso remoto y avanzamos al siguiente paso

Seleccionar roles de servidor

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Acceso remoto

Servicios de rol

Confirmación

Resultados

Seleccione uno o varios roles para instalarlos en el servidor seleccionado

Roles	Des
<input checked="" type="checkbox"/> Acceso remoto	Acc
<input type="checkbox"/> Active Directory Lightweight Directory Services	con
<input type="checkbox"/> Active Directory Rights Management Services	trav
<input type="checkbox"/> Atestación de mantenimiento del dispositivo	pro:
<input type="checkbox"/> Controladora de red	Dire
<input type="checkbox"/> Hyper-V	exp
<input type="checkbox"/> Servicio de protección de host	sien
<input type="checkbox"/> Servicios de acceso y directivas de redes	pro
<input type="checkbox"/> Servicios de archivos y almacenamiento (2 de 12 in	trac
<input type="checkbox"/> Servicios de certificados de Active Directory	con
<input checked="" type="checkbox"/> Servicios de dominio de Active Directory (Instalado)	(ba:
<input type="checkbox"/> Servicios de Escritorio remoto	nub
<input type="checkbox"/> Servicios de federación de Active Directory	hab
<input type="checkbox"/> Servicios de implementación de Windows	apli
<input type="checkbox"/> Servicios de impresión y documentos	HTI
<input type="checkbox"/> Servidor de fax	en c
<input type="checkbox"/> Servidor DHCP	dicl
<input checked="" type="checkbox"/> Servidor DNS (Instalado)	pro
<input type="checkbox"/> Servidor web (IIS)	trac
	que
	nor

< Anterior **Siguiente >**

- La ventana de características no necesitamos nada por lo que continuamos a la ventana de acceso remoto, daremos click en siguiente y se abrirá la ventana de los servicios del rol. Aquí haremos click en la opción DirectAccess y VPN(RAS)

Seleccionar servicios de rol

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Acceso remoto

Servicios de rol

Confirmación

Resultados

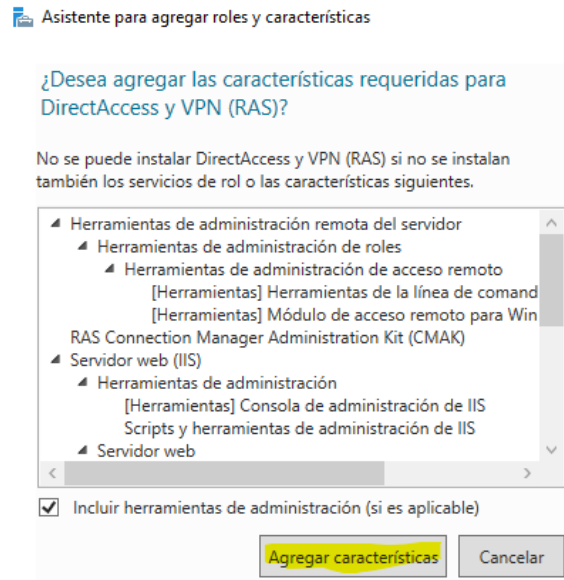
Seleccione los servicios de rol que desea instalar para Acceso remoto

Servicios de rol	De
<input checked="" type="checkbox"/> DirectAccess y VPN (RAS)	Di
<input type="checkbox"/> Enrutamiento	us
<input type="checkbox"/> Proxy de aplicación web	co
	co
	qu
	Di
	se
	mi
	co
	ga
	pe
	dii
	sis
	co
	un
	cif
	co
	ofi

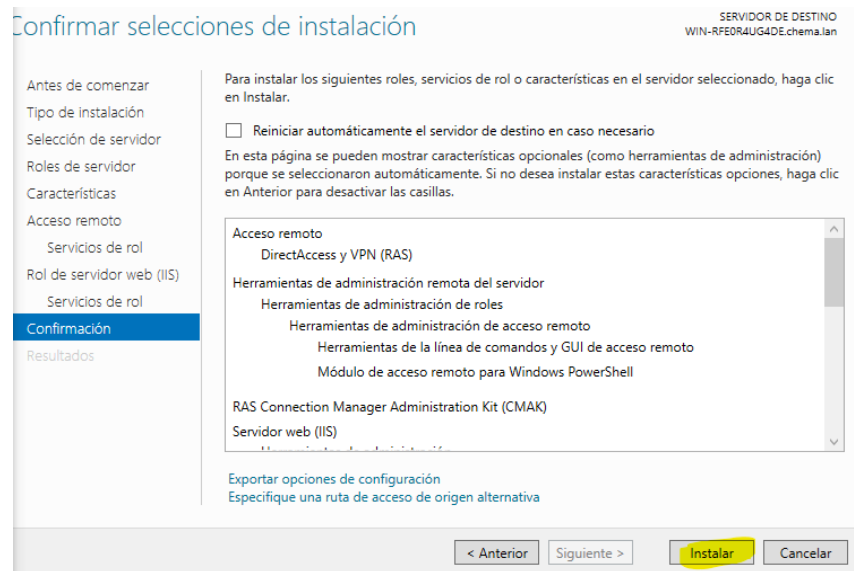
< Anterior Siguiente >



- Esto abrirá una ventana que mostrará todas las características que se le agregaran al rol, se hace clic en agregar características.

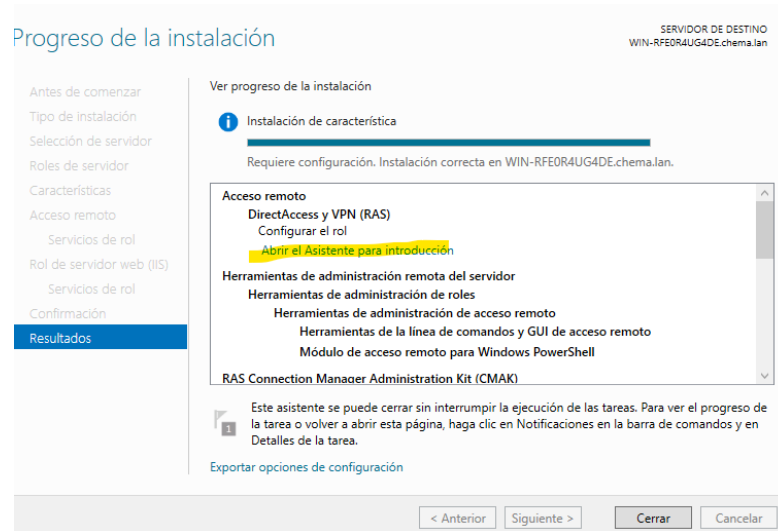


- En las ventanas Rol de servidor web-> Servicios de rol avanzamos con siguiente y en la ventana de confirmación seleccionamos instalar.





- Tras la instalación abrimos el Asistente para introducción que aparece en el lugar indicado en la imagen



- A continuación accederemos a implementar solo VPN



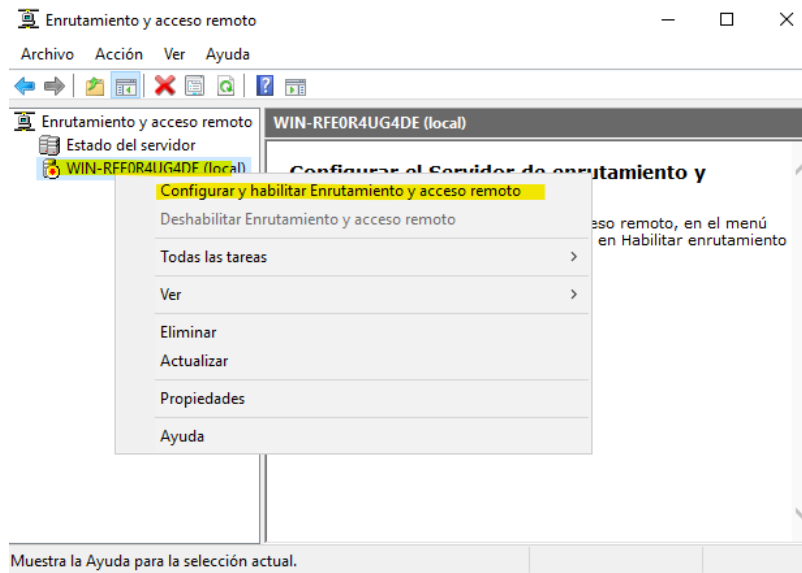
Acceso remoto

Use las opciones de esta página para configurar DirectAccess y VPN.

- Implementar DirectAccess y VPN (recomendado)
Configure DirectAccess y VPN en el servidor y habilite los equipos cliente de DirectAccess. Permita que los equipos cliente no compatibles con DirectAccess se conecten mediante VPN.
- Implementar solo DirectAccess
Configure DirectAccess en el servidor y habilite los equipos cliente de DirectAccess.
- **Implementar solo VPN**
Configure VPN mediante la consola de Enrutamiento y acceso remoto. Los equipos cliente remotos pueden conectarse con VPN y se pueden conectar varios sitios mediante conexiones VPN de sitio a sitio. Los clientes no compatibles con DirectAccess pueden usar VPN.



- Aparecerá la siguiente ventana de enrutamiento y acceso remoto, en esta seleccionaremos nuestro servidor y haremos click derecho para mostrar el desplegable de configuración, a continuación seleccionamos la opción de configurar y habilitar enrutamiento y acceso remoto.



- Se mostrará la ventana “Asistente para la instalación del servidor de enrutamiento y acceso remoto”, haremos click en siguiente y en la ventana de configuración seleccionaremos la opción de configuración personalizada

Asistente para la instalación del servidor de enrutamiento y acceso remoto

Configuración

Puede habilitar cualesquiera de las siguientes combinaciones de servicios o puede personalizar este servidor.

☐ Acceso remoto (acceso telefónico o red privada virtual)
 Permitir a clientes remotos conectarse a este servidor a través de una conexión de acceso telefónico o una conexión segura a Internet de red privada virtual (VPN).

☐ Traducción de direcciones de red (NAT)
 Permitir a clientes internos conectarse a Internet usando una dirección IP pública.

☐ Acceso a red privada virtual (VPN) y NAT
 Permitir que los clientes remotos se conecten a este servidor a través de Internet y que los clientes locales se conecten a Internet usando una sola dirección IP pública.

☐ Conexión segura entre dos redes privadas
 Conectar esta red a una red remota, como a una oficina sucursal.

☒ Configuración personalizada
 Seleccionar cualquier combinación de características disponibles en Enrutamiento y acceso remoto.



- En la siguiente ventana seleccionamos Acceso a VPN , siguiente y finalizar.

Asistente para la instalación del servidor de enrutamiento y acceso remoto

Configuración personalizada

Cuando se cierra este asistente, puede configurar los servicios seleccionados en la consola Enrutamiento y acceso remoto.

Seleccione los servicios que desea habilitar en este servidor.

☒ Acceso a VPN

☐ Acceso telefónico

☐ Conexiones de marcado a petición (utilizadas para enrutamiento de oficinas sucursales)

☐ NAT

☐ Enrutamiento LAN

< Atrás **Siguiente** > Cancelar

- Tras hacer clic en finalizar aparecerá una ventana emergente donde tendremos que seleccionar iniciar servicio

POSSIBLE PARA INSTALAR LOS SERVICIOS DE ENRUTAMIENTO Y ACCESO REMOTO

Finalización del Asistente para instalación del servidor de enrutamiento y acceso remoto

Ha completado con éxito el Asistente para instalación de Servidor de enrutamiento y acceso remoto.

Resumen de las selecciones:

Acceso a VPN

Enrutamiento y acceso remoto

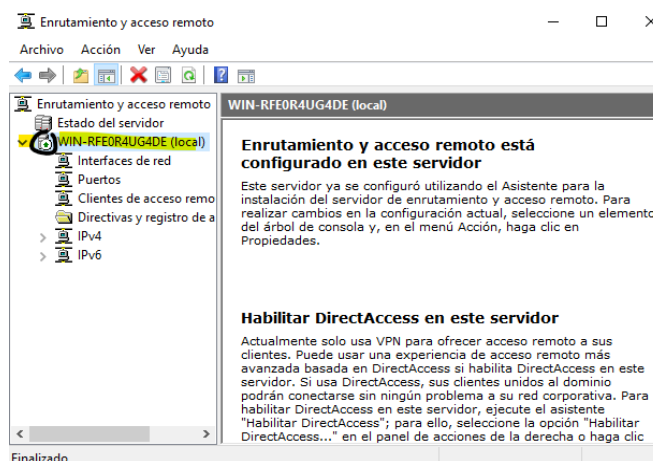
Iniciar el servicio

☒ El Servicio de enrutamiento y acceso remoto está listo para usarse.

