Introducción

Moisés Sepúlveda

BitLocker Drive Encryption (BDE) es la solución de cifrado de disco nativa de Microsoft para sistemas operativos y unidades de datos. BitLocker, junto con Boot Configuration Database (BCD), se introdujo originalmente en Windows Vista.

Originalmente, el BCD es una base de datos independiente del firmware que almacena datos de configuración de arranque de Windows. En Windows Server 2016, el BCD se encuentra en una partición reservada para el sistema de 500MB sin letras en su disco de estado.

BitLocker permite cifrar todo el disco, o solo la parte que está en uso. La idea del cifrado de todo el disco es bastante simple: queremos codificar todo el contenido del disco al nivel del sector, de modo que solo las partes autorizadas puedan leer los datos.

Las principales GPOs que nos pueden servir a la hora de usar BitLocker, estan almacenadas en: *Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives.*

TPM (Trusted Platform Module) es un componente de hardware instalado en equipos más nuevos por fabricantes de equipos que

ayuda a BitLocker a proteger los datos de usuario y garantizar que un equipo no se manipule mientras el sistema estaba sin conexión.

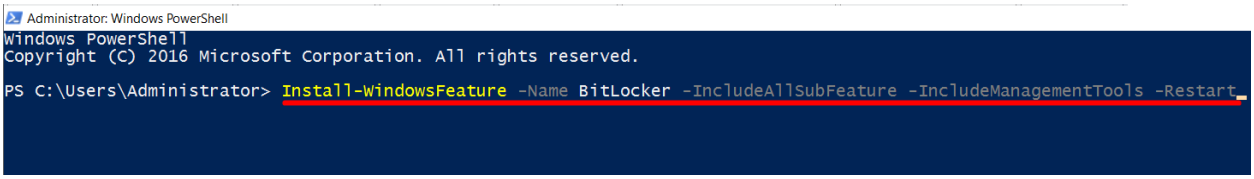
BitLocker brinda múltiples opciones para bloquear el proceso de inicio normal para que el usuario proporcione un número de identificación personal (PIN) o inserte un dispositivo USB extraíble, como una unidad flash, que contenga una clave de inicio. Cabe destacar, que para configurar un PIN de bloqueo, la máquina debe contar con un chip TPM, de lo contrario, solo se podría configurar por contraseña o por USB en la máquina, y por esta forma no se proporciona la verificación de integridad del sistema previa al inicio que ofrece BitLocker al trabajar con TPM.

Protectores de clave de BitLocker

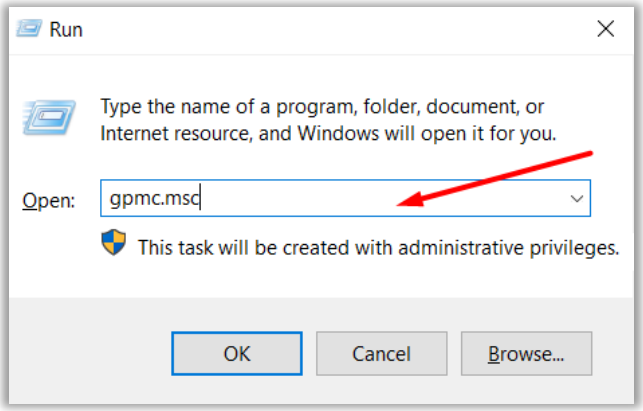
Protector de clave	Descripción
TPM	Un dispositivo de hardware usado para ayudar a establecer una raíz segura de confianza. BitLocker solo admite la versión de TPM 1,2 o versiones posteriores.
PIN	Un protector de clave numérica introducido por el usuario que solo se puede usar además del TPM.
PIN mejorado	Un protector de clave alfanumérica introducido por el usuario que solo se puede usar además del TPM.
Clave de inicio	Una clave de cifrado que puede almacenarse en la mayoría de los medios extraíbles. Este protector de clave se puede usar solo en equipos que no sean TPM o junto con un TPM para mayor seguridad.
Contraseña de recuperación	Número de 48 que se usa para desbloquear un volumen cuando está en modo de recuperación. A menudo, los números se pueden escribir en un teclado normal, si los números del teclado normal no responden, siempre puede usar las teclas de función (F1-F10) para introducir los números.
Clave de recuperación	Una clave de cifrado almacenada en medios extraíbles que se puede usar para recuperar datos cifrados en un volumen de BitLocker.

Implementación de Cifrado de Unidad con BitLocker por GPO, Desbloqueo por Contraseña y Almacenamiento de Clave de Recuperación en AD

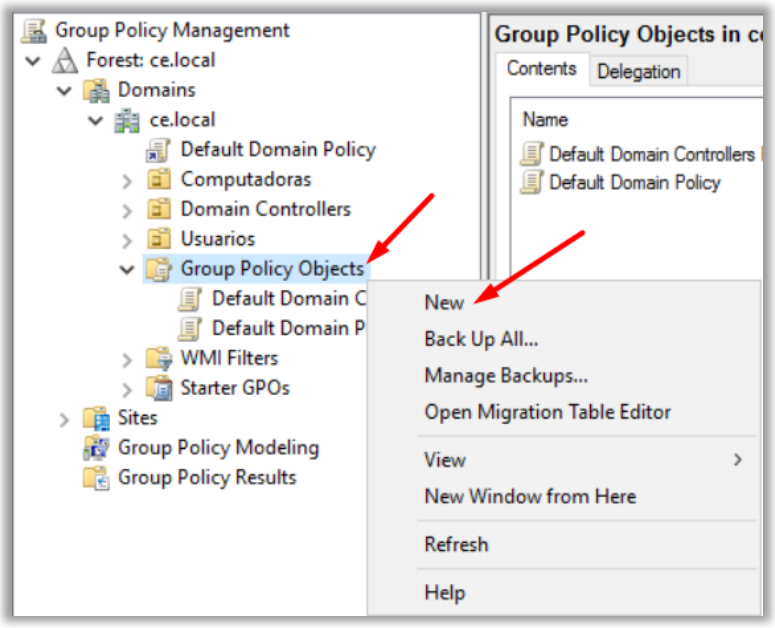
1-Lo primero que hacemos es habilitar o instalar BitLocker desde el Power Shell. El servidor se reiniciará luego de la instalación



