M-SOP-001

Manual de Controles de Seguridad para Instalación de Sistemas Operativos en Equipos de Cómputo.

Responsables

Elaboró:	Soporte Técnico
Revisó:	Control de Documentos
Aprobó:	Gerente de Operaciones

Control de versiones

Versión	Fecha	Descripción del cambio
1	08/10/21	Emisión inicial
2	28/04/22	Revisión y mejora derivado de auditoría interna 2022
3	11/10/2022	Actualización de formato y revisión general del documento.

Clave del formato de manual: F-SGI-004 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Introducción

El presente documento contiene los pasos y controles de seguridad para instalación de sistemas operativos en equipos de cómputo.

2. Alcance

El presente documento se limita a las actividades requeridas los pasos y controles de seguridad para instalación de sistemas operativos en equipos de cómputo.

3. Definiciones

- **Hardening:** El hardening o endurecimiento es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuantas más funciones desempeña; en principio un sistema con una única función es más seguro que uno con muchos propósitos

- **Firewall:** Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

- **DHCP:** El protocolo DHCP (Protocolo de configuración dinámica de host) o también conocido como «Dynamic Host Configuration Protocol«, es un protocolo de red que utiliza una arquitectura cliente-servidor.

- **Ethernet:** Ethernet es la tecnología tradicional para conectar dispositivos en una red de área local (LAN) o una red de área amplia (WAN) por cable, lo que les permite comunicarse entre sí a través de un protocolo: un conjunto de reglas o lenguaje de red común.

- **Wireless:** En un sentido amplio, Wireless es un término utilizado para definir la transmisión de datos entre una variedad de dispositivos, sin conexiones por cables, es decir, de forma inalámbrica, a través de ondas electromagnéticas.

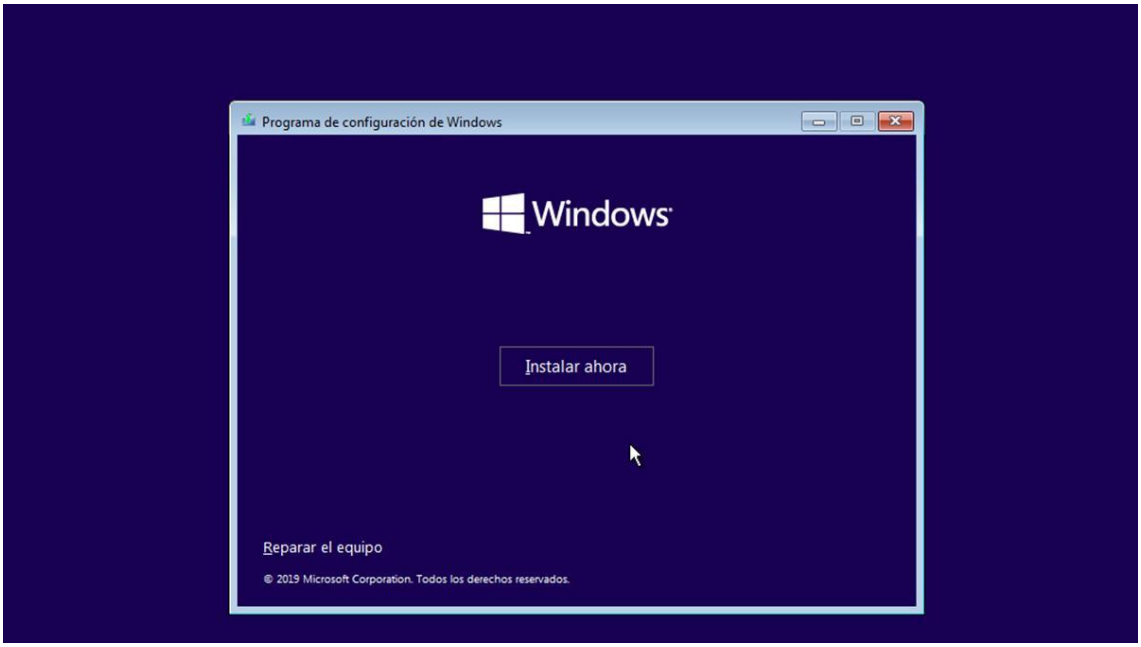
- **Cifrado:** El cifrado en ciberseguridad es la conversión de datos de un formato legible a un formato codificado. Los datos cifrados solo se pueden leer o procesar luego de descifrarlos.

- **Bitlocker:** BitLocker es un producto de cifrado de Microsoft diseñado para proteger los datos del usuario en una computadora.

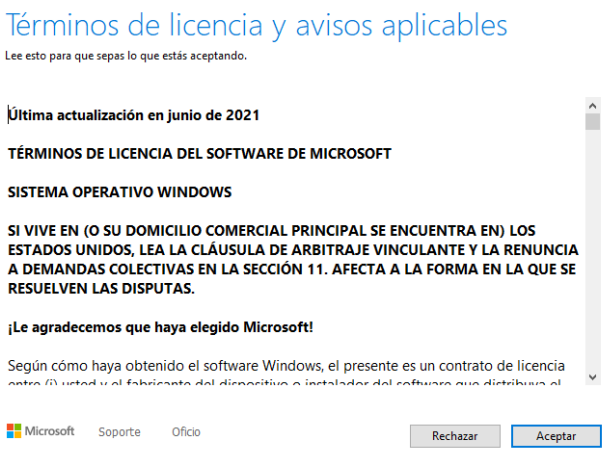
- **Endpoint:** Un endpoint es cualquier dispositivo que sea físicamente la parte final de una red. Las computadoras de escritorio, las tablets, los smartphones, los dispositivos de oficina de red, como los routers, las impresoras y las cámaras de seguridad también son considerados endpoints.

