

Tareas administrativas en

Windows Server 2019

Índice:

1. [Compartir una impresora del dominio con los clientes](#)
 - a. [Ajustes en el servidor](#)
 - b. [Ajustes en el cliente](#)
2. [Copia de seguridad y recuperación](#)
 - a. [Formateo del nuevo disco](#)
3. [Copia de seguridad programada](#)
4. [Recuperación completa del sistema desde una copia de respaldo](#)
5. [Tareas programadas](#)
6. [Visor de eventos](#)

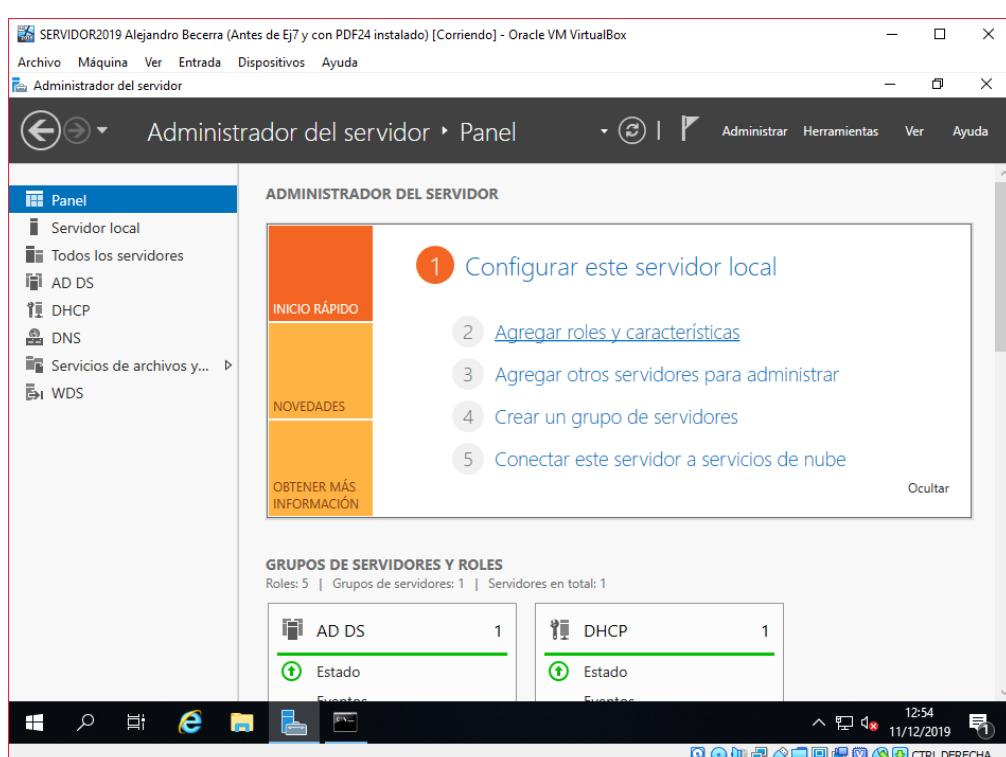
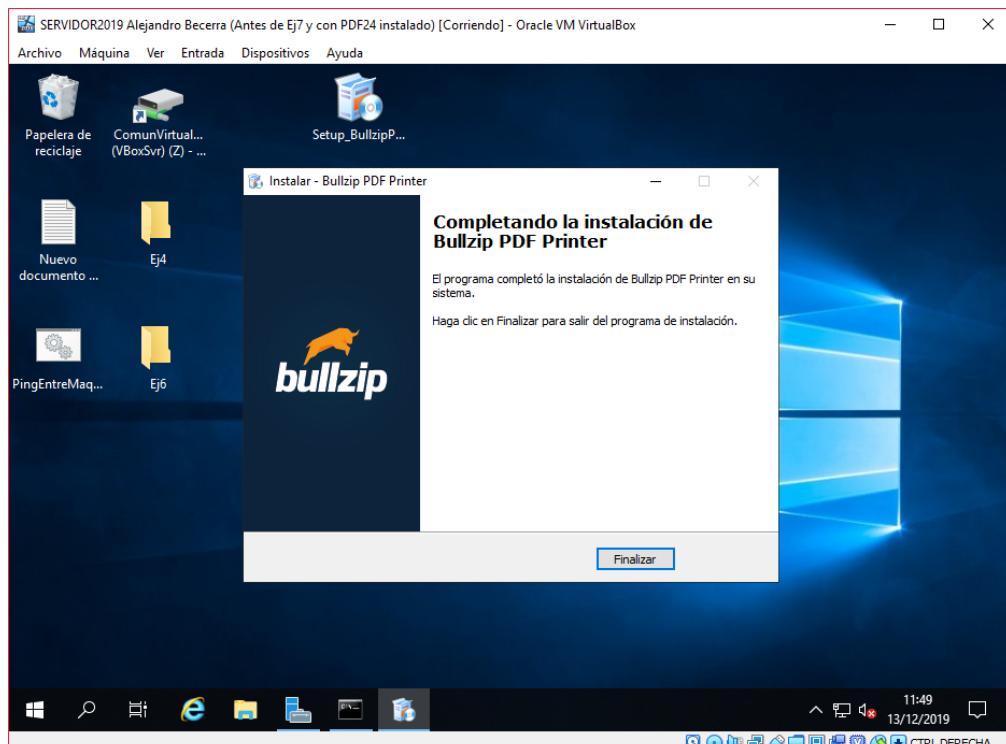
Compartir una impresora del dominio con los clientes

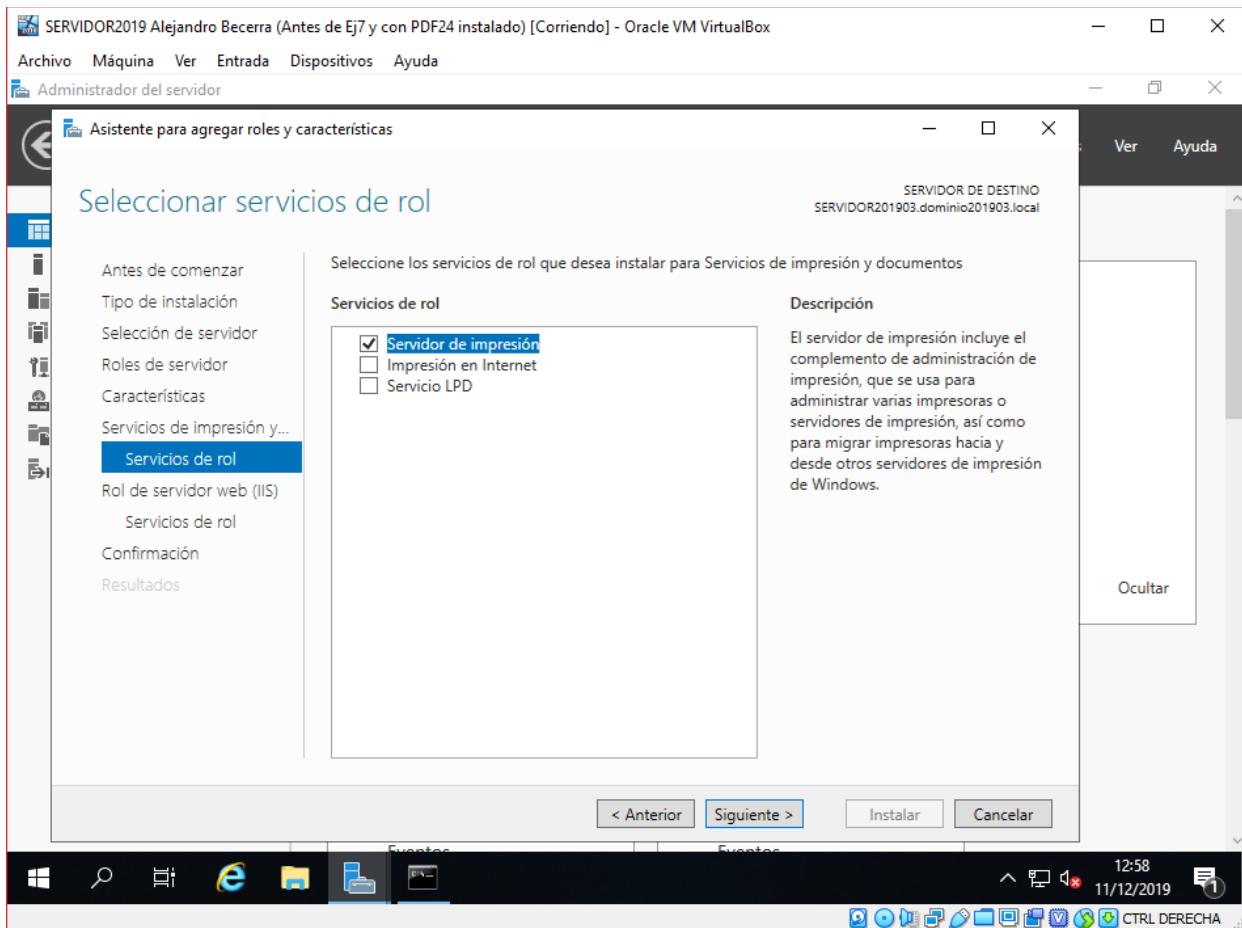
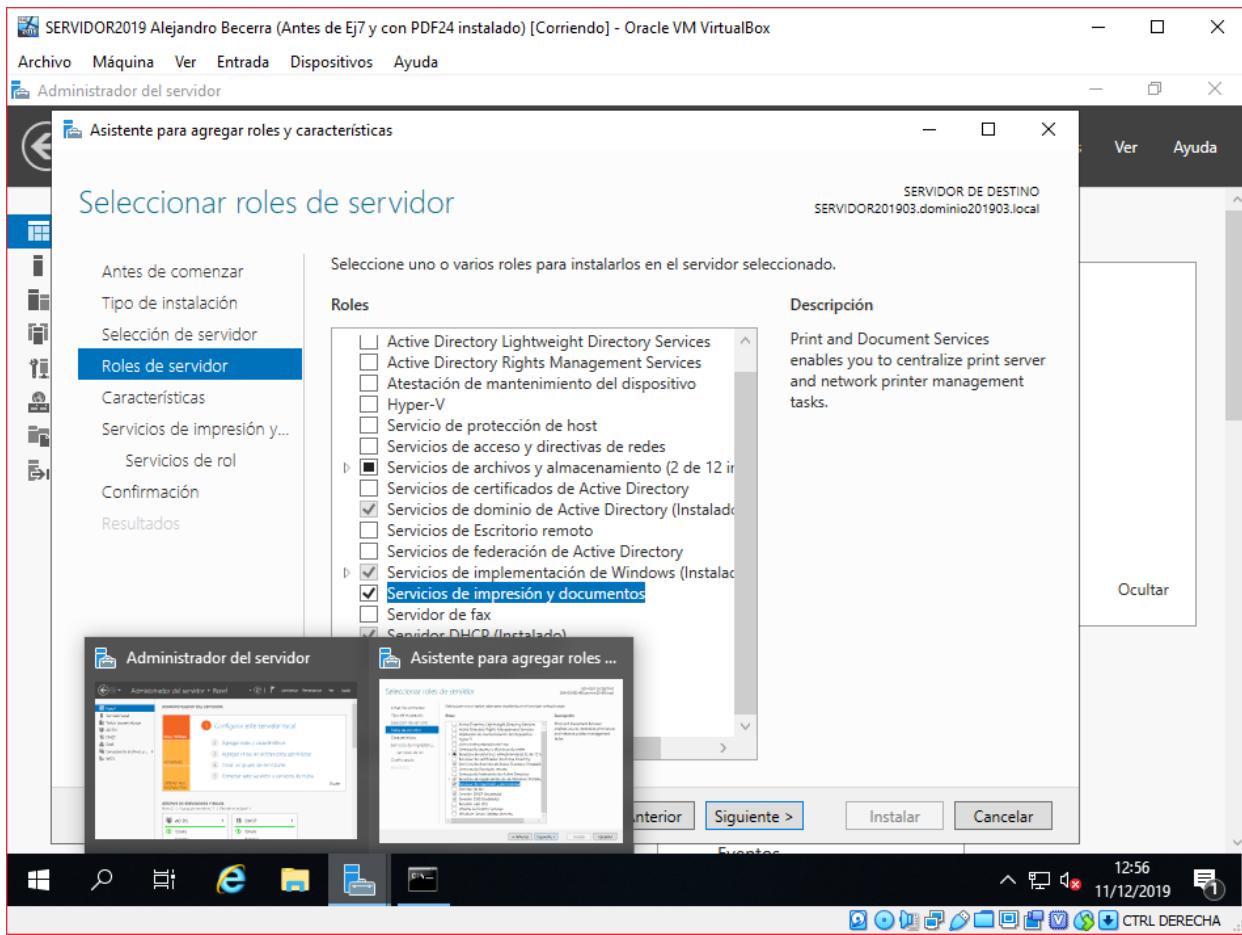
Ajustes en el servidor

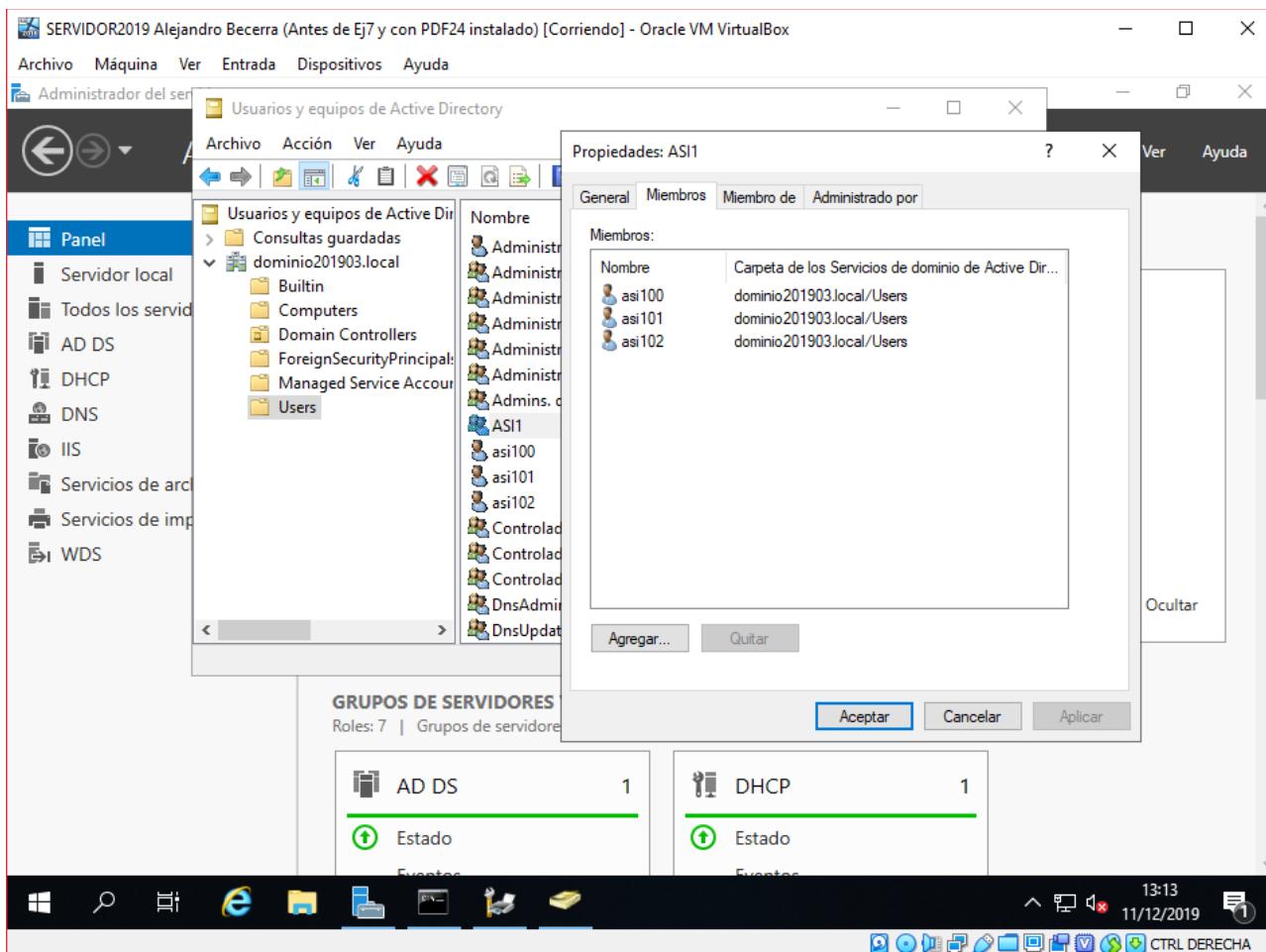
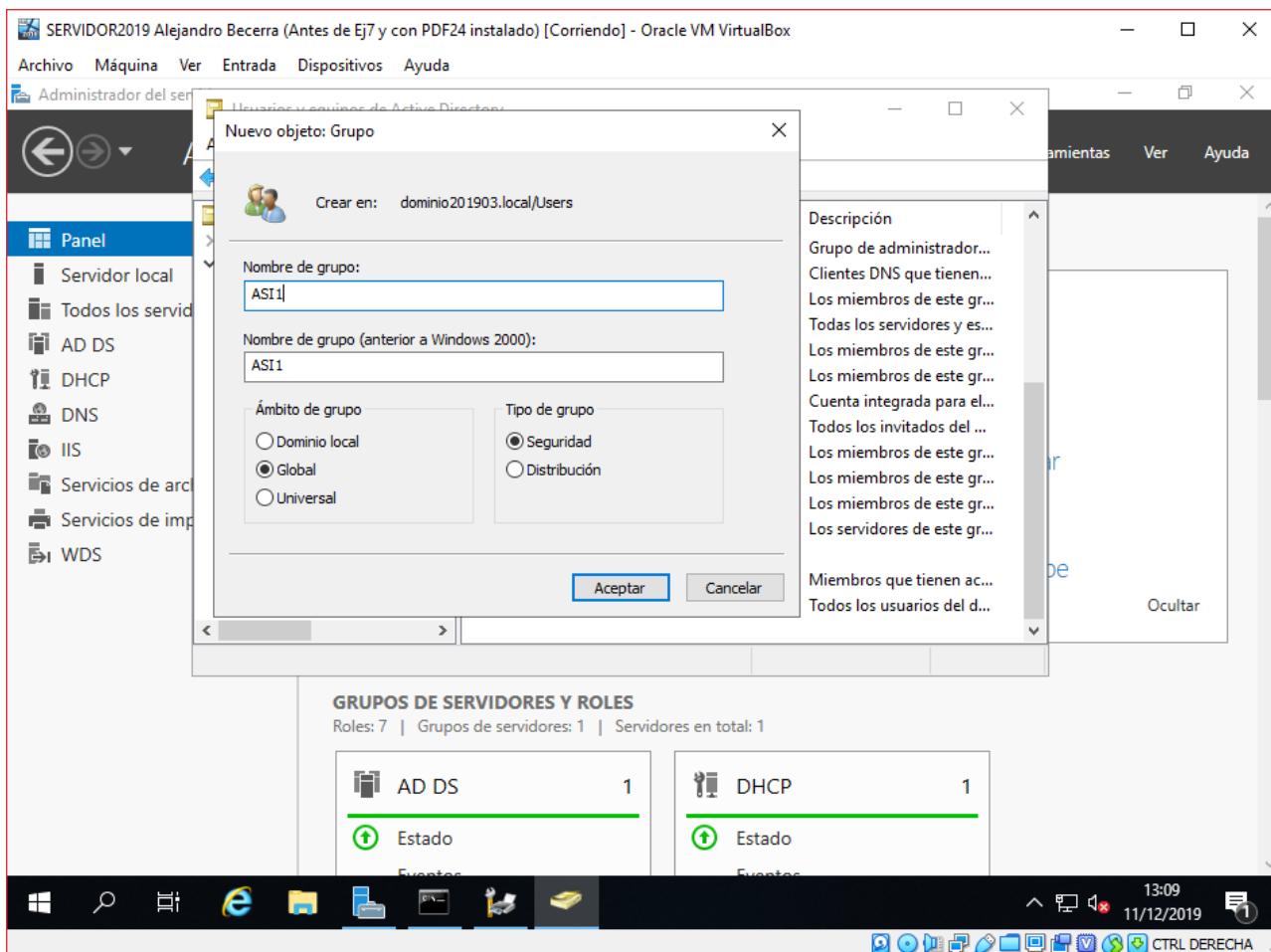
Este apartado de la práctica la haremos con una impresora virtual de PDF virtual, usaremos el “BullZIP”, una herramienta gratuita de terceros.