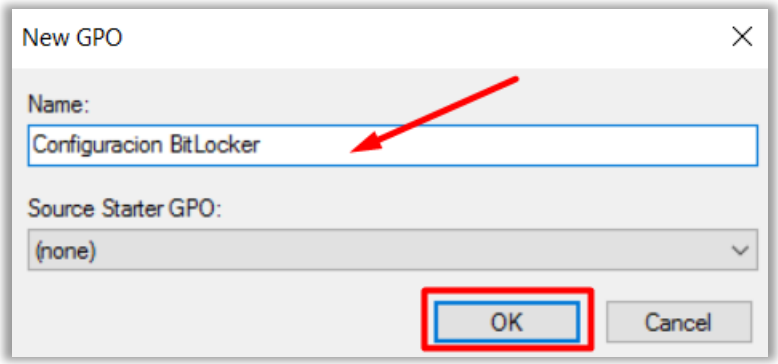
2-A continuación, nos dirigimos al Group Police Management Console.



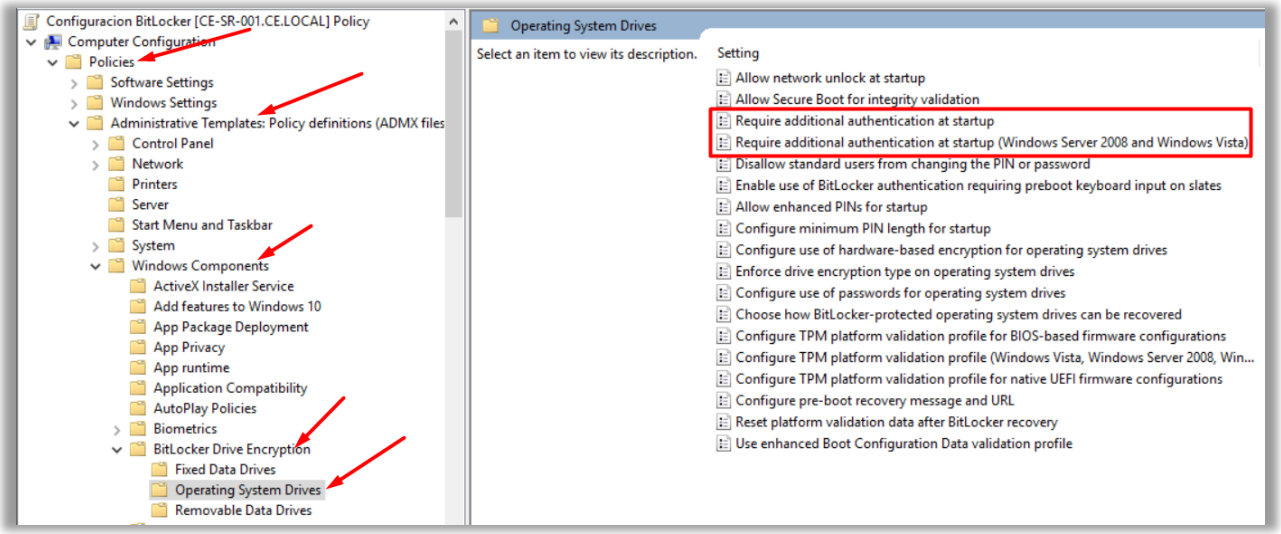
3-A continuación, creamos un nuevo GPO.



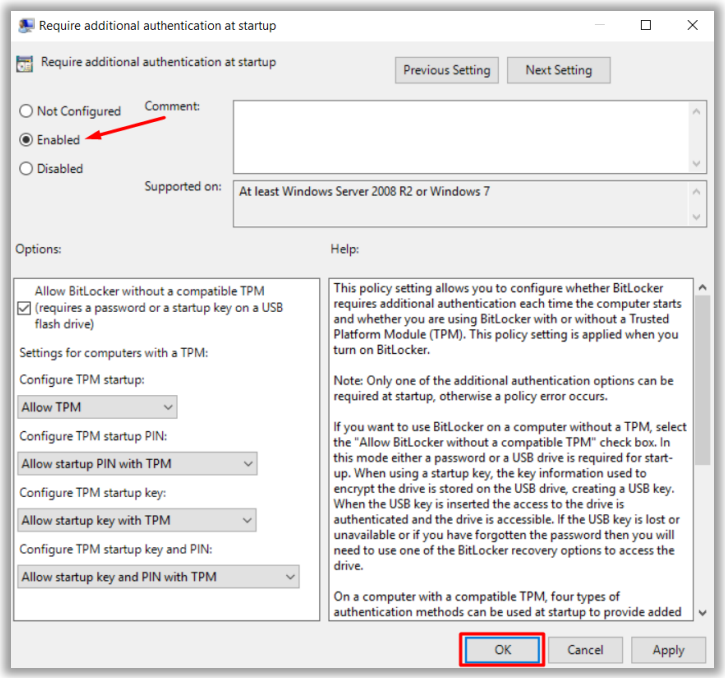
4-Establecemos el nombre del GPO, y hacemos clic en OK.



