Presentación

- **Nombre del estudiante:** Jamiel Santana.
- **Matricula:** 2019-8095
- Nombre del profesor: Geancarlos Sosa
- **Mat:** Seguridad de SO.
- Tema: Bitlocker
- **Centro Educativo:** Instituto tecnológico de las Américas.

Microsoft®
BitLocker®

Temas a tratar:

a. Crear una GPO para desplegar bitlocker y habilitar encriptación del disco C.

b. Configurar desbloqueo por PIN.

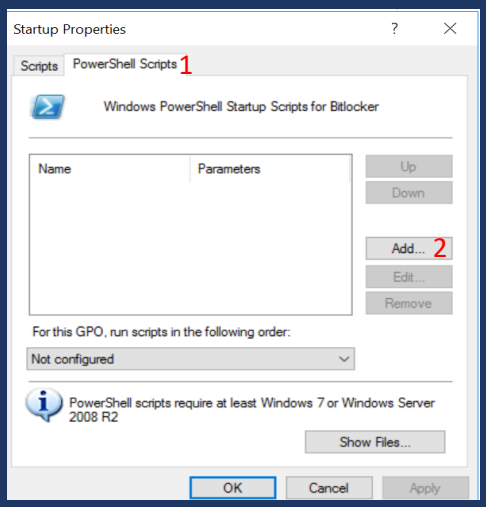
c. Habilitar que se guarden las contraseñas de los clientes encriptados en Active Directory.

A. Crear una GPO para desplegar bitlocker y habilitar encriptación del disco C.

- Debemos tener en cuenta, que para realizar todas las configuraciones debemos tener instalado bitlocker en nuestro servidor.
- Para poder desplegar bitlocker en máquinas clientes, siempre y cuándo dicha máquina se encuentre conectada a nuestro domino, lo que haremos es crear una **GPO** de tipo **logon script**, donde el script contendrá la habilitación automática de **bitlocker** sin la intervención de un usuario, para lograr esto crearemos un script en powershell, con **powershell ise,** el script quedará de la siguiente manera y lo guardaremos en formato ps1.

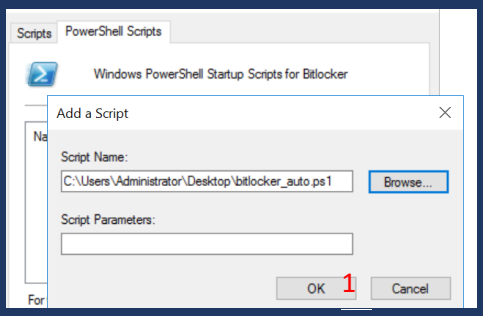
```
bitlocker_auto.ps1*
1  $SecureString = ConvertTo-SecureString '123456' -AsPlainText -Force
2  Enable-BitLocker -MountPoint 'C:' -EncryptionMethod Aes256 -UsedSpaceOnly -Pin $SecureString -TPMandPinProtector
```

- Luego de esto nos dirigimos a **Group policy management**, nos dirigimos a nuestra OU, y procedemos a crear nuestra GPO, una vez creada nuestra GPO procedemos a editarla, donde se nos abrirá el GROUP POLICY MANAGEMENT EDITOR, y nos dirigimos a la siguiente ruta, **/Windows settings/scripts, y** escogeremos la opción de startup, donde se nos abrirá una ventana como esta.

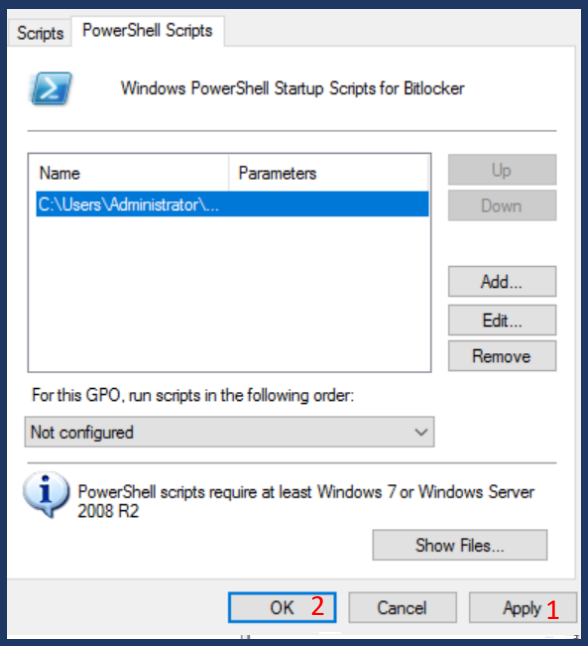


Microsoft® BitLocker

- Ya marcado add se nos abrirá una ventana donde tenemos que buscar y seleccionar nuestro script powerhsell. Escogido nuestro archivo damos a **ok.**