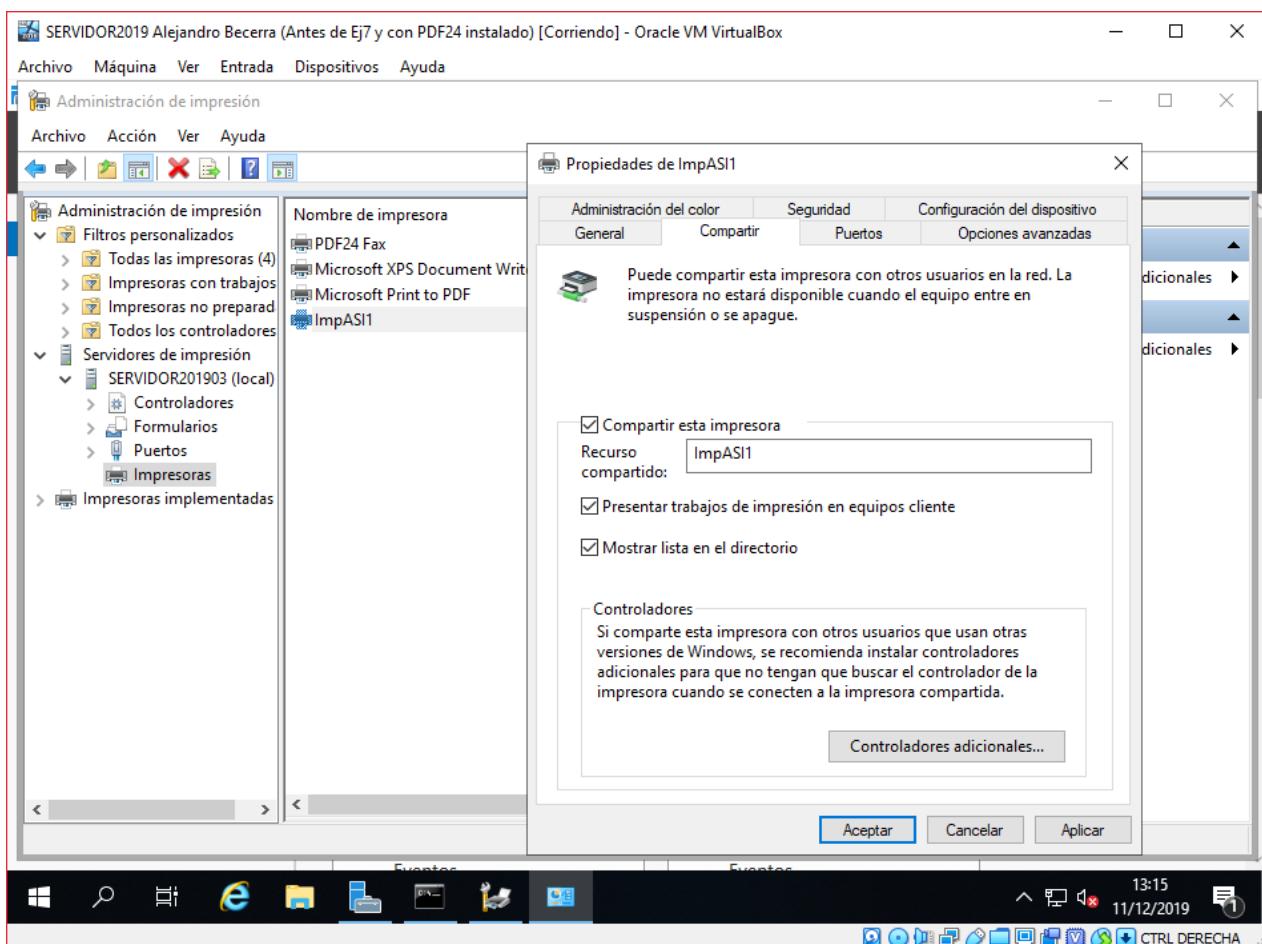
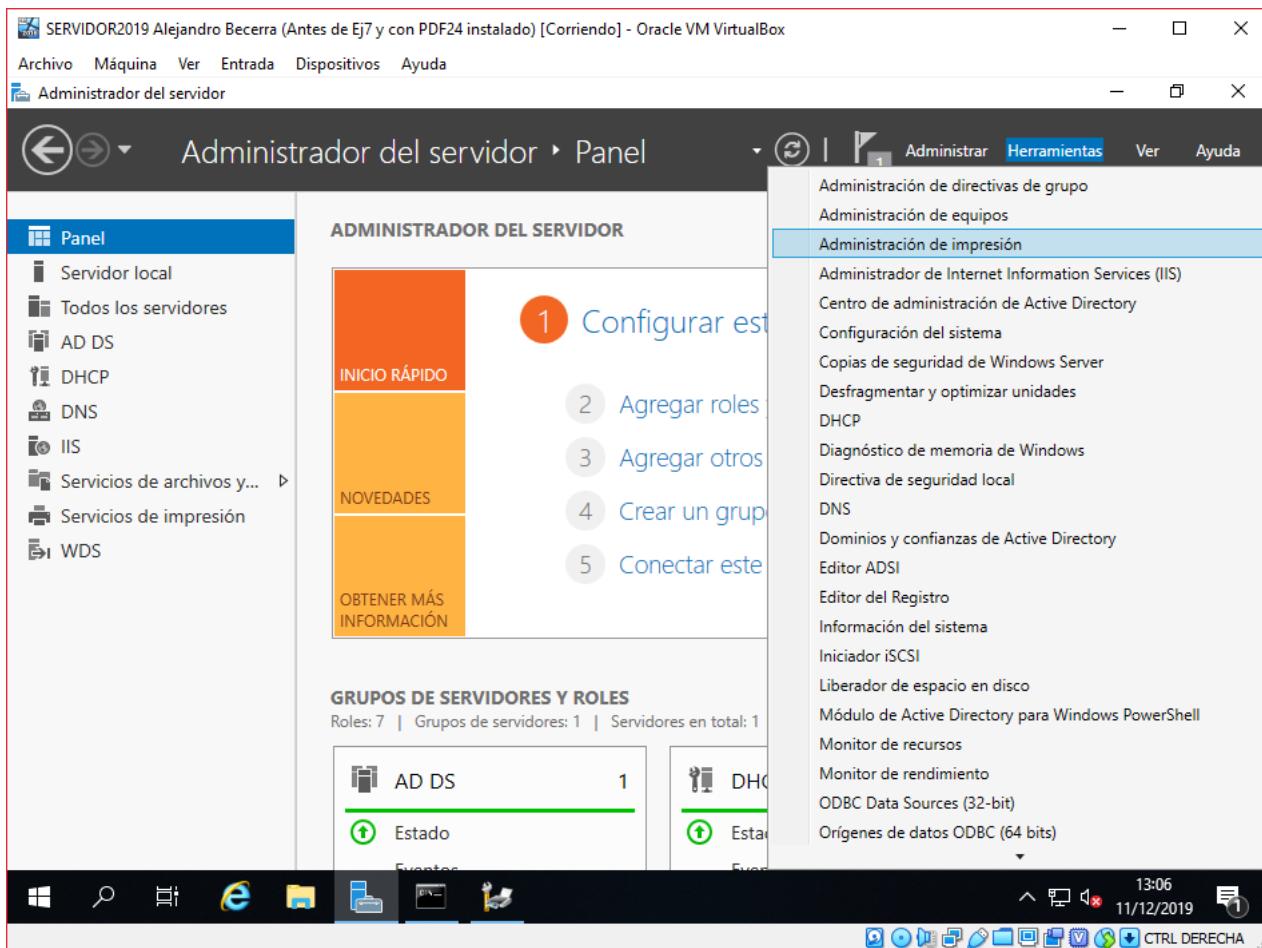
Comenzaremos instalando la impresora virtual y posteriormente en el “Administrador del servidor” agregaremos el rol de “Servicios de impresión y documentación”. A continuación, mientras se instala iremos a “Usuarios y equipos de Active Directory” para crear un grupo de usuarios que puedan usar la impresora del dominio, para ello crearemos un grupo llamado ASI1 y meteremos tres usuarios.

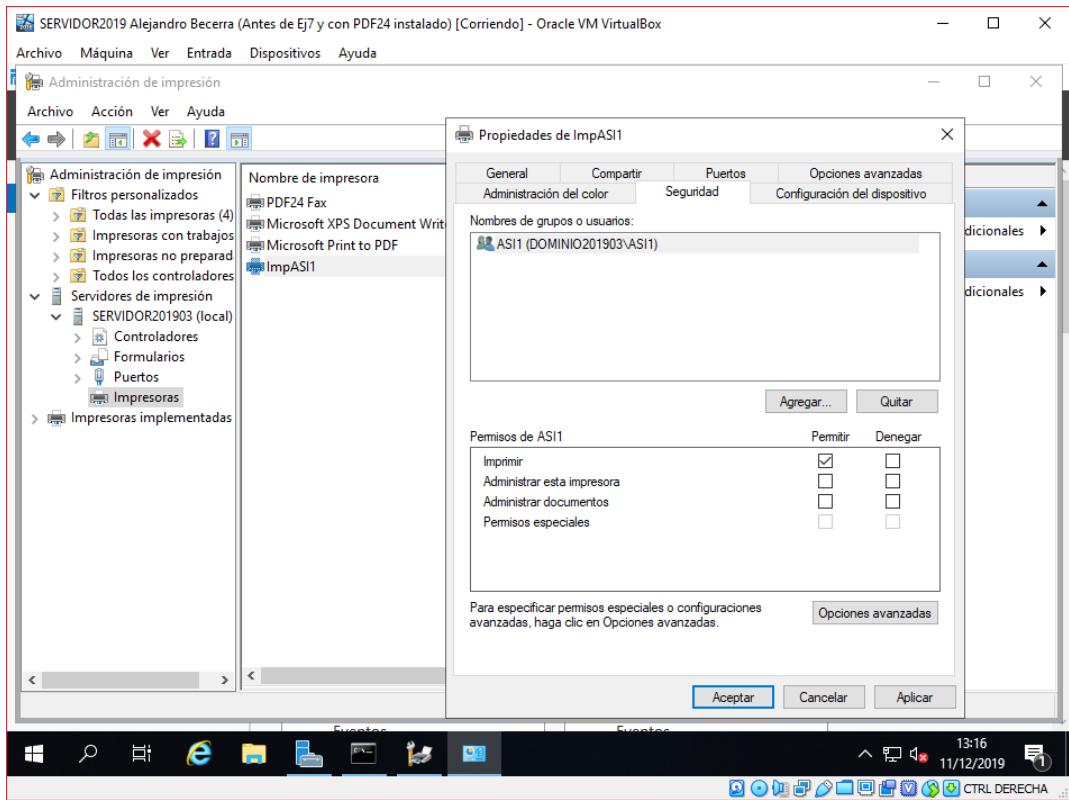
Finalmente, con el grupo creado y el rol instalado, cambiaremos el nombre a la impresora y lo compartiremos únicamente con el grupo que creamos.





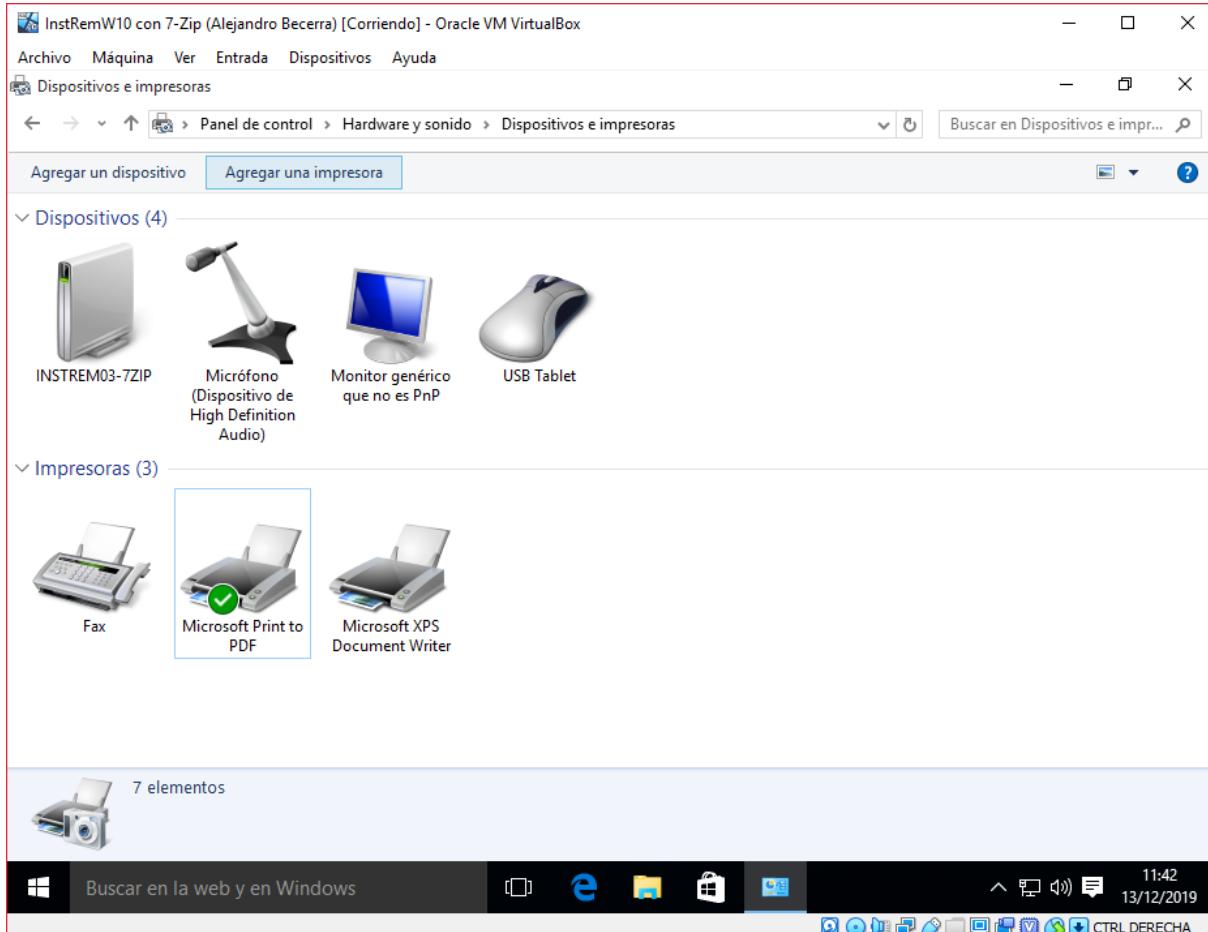


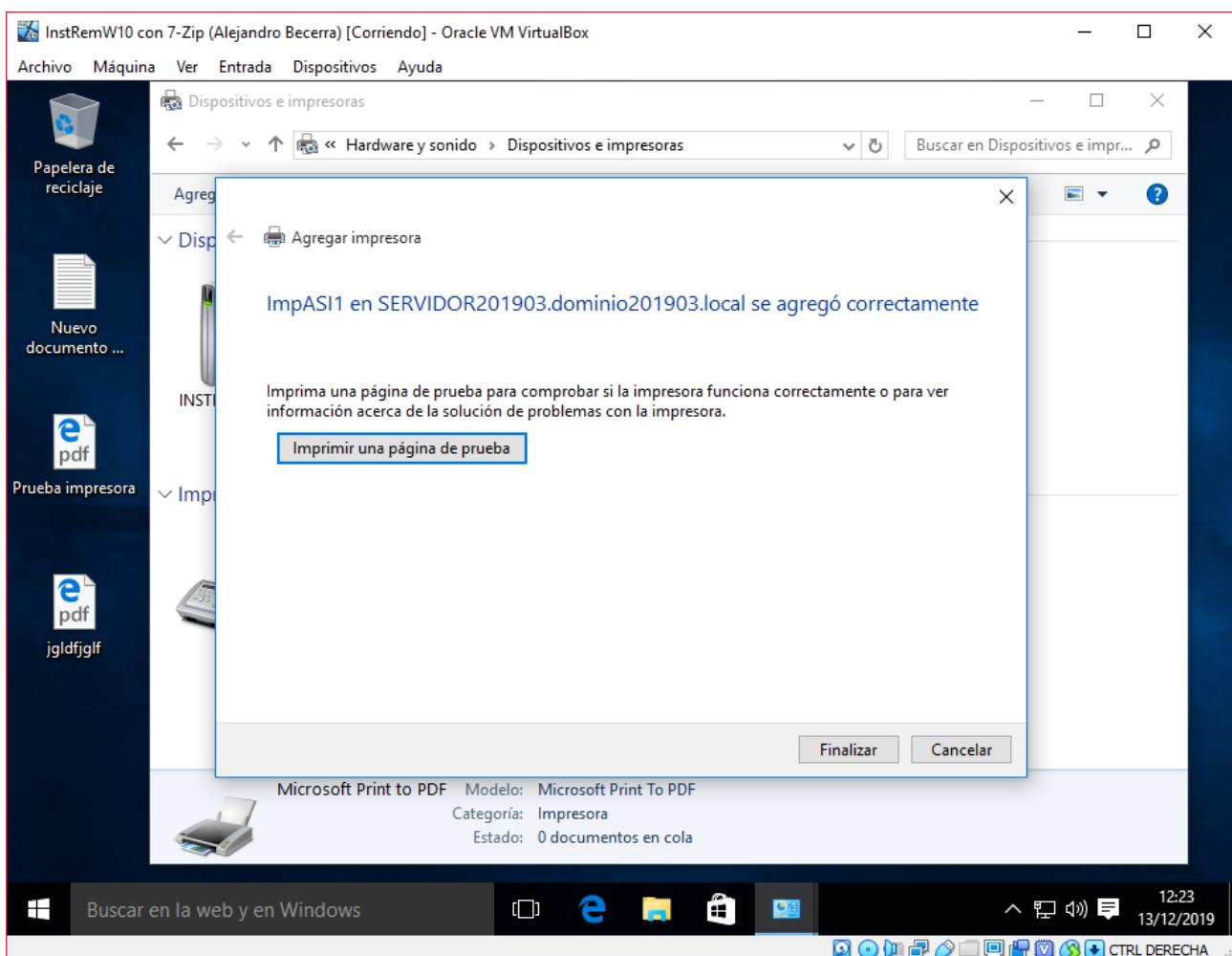
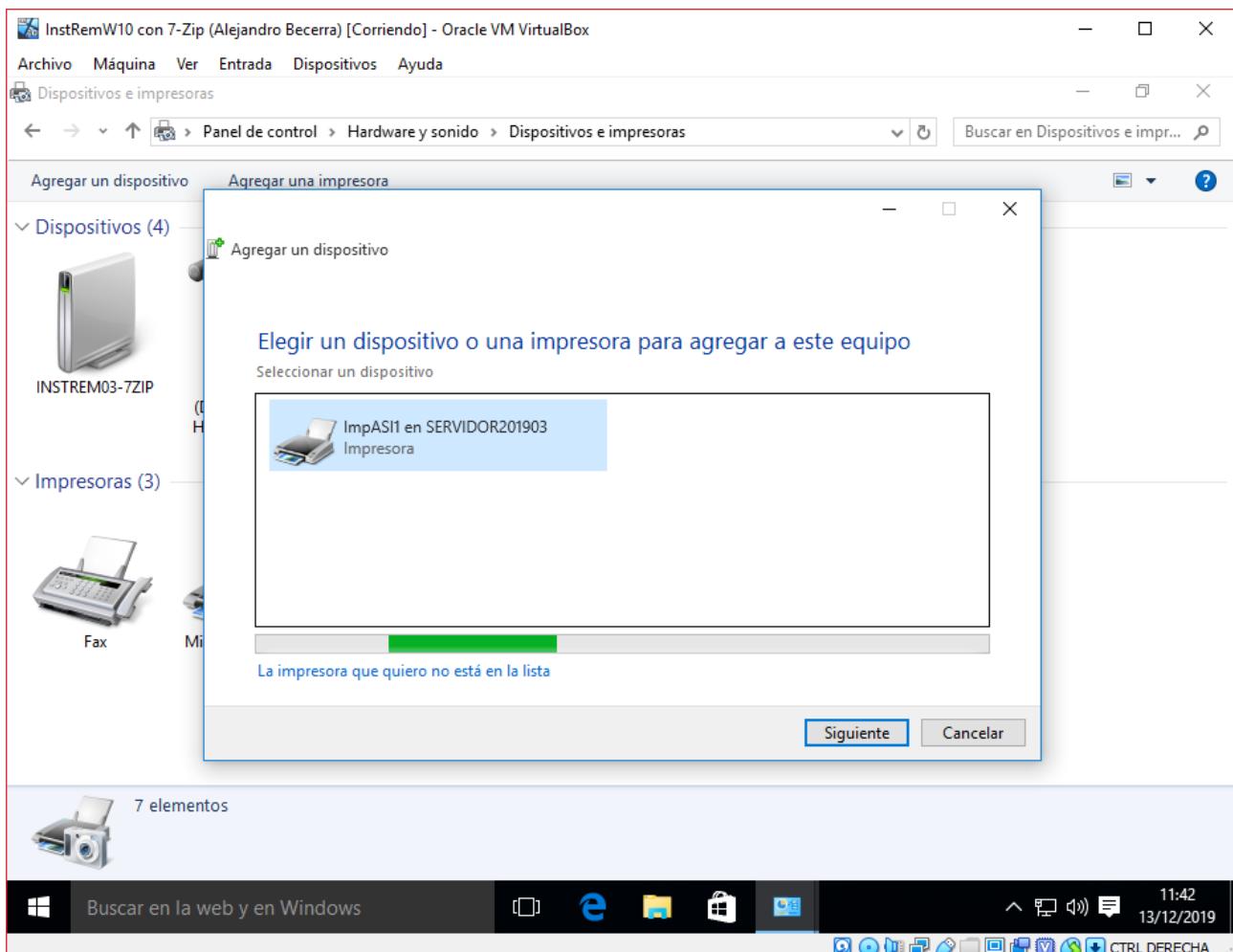


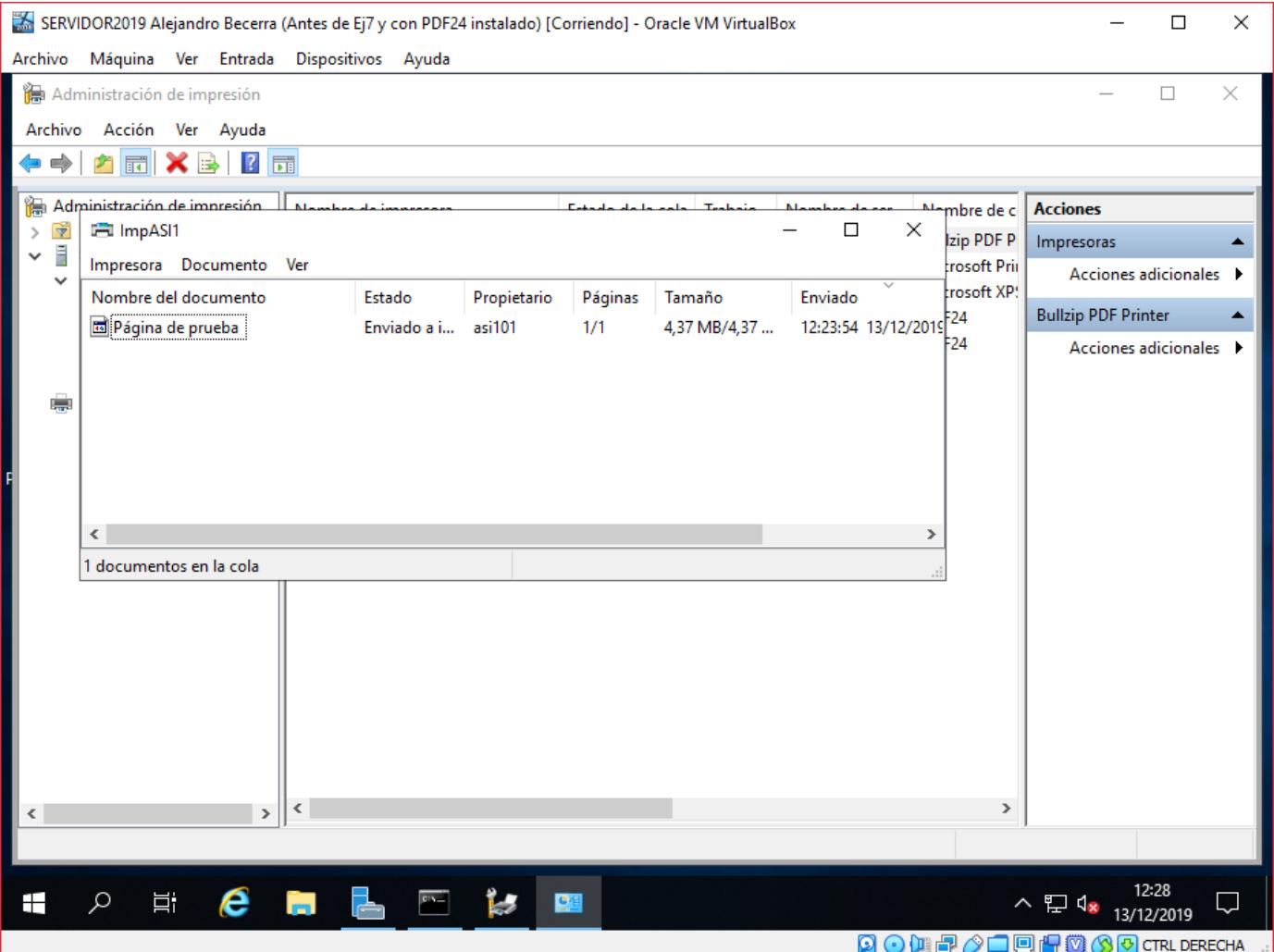


Ajustes en el cliente

Ahora después de los ajustes del servidor, los haremos en el cliente. Para ellos iremos al panel de control y en “Dispositivos e impresoras” agregaremos una impresora, seleccionaremos la que corresponde con este usuario e imprimiremos una página de prueba que podremos ver en el servidor.