Iniciar servicio Cancelar

< Atrás **Finalizar** Cancelar

- Si todo ha salido satisfactoriamente se mostrara tu servidor con el siguiente icono de color verde





- A partir de este punto si el usuario utiliza DHCP ha de configurar su usuario VPN y el acceso a la red , además de abrir los puertos del firewall y reenviarlos al servidor de windows con su correspondiente protocolo. En el caso de que estemos haciendo uso de una IP estática habría que habilitar el acceso remoto a todos los usuarios , además de habilitar el static address pool.

DMZ

Una red DMZ o zona desmilitarizada es una red local que se encuentra entre nuestra red local de trabajo e internet o cualquier otra red externa. Estas DMZ suelen ser utilizadas para hospedar el servidor de tu página web, ya que esta va a recibir tanto tráfico externo como interno pero denegara el tráfico desde tu DMZ a tu red local.

Las DMZ se protegen con un firewall, cuya función principal es filtrar el tráfico de red entrante y saliente. Es recomendable el uso de dos firewalls (firewall de contención entre internet y tu dmz y el firewall bastión en tu red privada) en caso de crear tu DMZ siendo esta la opción más segura, y a poder ser que estos firewalls sean diferentes versiones entre sí ya que así no se compromete la vulnerabilidad del otro si uno cae.

Si uno de estos Firewalls estuviera mal configurado con unas restricciones demasiado permisivas pondría en compromiso toda la información interna de la empresa, así como la de los usuarios registrados en la página web siendo esto catastrófico para la empresa. A su vez si las restricciones son demasiado altas esto podría llevar a la pérdida de información , datos o ingresos.

La empresa requerirá de la implementación de una red DMZ para el correcto funcionamiento seguro de su red ya que utilizan un servidor propio para hospedar su página web.

Implementación de DMZ

Implementación de una DMZ con el uso de Cisco Packet Tracer:

1. Para añadir una nueva DMZ click en Add.
2. En la ventana de Basic Settings se deben rellenar los siguientes apartados
Name : nombre de tu DMZ
IP Address : Subnet IP para tu DMZ
NetMask: Máscara subnet para tu DMZ
Spanning Tree: Activalo si hay algún ciclo cerrado en tu topología
Port: Especifica los puertos para tu DMZ, los puertos disponibles te aparecerán en la lista de puertos, estos los tendrás que añadir a la lista de miembros.
Zone :Escoge la zona de tu DMZ, la puedes configurar o dejar una predeterminada.
3. En la pestaña de DHCP Pool Settings
Disable: Esta opción es para cuando los ordenadores que se encuentran en tu DMZ están configurados con una IP estática
DHCP Server: La DMZ actúa como un DHCP server , asignando direcciones IP a cada dispositivo que se conecte.
DHCP Relay : Este te pedirá que rellenes un campo con la dirección IP del servidor DHCP remoto que quieras utilizar
4. Si seleccionas DHCP Server debes introducir la siguiente información
Start IP : Rango inicial de IP dentro del DHCP range
End IP : Rango final de IP dentro del DHCP range
Lease Time: tiempo de conexión de la dirección IP dinámica antes de que esta tenga que ser renovada nuevamente
DNS : Introducir la dirección IP del servidor DNS primario
Default Gateway: introduce la dirección IP de tu gateway
5. En las configuraciones de IPv6 se activan si activas el modo IPv6 y tendrías que introducir una dirección IPv6 basada en los requerimientos de tu network y la longitud del encabezado de la misma



6. Ok para guardar tu configuración
7. Save para aplicar tu configuración

NAT (Network Address Translation)

También conocido como enmascaramiento IP surge como la solución momentánea al agotamiento de direcciones IPv4. Consiste en hacer que las redes privadas de ordenadores utilizan una dirección IP privada entre sí pero al salir a internet sea con una misma dirección pública.

Hay diferentes tipos de NAT:

NAT estático que asigna una IP privada a una IP pública

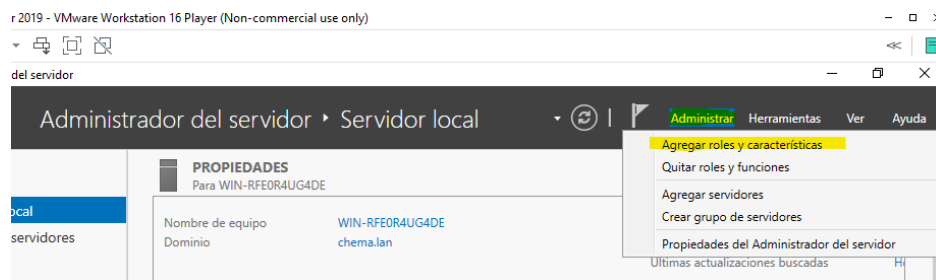
NAT Dinámico , el router tiene asignadas varias direcciones IP públicas, cada vez que un equipo de tu red privada quiere conectarse a internet se le asigna una de estas IP públicas.

NAT Sobrecargado donde se mapean múltiples direcciones privadas en una única dirección pública, ahorrando direcciones IPv4. Este tipo de NAT funciona como un multiplexor

Implementación NAT

Para la implementación de la red NAT se requiere de dos redes , una que será la red LAN siendo esta tu red local que no dispondrá de acceso a internet hasta que la NAT sea implementada y otra será la red WAN que será la red que tendrá la conexión a internet.

- Abrimos el administrador de Windows Server y clicamos en administrar. Tal y como se muestra en la imagen aparecerá un desplegable y seleccionaremos la opción “agregar roles y características”





- Seleccionar tipo de instalación usaremos la opción de instalación basada en características o en roles y presionaremos siguiente.

Asistente para agregar roles y características

Seleccionar tipo de instalación

SERVIDOR DE DESTINO
WIN-RFE0R4UG4DE.chema.lan

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

Resultados

Seleccione el tipo de instalación. Puede instalar roles y características en un equipo físico, en una máquina virtual o en un disco duro virtual (VHD) sin conexión.

☒ **Instalación basada en características o en roles**
Para configurar un solo servidor, agregue roles, servicios de rol y características.

☐ **Instalación de Servicios de Escritorio remoto**
Instale los servicios de rol necesarios para que la Infraestructura de escritorio virtual (VDI) cree una implementación de escritorio basada en máquinas o en sesiones.

< Anterior **Siguiente >** Instalar Cancelar

- Seleccionar servidor de destino tendremos que seleccionar nuestro servidor donde queremos aplicar la VPN y darle a siguiente

Asistente para agregar roles y características

Seleccionar servidor de destino

Antes de comenzar

Tipo de instalación

Selección de servidor

Roles de servidor

Características

Confirmación

Resultados

Seleccione un servidor o un disco duro virtual en el que se instalarán roles y características.

☒ **Seleccionar un servidor del grupo de servidores**

☐ Seleccionar un disco duro virtual

Grupo de servidores

Filtro:

Nombre	Dirección IP	Sistema operativo
WIN-RFE0R4UG4DE.chema.lan	192.168.1.200	Microsoft Windows Server 2012

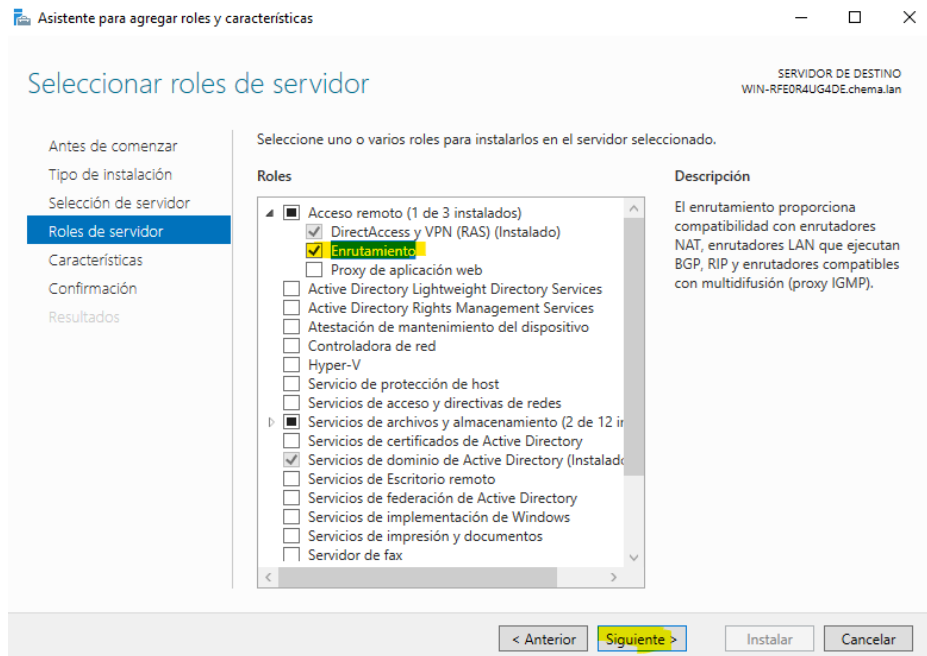
1 equipo(s) encontrado(s)

Esta página muestra los servidores que ejecutan Windows Server 2012 o una versión posterior de Windows Server, y que se agregaron mediante el comando Agregar servidor. No se muestran los servidores sin conexión ni los servidores recién recopilación de datos aún está incompleta.

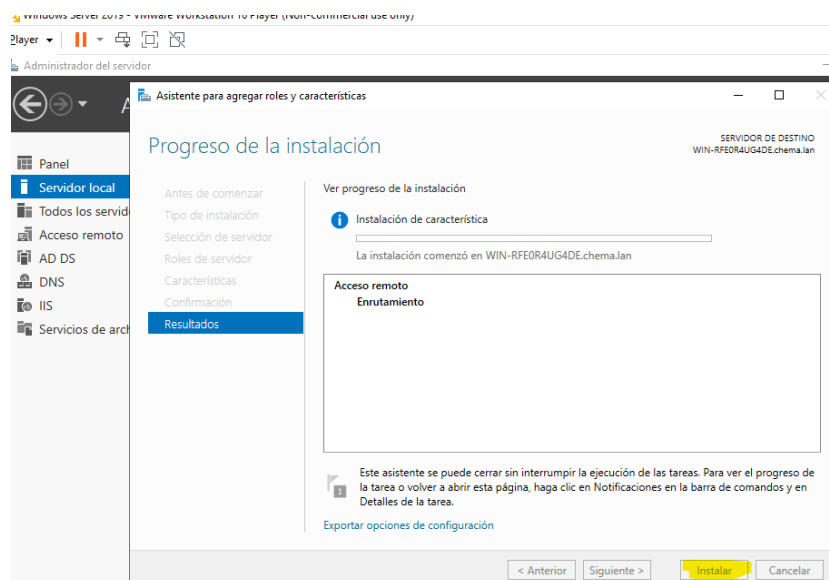
< Anterior **Siguiente >**



- En los roles del servidor seleccionamos la opción de acceso remoto y hacemos clic en enrutamiento. Esto sucede porque ya hemos instalado previamente el servicio VPN

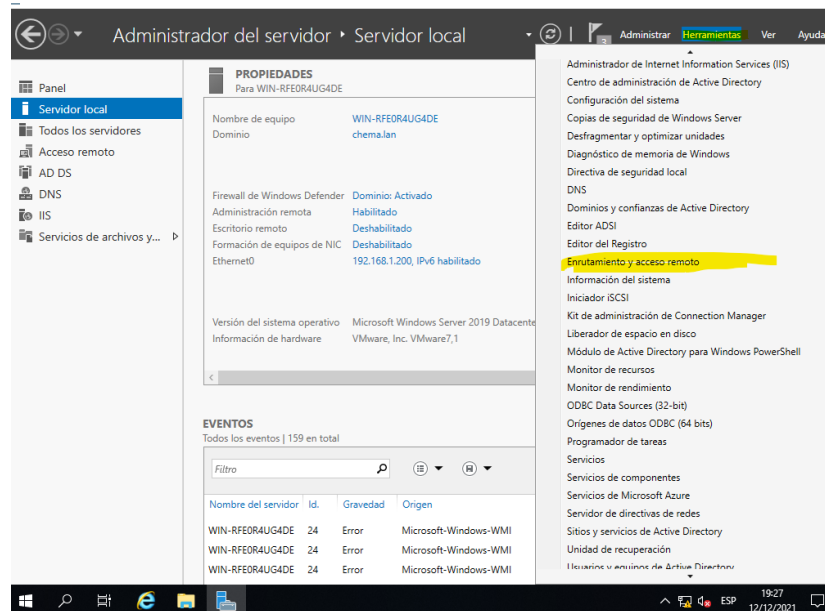


- La ventana de características no necesitamos nada por lo que continuamos a la ventana de acceso remoto, daremos click en siguiente y se abrirá la ventana de los servicios del rol. Aquí haríamos click en la opción Enrutamiento. Si ya está instalada la VPN como es mi caso, esta ventana no se mostrará. En cualquiera de los casos proseguir hasta la ventana de instalación e instalar.