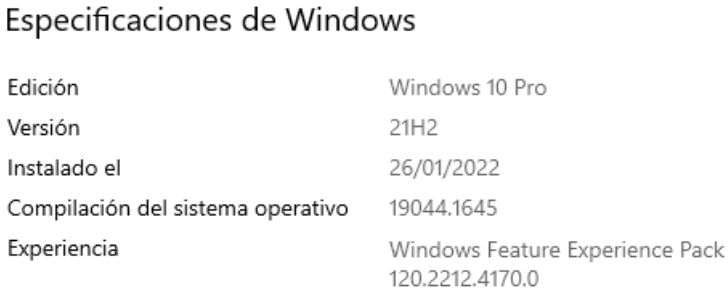
4. Descripción del manual

1. Instalación de imagen de Sistema Operativo oficial descargada desde el portal de fabricante.

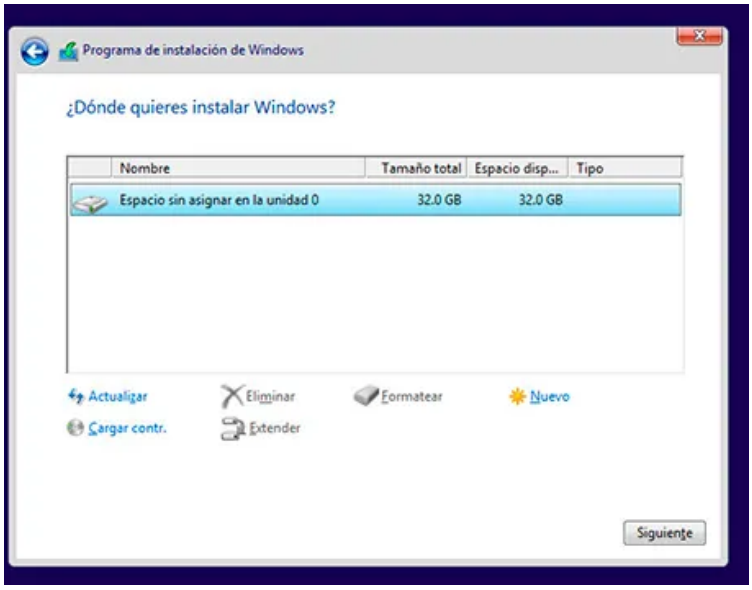


2. Validación de hash del sistema operativo.



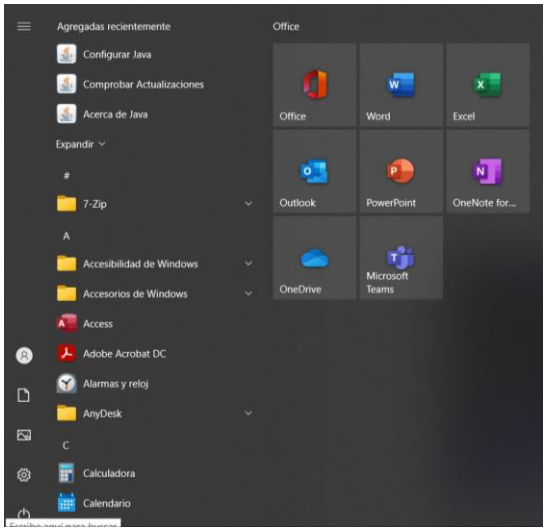


3. Se habilita el inicio de sistema operativo solo por la partición donde reside el Sistema operativo.

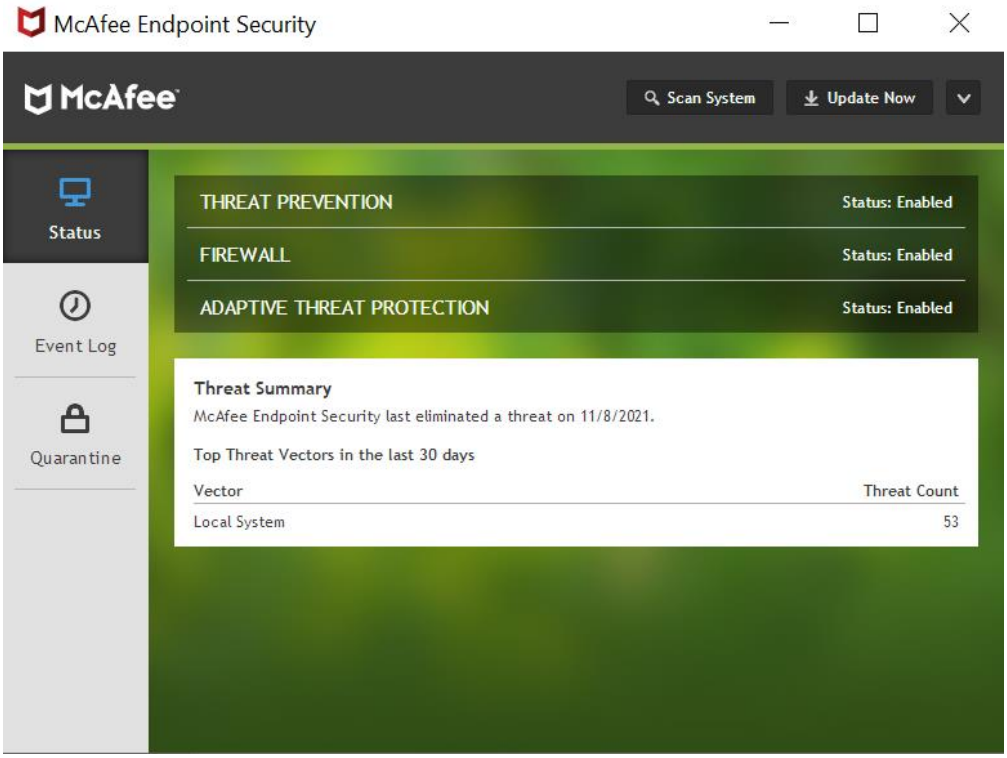


4. Actualización de sistema operativo con los últimos parches de seguridad.

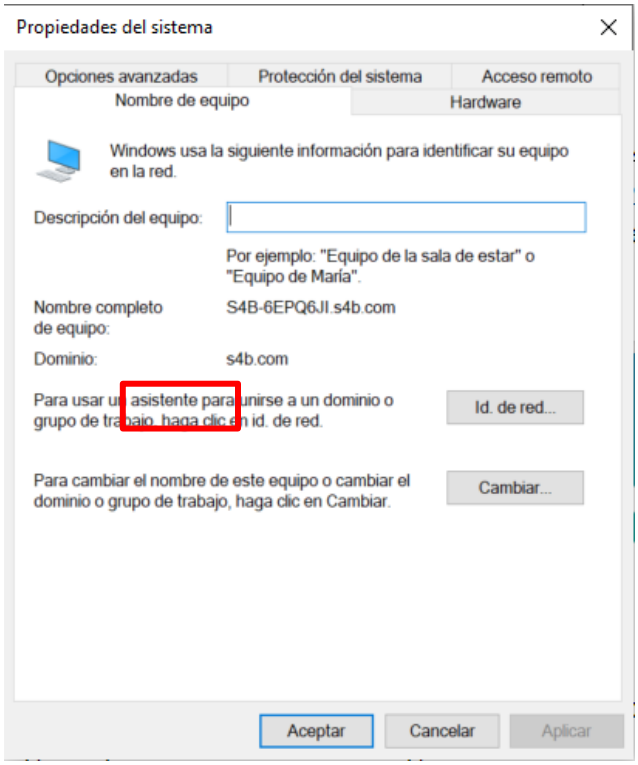
5. Desinstalación de software no necesario que incluya el sistema operativo.