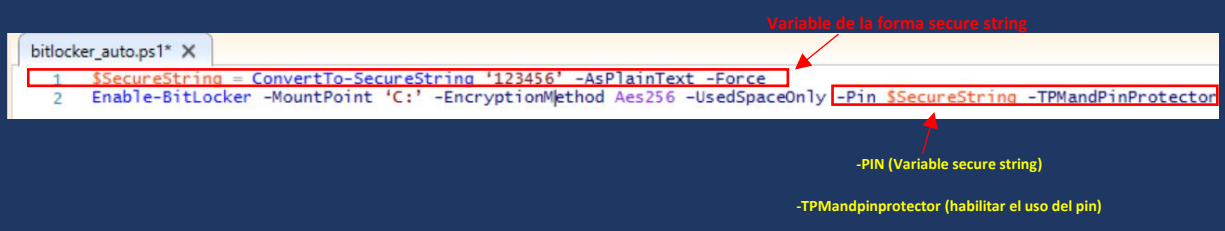
- Después en la ventana de startup properties damos a apply y luego a ok.



- Realizado todo esto tendremos todo listo para cuando cualquier pc se una al dominio automáticamente.

B. Configurar desbloqueo por PIN:

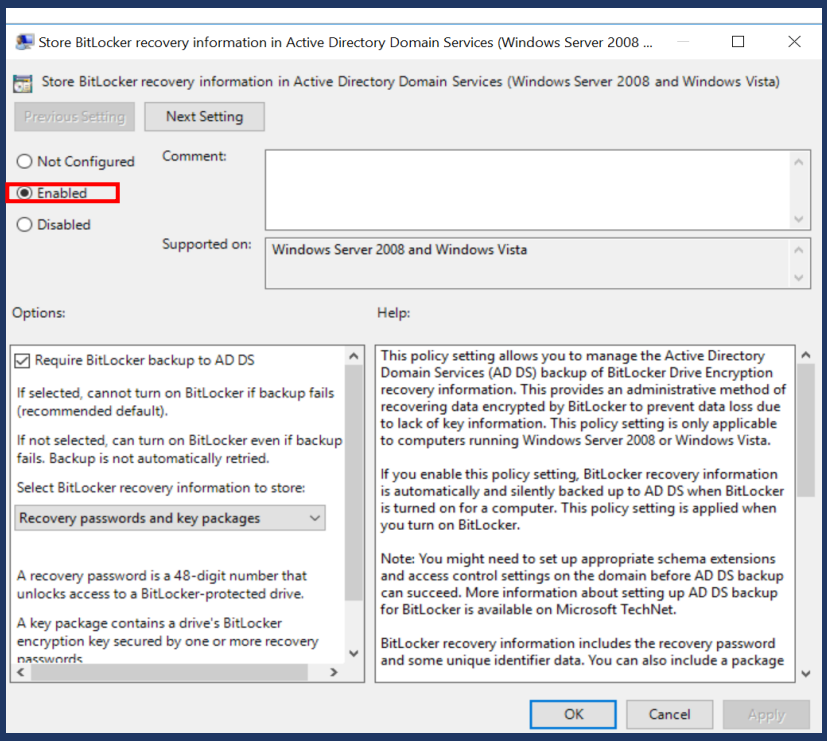
- Esto se configura dentro del mismo script con los siguientes parámetros.



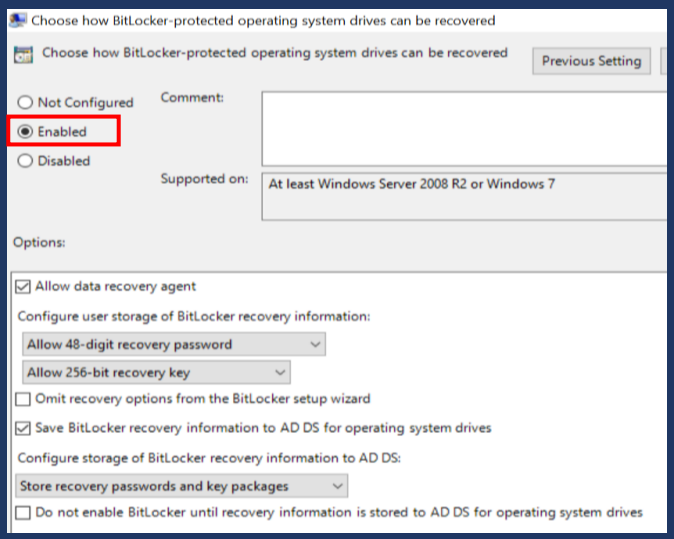
Microsoft BitLocker

C. Habilitar que se guarden las contraseñas de los clientes encriptados en Active Directory:

- Para poder habilitar que se guarden las key de recuperación en AD, tendremos que irnos a nuestra GPO creada y habilitar la directiva **storage bitlocker recoery information in Active Directory,** esta se encuentra en la ruta **/policies/Administrative Templates/Windows Component/Bitlocker drive encryption/. Dejaremos todo por default.**