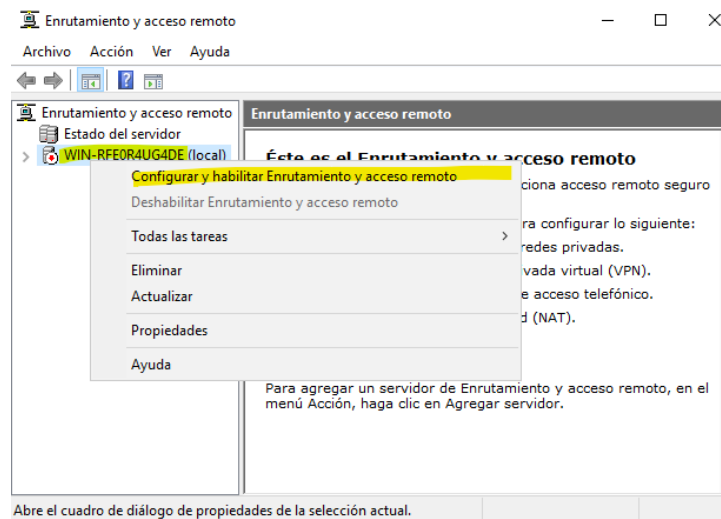




- Tras finalizar la instalación volvemos a la ventana de administrador del servidor, al apartado de herramientas y seleccionamos la opción de enrutamiento y acceso remoto



- Click derecho en nuestra red y accedemos a configurar y habilitar acceso remoto





- Se abrirá una ventana con el Asistente de instalación del servidor de enrutamiento y acceso remoto. Hacemos click en siguiente y en la pestaña de configuración seleccionamos Traducción de direcciones de red NAT

Asistente para la instalación del servidor de enrutamiento y acceso remoto

Configuración

Puede habilitar cualesquiera de las siguientes combinaciones de servicios o puede personalizar este servidor.

☐ Acceso remoto (acceso telefónico o red privada virtual)
 Permitir a clientes remotos conectarse a este servidor a través de una conexión de acceso telefónico o una conexión segura a Internet de red privada virtual (VPN).

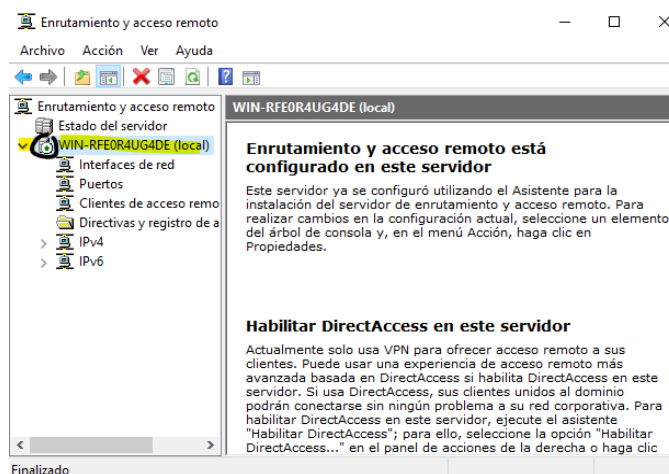
☒ Traducción de direcciones de red (NAT)
 Permitir a clientes internos conectarse a Internet usando una dirección IP pública.

☐ Acceso a red privada virtual (VPN) y NAT
 Permitir que los clientes remotos se conecten a este servidor a través de Internet y que los clientes locales se conecten a Internet usando una sola dirección IP pública.

☐ Conexión segura entre dos redes privadas
 Conectar esta red a una red remota, como a una oficina sucursal.

☐ Configuración personalizada
 Seleccionar cualquier combinación de características disponibles en Enrutamiento y acceso remoto.

- Seleccionamos Utilizar esta interfaz pública para conectarse a internet, y seleccionamos nuestra red WAN después click en siguiente y en finalizar.
- Si todo ha salido satisfactoriamente se mostrara tu servidor con el siguiente icono de color verde





IP Estática

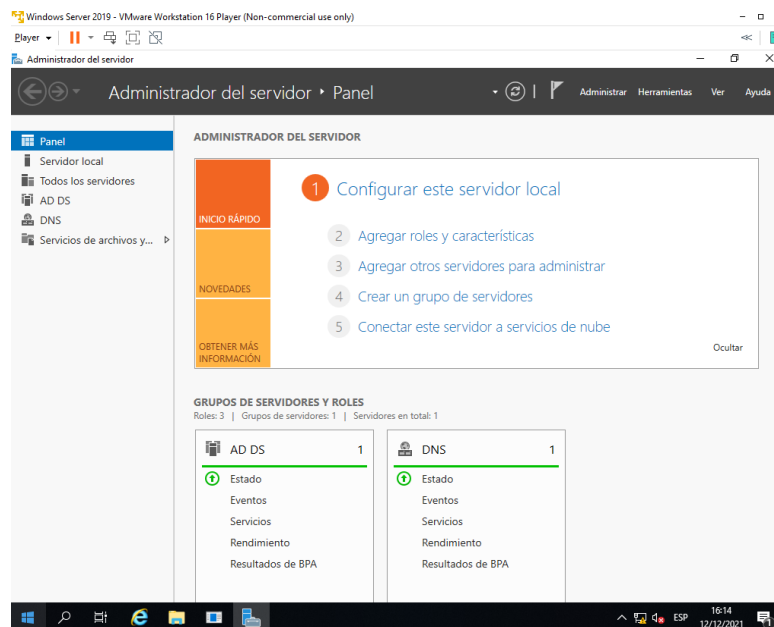
La IP estática como su propio nombre indica es la asignación de una ip propia por tu proveedor. Esta dirección ip no cambiará, dando una conexión más estable y fiable , obteniendo mayores velocidades , siendo esto beneficioso en videojuegos online.

Como nuestra empresa no posee el servidor de los juegos que produce si no que tiene un servidor externo contratado, la implementación de esta no es necesaria, ya que es más seguro que la IP no sea estática.

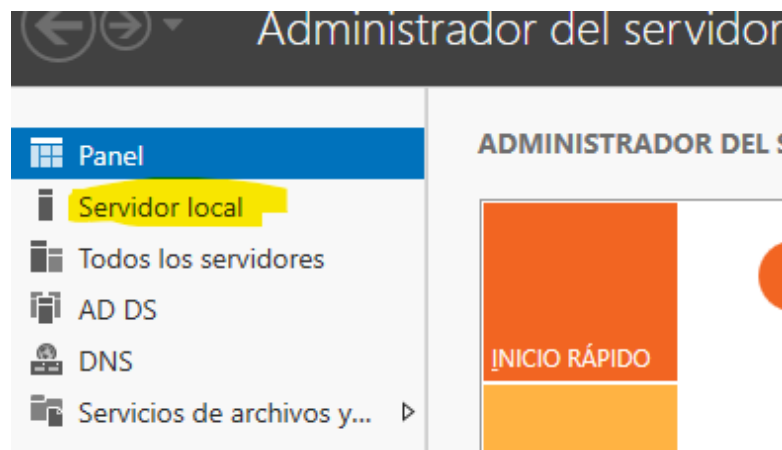
Implementación IP Estática

Para la implementación de la IP estatica en Windows Server seguimos los siguientes pasos:

- Abrimos el administrador del servidor

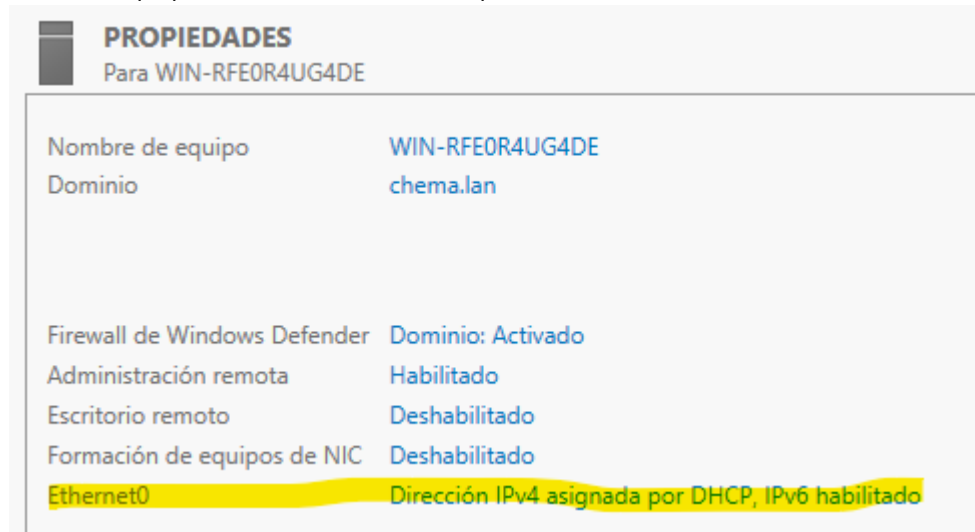


- Servidor local

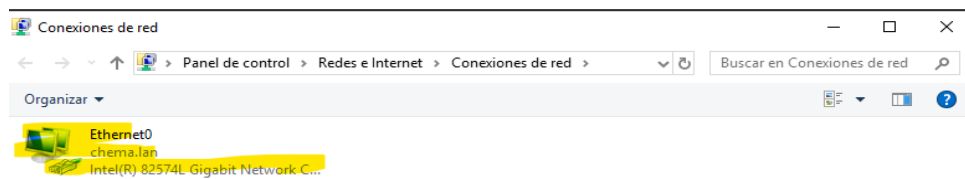




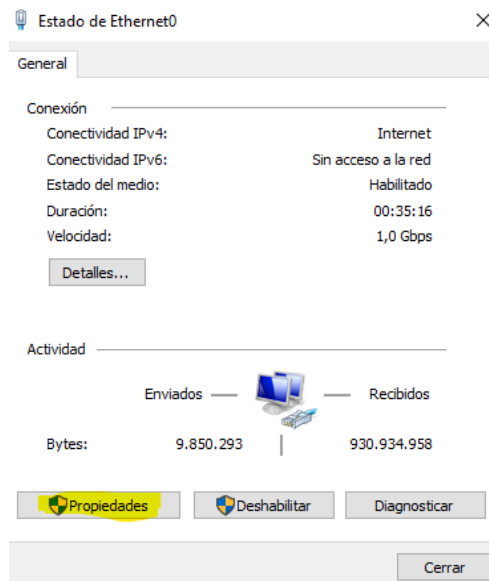
- En propiedades seleccionamos la opcion de Ethernet0 mostrada a continuación



- Se abrirá la ventana de conexiones de red, accederemos a nuestra conexión.