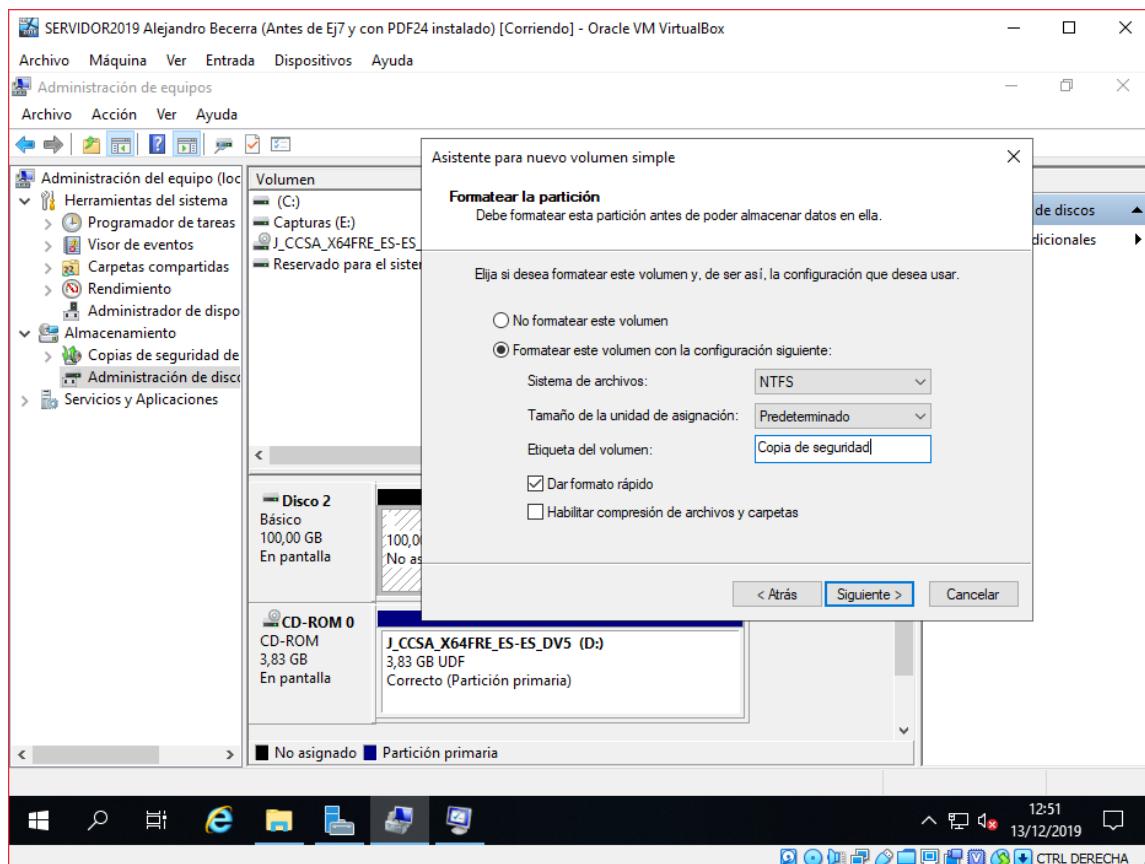
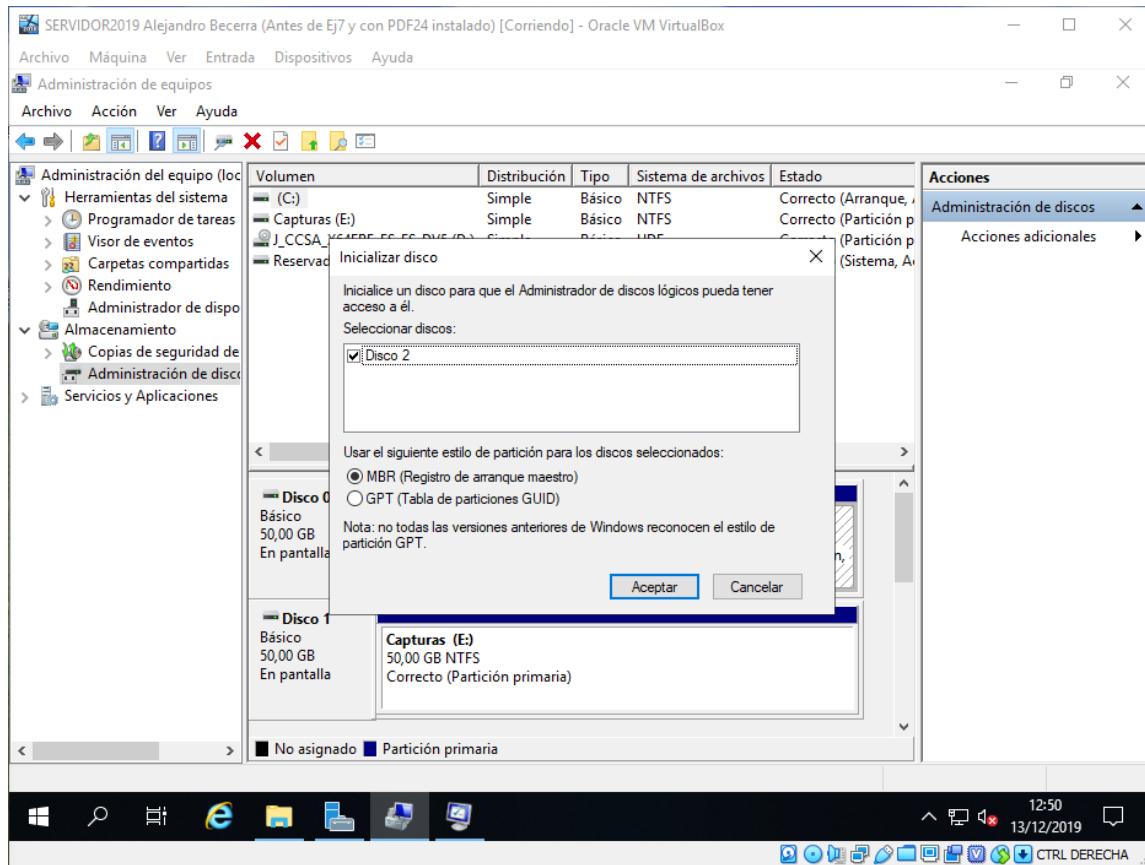


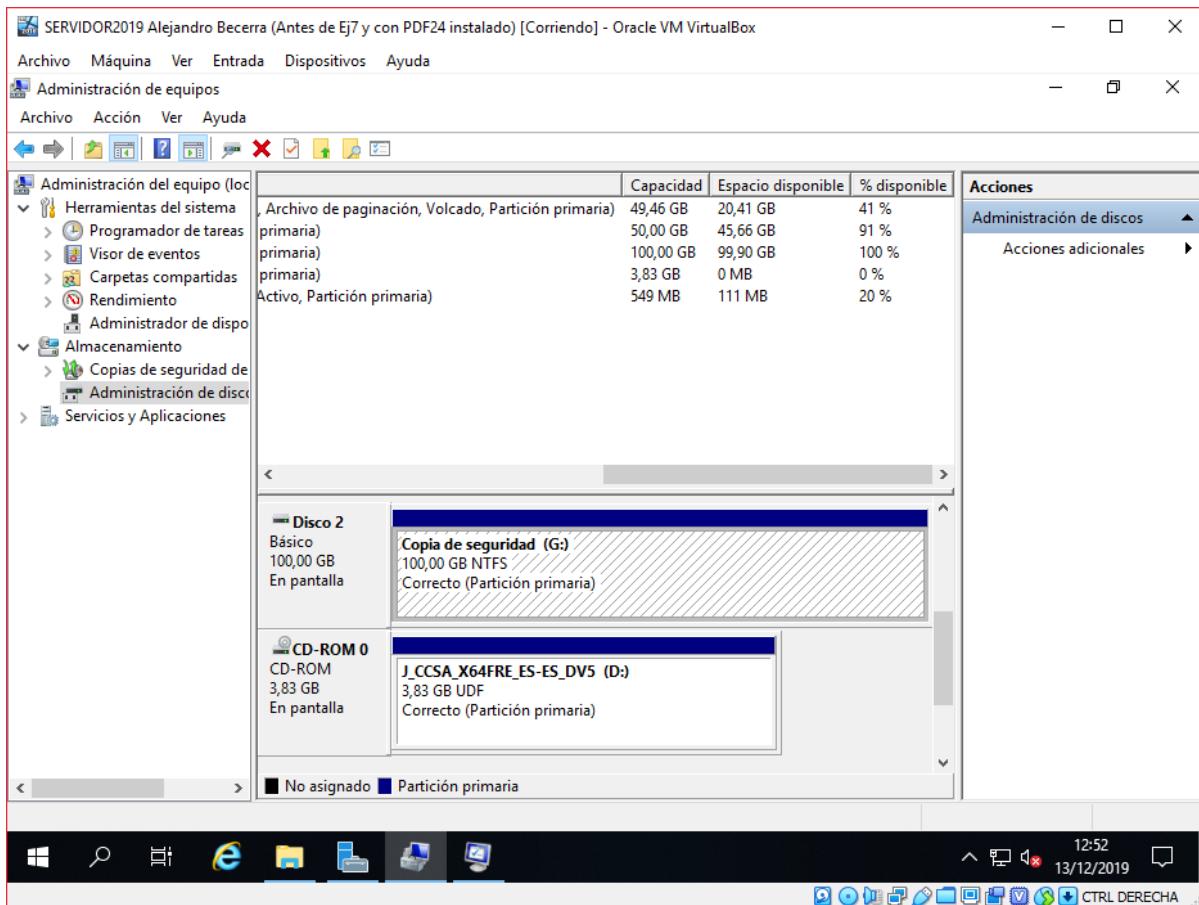


Copia de seguridad y recuperación

Formateo del nuevo disco

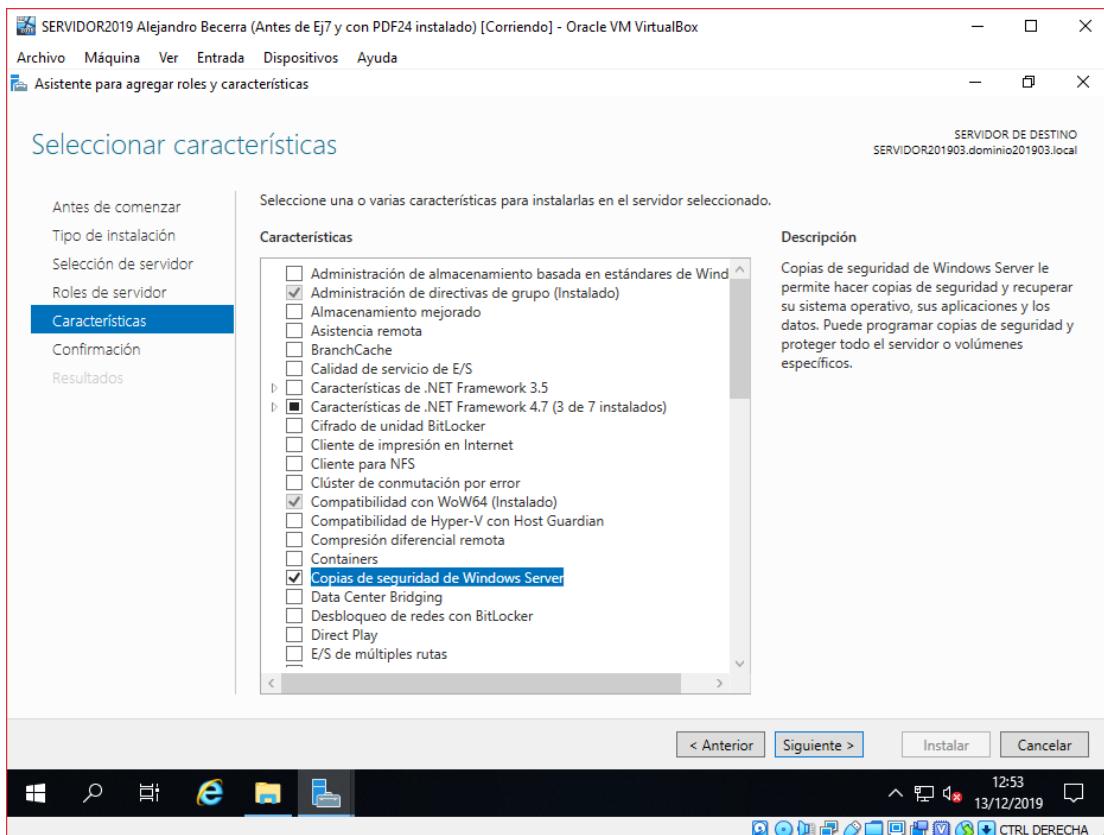
Para esta parte comenzaremos instalando un nuevo disco duro que tenga tanta memoria como tiene el servidor, una vez instalado lo formatearemos en la “Administración del equipo” dándole una partición MBR y que sea un nuevo volumen simple.

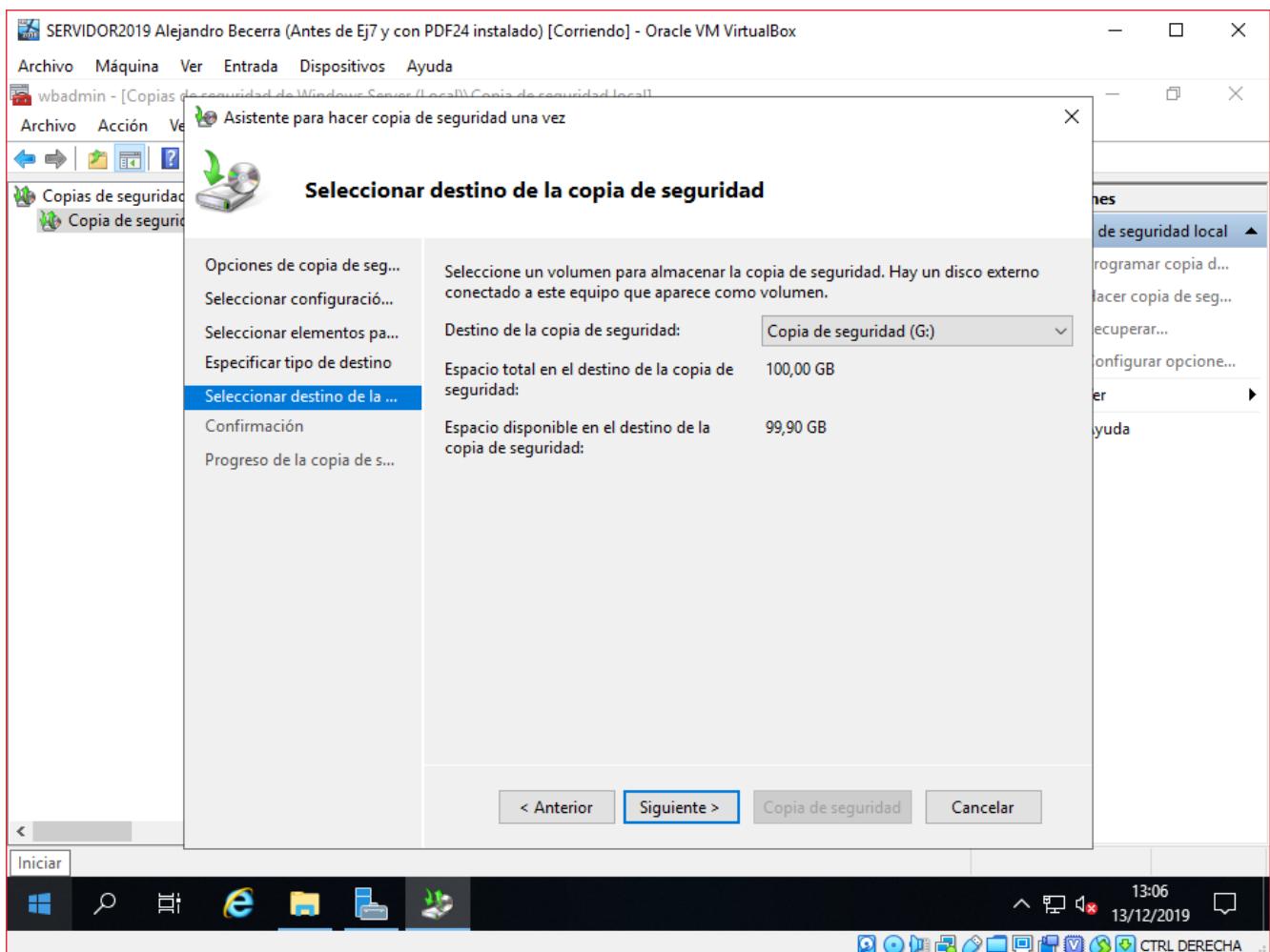
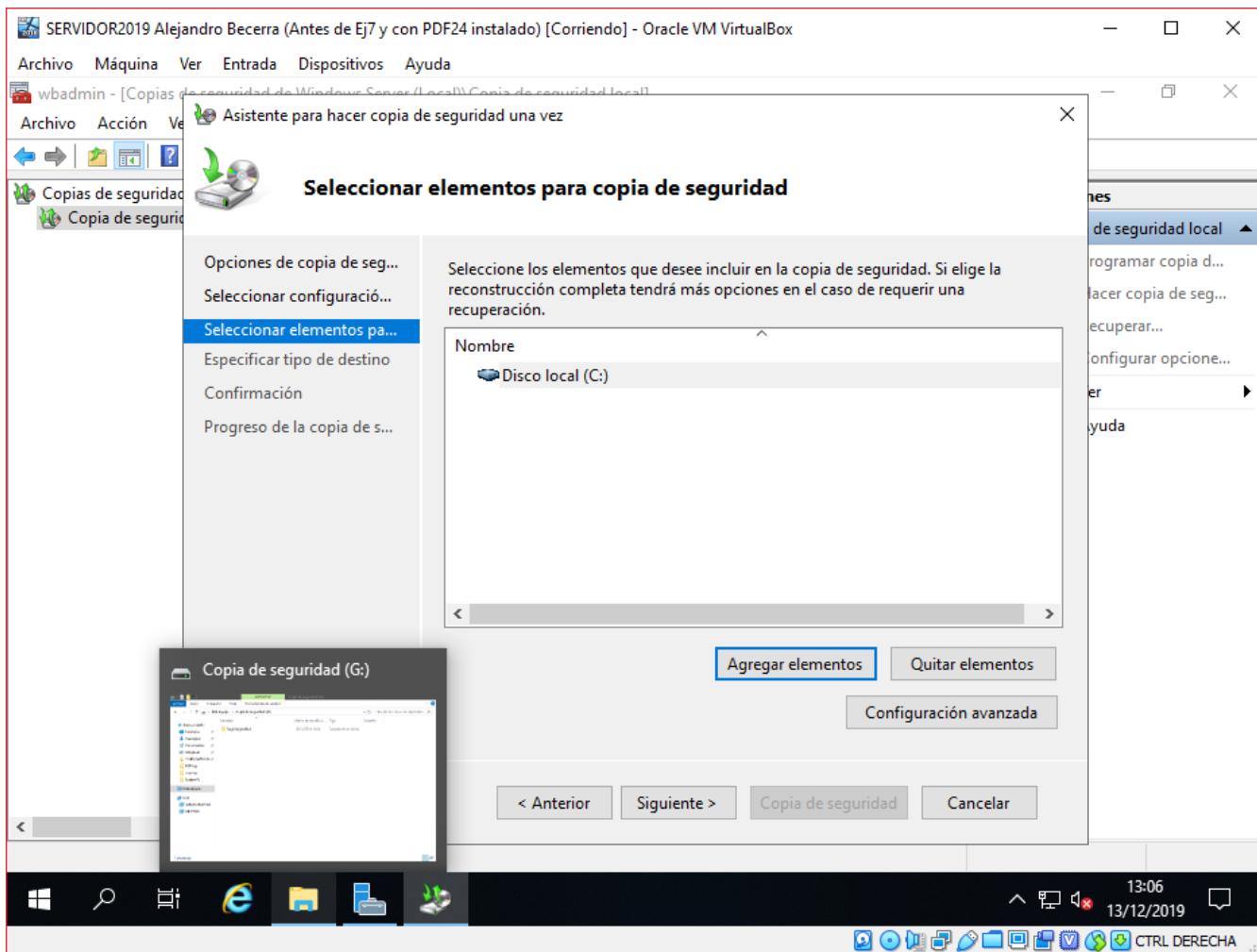