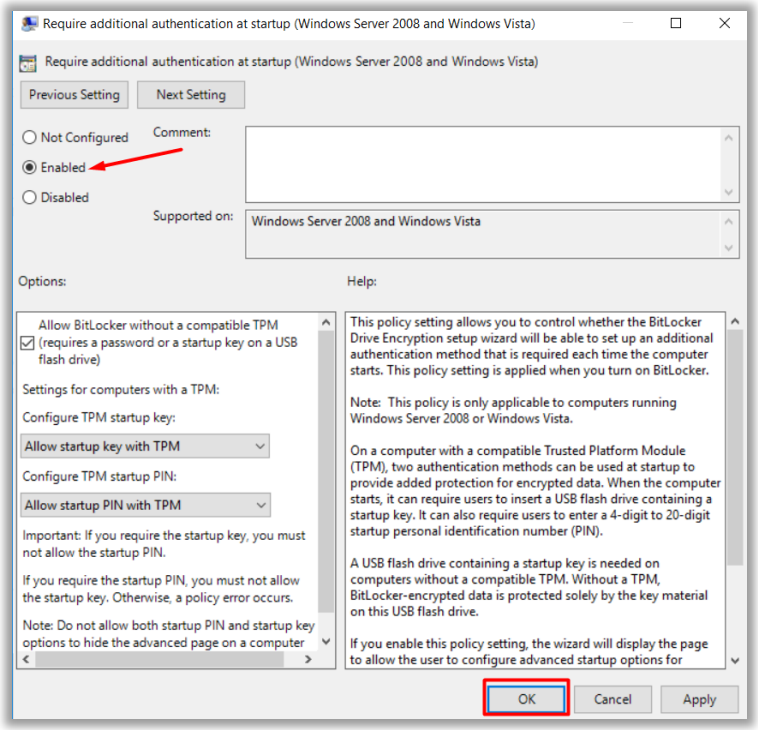
5-Una vez establecido el nombre, editamos nuestro GPO, dirigiendonos a Computer Configuration/Policies/Administrative Templates/Windows Components/BitLocker Drive Encryption/Operating System. Las GPO que modificaremos pueden verse en la imagen.



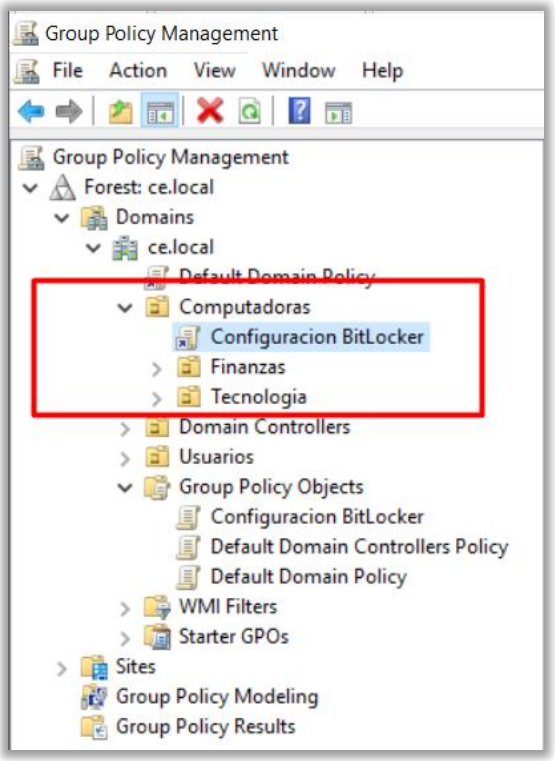
6-A continuación, vamos a habilitar la primera GPO. En la opción Configure TPM Startup PIN, lo permitimos, pero no es obligatorio, por lo que podremos desplegar BitLocker por Contraseña, como se ve en el Check Box que dice Allow BitLocker without compatible TPM.



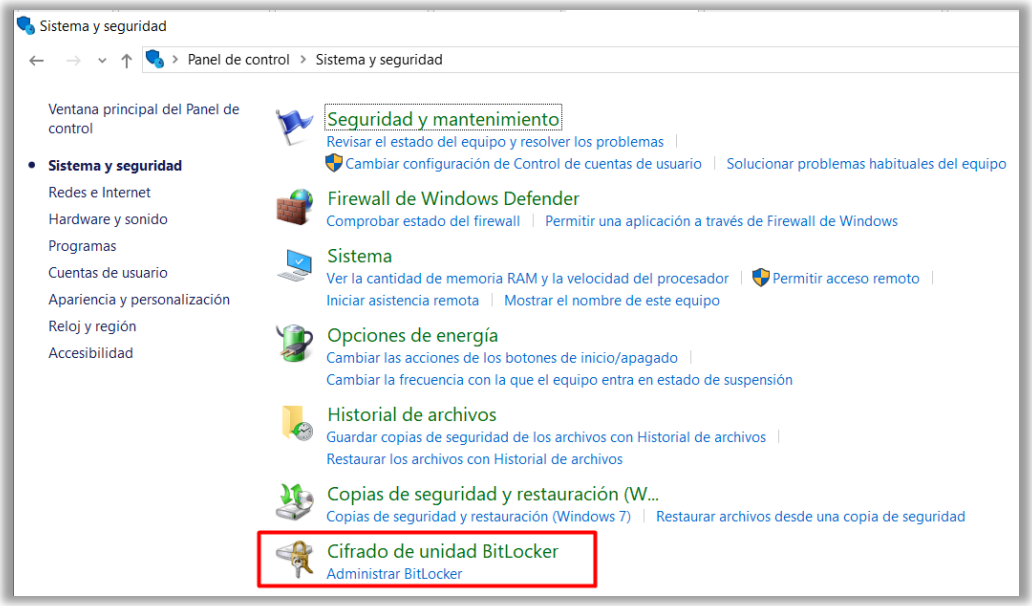
7-A continuación habilitamos la segunda.