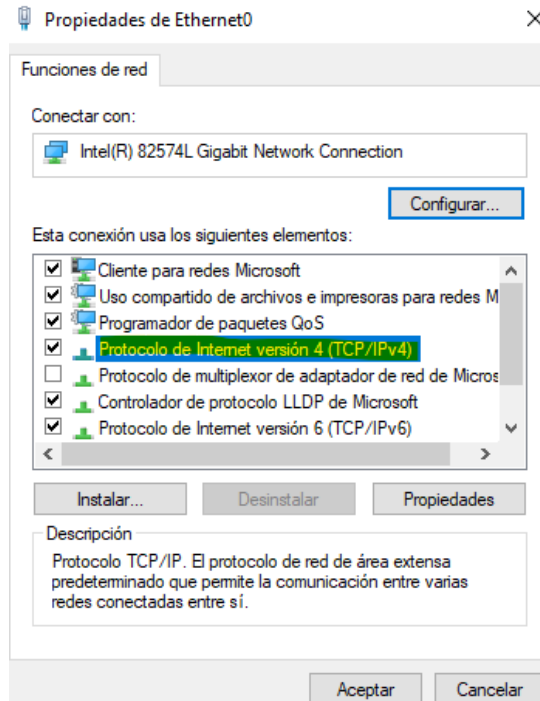


- En la ventana emergente hacemos click en propiedades.

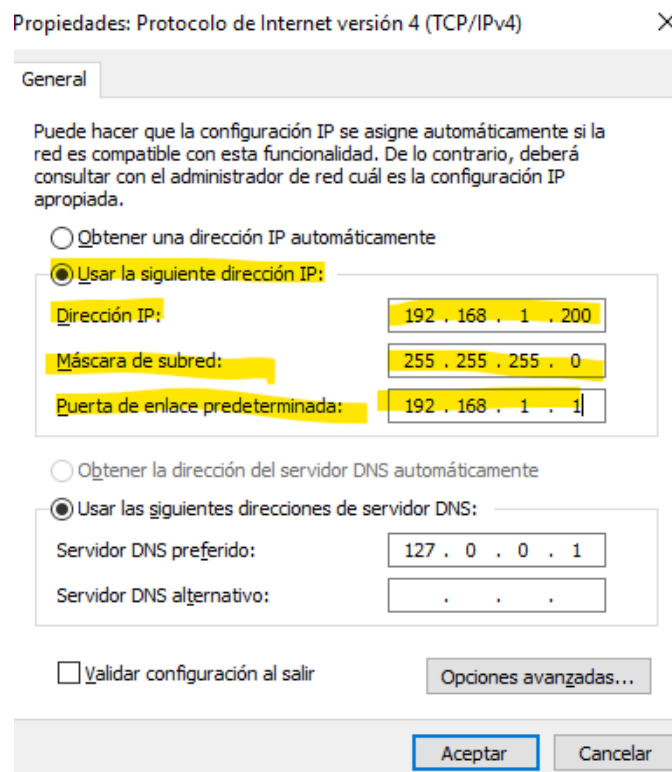




- Seleccionamos la opción protocolo de Internet versión 4 (TCP/IPv4)

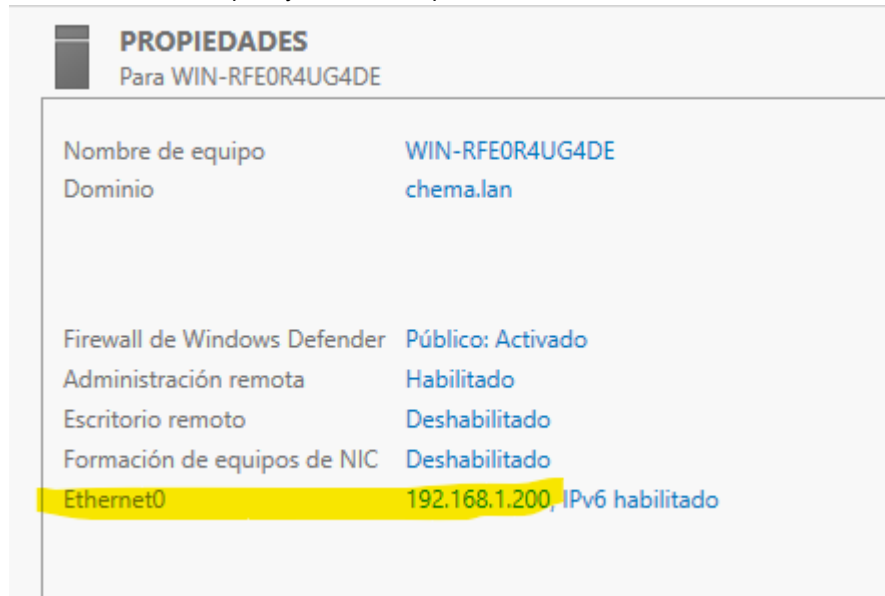


- A continuación se marcará la opción: Usar la siguiente dirección IP y se introducirán la que será la nueva IP estática, máscara de subred y la puerta de enlace





- Click en aceptar, y tendremos que reiniciar el servidor.



- Como se puede observar en la imagen ya tendremos activada nuestra IP estática.



4.- Plan de gestión de riesgos

La empresa debe contar con un plan de riesgos para poder afrontar las diferentes amenazas de una forma óptima y así reducir los daños y los riesgos en medida de lo posible.

Tras cualquier tipo de ataque. Los empleados deberán informar al servicio técnico de la empresa inmediatamente tras esto, habrá que mantener la calma e identificar el tipo de ataque que se está realizando y actuar de forma pertinente a él adoptando la resolución más oportuna.

Los ataques más perjudiciales por lo general, son perpetrados por script Kiddies ciberdelincuentes. Ya que los script kiddies son impredecibles dado a su falta de experiencia y los ciberdelincuentes suelen buscar un beneficio o rédito económico.

Si uno de los equipos ha sido infectado por un malware será desconectado de la subred aislándola a esta en una cuarentena para evitar la expansión de la amenaza y el posible escalado en los privilegios del servidor local.

La pérdida de información interna tal como el motor propio, el código y assets de los proyectos puede ser catastrófico este tiempo de información suele ser el objetivo de algunos ciberdelincuentes con el objetivo de venderlas en el mercado negro o difundirla e incluso pedir un rescate por la misma.

Para evitar la pérdida de este tipo de archivos se realizarán copias de seguridad al final de cada jornada laboral, además, los trabajadores tendrán que utilizar un repositorio privado de la empresa al que se deben conectar por túnel SSH siendo este otro punto de back up si fuese necesario.

Para evitar tácticas de phishing y Malware no deseoso via E-mail quedará terminantemente prohibido iniciar sesión en un correo que no sea el de la empresa, además el correo de la empresa no deberá utilizarse para registros en páginas que no estén relacionadas por el trabajo, adicionalmente nunca se enviará un correo a los trabajadores con ningún tipo de archivo descargable por lo que cualquier correo que contenga archivos adjuntos será descartado automáticamente.

Utilización de un antivirus con licencia para que pueda examinar los posibles descargables antes de realizar la descarga, además este tendrá que estar siempre actualizado a sus últimas versiones para la detección de nuevas potenciales amenazas.

El hardware externo está prohibido, tanto USB como discos duros pueden contener Malware e infectar uno de los equipos tras su conexión sin el previo conocimiento del propietario del dispositivo.

Se deberán seguir las políticas de contraseñas de la empresa, los empleados no pueden iniciar sesión en una cuenta que no sea la suya y deberán respetar las políticas de auditorías.

Para garantizar la seguridad de la red de ordenadores, estos no deben quedarse desfasados en versión, deberán actualizarse periódicamente y evitar versiones de sistemas operativos antiguos que pueden ser vulnerables.

En el contrato de trabajo se informará de las cláusulas específicas de todos estos puntos, además se notificará a los trabajadores de las consecuencias penales si cometiera un delito como insider.



El uso de una DMZ para la página web será obligatorio, además esta será protegida por un Firewall de contención y a su vez la red local será protegida por un Firewall de bastión. Estos Firewalls serán versiones distintas para evitar que los fallos en la vulnerabilidad de uno de ellos afecte al otro.

El sistema de seguridad se pondrá a prueba de forma periódica para poder realizar diferentes cambios y así mejorar el servicio ofrecido por la empresa.

RGPD Reglamento General de Protección de Datos

Es el reglamento europeo que concierne a la protección de las personas físicas en lo que respecta a sus datos personales y la circulación de los mismos. En lo que a nuestro trabajo respecta debemos asegurar una Confidencialidad (cifrado de información), Integridad de la información (Hashing), y Disponibilidad (balanceo) para ofrecer el mejor servicio posible ciñéndonos a la normativa.

El consentimiento para el tratado de estos datos se puede revocar en cualquier momento, esta revocación no sufrirá efectos retroactivos lo cual deberá de ser informado.

Según la ley se establece una edad límite para prestar consentimiento a la hora de manejar los datos, siendo 16 la normalizada pero se puede bajar según el país hasta los 13 años.

Base legal para tratamiento

Los datos solo se pueden tratar si existe al menos una base legal para hacerlo. Las bases legales para tratar datos son:

- El interesado ha dado su consentimiento para el tratamiento de sus datos personales con uno o más propósitos específicos.
- El tratamiento es necesario para la ejecución de un contrato del que el interesado es parte o para tomar medidas a petición del interesado antes de celebrar un contrato.
- El tratamiento es necesario para cumplir con una obligación legal a la cual el controlador está sujeto.
- El tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física.
- El tratamiento es necesario para la realización de una tarea llevada a cabo en interés público o en el ejercicio de la autoridad oficial conferida al controlador.
- El tratamiento es necesario para los fines de los intereses legítimos perseguidos por el responsable o por un tercero, salvo cuando dichos intereses sean anulados por los intereses o los derechos y libertades fundamentales del interesado que requieren protección de datos personales, en particular cuando el interesado es un niño.

Consentimiento

Cuando el consentimiento se utiliza como la base legal para el tratamiento, el consentimiento debe ser explícito para los datos recopilados y los fines para los que se utilizan los datos (Artículo 7, definido en el Artículo 4). El consentimiento para niños debe ser otorgado por el padre o tutor del niño, y verificable (Artículo 8). Los controladores de datos deben poder probar el "consentimiento" (opt-in) y el consentimiento puede ser retirado.



La cuestión del consentimiento de RGPD tiene una serie de implicaciones para las empresas que graban llamadas en la práctica. Los típicos avisos del tipo "esta llamada está siendo grabada por motivos de seguridad" ya no serán suficientes para obtener el consentimiento asumido para grabar llamadas. Además, cuando la grabación haya comenzado, si la persona que es grabada retira su consentimiento, entonces el agente que recibe la llamada debe ser capaz de detener una grabación previamente iniciada y asegurarse de que la grabación no se guarde.

Seguridad de los datos personales

Para aplicar los principios de protección de datos, los encargados y los responsables del tratamiento de datos personales deben establecer medidas técnicas y medidas organizativas. Y los procesos empresariales que manejan datos personales, deben estar diseñados y contruidos teniendo en cuenta los principios y proporcionando salvaguardias para proteger los datos (ejemplo, utilizando la anonimización completa cuando sea necesario).

Los responsables del tratamiento diseñan los sistemas de información teniendo en cuenta la privacidad. Por ejemplo, utilizando una configuración de privacidad lo más alta posible por defecto, de modo que los conjuntos de datos no estén disponibles públicamente y no puedan utilizarse para identificar a un sujeto. No se puede tratar ningún dato personal a menos que este tratamiento se realice en virtud de una de las seis bases legales especificadas por el reglamento (consentimiento, contrato, función pública, interés vital, interés legítimo o requisito legal). Cuando el tratamiento se basa en el consentimiento, el interesado tiene derecho a revocar en cualquier momento.