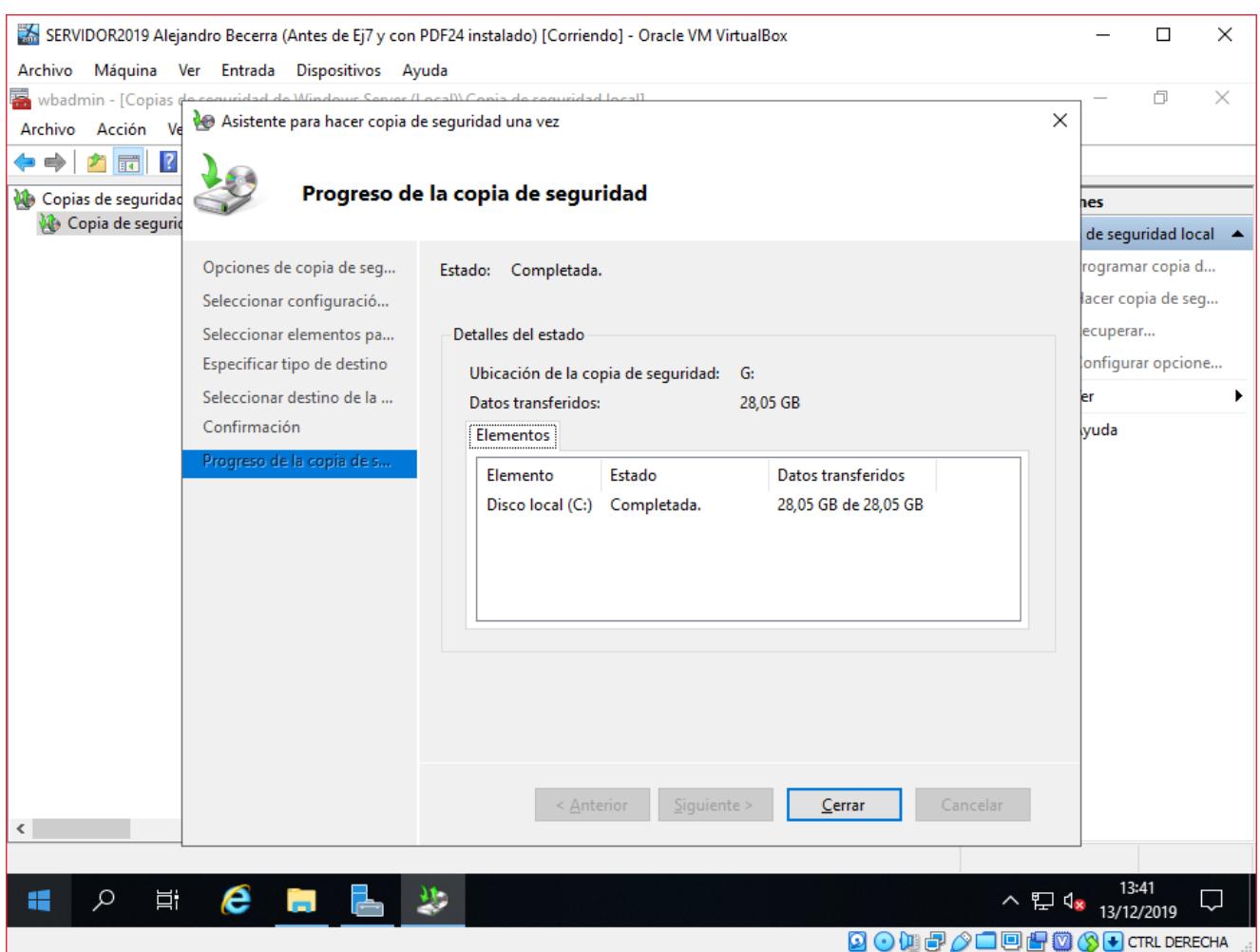
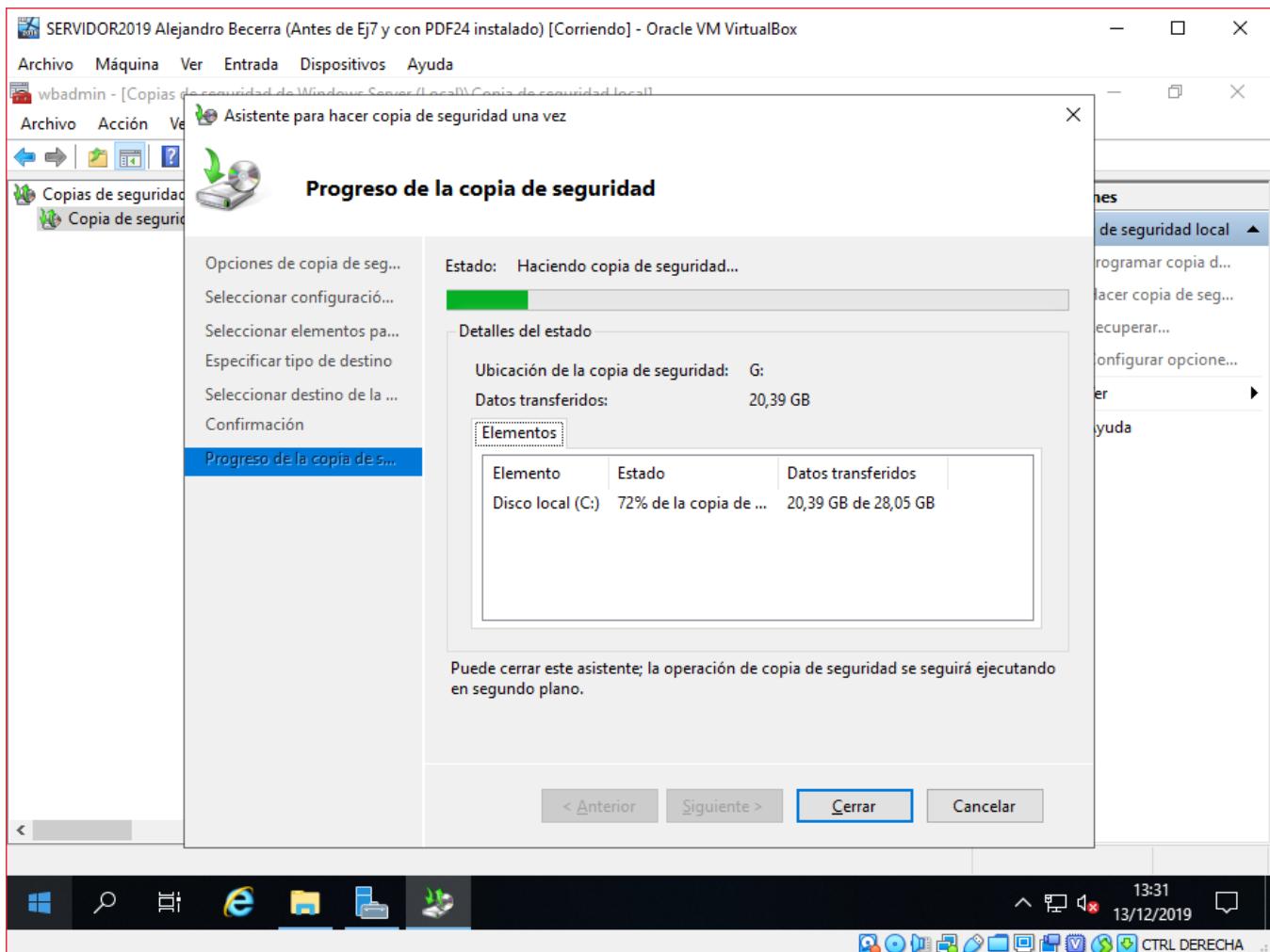


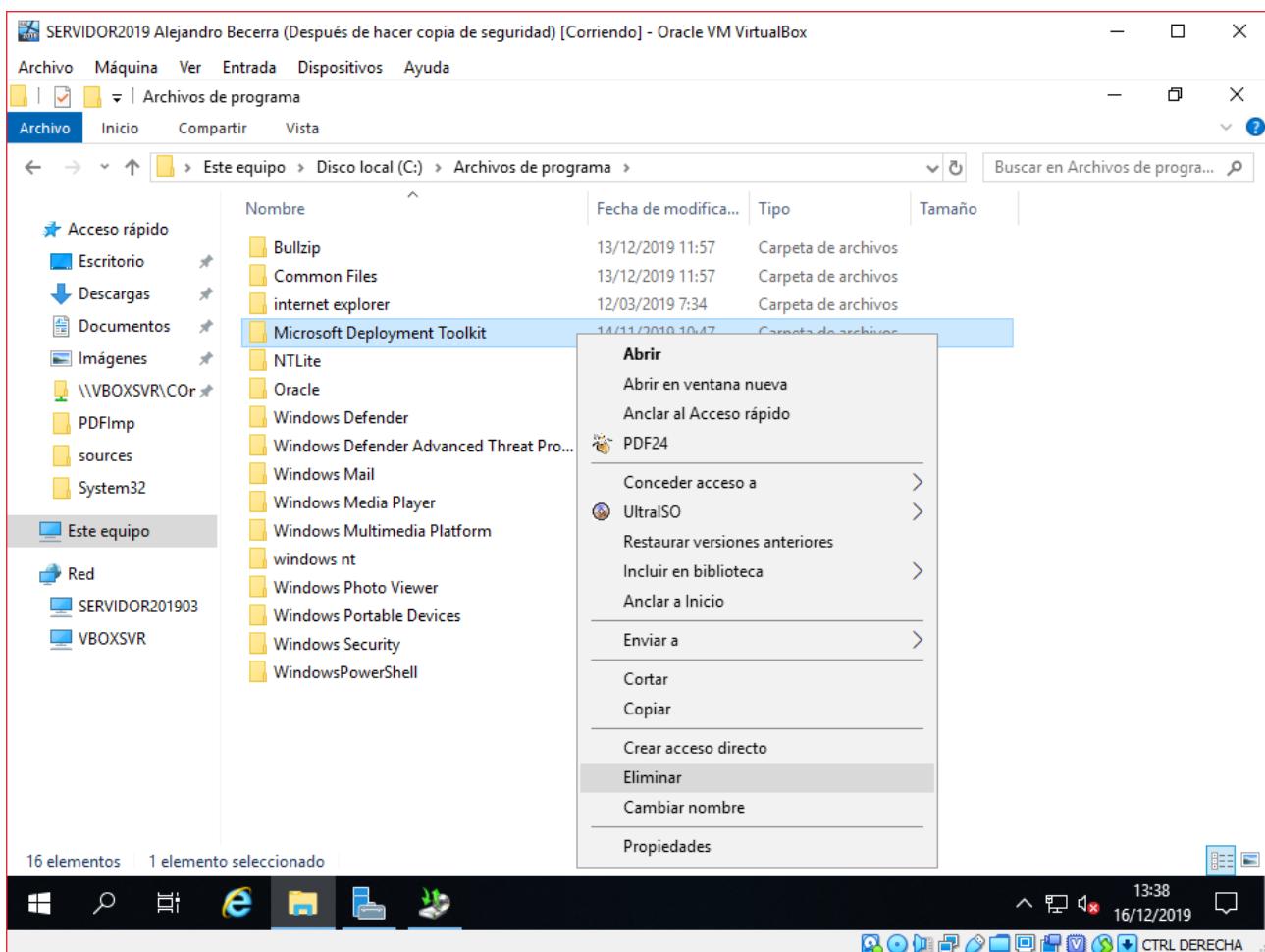
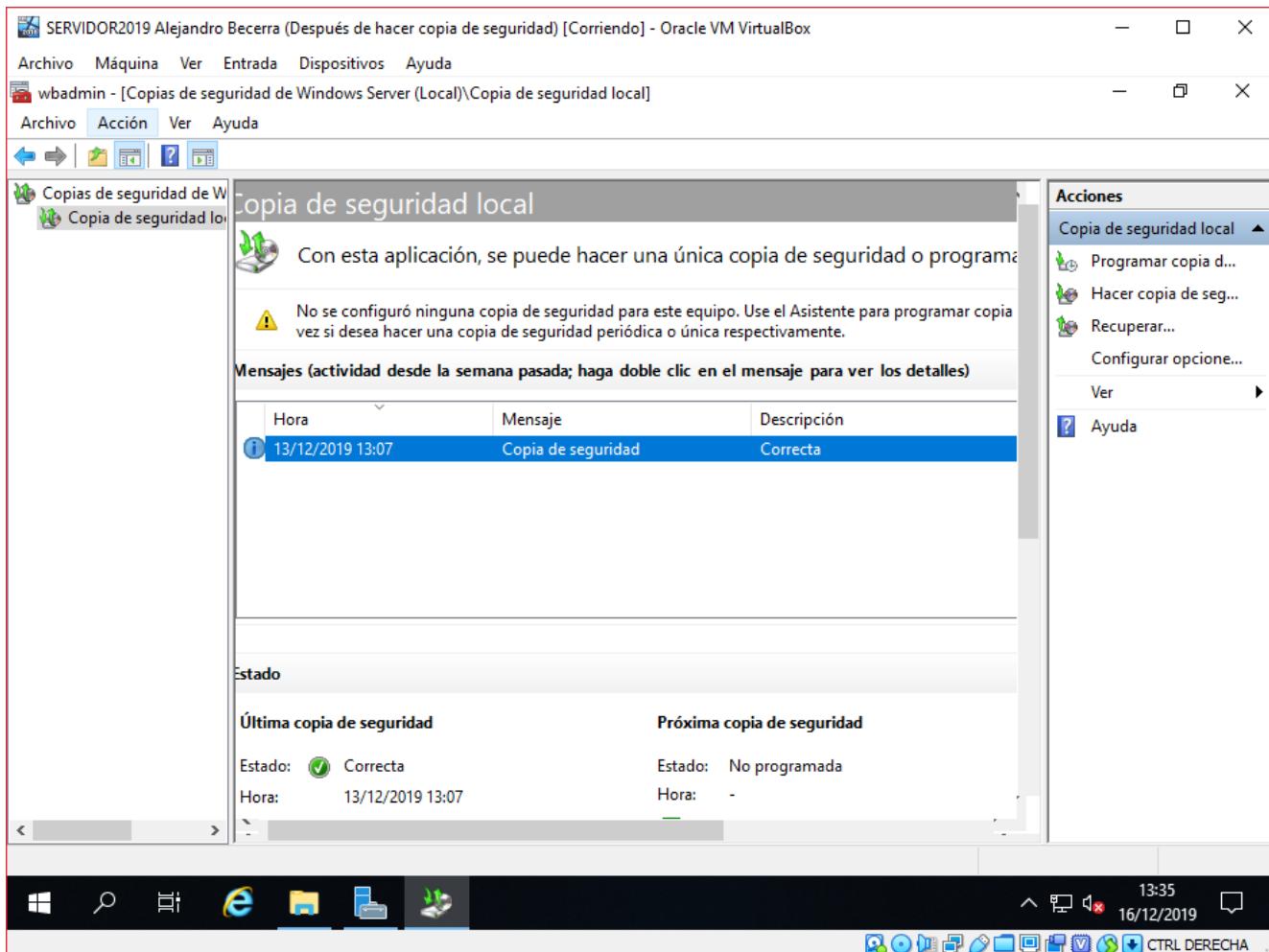
Realización de la copia de seguridad

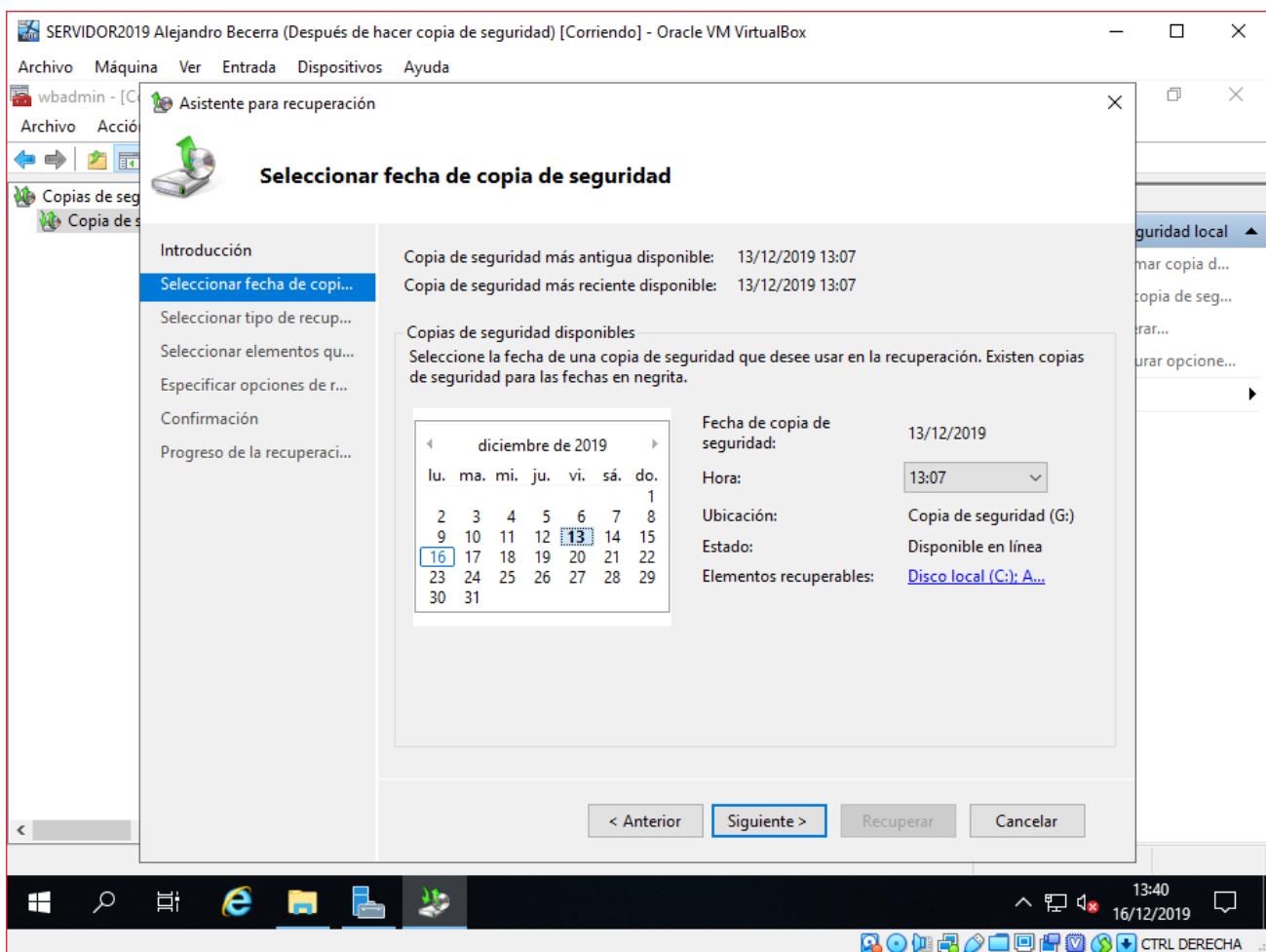
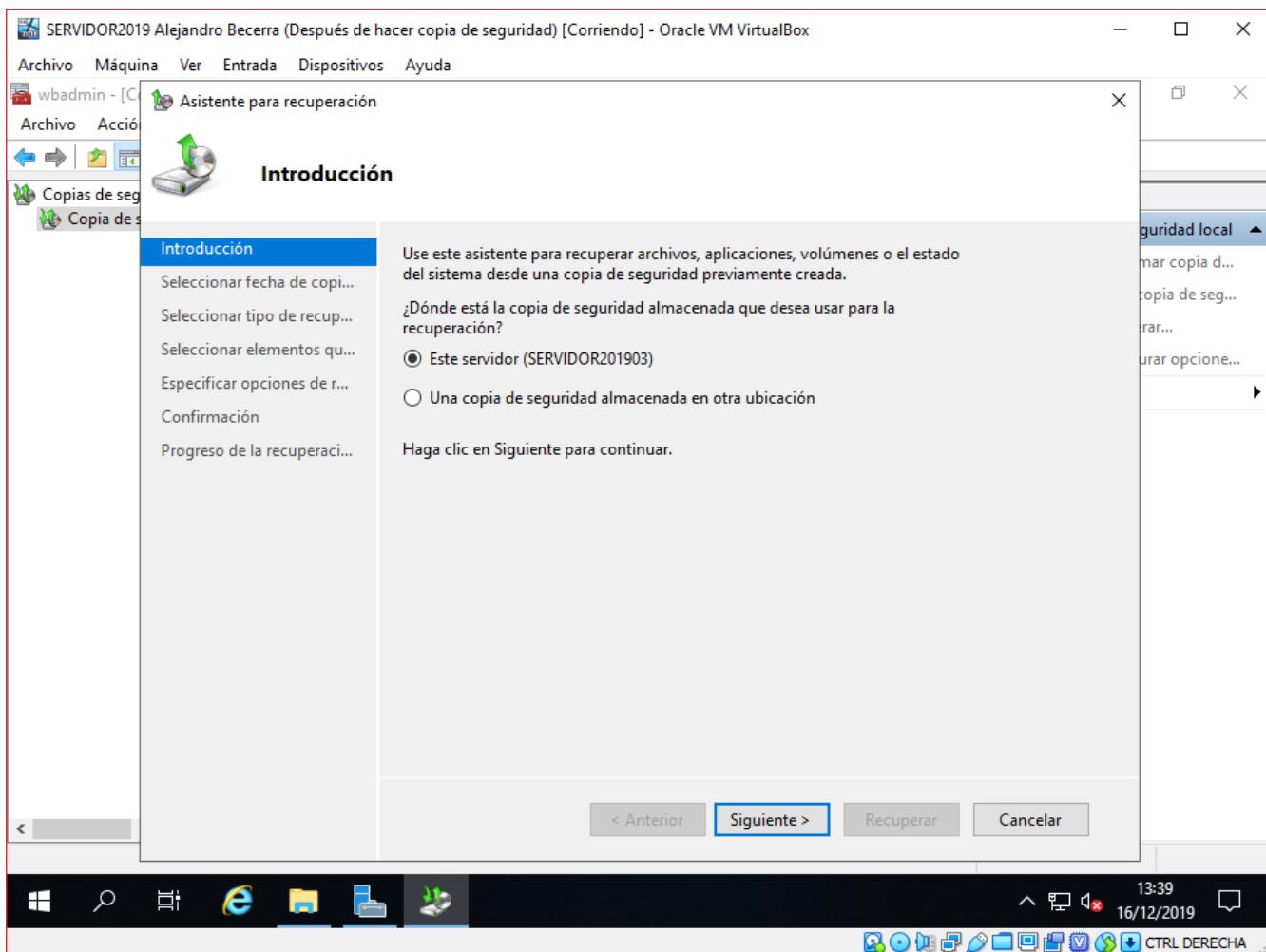
Después del formateo comenzaremos instalando la característica de “Copias de seguridad de Windows Server”. Una vez instalado haremos una prueba de copia únicamente el disco local C, cuando se acabe de hacer la copia borraremos una carpeta cualquiera de este disco para después restaurarla con la copia de seguridad.