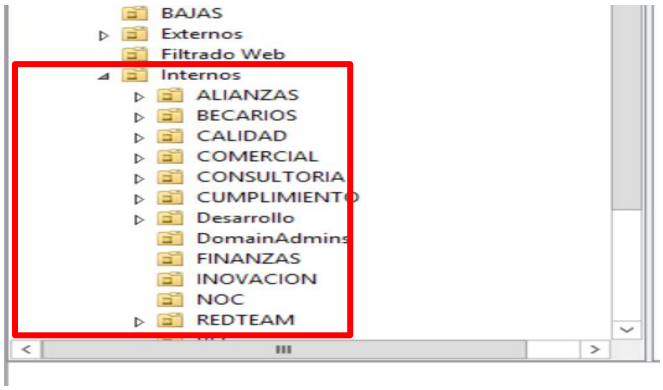
6. Se instala software de protección antivirus.



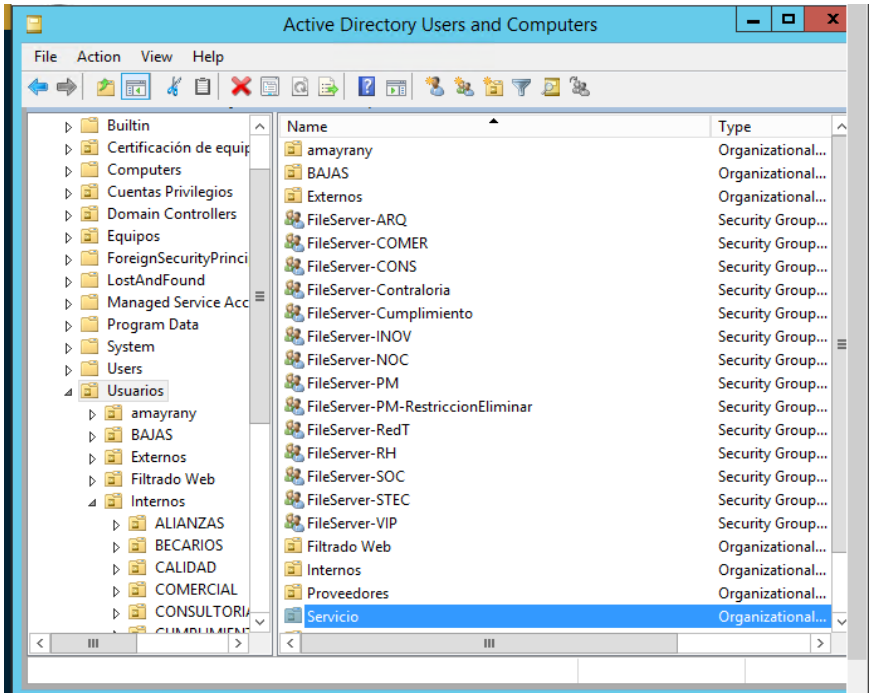
7. Se ingresa el equipo a dominio.

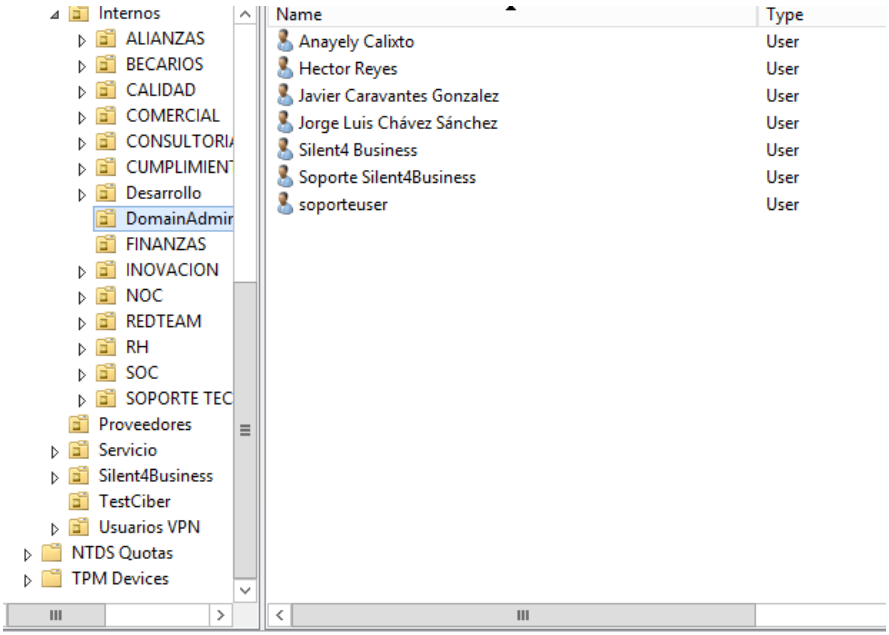


8. Todos los accesos y políticas de seguridad están regidas por el directorio activo.

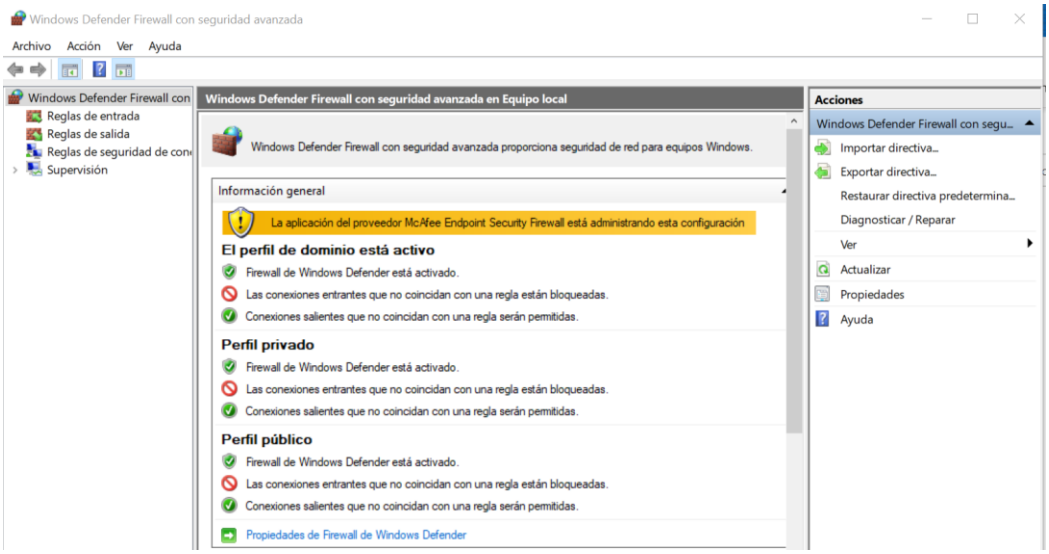


9. Los permisos de las cuentas de usuario son definidos de acuerdo con el perfil y al área perteneciente y con aprobación del SGI.