Sanciones

Las siguientes sanciones pueden ser impuestas:

- Una advertencia por escrito en los casos de incumplimiento previo e intencional,
- Auditorías periódicas de protección de datos,
- Una multa de hasta 10 000 000 de euros o hasta el 2 % del volumen de negocios mundial anual del ejercicio anterior en el caso de una empresa, cualquiera que sea mayor, cuando haya habido una infracción de las siguientes disposiciones (Artículo 83, Párrafo 4):
 - Las obligaciones del controlador y del procesador de conformidad con los artículos 8, 11, 25 a 39, 42 y 43,
 - Las obligaciones del organismo de certificación de conformidad con los artículos 42 y 43,
 - Las obligaciones del organismo de supervisión de conformidad con el artículo 41 (4).
- Una multa de hasta 20 000 000 de euros o hasta el 4 % del volumen de negocios anual del año financiero anterior en el caso de una empresa, cualquiera que sea mayor, cuando se haya infringido las siguientes disposiciones: (Artículo 83, párrafos 5 y 6).
 - Los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento, de conformidad con los artículos 5, 6, 7 y 9,
 - Las transferencias de datos personales a un destinatario en un tercer país o una organización internacional de conformidad con los artículos 44 a 49,



- Cualquier obligación conforme a la ley de los Estados miembros adoptada en virtud del Capítulo IX,
- El incumplimiento de una orden o una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad supervisora de conformidad con el artículo 58 (2) o la falta de acceso en violación del artículo 58 (1).



5.- Políticas de seguridad implementadas

Diseño de Políticas de seguridad para la empresa

Usuario admin que controlara el equipo de Windows Server, este usuario será el propio director de la empresa, aunque si ésta siguiera creciendo debería ser delegado este puesto a un profesional de seguridad.

Administración correcta de carpetas compartidas.

Políticas de contraseñas, donde estas requerirán una longitud mínima, complejidad, exigirán un tamaño mínimo y tendrán una duración. Además las contraseñas antiguas no podrán volver a ser usadas hasta cierto tiempo.

Uso de ctrl+alt+supr antes del inicio de sesión para evitar pantallas de inicio de sesión falsas y así evitar la sustracción de contraseñas de, así serán redireccionados a la pantalla de inicio de sesión de windows

Auditorías de inicio de sesión para controlar el número de intentos fallidos de sesión en los diferentes sistemas.

Auditorías de eventos de sistema para controlar qué usuarios han intentado entrar a las configuraciones del sistema y otras carpetas sensibles.

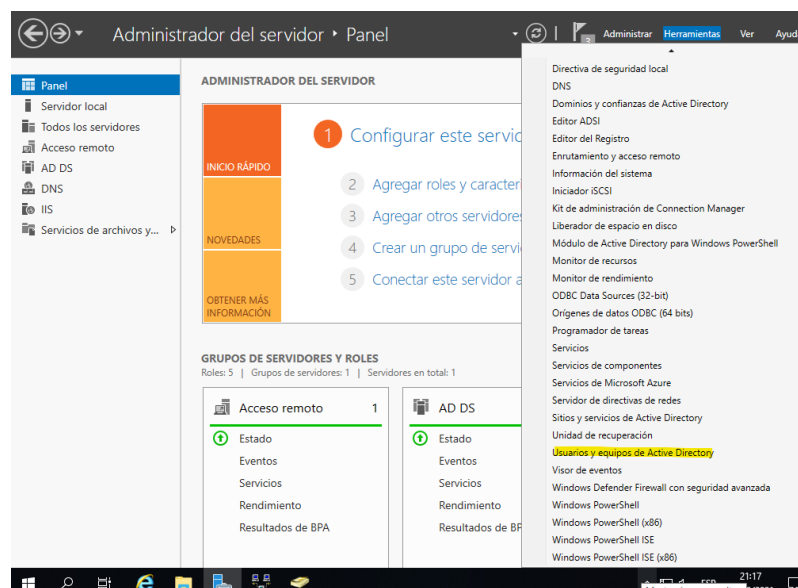
Control de copias de seguridad.

Control de correos electrónicos para evitar posibles malwares o las técnicas de phishing para eso se realizarán adicionalmente charlas para concienciar a los trabajadores de forma semestral. Estas charlas requerirán de la participación activa de los propios trabajadores por lo que serán más didácticas.

Implementación de las políticas

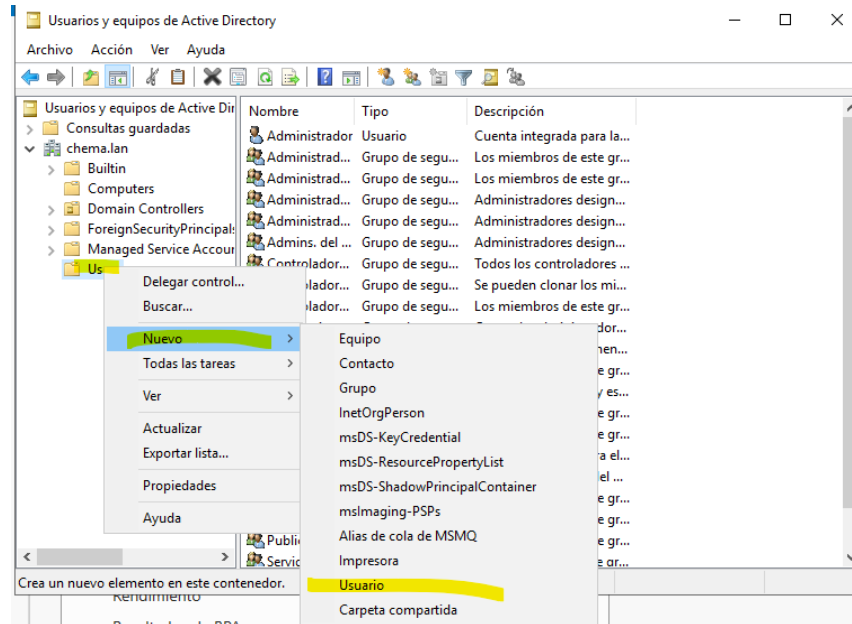
Implementación de roles de la empresa

- Antes de nada se requiere de la creación de un Usuario , para esto En el administrador del servidor -> herramientas -> Usuarios y equipos de Active directory





- Hacemos click derecho en la carpeta users -> nuevo -> usuario



- Se rellena la siguiente información

Nuevo objeto: Usuario

Crear en: chema.lan/Users

Nombre de pila: Iniciales:

Apellidos:

Nombre completo:

Nombre de inicio de sesión de usuario: @chema.lan

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

< Atrás **Siguiente >** Cancelar



- En la siguiente ventana introduciremos la contraseña por defecto que le daremos a nuestro nuevo usuario y activaremos la opción para que el usuario cambie la contraseña en su primera conexión

Nuevo objeto: Usuario

Crear en: chema.lan/Users

Contraseña:

Confirmar contraseña:

☒ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

☐ El usuario no puede cambiar la contraseña

☐ La contraseña nunca expira

☐ La cuenta está deshabilitada

< Atrás **Siguiente >** Cancelar

- Para añadir un rol de administrador al usuario se debe acceder al Administrador clave con doble click

Usuarios y equipos de Active Directory

Archivo Acción Ver Ayuda

Nombre	Tipo	Descripción
Administrador	Usuario	Cuenta integrada para la...
Administradores clave	Grupo de segu...	Los miembros de este gr...
Administradores clave...	Grupo de segu...	Los miembros de este gr...
Administradores de e...	Grupo de segu...	Administradores design...
Administradores de es...	Grupo de segu...	Administradores design...
Admins. del dominio	Grupo de segu...	Administradores design...
Controladores de do...	Grupo de segu...	Todos los controladores ...
Controladores de do...	Grupo de segu...	Se pueden clonar los mi...

- A continuación accedemos a la pestaña miembros y agregar

Propiedades: Administradores clave

General **Miembros** Miembro de Administrado por

Miembros:

Nombre	Carpeta de los Servicios de dominio de Active Dir...

Agregar... Quitar

Aceptar Cancelar Aplicar



- Se introduce el nombre del usuario al que le quieras asignar el rol, comprobar nombres, y se selecciona el usuario a asignar el rol.

Seleccione Usuarios, Contactos, Equipos, Cuentas de servicio, o Grupos

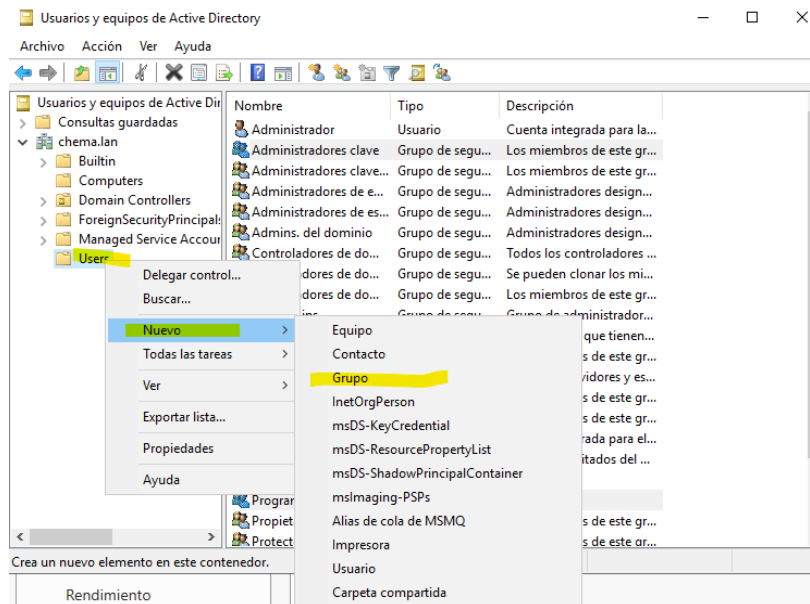
Seleccionar este tipo de objeto:

Desde esta ubicación:

Escriba los nombres de objeto que desea seleccionar (ejemplos):

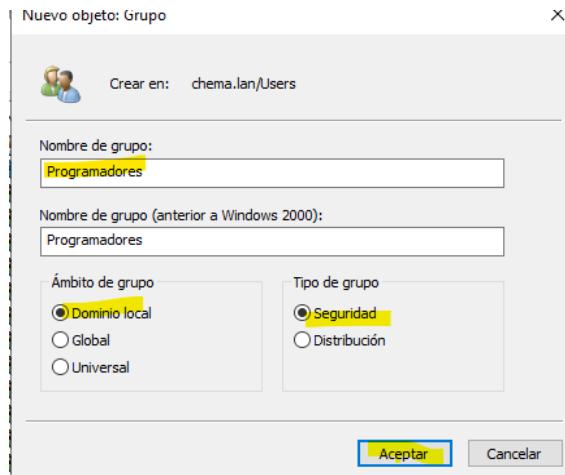
Creación de grupos

- Para crear un grupo click derecho en users, crear , grupos



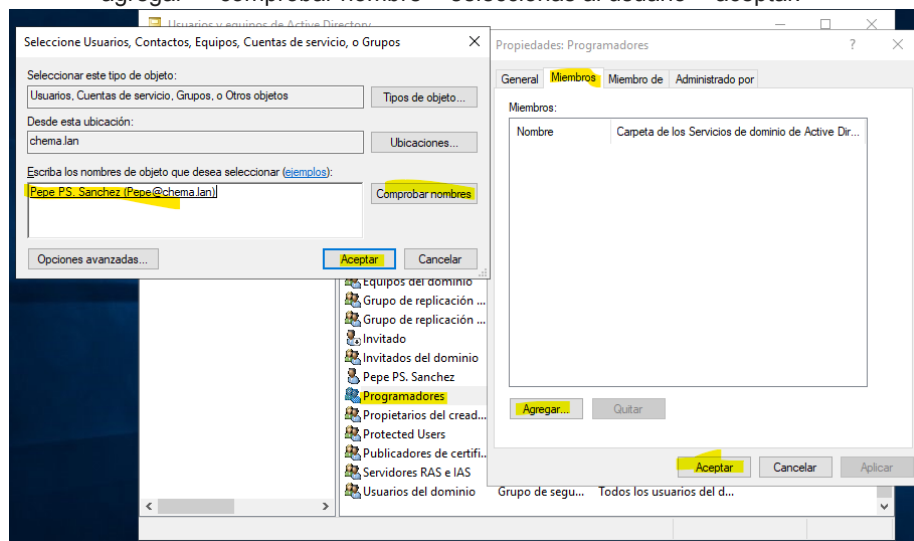


- En el nuevo grupo daremos un nombre , le seleccionaremos un dominio local , y tipo seguridad



Agregar usuarios a un grupo

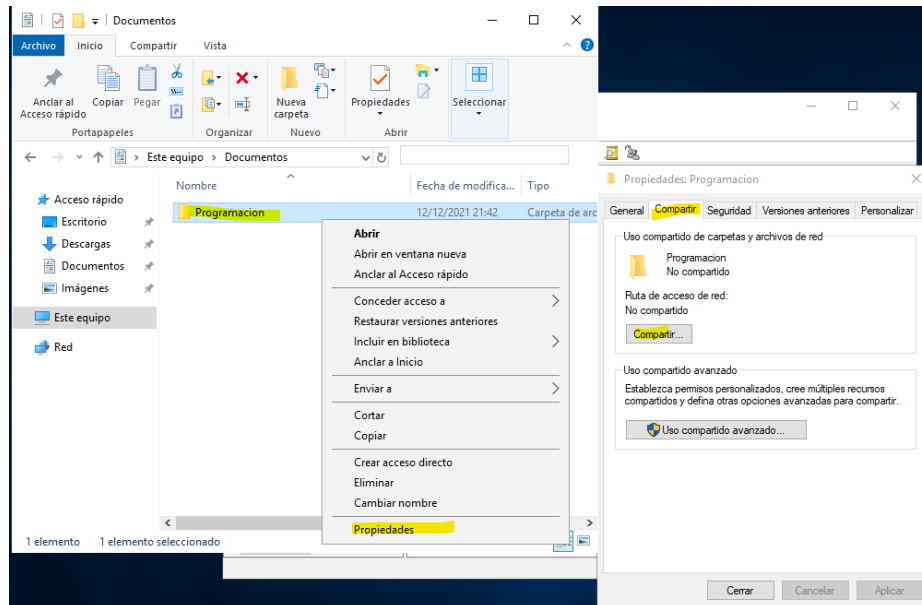
- Para agregar un usuario a un grupo se hace doble click en el grupo , tras esto accedes a la pestaña de miembros y agregar, introduces el nombre del usuario a agregar -> comprobar nombre-> seleccionas al usuario ->aceptar.