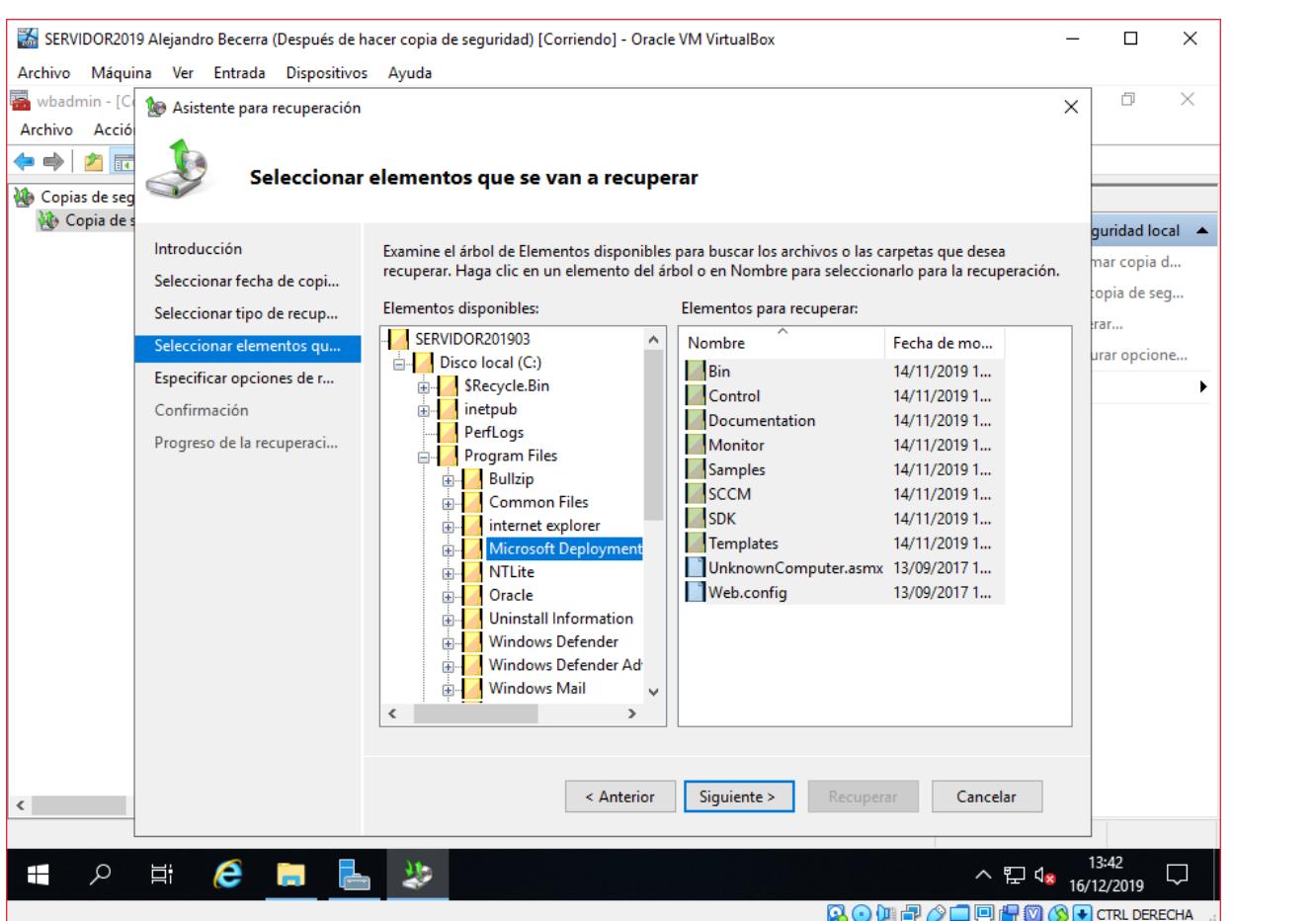
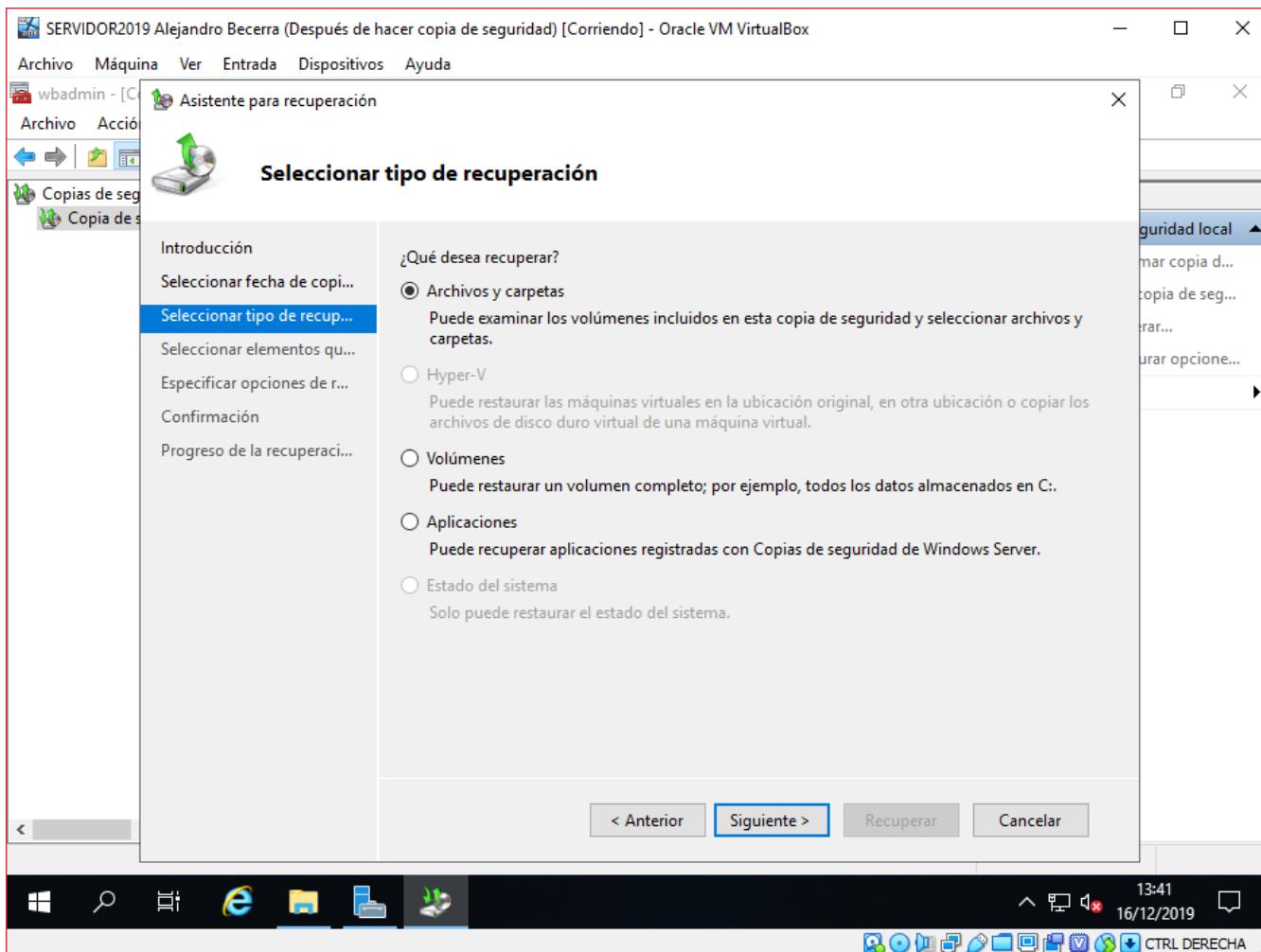


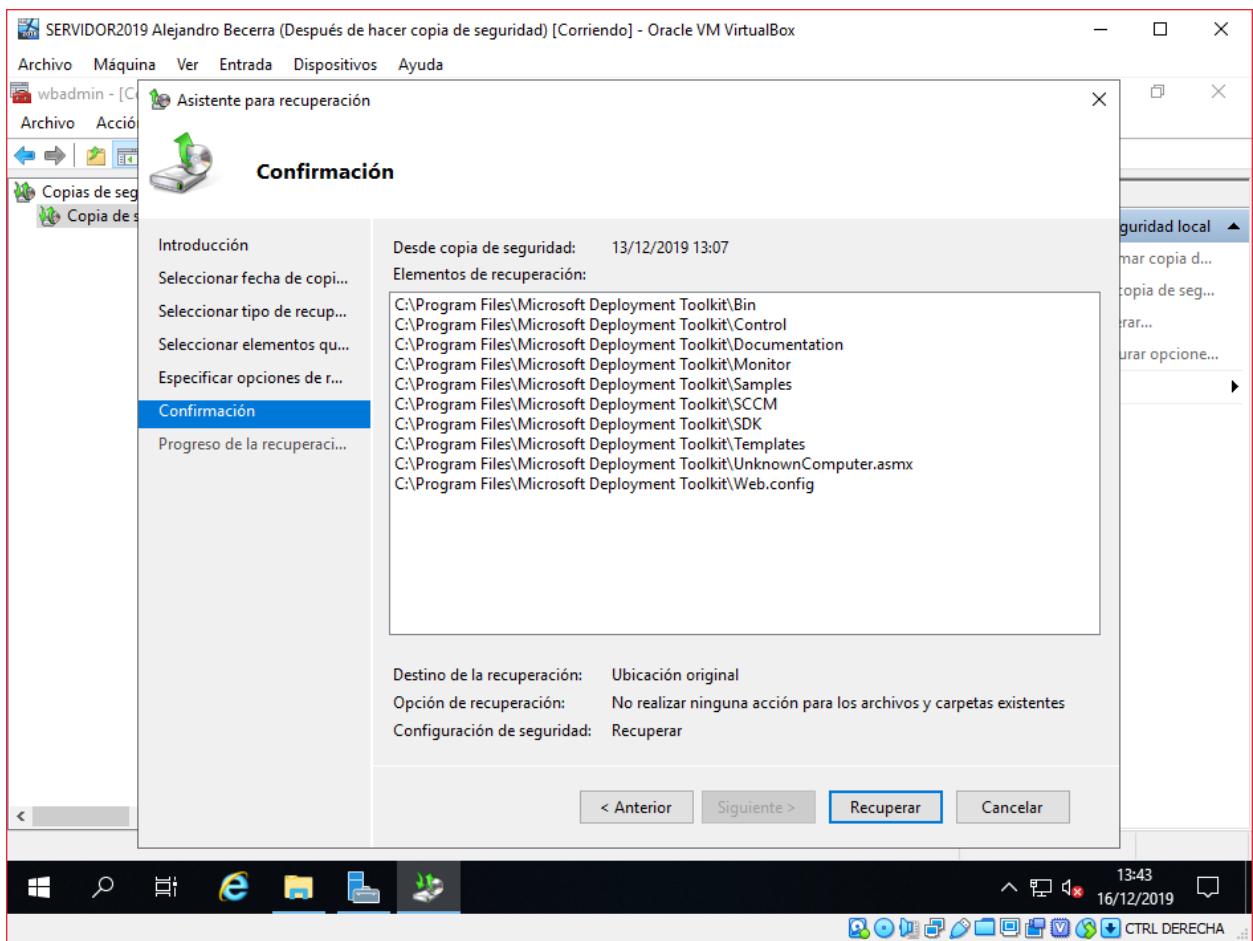
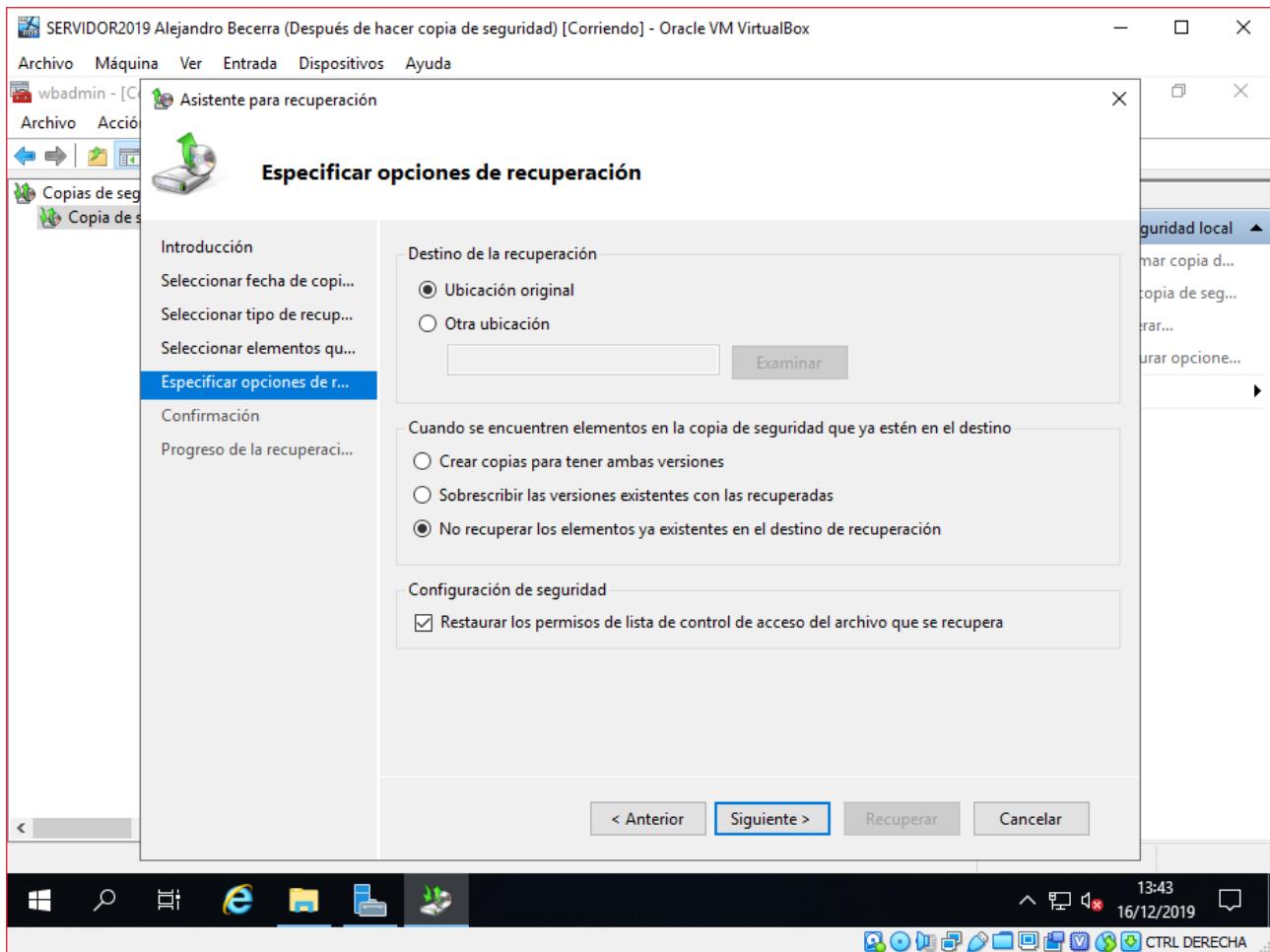