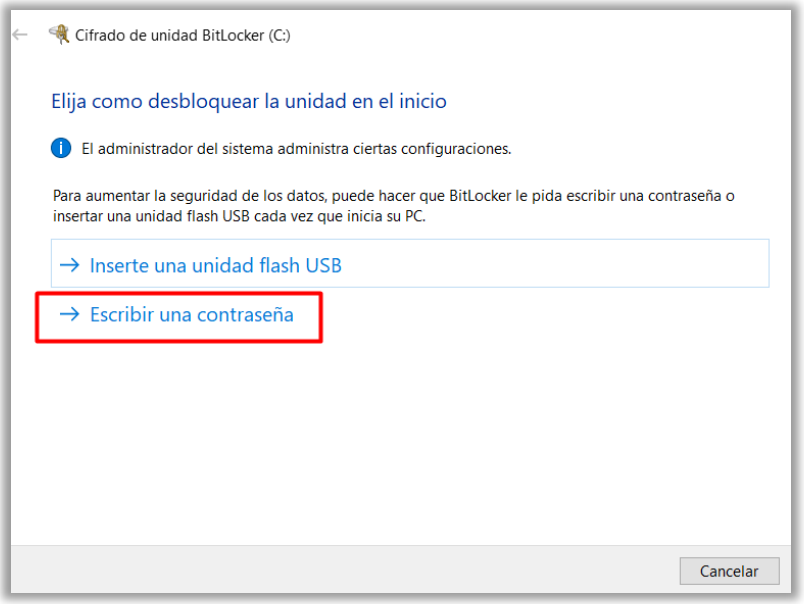
8-A continuación, aplicamos la GPO en las unidades organizativas de las computadoras que queramos cifrar por BitLocker.



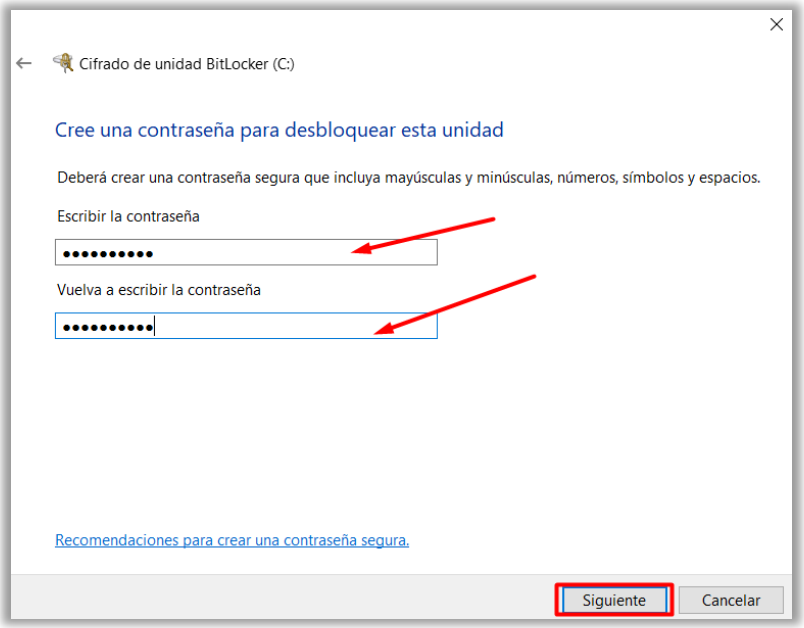
9-Nos dirigimos a una de las máquinas que vayamos a cifrar con BitLocker.



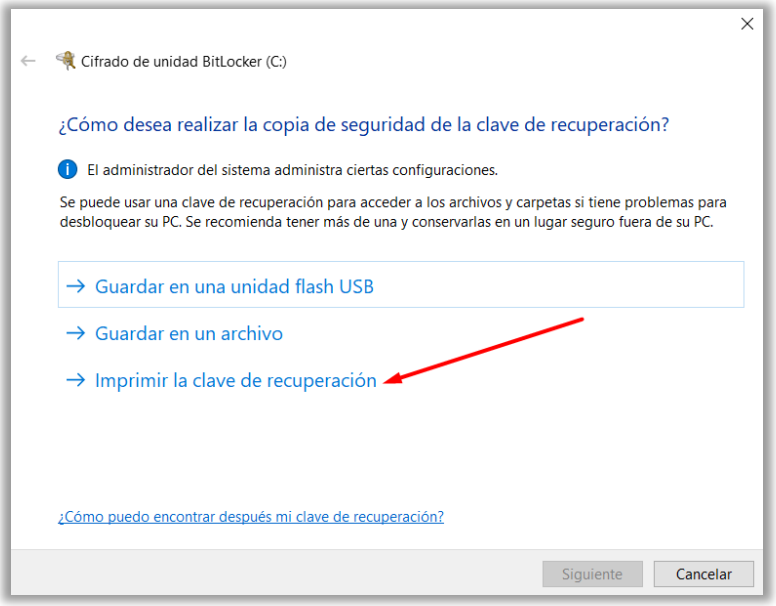
10-Estas opciones que se ven a continuación, se presentan gracias a la GPO y por marca la el Check Box que dice Allow BitLocker without compatible TPM. De no a ver configurado este Check Box en la GPO, no se nos desplegarían estas opciones y nos daría un mensaje de error si la computadora, ya que nuestra computadora no tiene un chip TPM y la única forma que tenemos de configurarlo es por Contraseña o mediante un USB. Elegimos la opción Escribir contraseña, para establecerle una contraseña.