Carpeta compartida

- Vamos a la ruta donde queramos crear nuestra carpeta compartida->click derecho->nuevo->carpeta->click derecho->propiedades->compartir->compartir

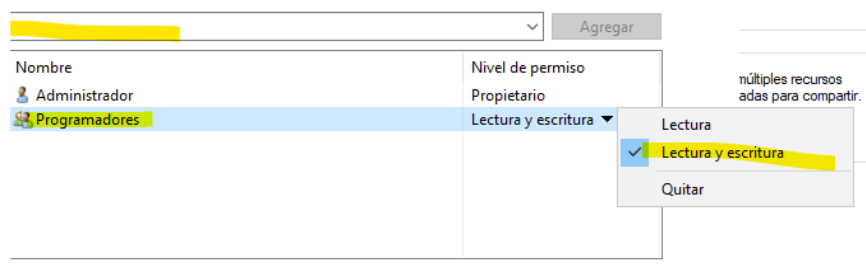


- En la ventana emergente introducimos el nombre del grupo que tendrá acceso a la carpeta y tras eso le podemos asignar los permisos correspondientes.



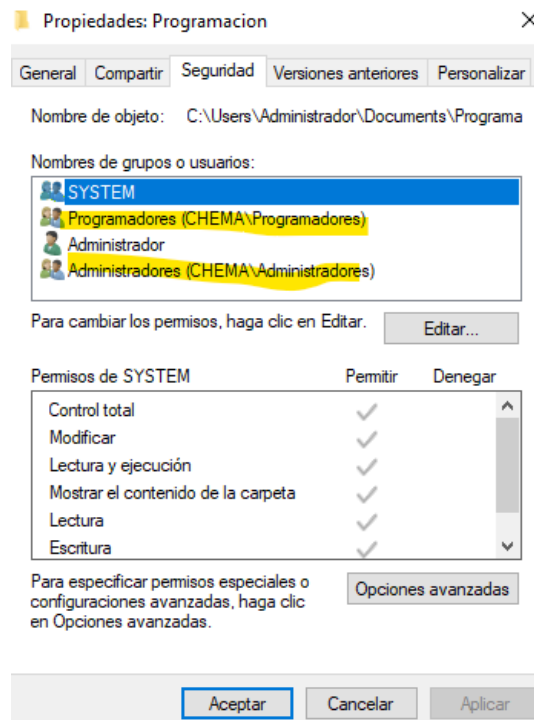
Elige los usuarios de la red con los que desea compartir recursos.

Escribe un nombre y haga clic en Agregar, o haga clic en la flecha para buscar usuarios.



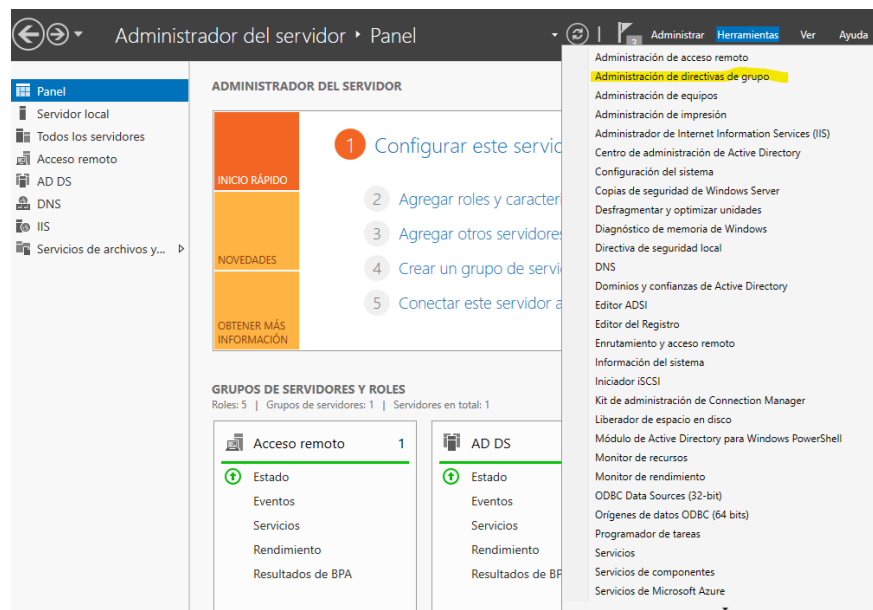


- Compartir->Listo. Tras esto tendremos una carpeta compartida para el grupo asignado.



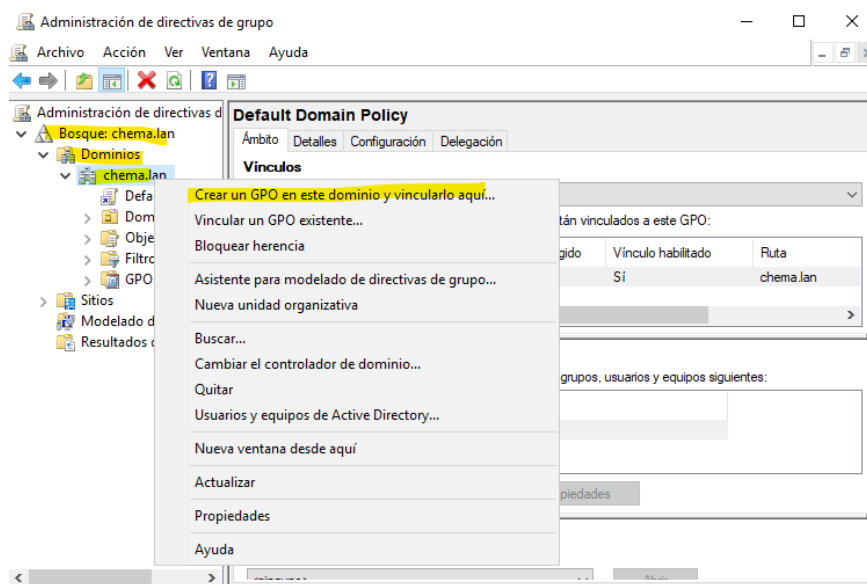
Implementación de las políticas de contraseñas

- Tendremos que ir al panel de administrador del servidor-> herramientas-> administración y directivas de grupo

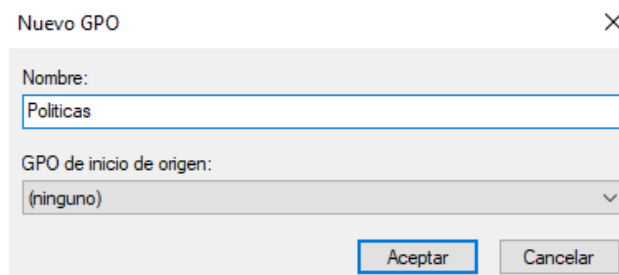




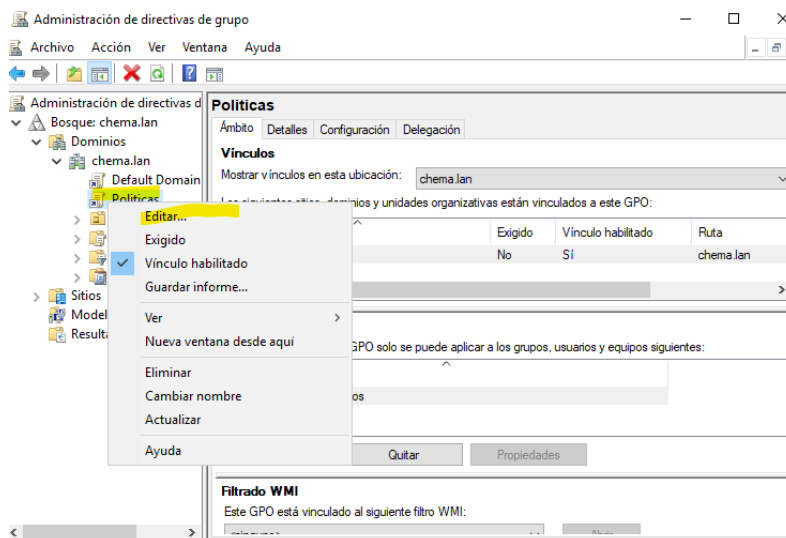
- Acceder al dominio donde quieras aplicar las políticas-> click derecho -> Crear GPO



- Seleccionamos un nombre y aceptar

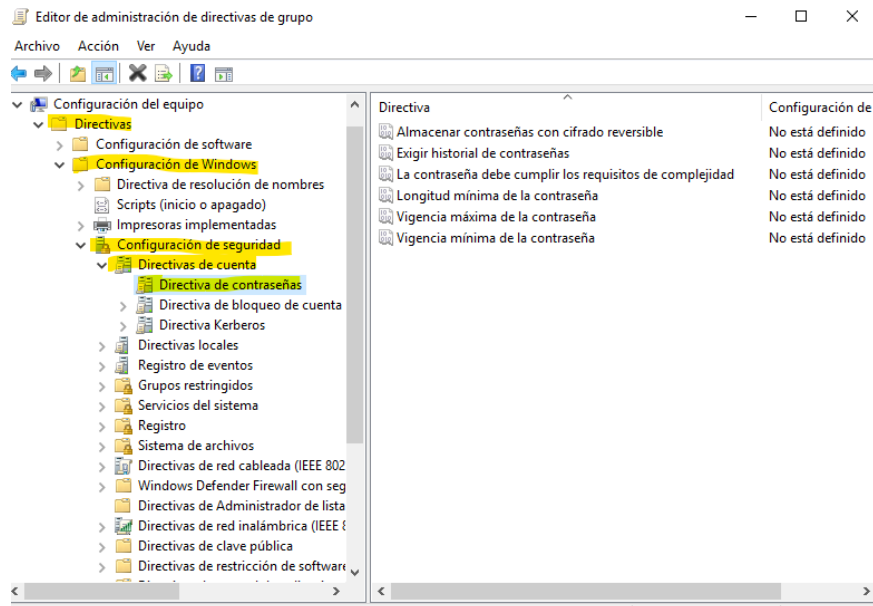


- Accedemos a la nueva GPO con click derecho->editar

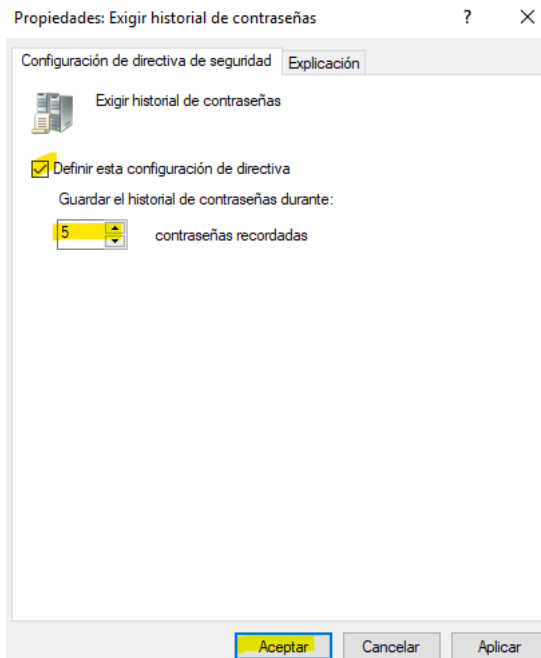




- Accedemos a Configuración del equipo-> Directivas ->configuración de Windows -> configuración de seguridad-> directivas de cuenta->directiva de contraseñas