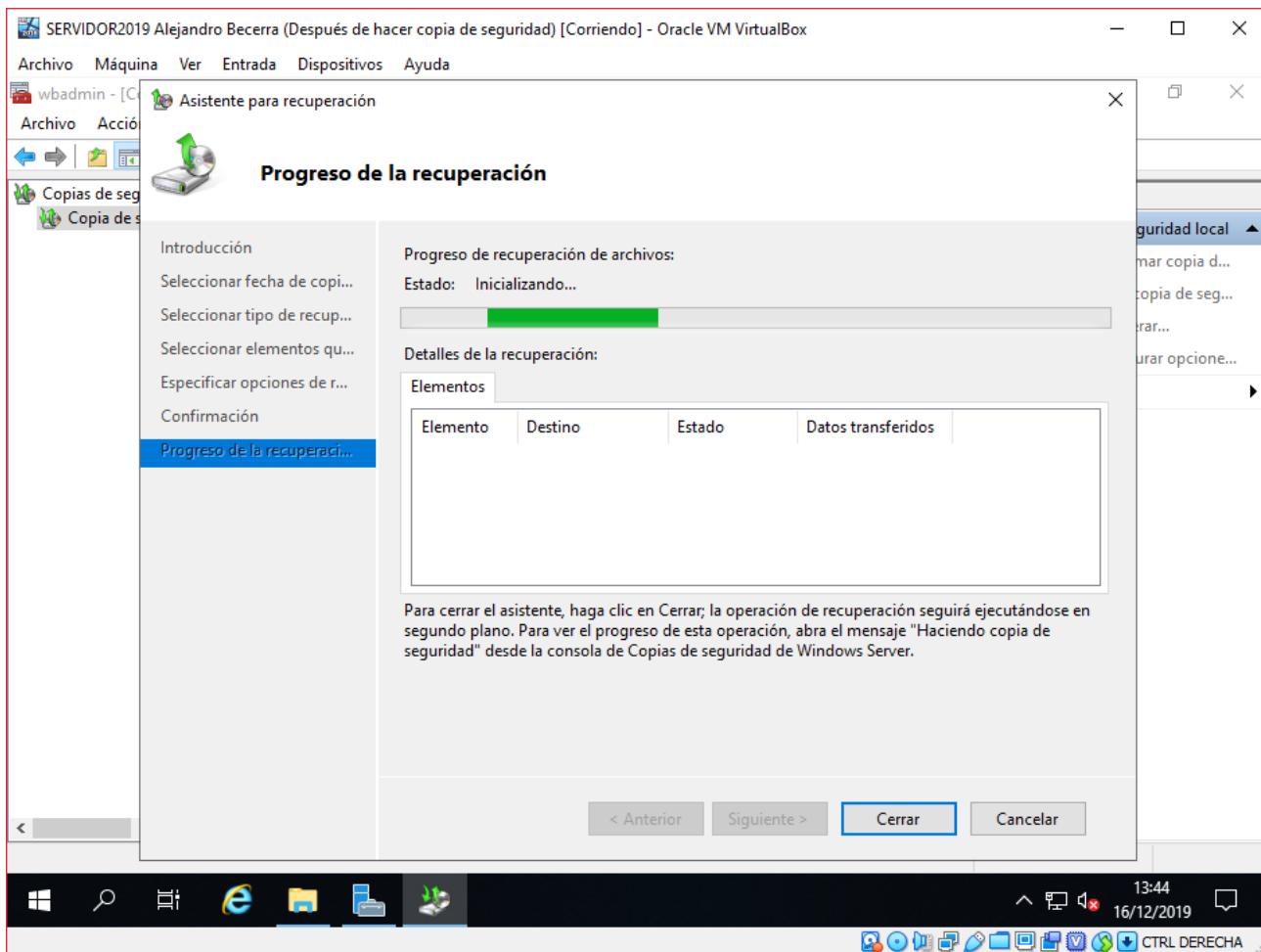






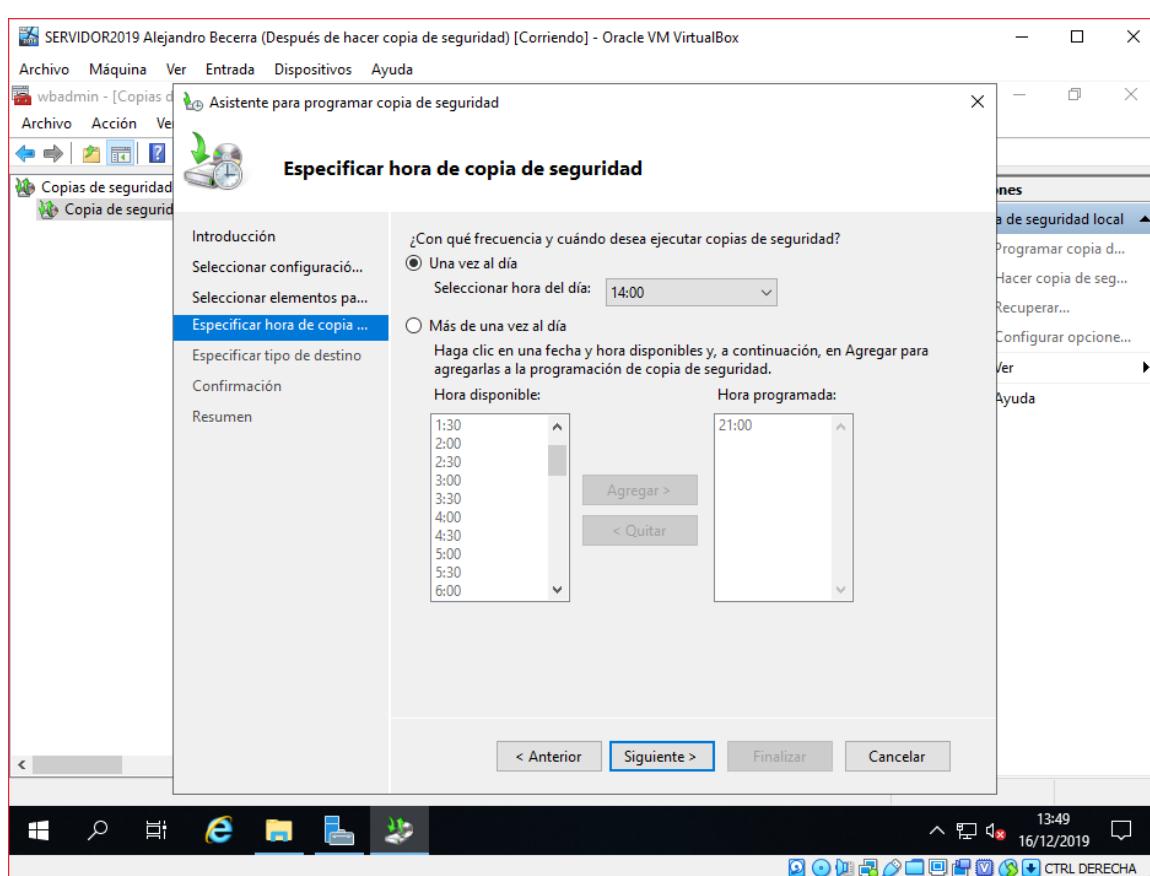
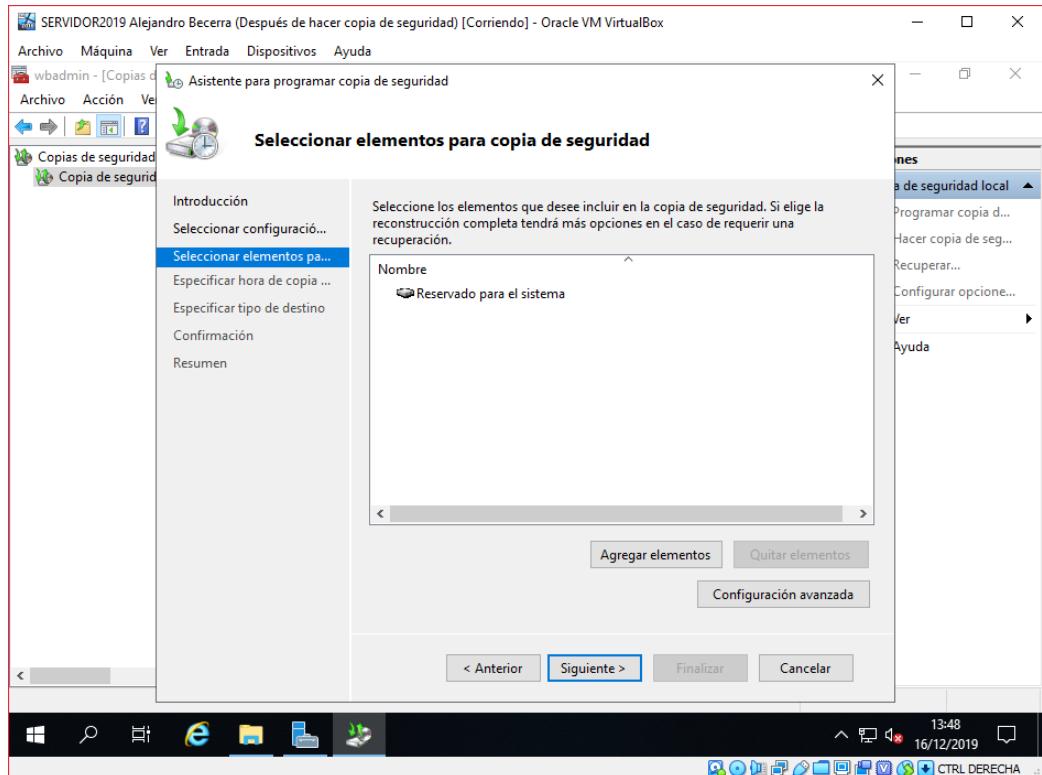


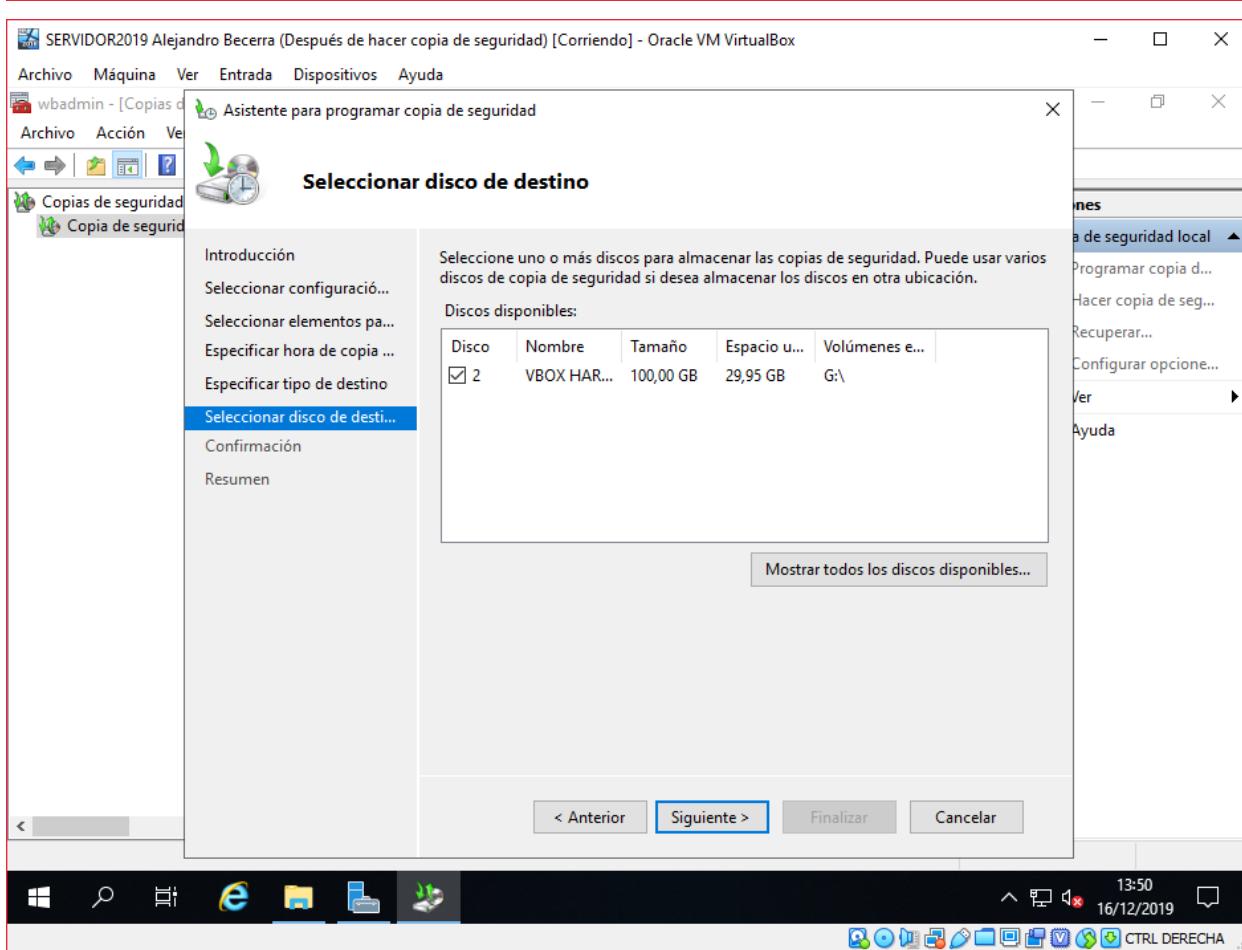
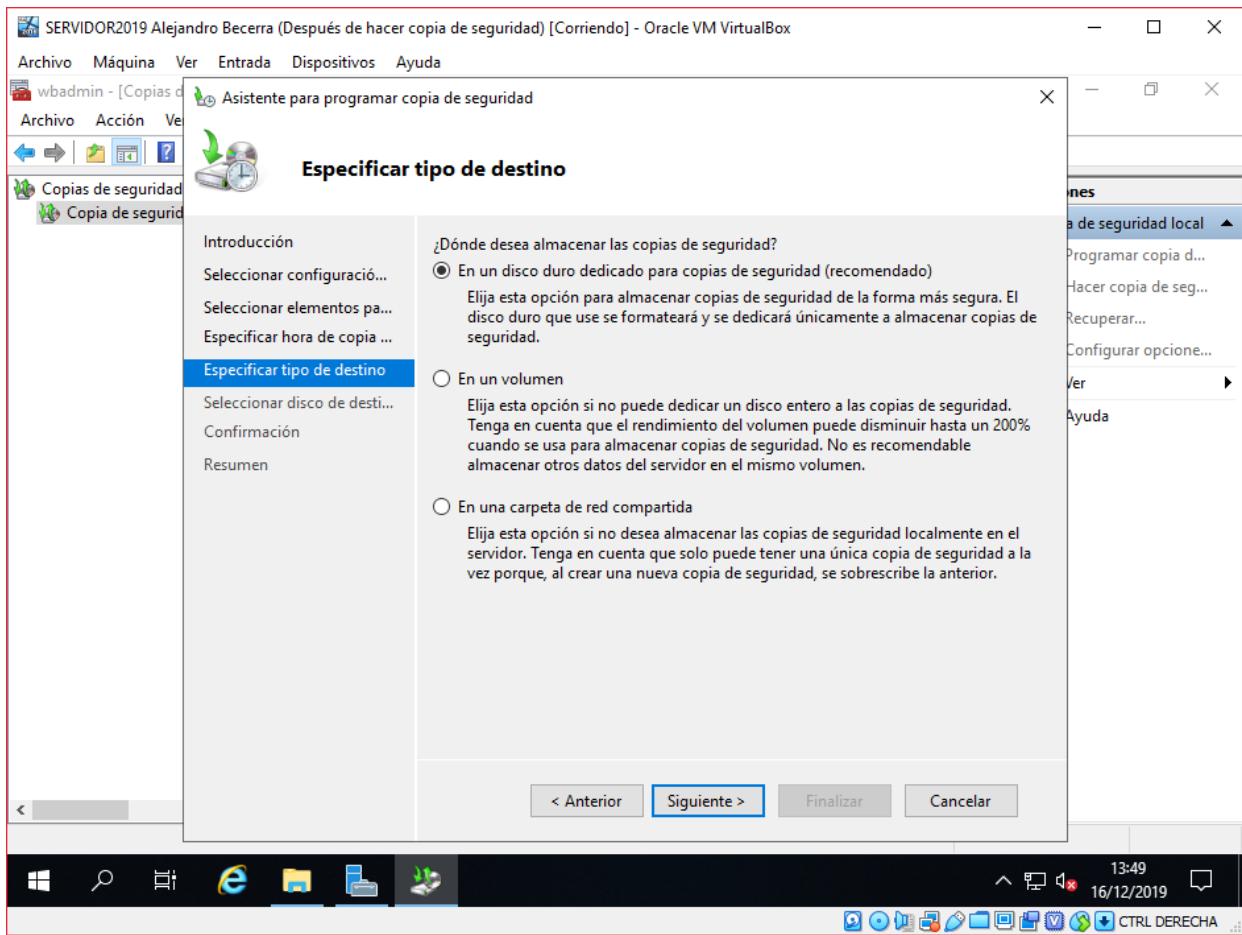


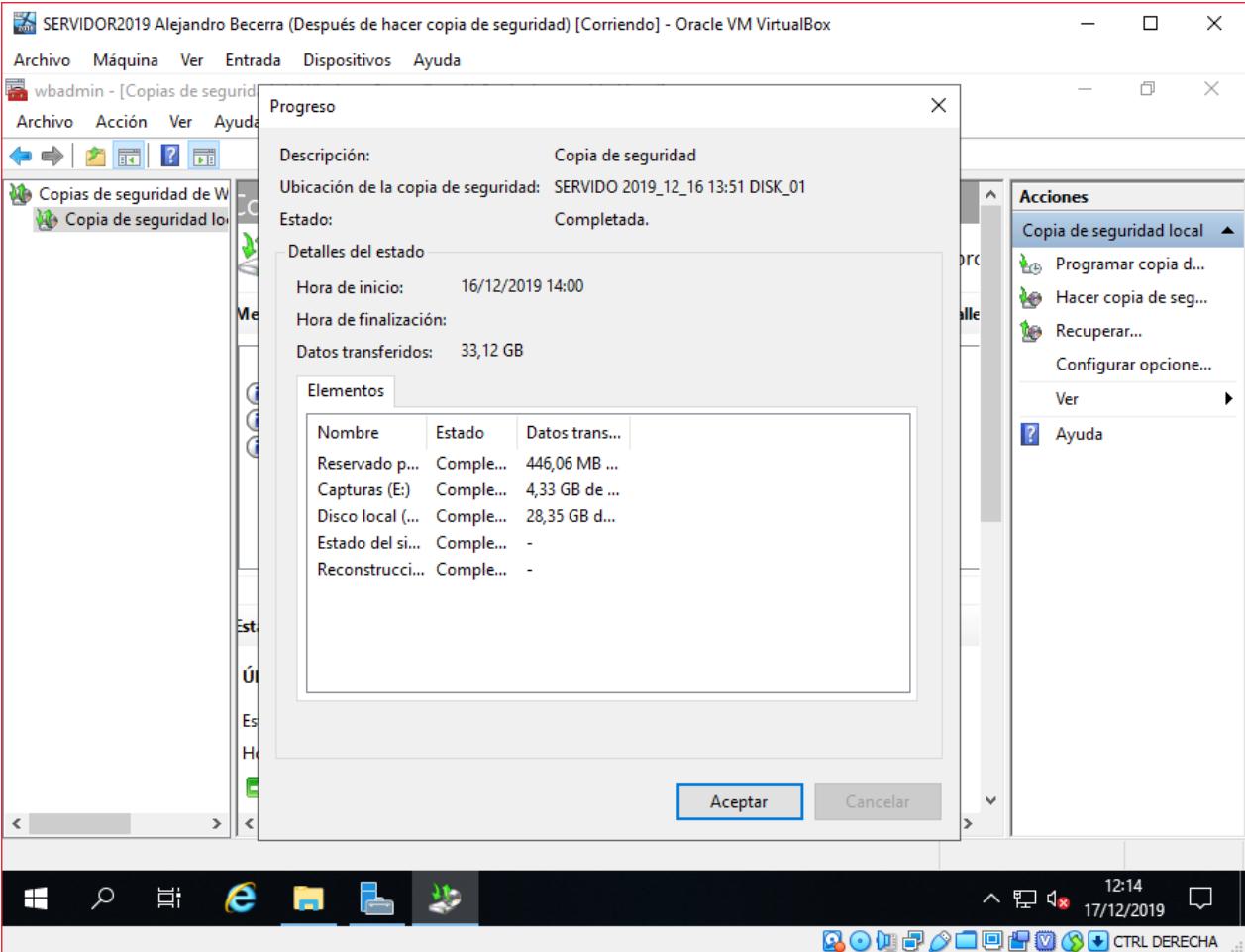


Copia de seguridad programada

A continuación haremos una copia de seguridad programada que hará una copia de la parte reservada del disco duro para el sistema, lo haremos con esto para pasar al siguiente punto más rápido, ya que programar una copia de seguridad se realiza de la misma forma que creando una copia en el anterior punto. Solo habrá que escoger en el panel de la derecha “Programar una copia de seguridad” y decidir con qué frecuencia se efectuará la copia del servidor.



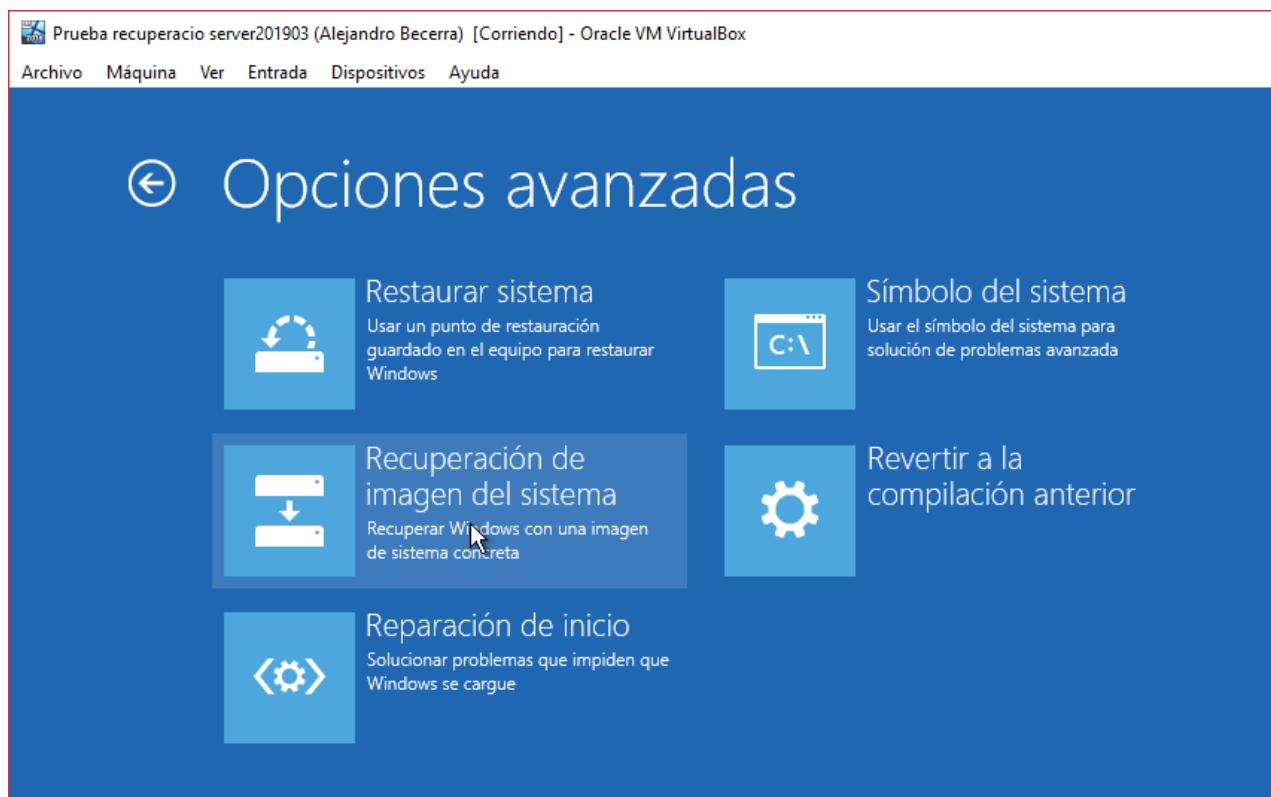
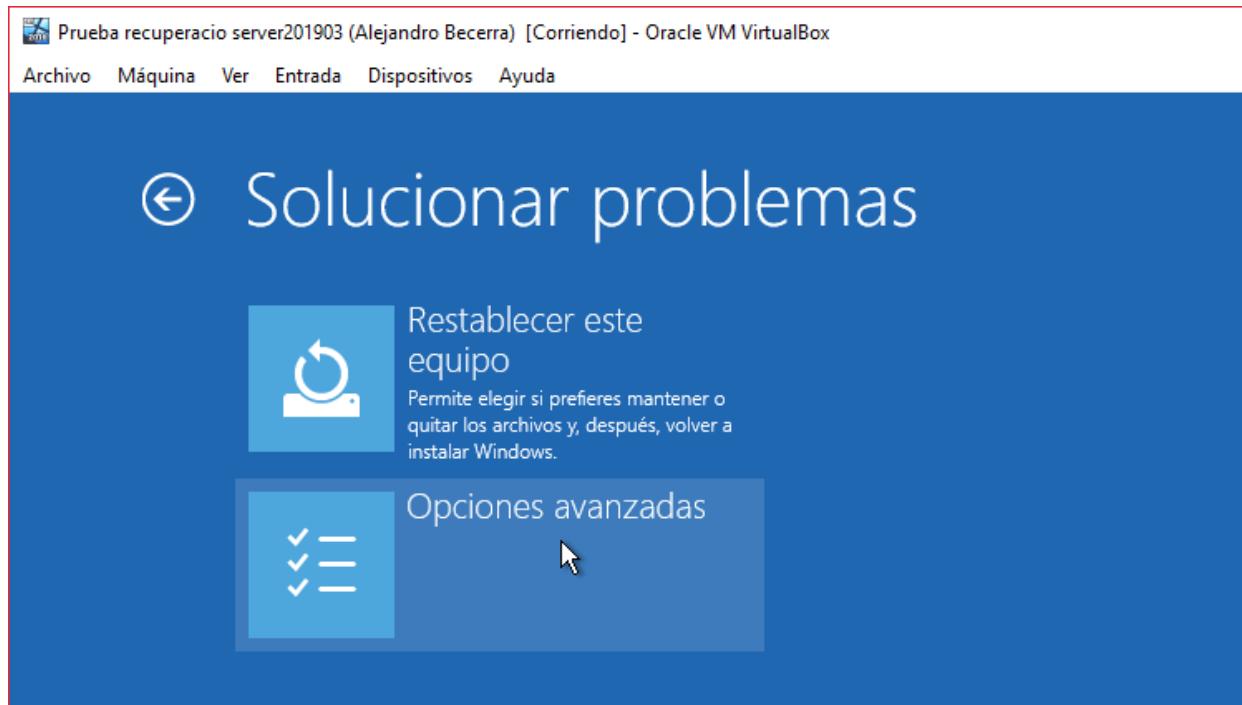