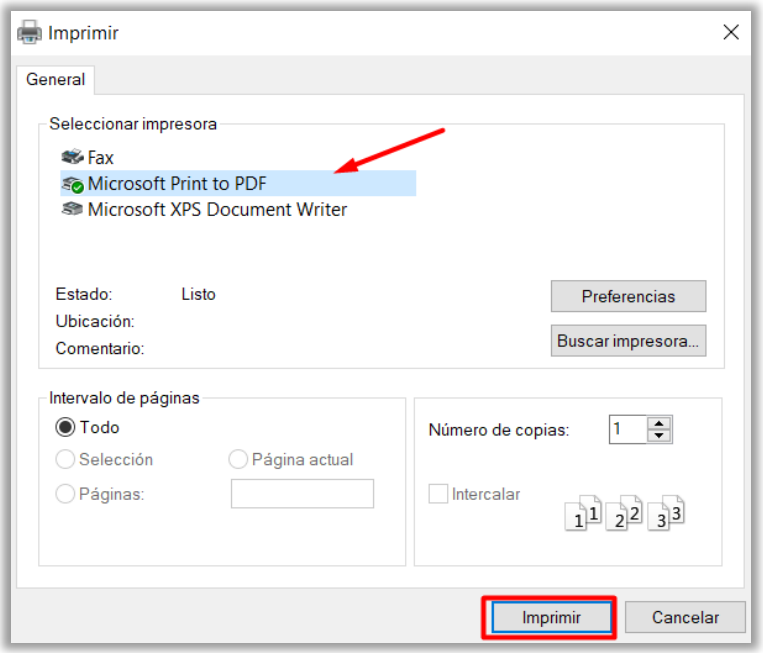
11-Indicamos la contraseña y siguiente.



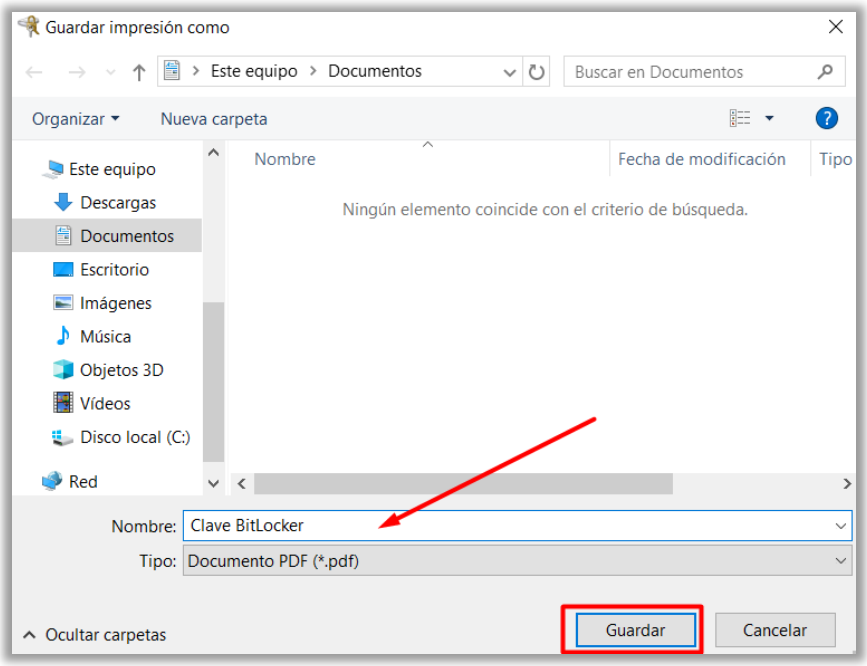
12-A continuación, seleccionamos la opción Imprimir la clave de Recuperación.



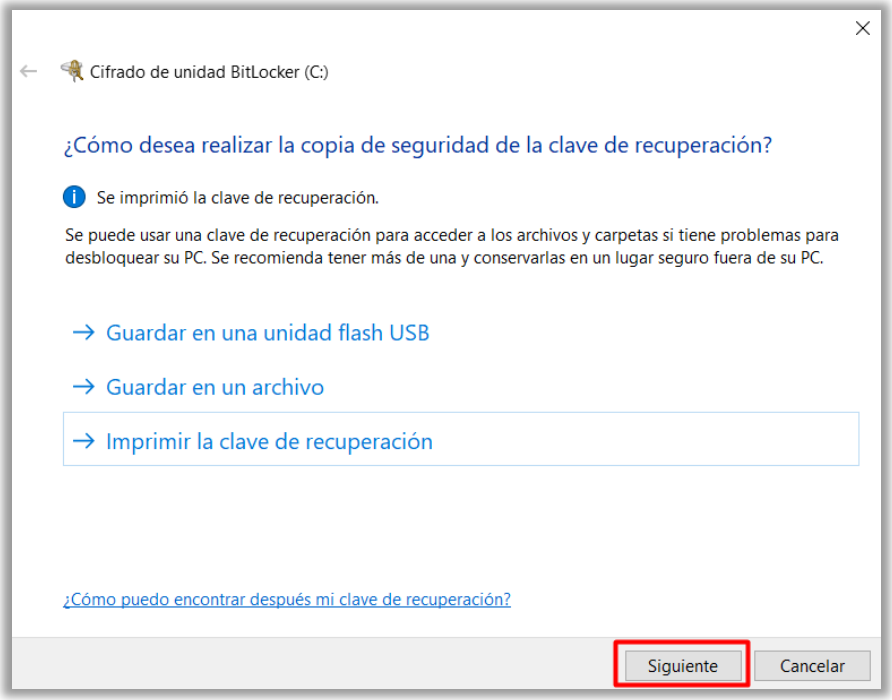
13-Seleccionamos con que impresora imprimir la clave.