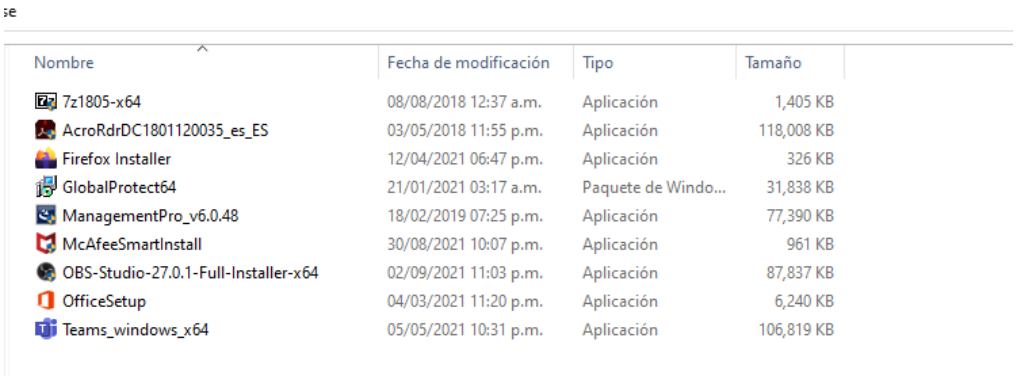




10. Protección de firewall local, administrado por Mcafee Endpoint, donde se establecen los permisos de comunicación.



11. Instalación de software base declarado en el SGI.



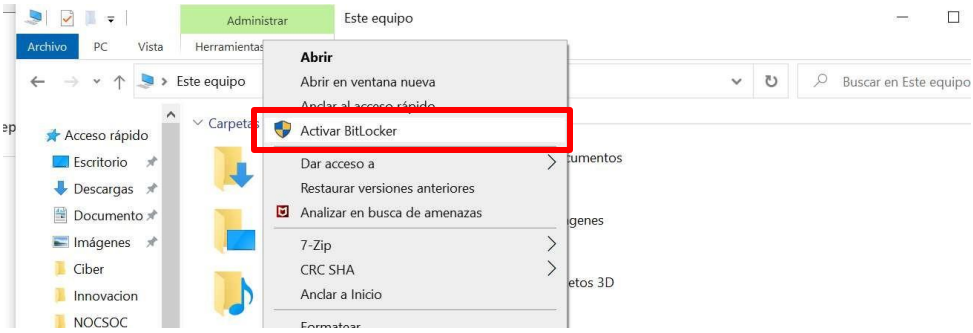
Nombre	Fecha de modificación	Tipo	Tamaño
7z1805-x64	08/08/2018 12:37 a.m.	Aplicación	1,405 KB
AcroRdrDC1801120035_es_ES	03/05/2018 11:55 p.m.	Aplicación	118,008 KB
Firefox Installer	12/04/2021 06:47 p.m.	Aplicación	326 KB
GlobalProtect64	21/01/2021 03:17 a.m.	Paquete de Windo...	31,838 KB
ManagementPro_v6.0.48	18/02/2019 07:25 p.m.	Aplicación	77,390 KB
McAfeeSmartInstall	30/08/2021 10:07 p.m.	Aplicación	961 KB
OBS-Studio-27.0.1-Full-Installer-x64	02/09/2021 11:03 p.m.	Aplicación	87,837 KB
OfficeSetup	04/03/2021 11:20 p.m.	Aplicación	6,240 KB
Teams_windows_x64	05/05/2021 10:31 p.m.	Aplicación	106,819 KB

12. Cifrado de unidades de disco de equipos portátiles.

Cifrado de Disco BitLocker

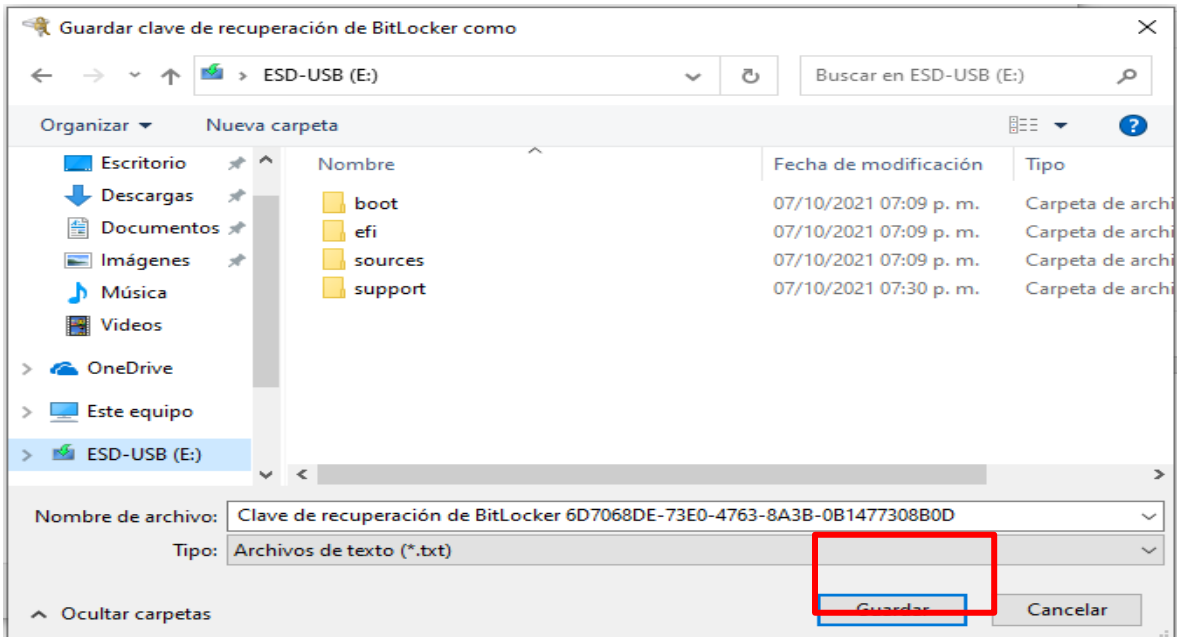
1.- Seleccionar la unidad a cifrar, en este caso nos interesa la unidad “c:”