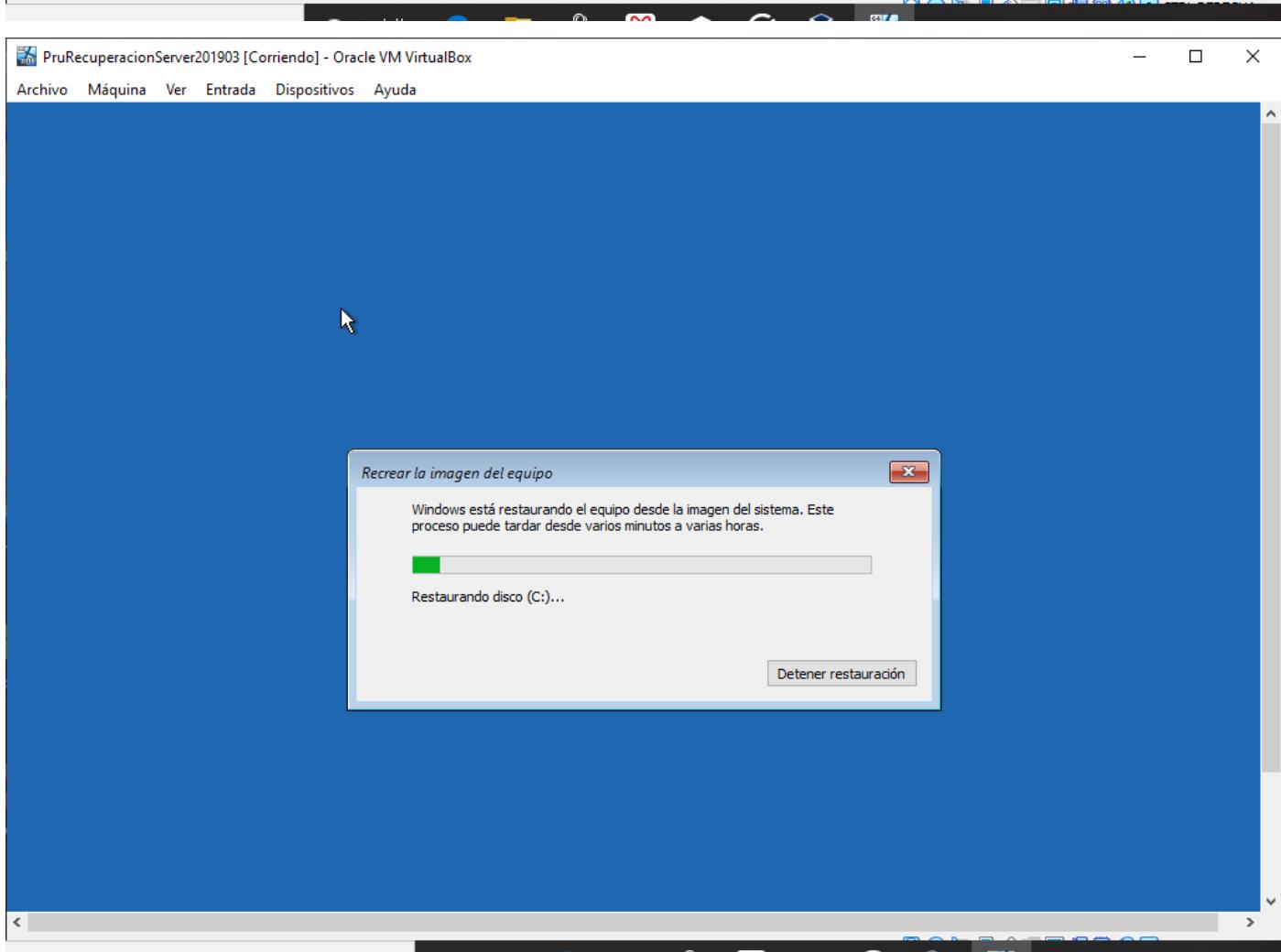
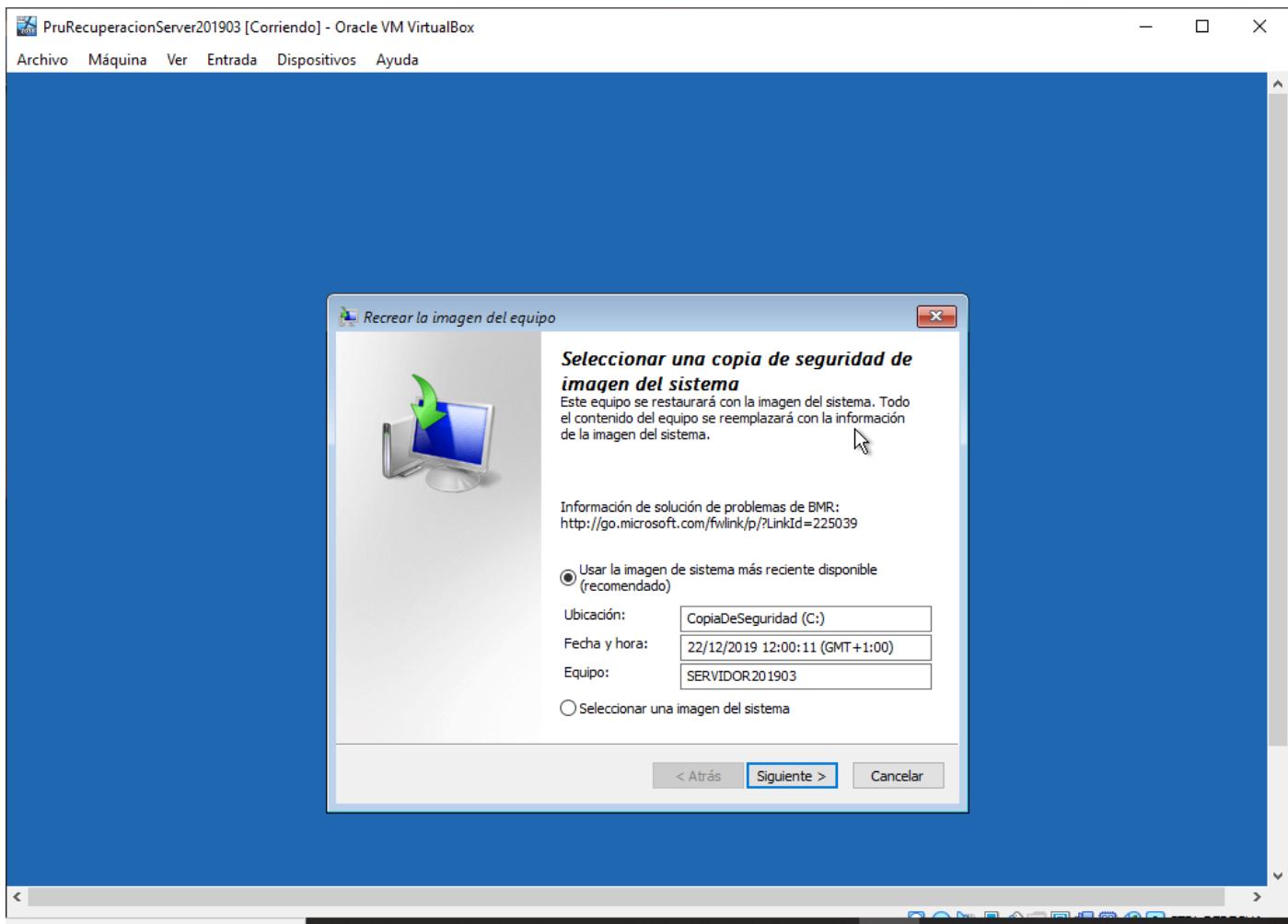


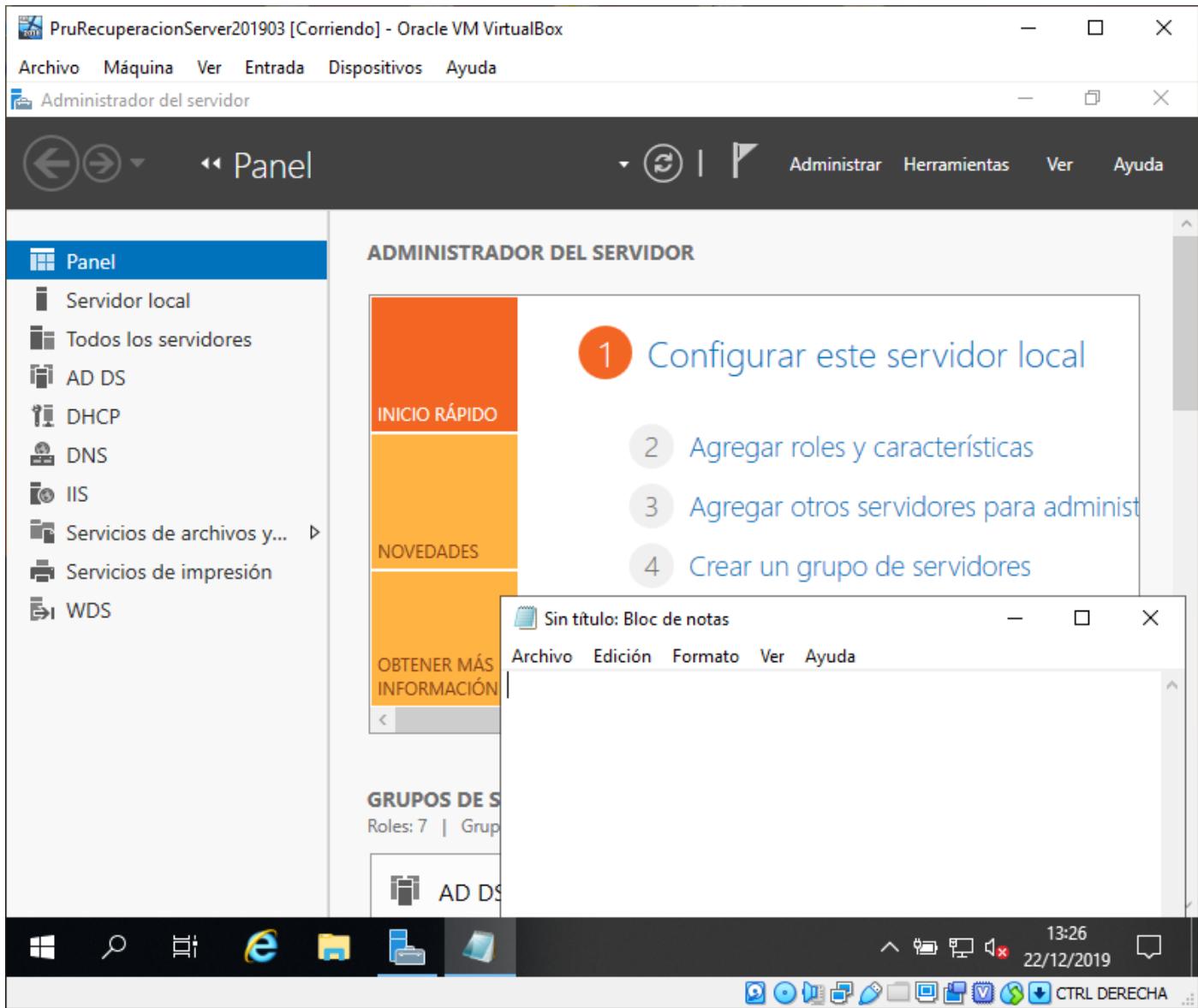
Recuperación completa del sistema desde una copia de respaldo

Esta recuperación la haremos en una máquina vacía usando el disco en el que anteriormente hicimos la copia de seguridad del servidor.

Para esto tendremos que insertar en la nueva máquina una cantidad igual o superior al número de discos que poseía el servidor aparte de también incorporar el disco donde se realizó la copia de seguridad. Comenzaremos instalando los discos necesarios y además pondremos el CD de instalación de Windows 10 para que pueda arrancar y nosotros podamos darle a la reparación del equipo, en vez de la instalación normal del Sistema Operativo. Después, solo habrá que darle a “Recuperación de imagen del sistema” y posteriormente escogeremos la imagen del sistema y esperaremos a que termine de restaurarse.





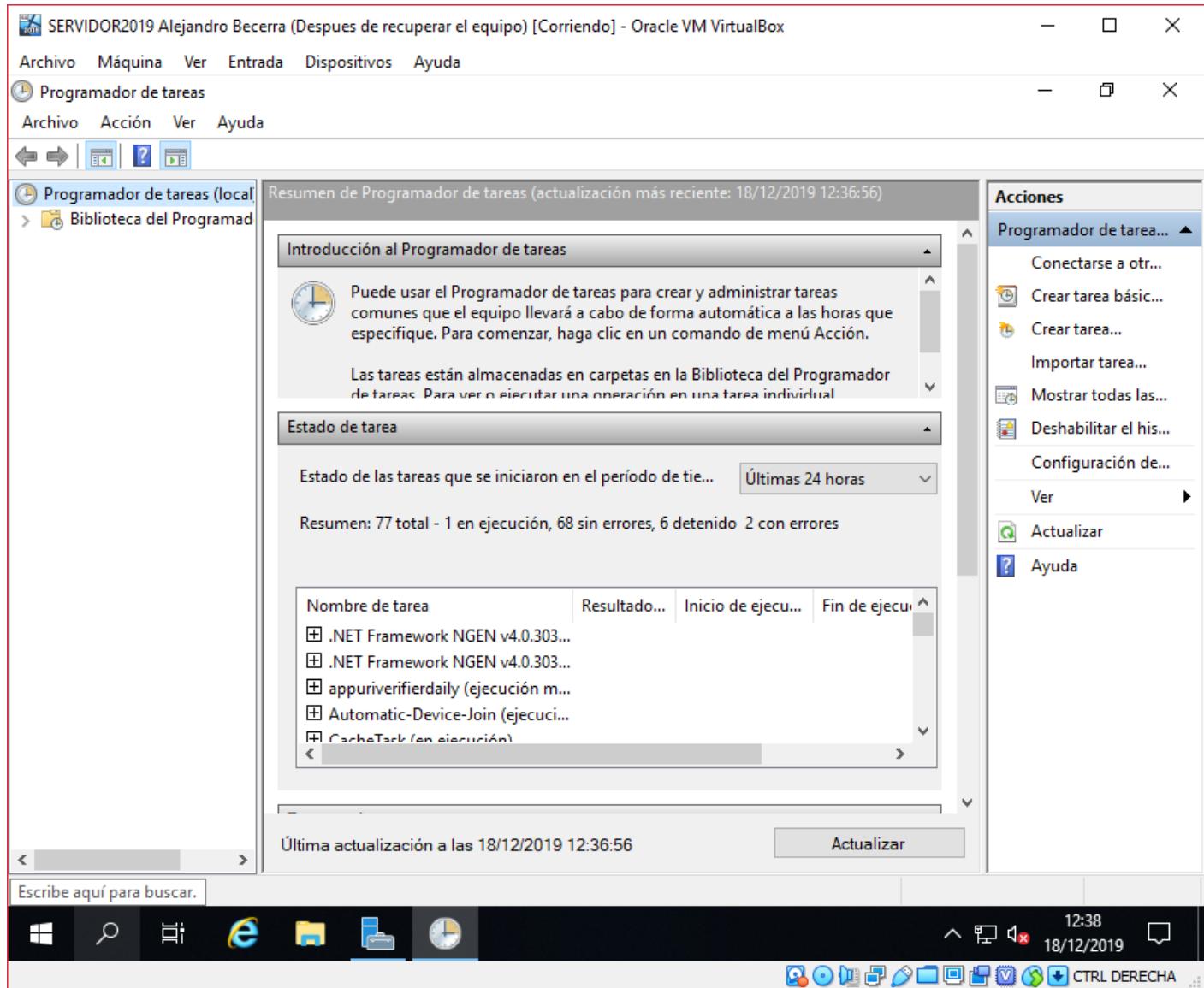


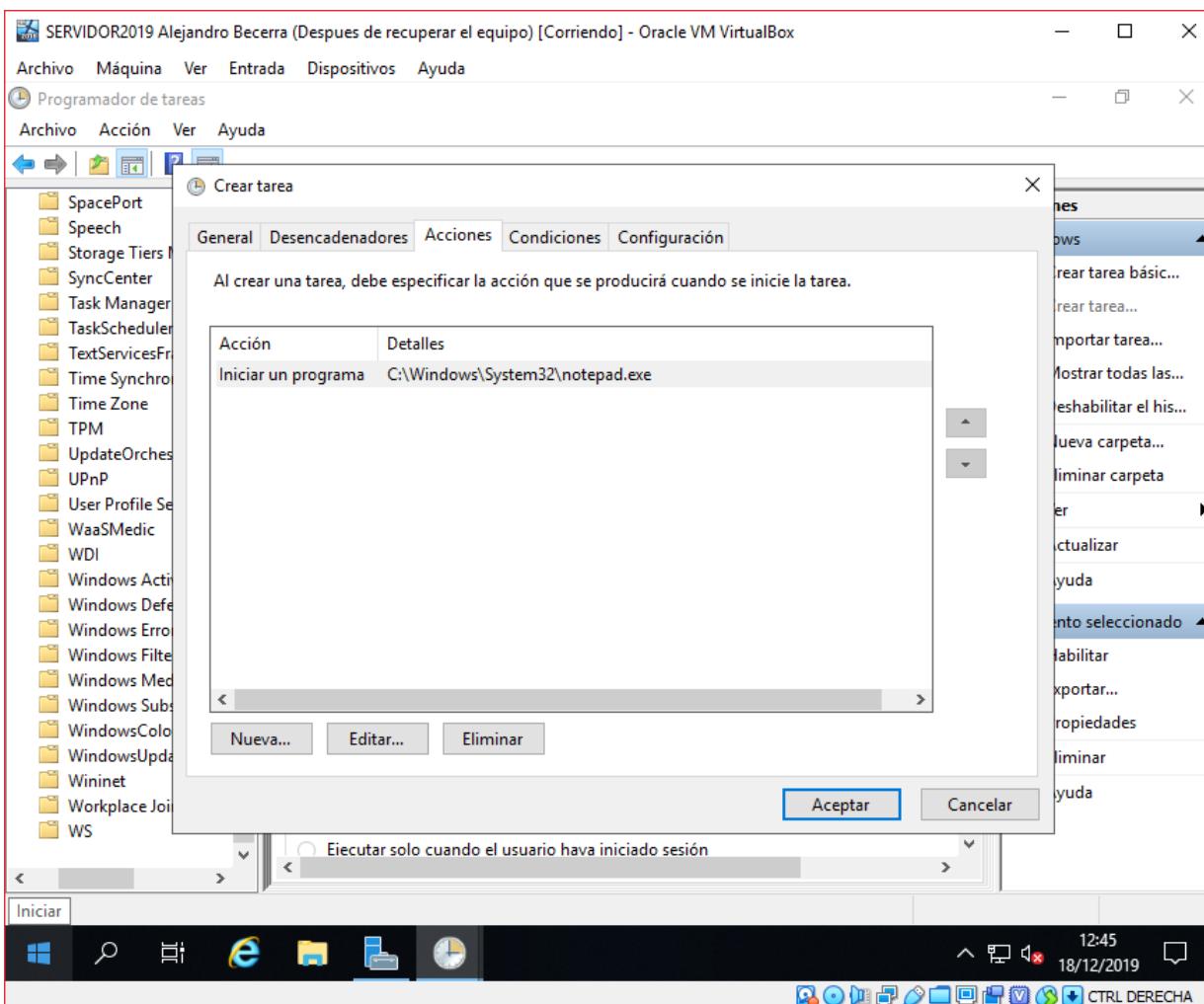
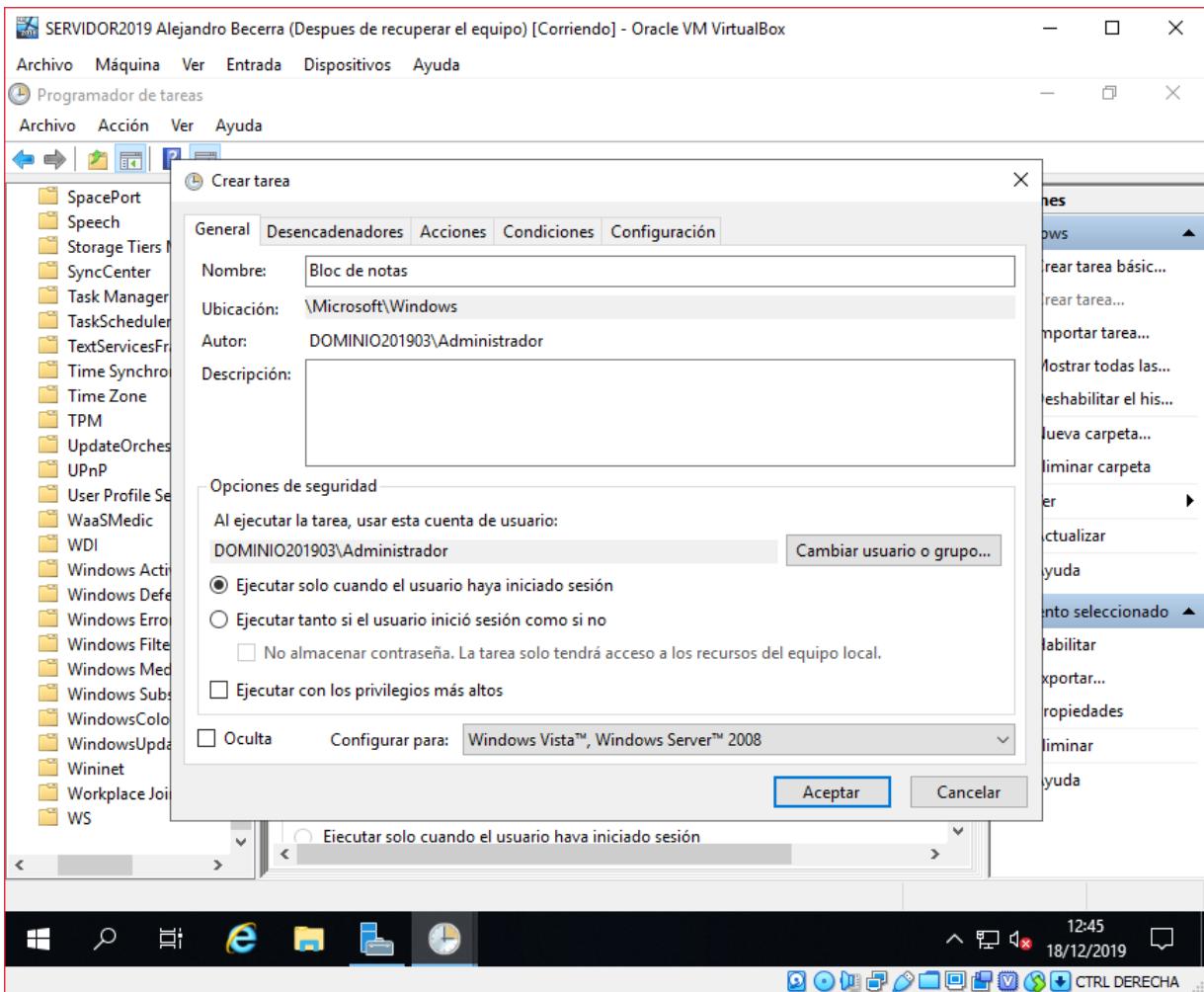
Tareas programadas