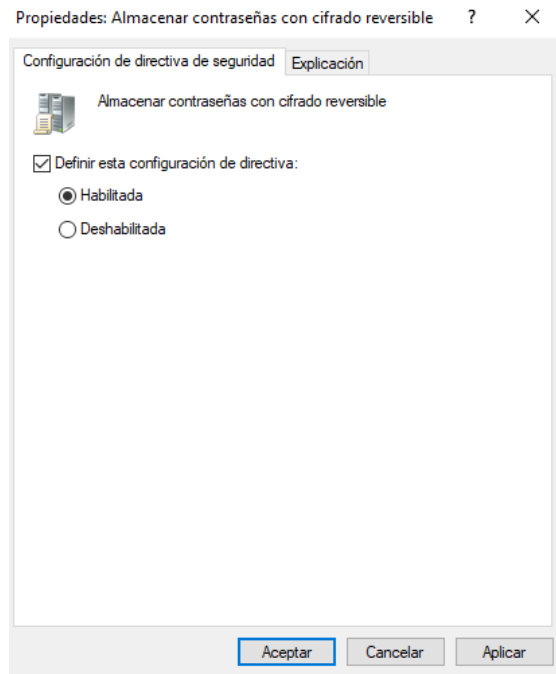


- Exigir historial de contraseñas, para que el usuario no repita la misma contraseña cuando a este se le acabe la vigencia.

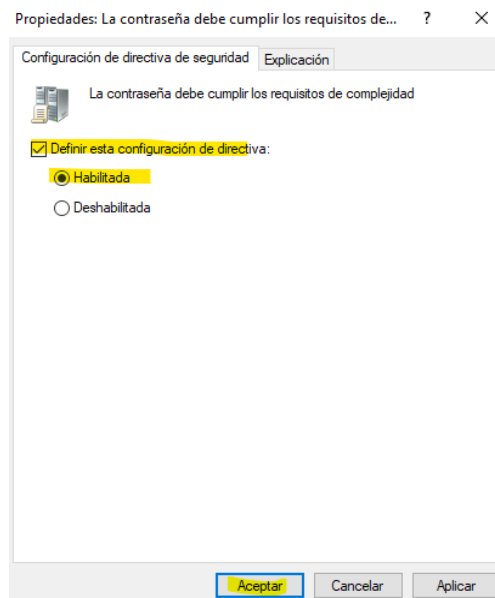




- Las contraseñas se almacenan con un cifrado reversible para prevenir posibles entradas no deseadas

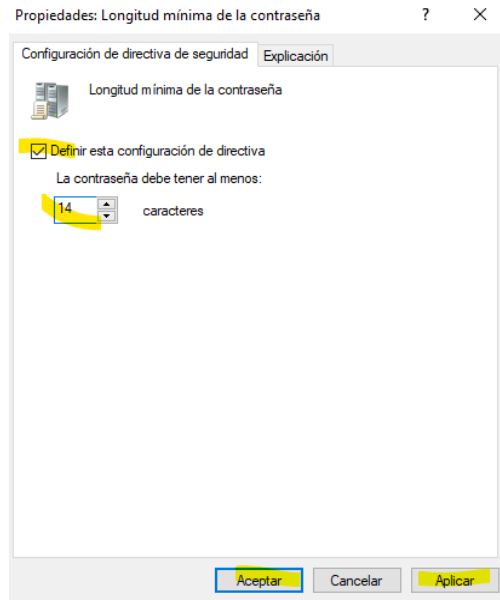


- Complejidad de las contraseñas

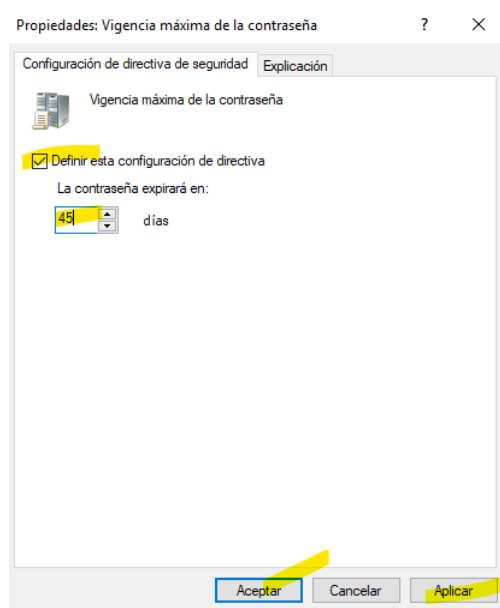




- Longitud mínima de las contraseñas

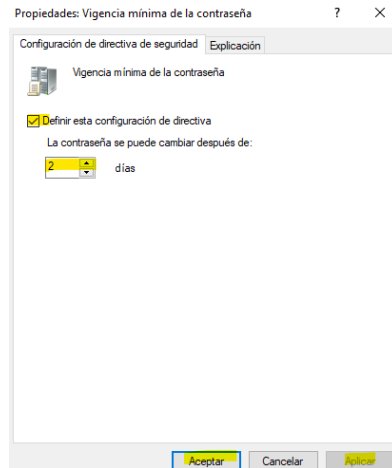


- Vigencia de la contraseña antes de tener que ser actualizada nuevamente

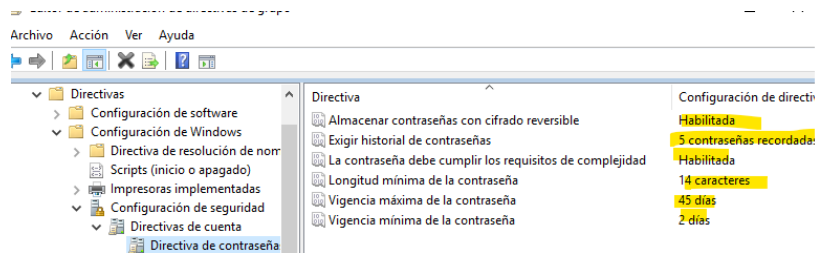




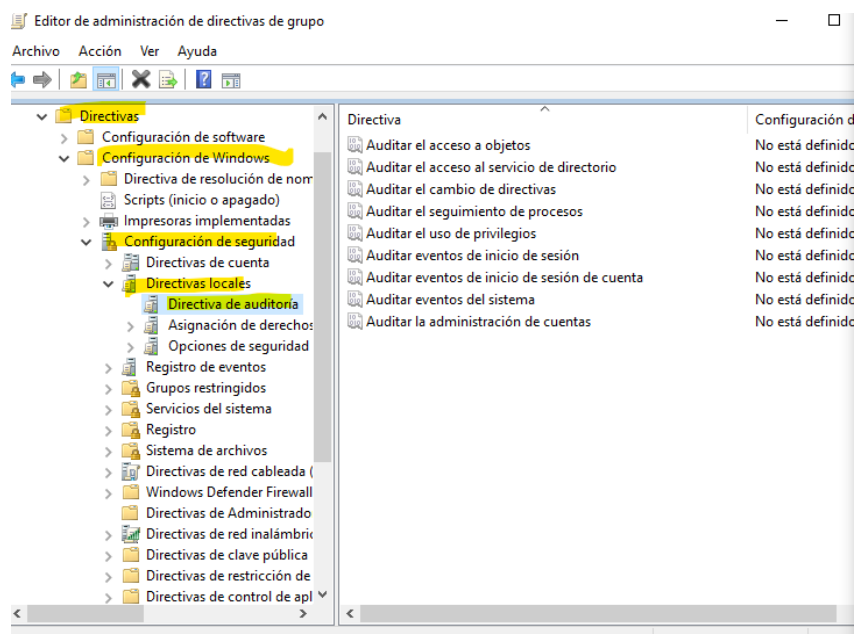
- Vigencia mínima de contraseña



- Al final nuestras políticas de contraseña serán las siguientes

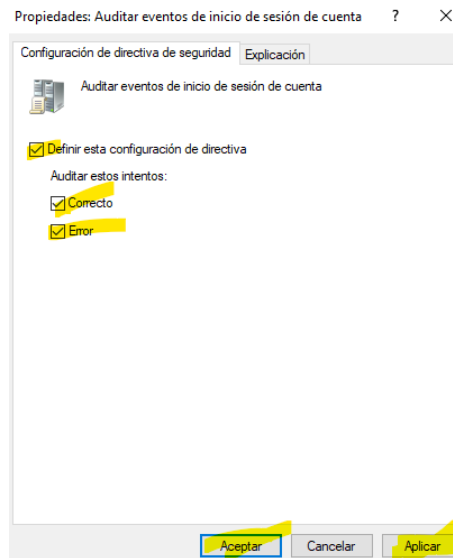


- Directivas de auditoría
- En la misma pestaña de las directivas de cuenta encontramos con las directivas locales-> directivas de auditoría

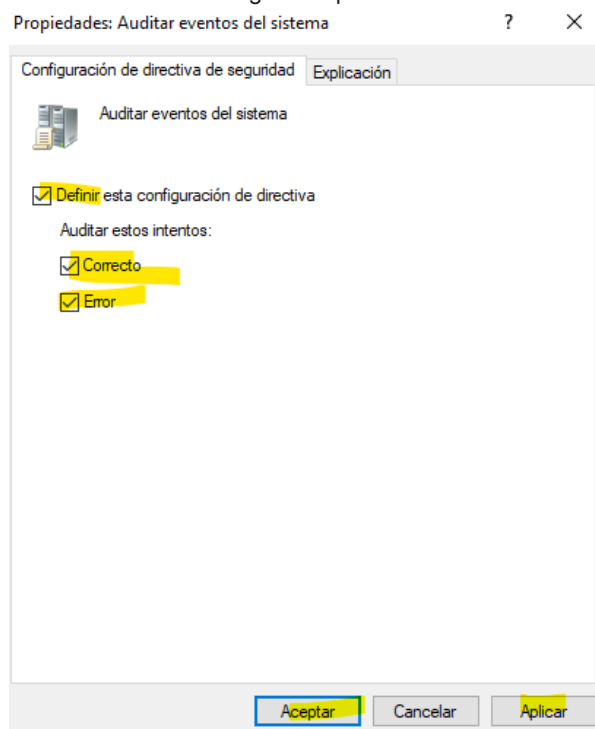




- Auditoría de inicios de sesión donde se recogerán los inicios de sesión tanto como válidos como inválidos