2.- Damos clic derecho y seleccionamos Activar BitLocker

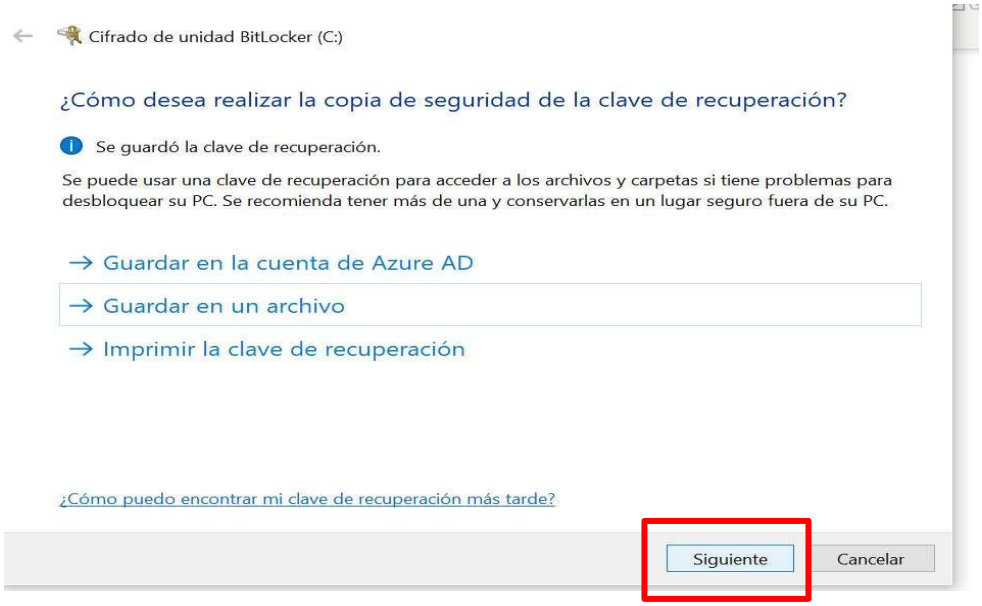


3.-Dar clic izquierdo en la opción “Guardar en la cuenta de Azure AD” (esta opción se encontrará disponible solo si Windows 10 se encuentra totalmente actualizado, en caso de no estar disponible saltarse al paso 4).

4.-Dar clic izquierdo en la opción “Guardar en un archivo”, guardamos de preferencia en una memoria USB que tengamos disponible seleccionamos la ruta del dispositivo USB y damos “Guardar”.

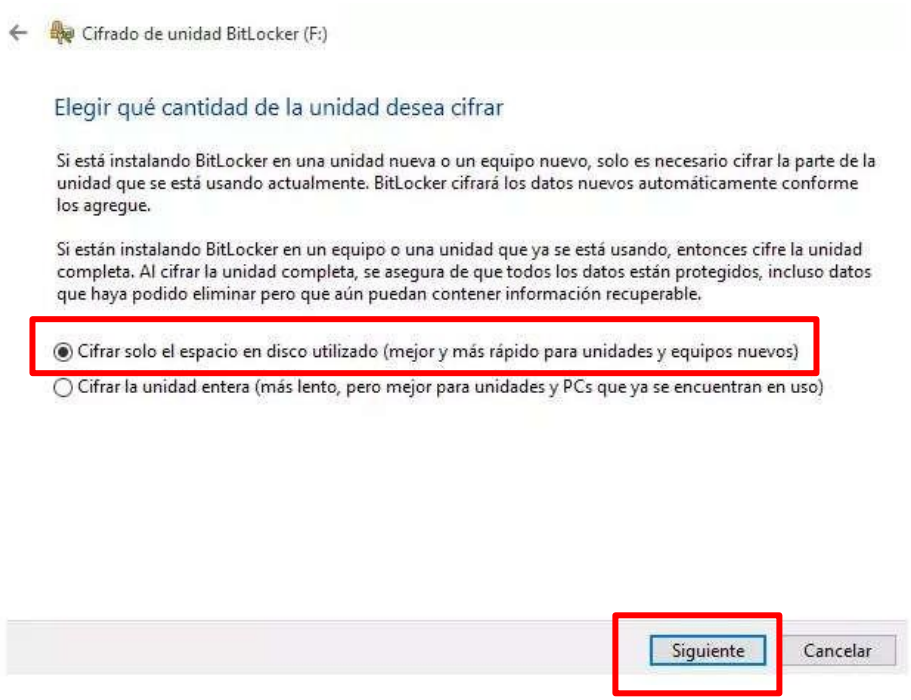


5.-Una vez seleccionada la ruta, se activará la casilla “siguiente”.

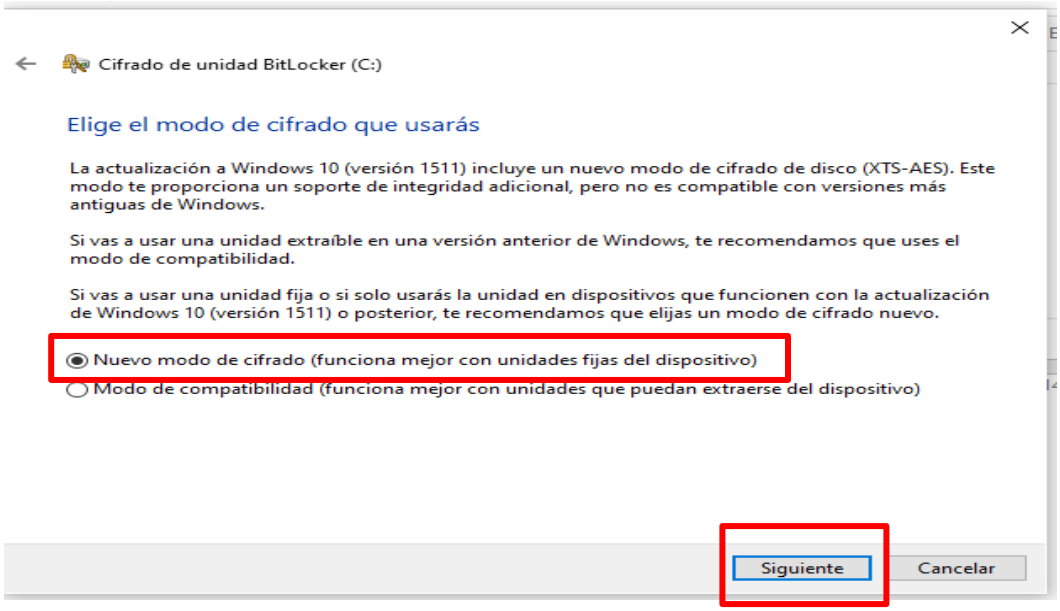


6.-Activamos BitLocker, “Activar BitLocker”