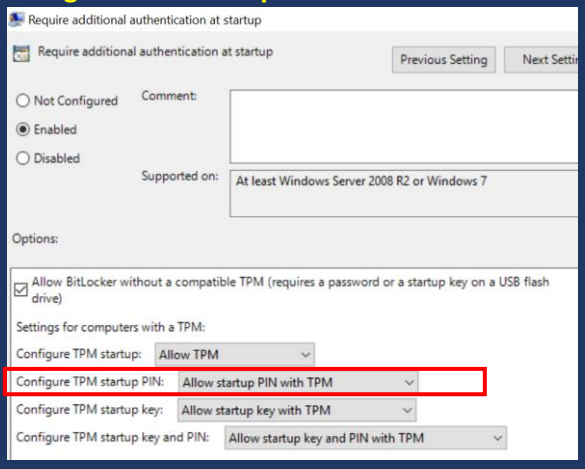
- Ahora nos vamos a dirigir a la ruta, **/policies/Administrative Templates/Windows Component/Bitlocker drive encryption/operating system drives,** y buscaremos la directiva llamada **choose how bitlocker-protected operatig system drives can be recovered,** donde la habilitaremos y dejaremos todo por defautl.



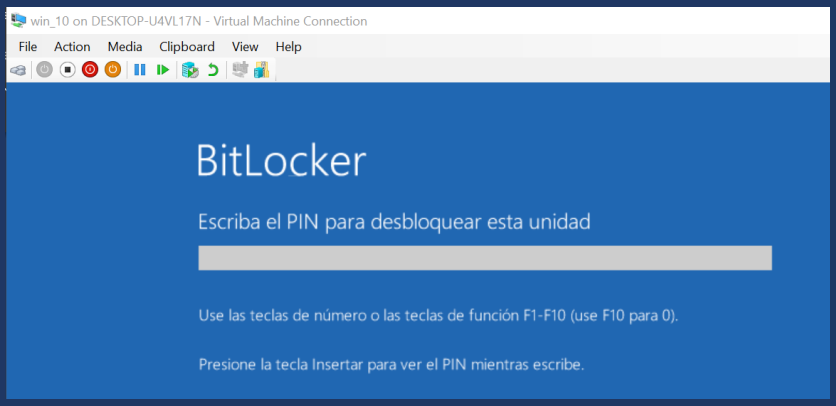
Microsoft® BitLocker®

- Y por último paso, pero no menos importante, habilitaremos la autentificación adicional, dado que si no la activamos el script ni el pin van a funcionar.

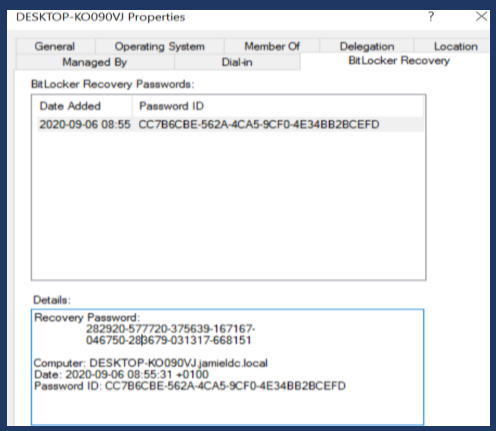
- Esta directiva se encuentra en la ruta **/policies/Administrative Templates/Windows Component/Bitlocker drive encryption/operating system drives,** nos fijamos que la opción **configure TPM startup PIN** este en **ALLOW STARTUP PIN WITH TPM.**



- Realizado todo esto damos por finalizada la configuración ahora vamos a probar que todo funcione a la perfección, conectaremos un equipo cliente al domino y veremos si la configuración ha funcionado.
- Vemos como al reinicar nuestro pc ya nos pide un pin para podes desbloquear el disco.



- Y si nos dirigimos a nuestro directorio activo y buscamos el pc cliente, le damos click derecho > propiedades > bitlocker recovery, vemos como ya se nos almacena la key en nuestro bitlocker.



Microsoft® BitLocker®