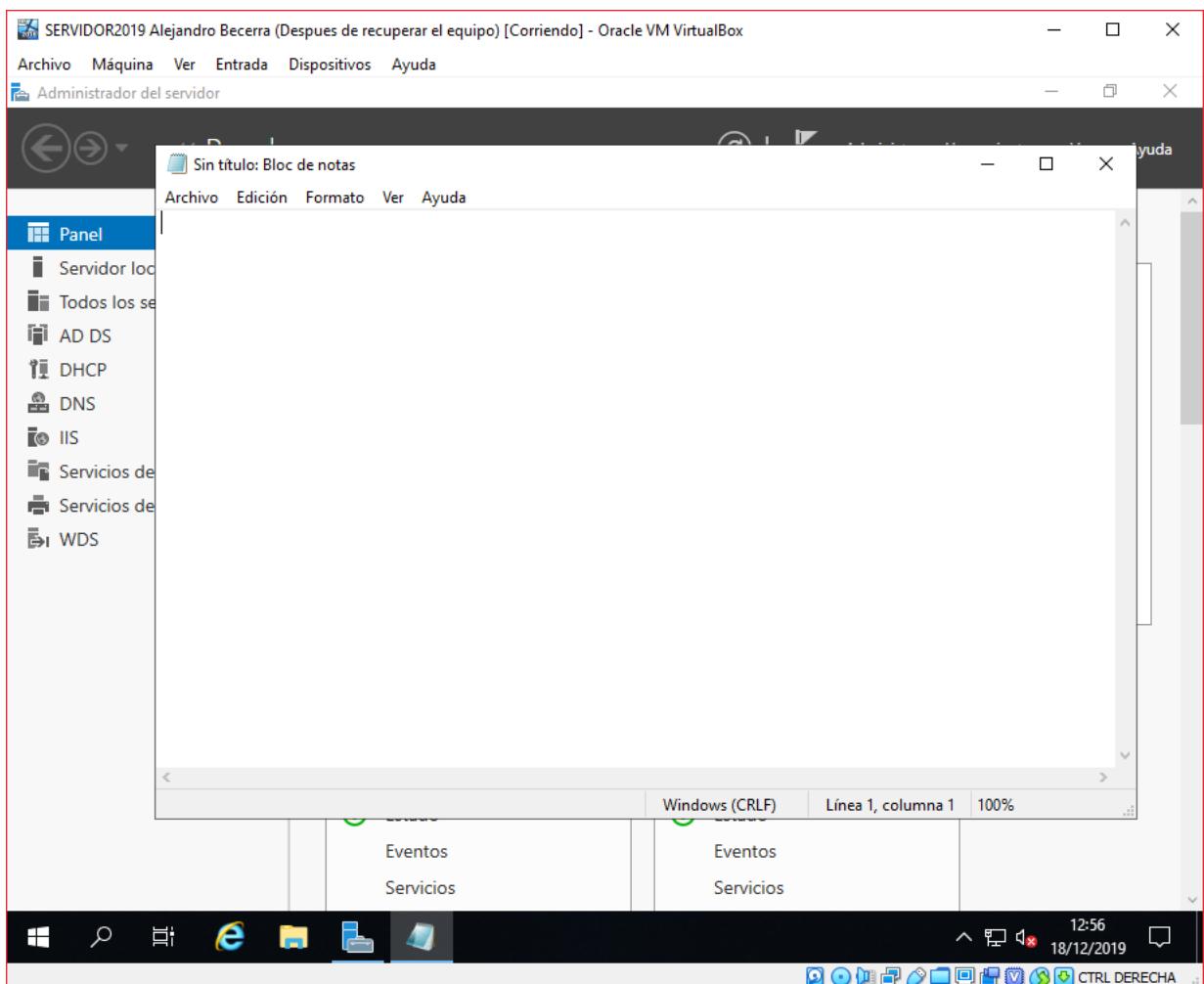
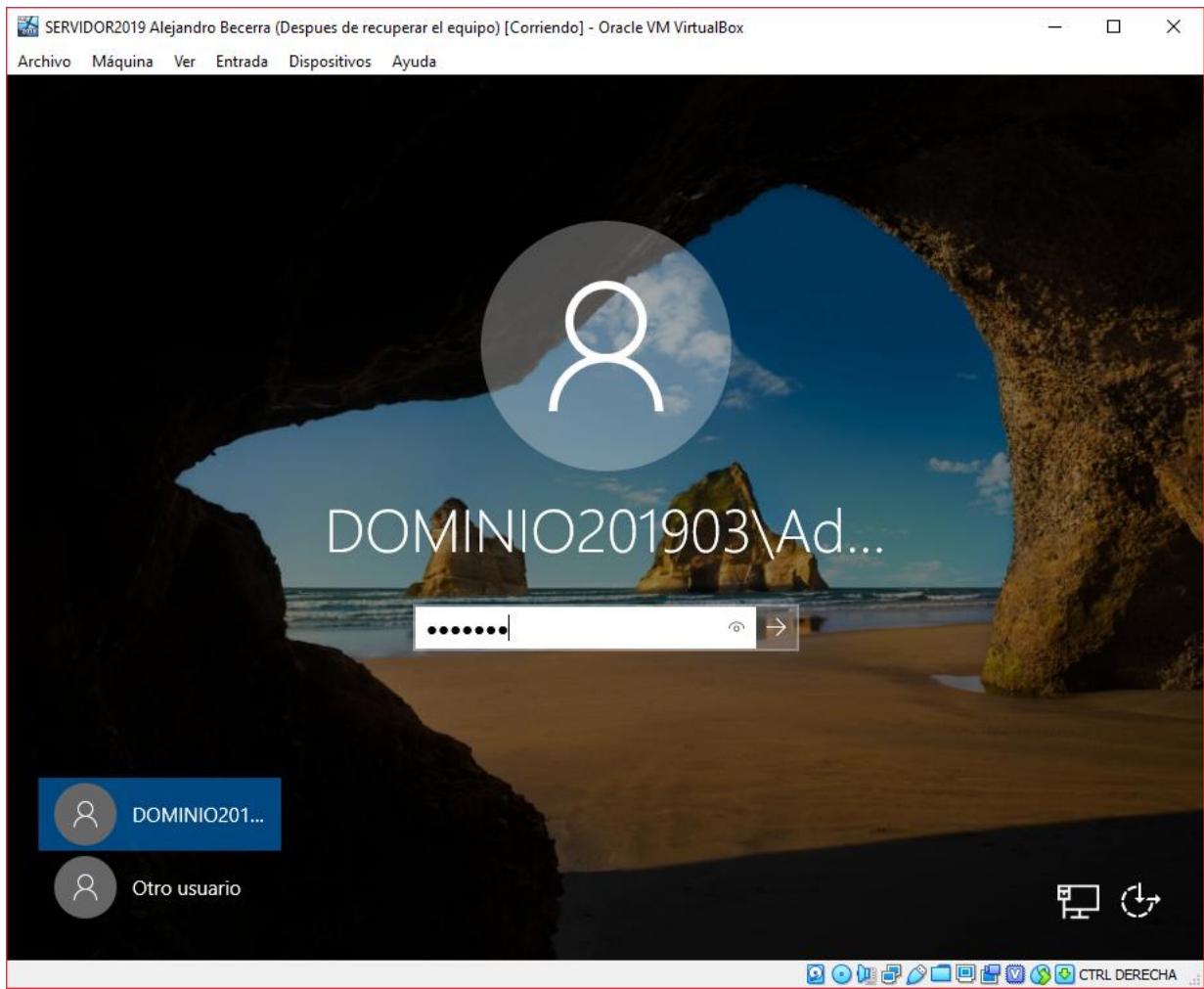
Para esta tarea usaremos el “Programador de tareas”, esta herramienta es propia de Windows y no es única en las versiones de servidores, ya que en las versiones de cliente también la hay.

Lo que haremos en esta práctica será crear una tarea que abrirá el bloc de notas siempre que abramos la sesión de administrador en el servidor. Para ello iremos al programa nombrado anteriormente y crearemos una tarea dándole al apartado correspondiente en la columna de la derecha y en acciones escogeremos que se ejecute el bloc de notas que se haya en “C:\Windows\System32\notepad.exe”.

Una vez hecha la tarea procederemos a salir de la sesión y volveremos a entrar para ver que funciona correctamente.

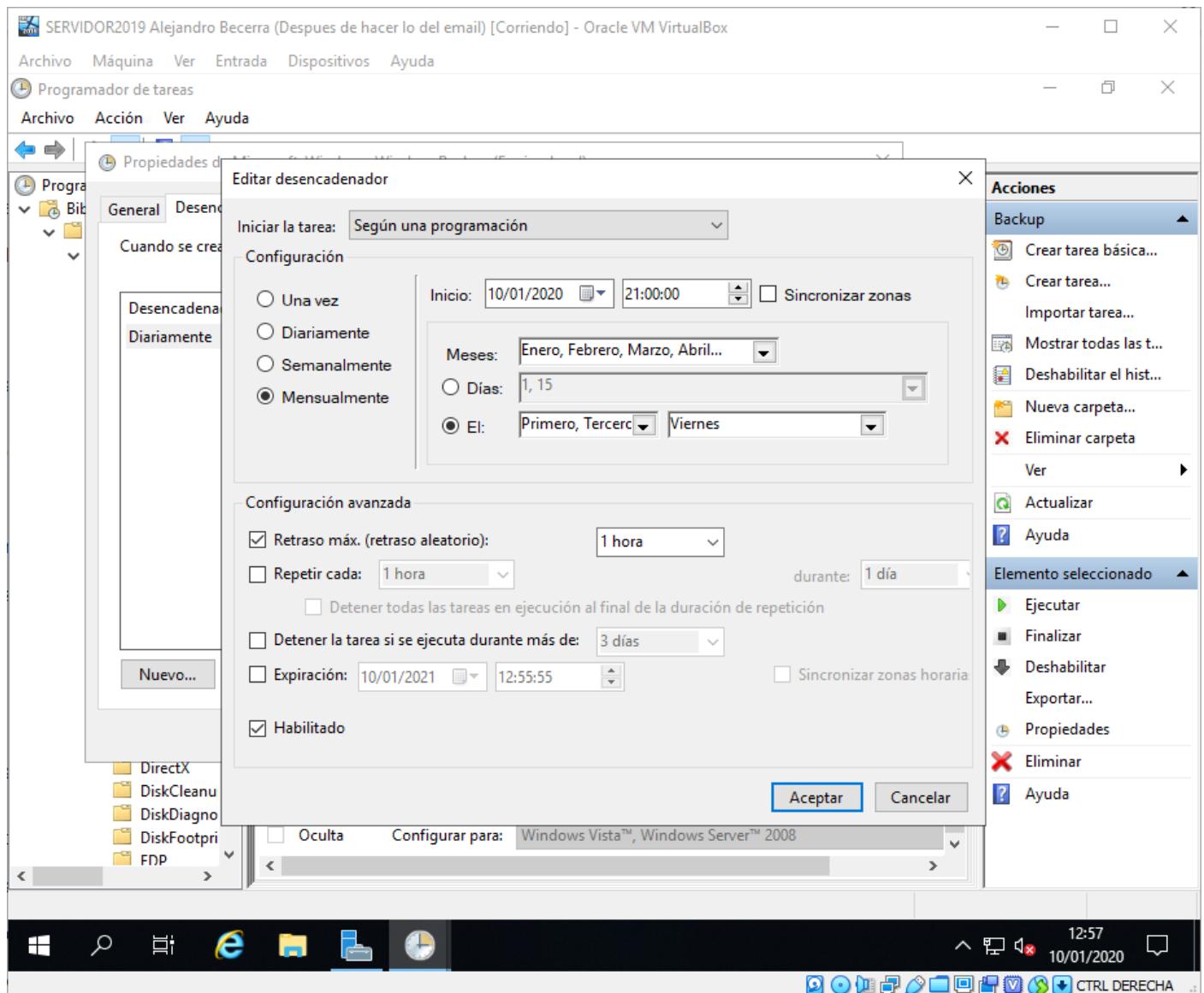






Modificación de la copia de seguridad programada

En este apartado modificaremos la copia de seguridad programada para que se ejecute lo viernes de las semanas impares a una hora distinta.



Visor de eventos

Para esta última tarea administrativa, usaremos el visor de eventos para detectar un intento de entrada en el servidor, al que se responderá mandando un email al correo del administrador advirtiendo de un intento de entrada fallida.

Para esto, en el “Visor de eventos” iremos al apartado de seguridad y buscaremos el evento con la ID 4625, que corresponde con el poner mal una contraseña al querer iniciar una sesión con un usuario. Crearemos una tarea programada que se active cuando se dé este evento, el cual, activará un script de PowerShell que mandará un email al correo asignado.

El script de PowerShell es el siguiente:

```
$from      = "YourE-MailAddress"
$smtpServer = "smtp.gmail.com"
$to        = "AdminE-MailAddress"
$subject   = "Notificación de $($env:computername)"
$evento = Get-EventLog -LogName "Security" -Newest 1
$body = @"
Evento a revisar en $($evento.MachineName)
Identificador: $($evento.EventId)
Fuente: $($evento.Source)
Tipo: $($evento.EntryType)
Fecha / Hora: $($evento.TimeGenerated)
Texto: $($evento.Message)
"@
$smtpClient = New-Object System.Net.Mail.SmtpClient($smtpServer, 587)
$smtpClient.EnableSsl = $true
$smtpClient.Credentials = New-Object System.Net.NetworkCredential("UserE-MailWithout@~~~~", "Password")
$smtpClient.Send($from, $to, $subject, $body)
```

The screenshot shows the Windows Event Viewer window titled "SERVIDOR2019 Alejandro Becerra (Despues de recuperar el equipo) [Corriendo] - Oracle VM VirtualBox". The left pane shows navigation categories like "Visor de eventos (local)", "Registros de Windows", "Registros de aplicaciones y servicios", and "Suscripciones". The right pane displays the "Seguridad" log with 38,427 events. A context menu is open over an event entry for "Error de autenticación" on 10/12/2019 at 10:08:43. The menu options include "Propiedades de evento", "Adjuntar tarea a este evento...", "Copiar", "Guardar eventos seleccionados...", "Actualizar", and "Ayuda". The event details show it was generated by Microsoft and has ID 4625 with category Logon. The "Acciones" pane on the right also lists "Seguridad" and "Evento 4625, Microsoft ..." with their own set of actions like "Propiedades de ev...", "Adjuntar tarea a es...", "Copiar", "Guardar eventos se...", "Actualizar", and "Ayuda". The status bar at the bottom indicates "13:05 18/12/2019" and "CTRL DERECHA".

SERVIDOR2019 Alejandro Becerra (Después de hacer lo del email) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Administrador: Windows PowerShell ISE

Archivo Editar Ver Herramientas Depurar Complementos Ayuda

Visor.ps1

```

1 $from      = "servidor201903@gmail.com"
2 $smtpServer = "smtp.gmail.com"
3 $to        = "alex.becerra.suarez@gmail.com"
4 $subject   = "Notificación de $($env:computername)"
5 $evento = Get-EventLog -LogName "Security" -Newest 1
6 $body = @"
7 Evento a revisar en $($evento.MachineName)
8 Identificador: $($evento.EventId)
9 Fuente: $($evento.Source)
10 Tipo: $($evento.EntryType)
11 Fecha / Hora: $($evento.TimeGenerated)
12 Texto: $($evento.Message)
13 "
14 $smtpClient = New-Object System.Net.Mail.SmtpClient($smtpServer, 587)
15 $smtpClient.EnableSsl = $true
16 $smtpClient.Credentials = New-Object System.Net.NetworkCredential("servidor201903", "abc123.abc123.")
17 $smtpClient.Send($from, $to, $subject, $body)
18
19
20

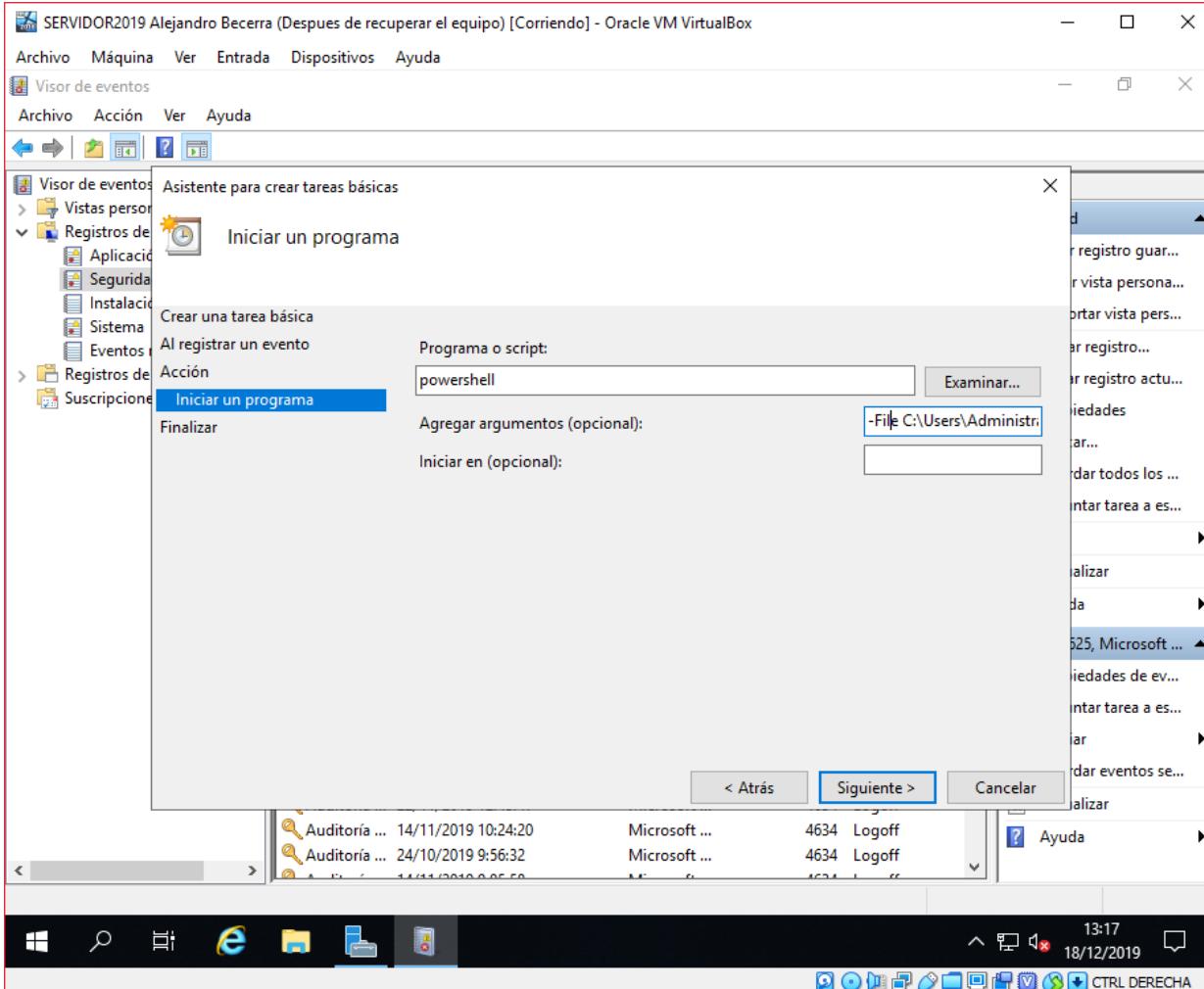
```

PS C:\Users\Administrador\Desktop>

Lín. 1 Col. 36 | 100 %

12:31 19/12/2019

CTRL DERECHA



SERVIDOR2019 Alejandro Becerra (Despues de recuperar el equipo) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Administrador del servidor

Panel

Propiedades de Acceso erroneo (Equipo local)

General Desencadenadores Acciones Condiciones Configuración Historial

Nombre: Acceso erroneo
Ubicación: \Tareas del Visor de eventos
Autor: DOMINIO201903\Administrador
Descripción:

Opciones de seguridad

Al ejecutar la tarea, usar esta cuenta de usuario: Administrador Cambiar usuario o grupo...

Ejecutar solo cuando el usuario haya iniciado sesión
 Ejecutar tanto si el usuario inició sesión como si no
 No almacenar contraseña. La tarea solo tendrá acceso a los recursos del equipo local.
 Ejecutar con los privilegios más altos

Oculta Configurar para: Windows Vista™, Windows Server™ 2008 Aceptar Cancelar

Acciones

Tareas del Visor de e... ▾

- Crear tarea básica...
- Crear tarea...
- Importar tarea...
- Mostrar todas l...
- Deshabilitar el h...
- Nueva carpeta...
- Eliminar carpeta

Ver Actualizar Ayuda

Elemento selecciona... ▾

- Ejecutar
- Finalizar
- Deshabilitar
- Exportar...
- Propiedades

13:21 18/12/2019 CTRL DERECHA

Curso: Impl UNIDAD 5 Práctica 7 V enviar corre Enviar corre Notific + X

https://mail.google.com/mail/u/0/#inbox/FMfcgxwGCOZDqpzPzlVRNrnzkhFVTI

Gmail Buscar correo Redactar

Recibidos 79

Destacados
Postpuestos
Enviados
Borradores 2
[Imap]/Sent
[Imap]/Trash 289
Más

Alejandro +

M Mercedes Vázquez Vázquez
Noela 78

Notificación de SERVIDOR201903 Recibidos x

servidor201903@gmail.com 12:29 (hace 5 minutos) Evento a revisar en SERVIDOR201903.dominio201903.local Identificador: 4634 Fuent...

servidor201903@gmail.com 12:31 (hace 3 minutos) para mí Evento a revisar en SERVIDOR201903.dominio201903.local Identificador: 4625 Fuent...

Sujeto:
Id. de seguridad: S-1-5-18
Nombre de cuenta: SERVIDOR201903\$
Dominio de cuenta: DOMINIO201903
Id. de inicio de sesión: 0x3e7

Tipo de inicio de sesión: 2

Cuenta con error de inicio de sesión:
Id. de seguridad: S-1-0-0
Nombre de cuenta: Administrador
Dominio de cuenta: DOMINIO201903

Información de error:
Motivo del error: %%2313
Estado: 0xc000006d
Subestado: 0xc000006a

Información de proceso:
Id. de proceso del autor de la llamada: 0x4cc
Nombre de proceso del autor de la llamada: C:\Windows\System32\svchost.exe

Información de red:
Nombre de estación de trabajo: SERVIDOR201903
Dirección de red de origen: 127.0.0.1