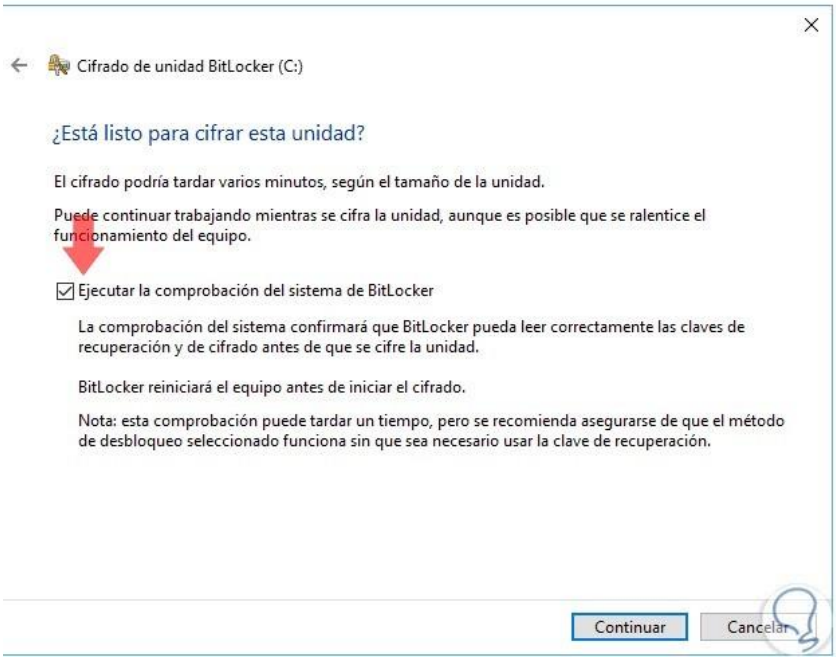
7.- Seleccionamos “Cifrar solo el espacio utilizado en disco”



8.- Seleccionamos “Nuevo modo de cifrado”

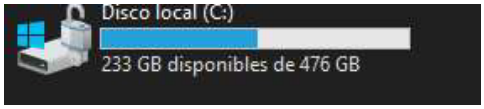


9.- Seleccionamos “Ejecutar la comprobación del sistema…”, y damos clic en continuar”.

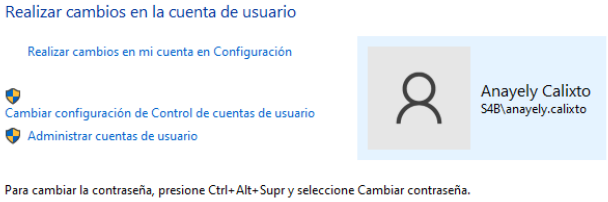


10.-En algunos casos solicitara el reinicio para ejecutar el cifrado con una ventana emergente.

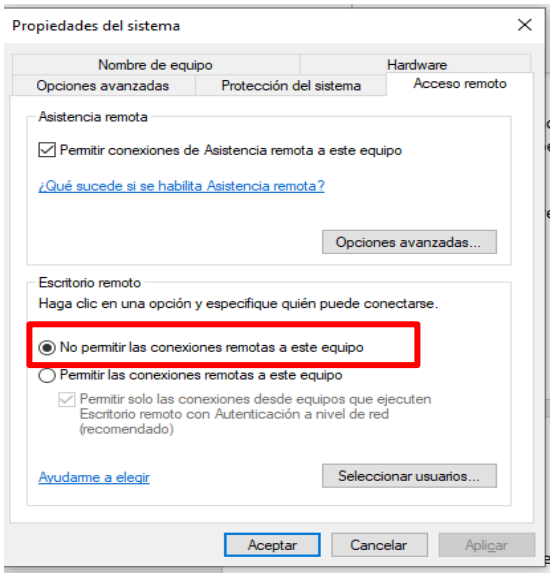
11.-Al finalizar el proceso veremos la unidad con un candado, lo cual indica que el disco ha sido cifrado.



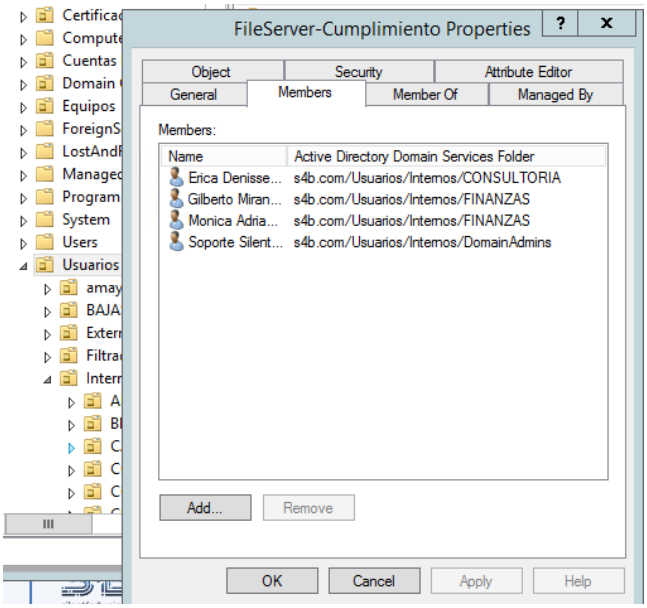
Cuenta de administrador local deshabilitada