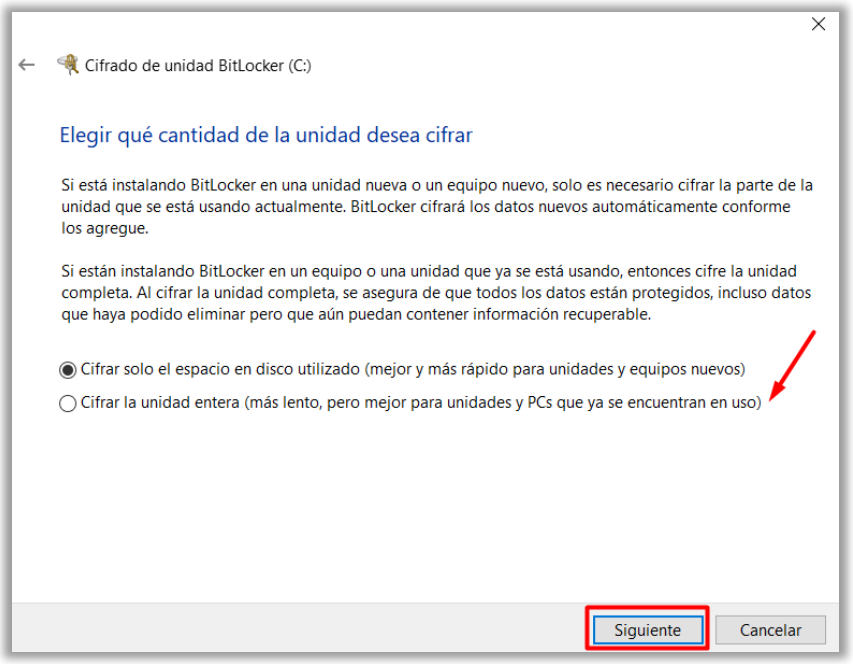
14-Le establecemos un nombre al PDF donde se almacenará la clave de recuperación y guardamos.



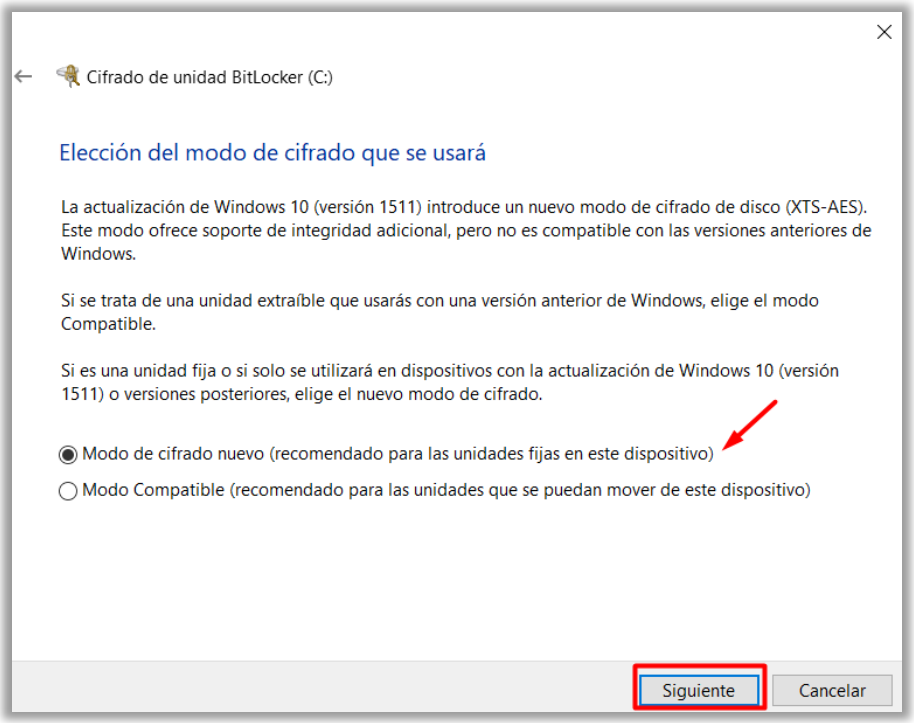
15-Hacemos clic en Siguiente para continuar.



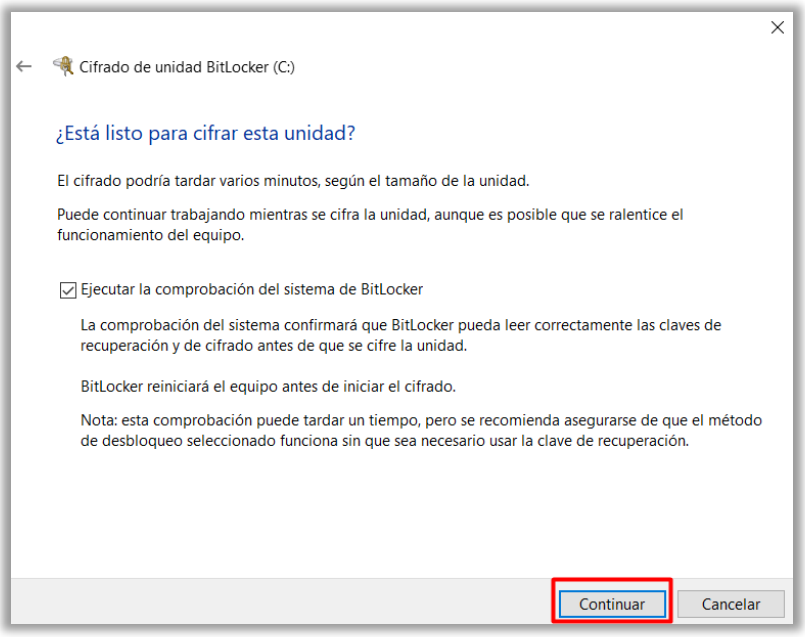
16-Podemos elegir la opción que deseemos, yo solo voy a cifrar el espacio en disco que se esta utilizando y clic en Siguiente.