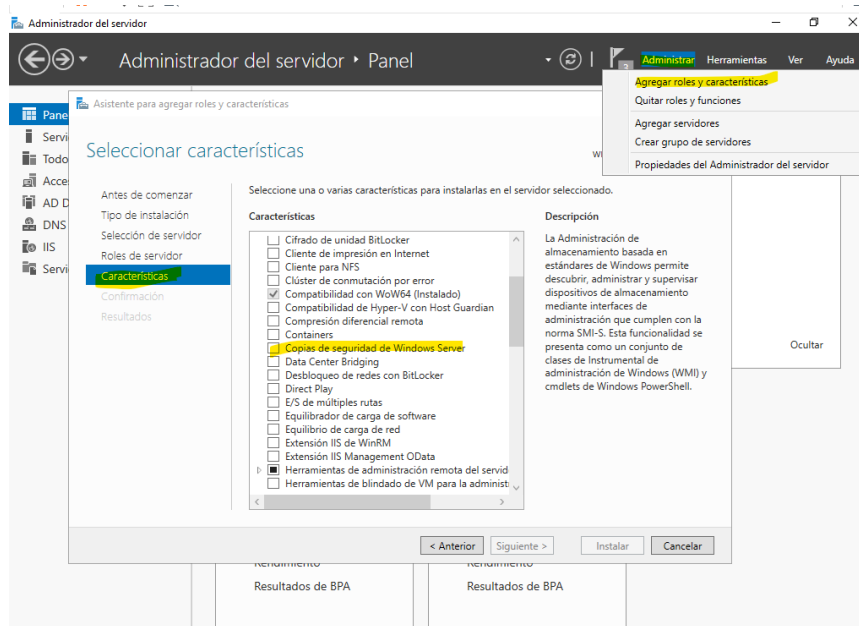
- Auditorías de eventos del sistema para controlar los intentos de cierre o inicio de sistema de seguridad por los usuarios



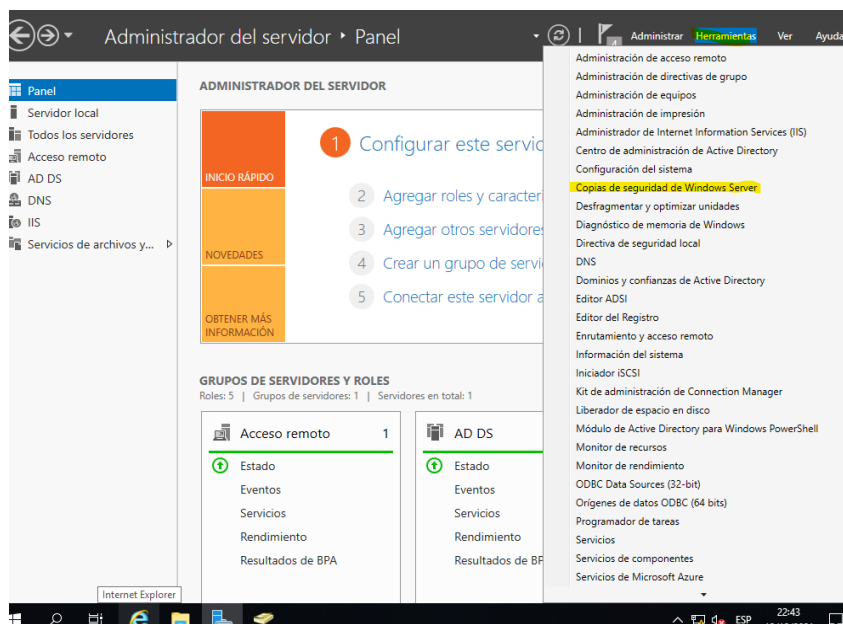


Copias de seguridad del sistema

- Para añadir esta característica a nuestro windows server tendremos que ir al Panel de Administrador del servidor-> agregar roles y características-> características y activamos copias de seguridad de Windows Server.

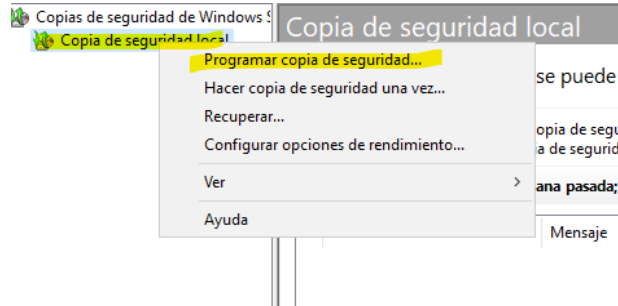


- Tras esto procedemos a instalar la nueva característica y reiniciamos el sistema.
- Para configurar las copias de seguridad accedemos al Panel de Administrador del servidor-> herramientas-> copias de seguridad de Windows Server.

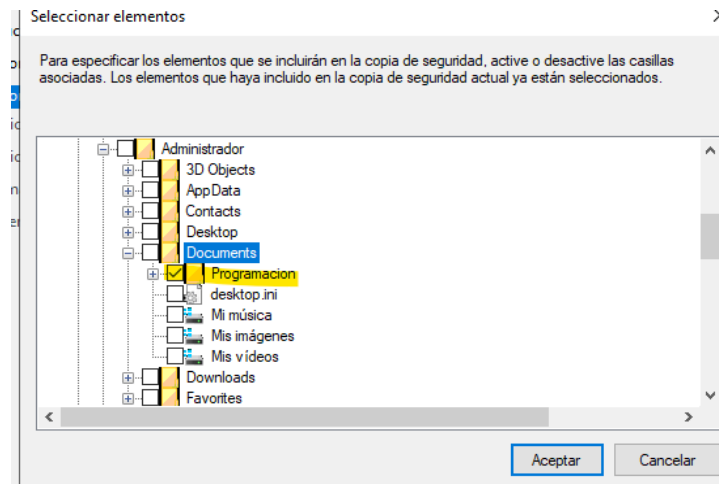




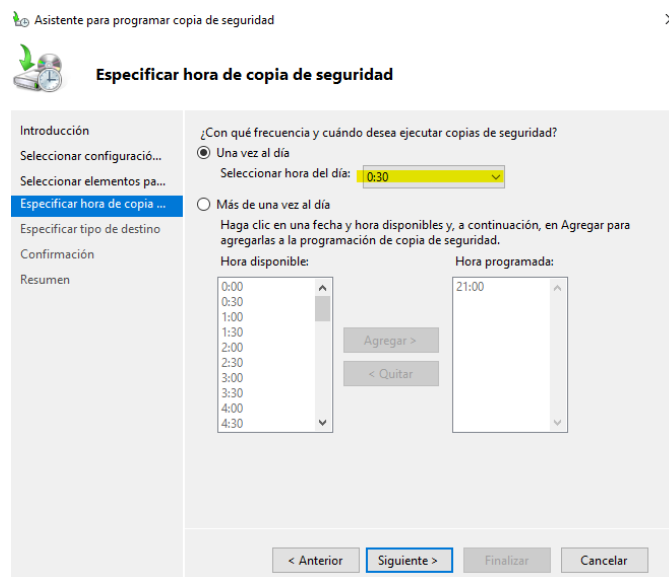
- Copia de Seguridad Local-> Programar copia de seguridad



- Seleccionamos una copia de seguridad personalizada y en mi caso seleccione las carpetas compartidas de la red local. Aquí se añadirán todas las carpetas importantes de la empresa.




- Tras esto indicamos la hora programada para realizar las copias de seguridad en mi caso será una vez al día al finalizar la jornada laboral.





- Las destinamos a un disco duro dedicado para la preservación de las mismas

 Asistente para programar copia de seguridad



Especificar tipo de destino

<p>Introducción</p> <p>Seleccionar configuració...</p> <p>Seleccionar elementos pa...</p> <p>Especificar hora de copia ...</p> <p>Especificar tipo de destino</p> <p>Seleccionar disco de desti...</p> <p>Confirmación</p> <p>Resumen</p>	<p>¿Dónde desea almacenar las copias de seguridad?</p> <p><input checked="" type="radio"/> En un disco duro dedicado para copias de seguridad (recomendado)</p> <p>Elija esta opción para almacenar copias de seguridad de la forma más segura. El disco duro que use se formateará y se dedicará únicamente a almacenar copias de seguridad.</p> <p><input type="radio"/> En un volumen</p> <p>Elija esta opción si no puede dedicar un disco entero a las copias de seguridad. Tenga en cuenta que el rendimiento del volumen puede disminuir hasta un 200% cuando se usa para almacenar copias de seguridad. No es recomendable almacenar otros datos del servidor en el mismo volumen.</p> <p><input type="radio"/> En una carpeta de red compartida</p> <p>Elija esta opción si no desea almacenar las copias de seguridad localmente en el servidor. Tenga en cuenta que solo puede tener una única copia de seguridad a la vez porque, al crear una nueva copia de seguridad, se sobrescribe la anterior.</p>
--	--

- Tras esto eliges la ruta de destino y confirmas la programación de las copias de seguridad.



6.- Planes de recuperación de desastres

Los activos de la empresa son :

- 30 ordenadores valorados en unos €1300 de media.
- 15 tabletas valorizadas en unos €3000 de media.
- Un router internet profesional valorado en unos €300.
- Dos switches de unos €80.
- Contrato con el dominio de la página web de €1000 anuales.

Cualquier problema con el software será con la empresa distribuidora del mismo. Este problema persiste. Se recomienda volver a una versión anterior del software o utilizar un software alternativo mientras el software necesario se encuentra inactivo.

Mantener el software de los sistemas operativos actualizado en las últimas versiones para garantizar la seguridad interna de los equipos.

Los problemas con el hardware se deberán consultar con el técnico correspondiente y valorar la reparación o sustitución de los dispositivos.

Sí, estos problemas con el hardware sucedieran con una de las tabletas se recomienda la introducción al equipo de al menos 3 tabletas menos potentes que puedan sustituir temporalmente a las tabletas más potentes para evitar paros en el ritmo de trabajo.

Si hubiere alguna circunstancia especial, enfermedad o problemas con el desplazamiento a la oficina, comunicar a dirección para poder trabajar telemáticamente.

En caso de ataque a la página web, proceder adecuadamente según el Protocolo.

En caso de una infección Malware interna aislar el foco de la infección del resto de la red.

En caso de robo de datos o extorsión informar a los cuerpos del Estado pertinentes y proceder según el protocolo.

En caso de una pérdida de información dentro del servidor local recurrir a la copia de seguridad más reciente.



7.- BIBLIOGRAFÍA

Imágenes:

Todas las imágenes han sido extraídas de mi propia maquina virtual Windows Server 2019

Bibliografía:

Threat Vector

Mary E. Shacklett Threat vector What is a threat Vector?

En techtarget.com Disponible en:

<https://www.techtarget.com/searchsecurity/definition/attack-vector>

[11/diciembre/2021]

VPN

Anonimo, What is a VPN? How it works, Types of VPN

En kaspersky.com Disponible en:

<https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>

[11/diciembre/2021]

Implementación VPN

MFST Webcast 24 Install and Configure a Remote VPN

En youtube.com Disponible en:

https://youtu.be/eTzHH8CQX_8

[11/diciembre/2021]

NAT

Joshelu 24 Agosto 2011 NAT ¿Qué es y cómo funciona?

En xacatamovil.com Disponible en:

<https://www.xacatamovil.com/conectividad/nat-network-address-translation-que-es-y-como-funciona>

[11/diciembre/2021]

Implementación NAT

JGAITPro Configuración e Instalación de Network Address Translation (NAT) en windows server 2019

En youtube.com Disponible en:

<https://youtu.be/lyb2y3R6IIM>

[11/diciembre/2021]

DMZ

INCIBE 19 septiembre 2019 Que es una DMZ y como te puede ayudar a proteger tu empresa

En incible.es Disponible en:

<https://www.incible.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa>

[11/diciembre/2021]

Implementación DMZ

Anonimo, 2012 Configuring DMZ

[11/diciembre/2021]

https://www.cisco.com/c/dam/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html

IP Estática

Direcciones IP estáticas frente a dinámicas.

En avast.com Disponible en:

<https://www.avast.com/es-es/c-static-vs-dynamic-ip-addresses#gref>

[11/diciembre/2021]



Implementación IP Estática

Pc Solucion, 2021 Establecer IP estática windows server

En youtube.com Disponible en:

https://youtu.be/J7Ffu_iOaFg

[11/diciembre/2021]

RGPD

Anónimo 2021, Reglamento General de Protección de Datos

En Wikipedia.org Disponible en :

https://es.wikipedia.org/wiki/Reglamento_General_de_Protecci%C3%B3n_de_Datos

[12/diciembre/2021]

Fuentes adicionales

Threads

The 10 Most common Website Security Attacks

En tripiwire.com Disponible en :

<https://www.tripwire.com/state-of-security/featured/most-common-website-security-attacks-and-how-to-protect-yourself/>

[11/diciembre/2021]

Firewall

Anónimo ¿Qué es un Firewall y cómo funciona?

En idgrup.com Disponible en :

<https://idgrup.com/firewall-que-es-y-como-funciona/>

[11/diciembre/2021]