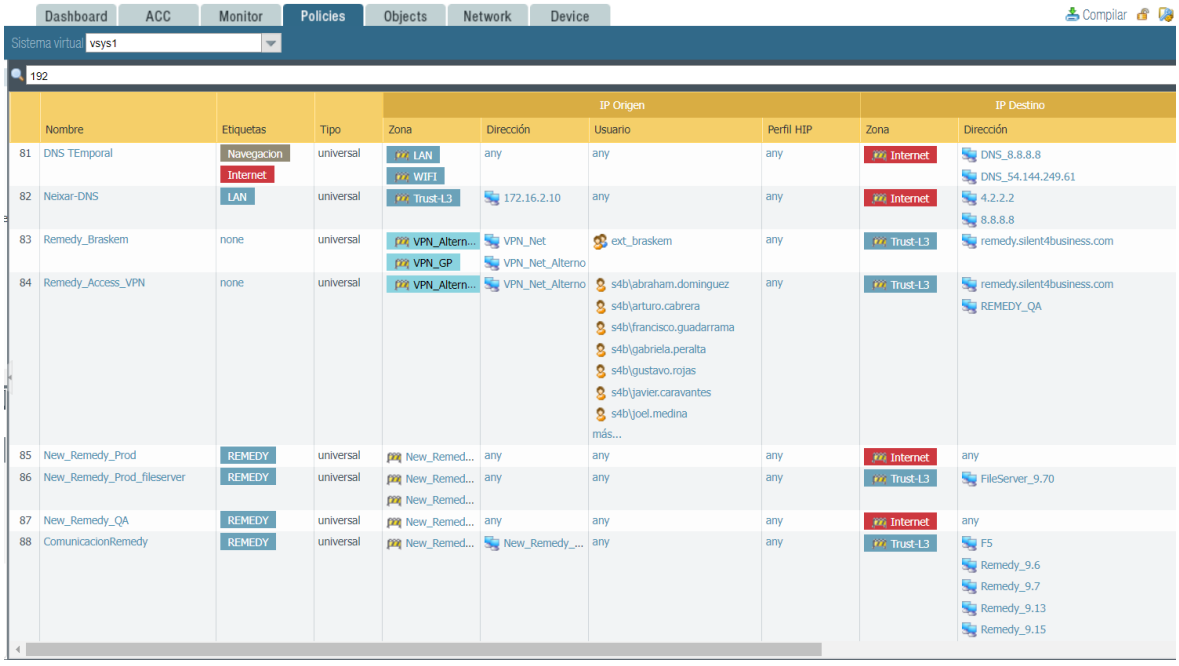
1. Escritorio remoto deshabilitado, solo habilitado para administración de servidores y equipos de operación.



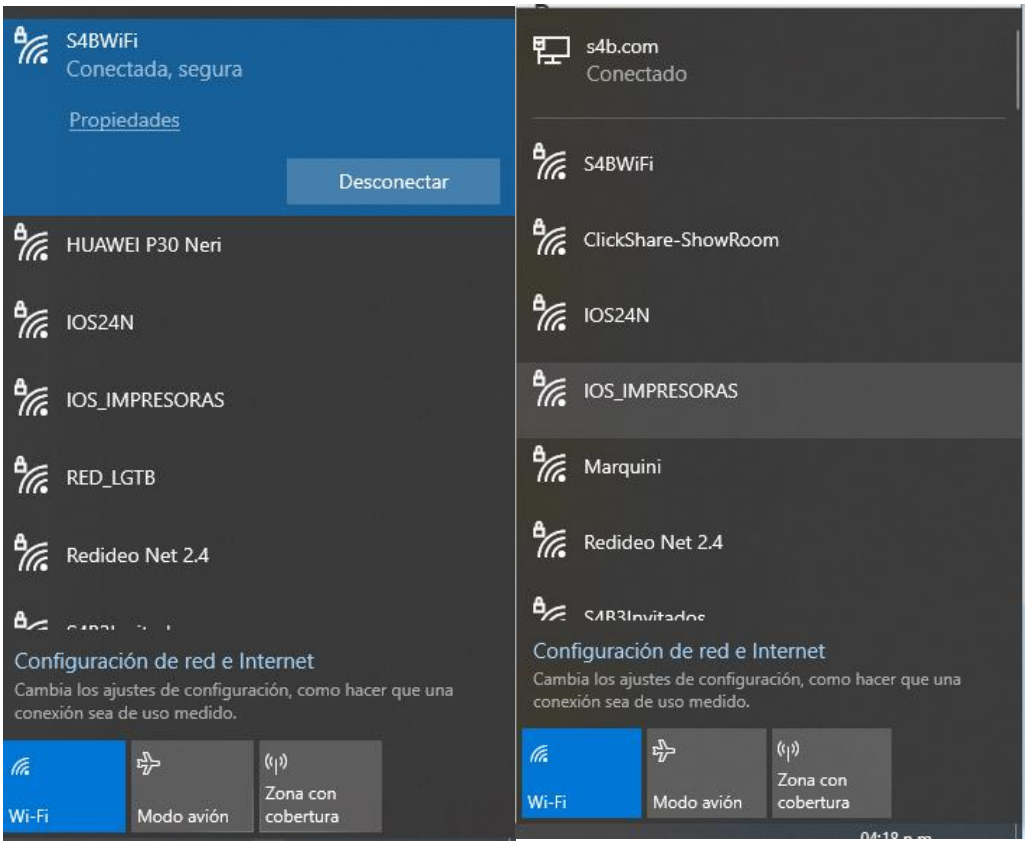
2. Permisos sobre accesos a carpetas y archivos administrados vía directorio activo.



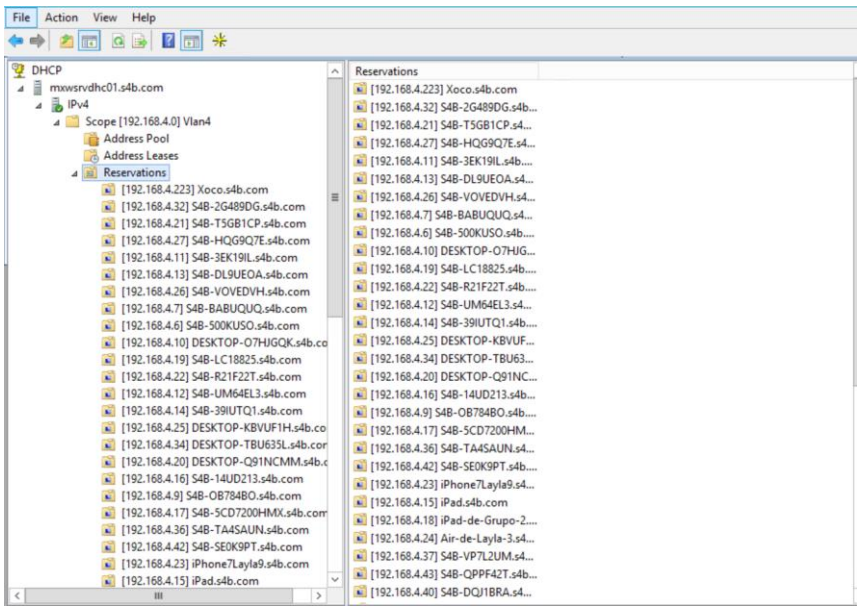
3. Permisos de red controlados por Firewall perimetral.