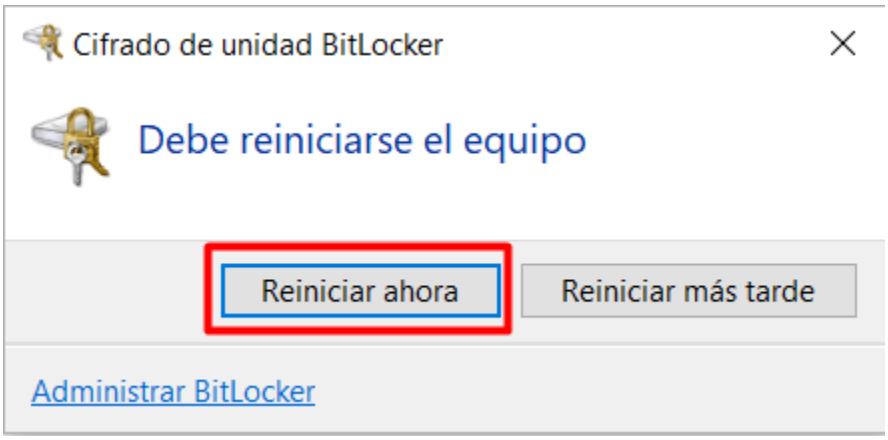
17-Como la versión de Windows que estoy usando en el cliente es reciente, marco la primera opción y clic en Siguiente para continuar.



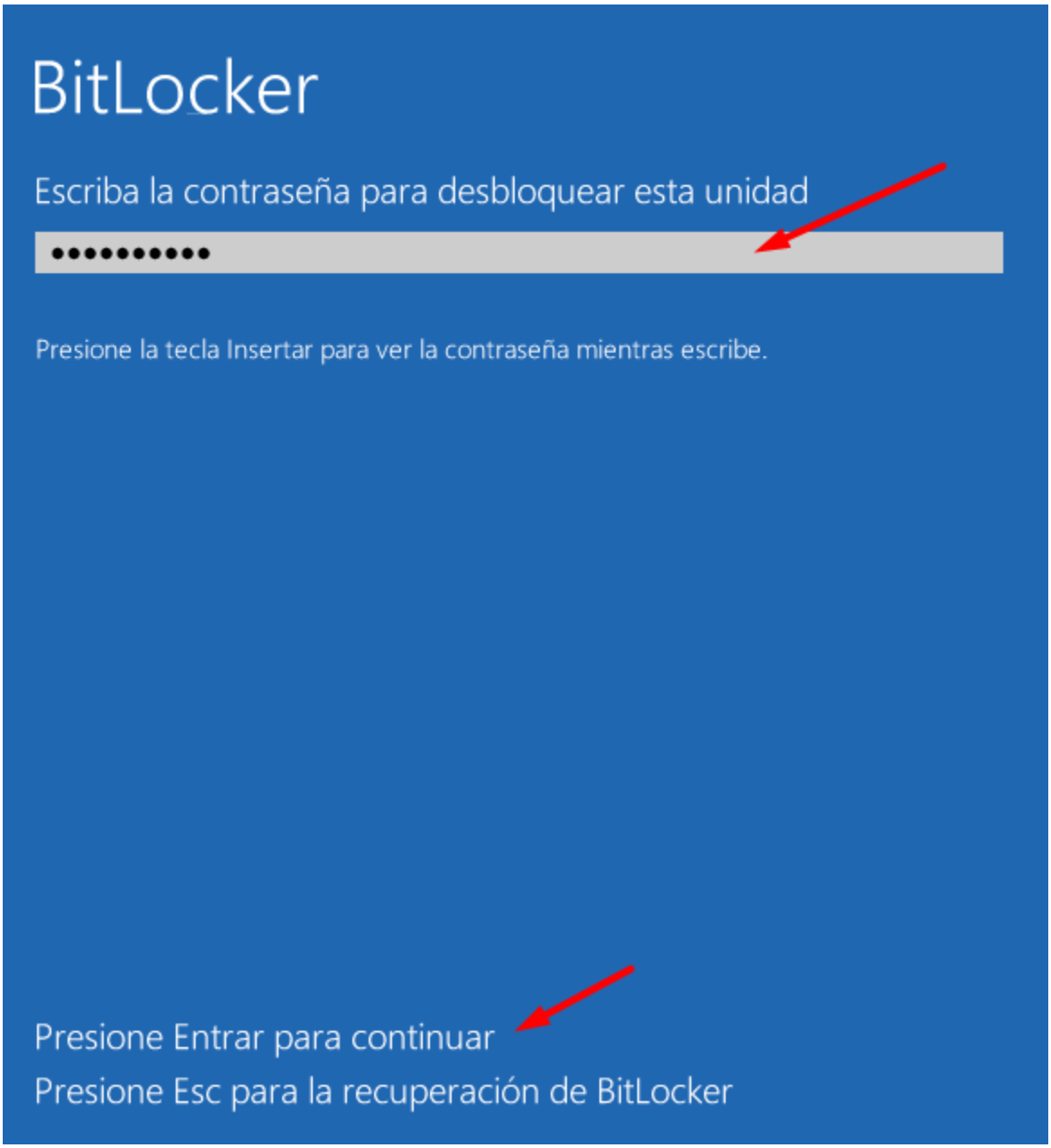
18-Ejecutamos la comprobación del Sistema para que BitLocker haga unas verificaciones y hacemos clic en Continuar.