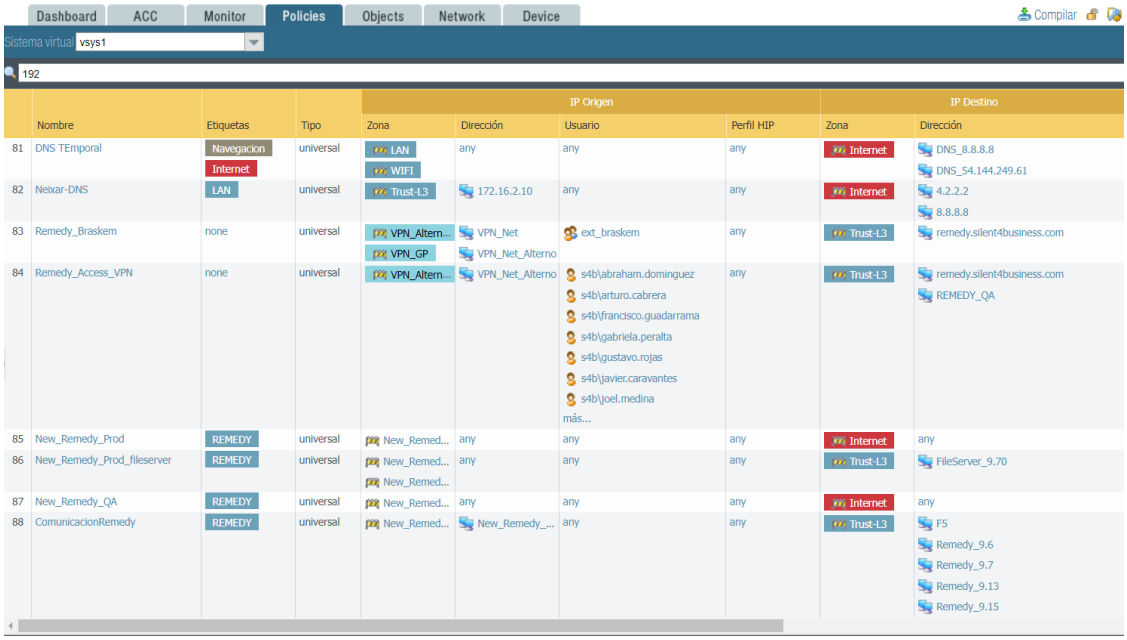
4. Conexiones ethernet y Wireless.



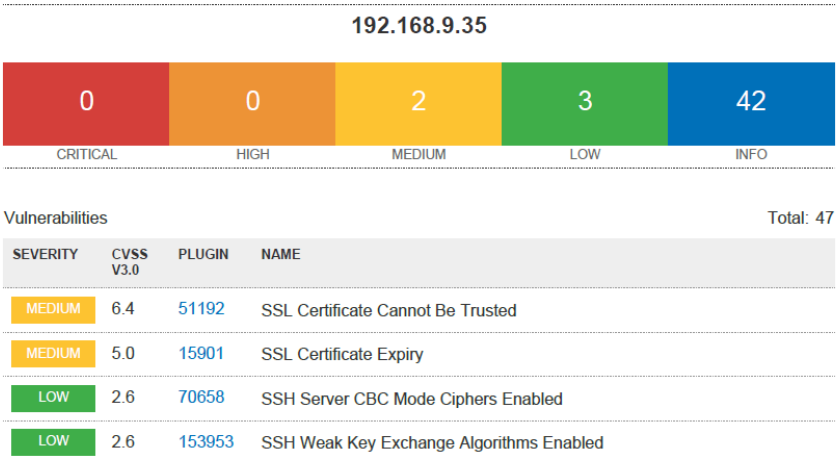
Asignación de direccionamiento IP: Todos los equipos reciben dirección IP por medio de DHCP, las cuales están mapeadas y reservadas para un control óptimo.



5. Todas las comunicaciones están protegidas de la siguiente forma:
   - Segmentación de redes
   - Firewall
   - IPS
   - Balanceador
   - Filtrado Web
   - Control de aplicaciones
   - Antivirus
   -
6. Todos los accesos a servidores están restringidos a solo personal de soporte, operativo y SOC/NOC dependiendo de sus funciones, y deben apegarse a los procesos aplicables.



7. Los servidores y servicios deben cumplir con los procesos de análisis de vulnerabilidades y pruebas de penetración, donde se identifican vulnerabilidades y brechas de seguridad, puertos no seguros, puertos no utilizados, servicios no necesarios, las cuales deben ser atendidas de acuerdo con el proceso.



192.168.9.35

0	0	2	3	42
CRITICAL	HIGH	MEDIUM	LOW	INFO

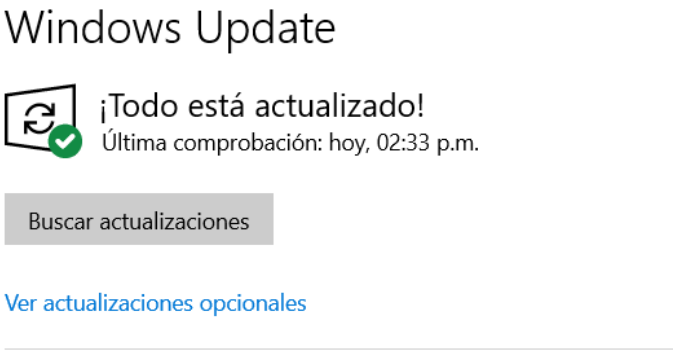
Vulnerabilities Total: 47

SEVERITY	CVSS V3.0	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.0	15901	SSL Certificate Expiry
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	153953	SSH Weak Key Exchange Algorithms Enabled

8. Los equipos con Sistemas operativos de fabricante cuentan con hardening desde su instalación.

El proceso de hardening se especifica en este manual.

9. Revisión y aplicación continua de parches de seguridad y actualizaciones de software de los fabricantes.



5. Anexos

No Aplica