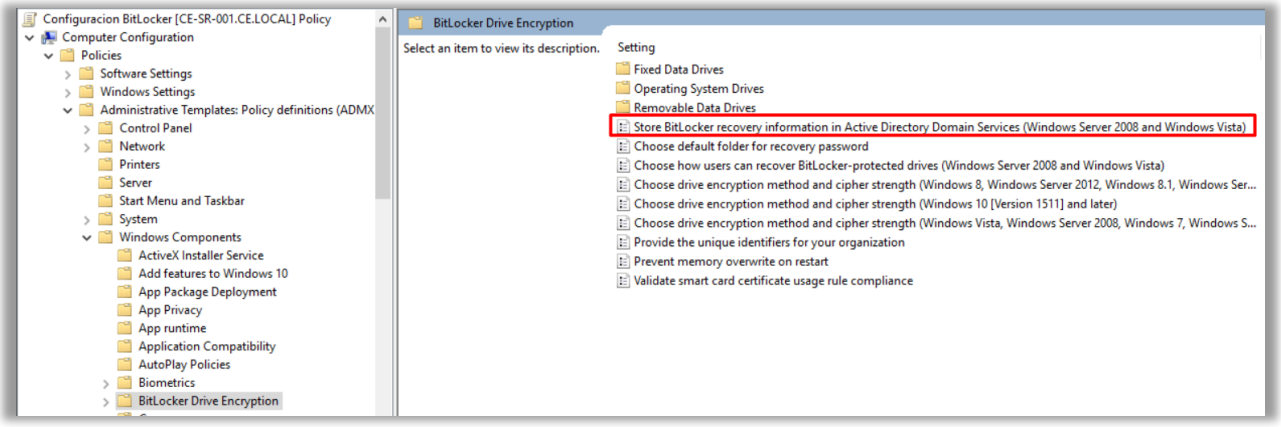
19-Hacemos clic en Reiniciar ahora, para que cuando vuelva a subir la máquina se empiece a cifrar.



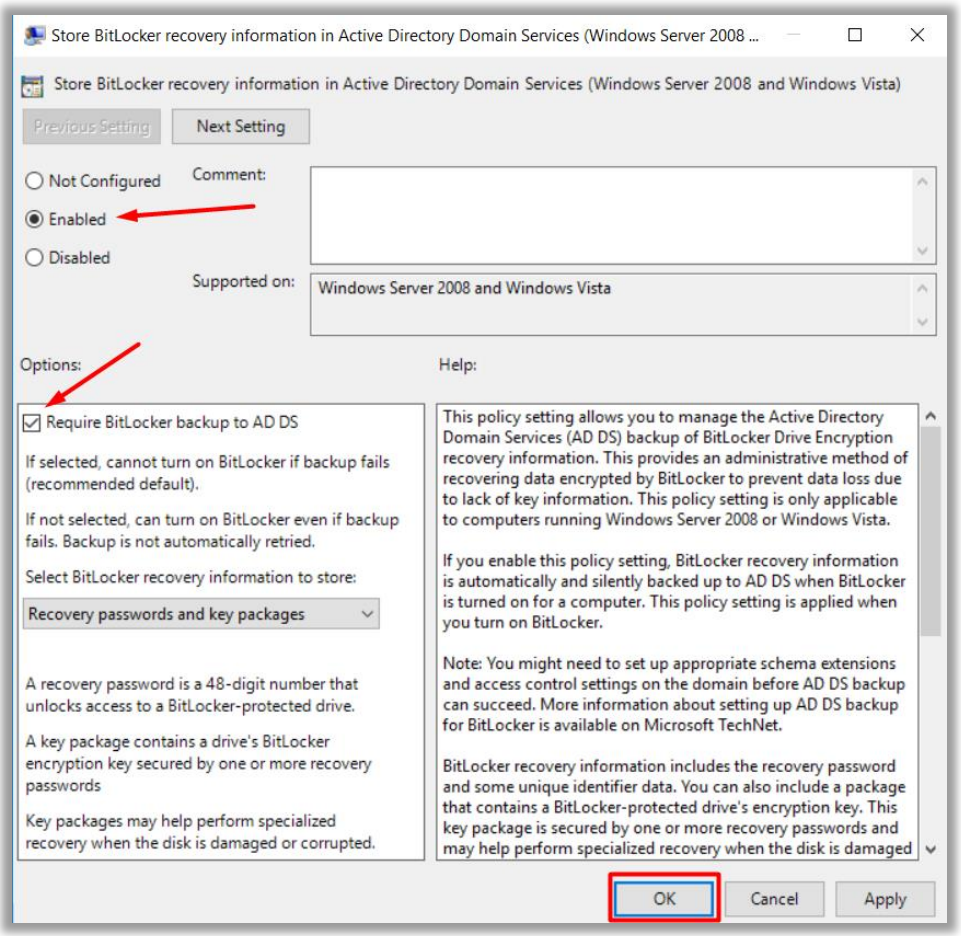
20-Como podemos ver, el cifrado se aplicó correctamente. Tener en cuenta que el cliente de BitLocker que estamos utilizando es en Windows 10. Luego de escribir la contraseña, presionamos Enter. Ya eso sería todo para la parte del cifrado. La siguiente parte, es Almacenar la clave en AD.



21-A continuación, modificaremos la política de seguridad que creamos anteriormente, para que la clave de recuperación de BitLocker se almacene en Active Directory.



22-Habilitamos, si se fijan el Check Box esta seleccionado, lo dejamos marcado y hacemos clic en OK para guardar, y amigos, eso sería todo.



Conclusión

En este proceso, hicimos la instalación de la característica de BitLocker Drive Encryption mediante Power Shell, creamos una política para desplegarla a los equipos miembros del dominio, esta política nos sirvió para que las máquinas que no tienen un chip TPM, se le pudiera configurar BitLocker por medio de una contraseña o mediante USB.

Luego, nos dirigimos a la máquina cliente, y en el panel de control entramos en Seguridad y Sistemas, y clic en Administrar BitLocker, esta máquina cliente la ciframos con una contraseña, y por último, modificamos la GPO que habíamos creado anteriormente para almacenará las claves de recuperación de BitLocker en Active Directory.

Enlaces

Aquí les dejo la información de donde saque la teoría y el link de mis plataformas digitales:

Prepara tu organización para BitLocker: planificación y directivas,

https://docs.microsoft.com/es-es/windows/security/information-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies

Moisés Sepúveda:

You Tube,

https://www.youtube.com/channel/UC4B67VEPdN461CyfAA1aTiw

Linkedin,

https://www.linkedin.com/in/mois%C3%A9s-sepulveda-847867183/

GitHub,

https://github.com/Moises-Sepulveda

Cybersecurity Expert IG,

https://www.instagram.com/csecurity_expert/