

TAREFAS ADMINISTRATIVAS

CON WINDOWS SERVER 2019

Índice (empregar a pestana de marcadores a modo de índice interactivo)

0. Consideracións previas	3
A. Compartir unha impresora do controlador de dominio	4
B. Copias de seguridade e recuperación	9
C. Copia de seguridade programada	13
D. Recuperación completa do sistema dende unha copia de respaldo	15
E. Tarefas programadas	18
F. Visor de eventos	21

0. Consideracións previas

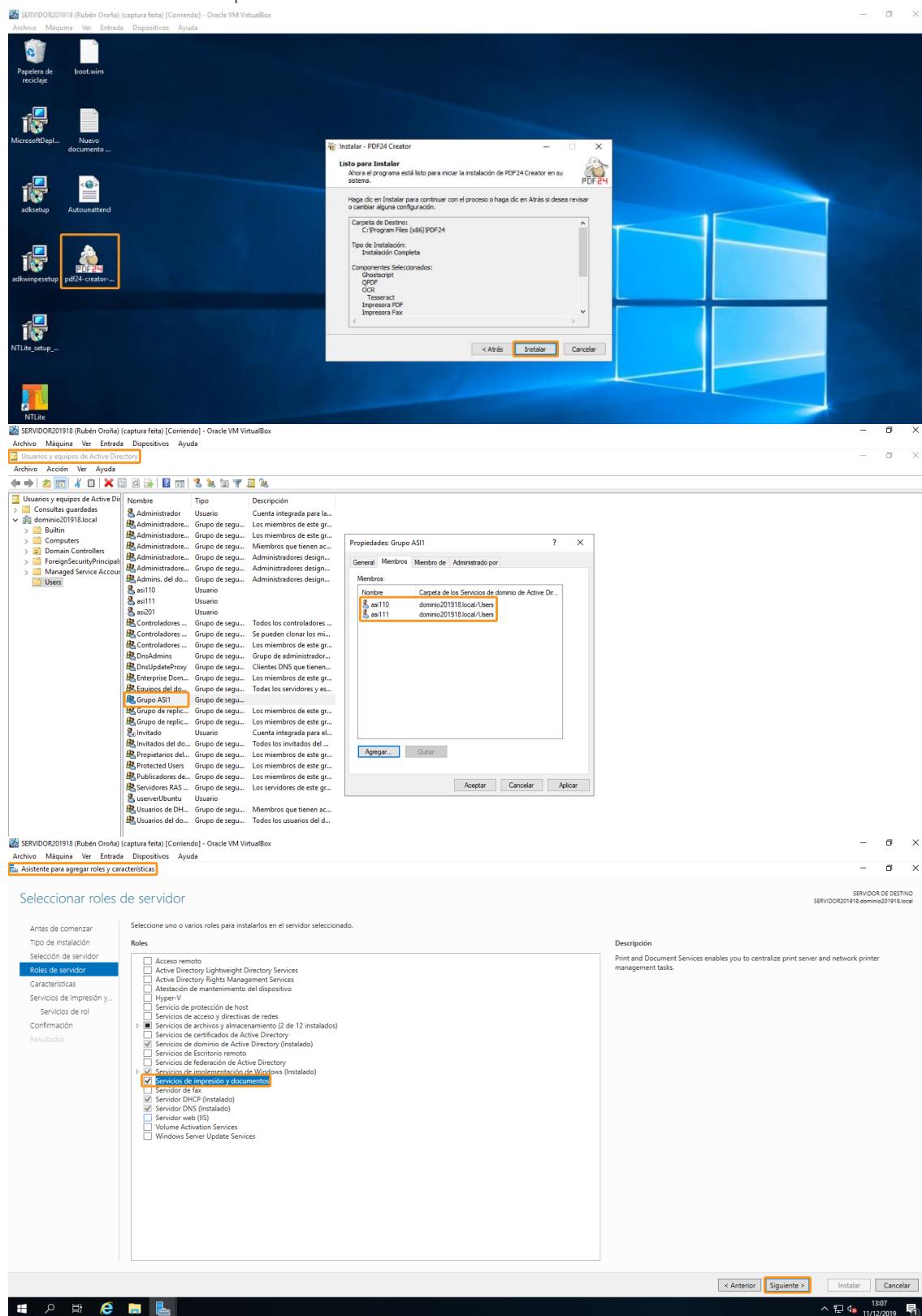
Para levar a cabo a instalación remota empregaremos o servidor Windows Server 2019 creado en prácticas anteriores, no que instalaremos os controladores de impresora e copia de seguridade. Así pois, poderemos compartir unha impresora no dominio, crear e restaurar copias de seguridade puntuais e programadas, programar tarefas e emplegar o visor de eventos.

Tanto o servidor como os clientes foron creados como máquinas virtuais empregando o software Oracle VM VirtualBox (versión 6.0.12). A modo de resumo, amosamos unha táboa que recolle a nomenclatura e configuración IP do servidor.

Sistema operativo:	Windows Server 2019
Nome do equipo:	SERVIDOR201918
Nome dominio:	dominio201918.local
Dirección IP:	192.168.18.12
Máscara de subrede:	255.255.255.0
Porta de enlace:	192.168.18.1
DNS preferido:	127.0.0.1
DNS alternativo:	10.42.68.254

A. Compartir unha impresora do controlador de dominio

Comezamos por instalar de maneira local o software pdf24. O obxectivo é compartila mediante o dominio, permitindo o seu uso a un grupo específico de usuarios. Este será o Grupo ASI1, que podemos crear dende o Active Directory. A continuación, debemos instalar o rol de servizos de impresión.



Dende o administrador de impresión recentemente instalado, premos en agregar controlador para poder compartir a impresora pdf24. Na pestana de compartir, habilitamos as xanelas para presentar os traballos en equipos cliente e para amosar a lista no directorio. Por último, na pestana de seguridade desactivamos a impresión para o grupo Todos, xa que o que queremos é habilitala unicamente para os usuarios do Grupo ASI1.

The screenshots illustrate the configuration of the PDF24 printer in the Windows Print Management interface:

- Screenshot 1:** Shows the 'Controladores' (Drivers) section of the 'Administración de impresión' (Print Management) window. A context menu is open over the PDF24 driver, with the 'Compartir' (Share) option highlighted.
- Screenshot 2:** Shows the 'Propiedades de PDF24' (PDF24 Properties) dialog box. The 'Compartir' tab is selected. The 'Compartir esta impresora' (Share this printer) checkbox is checked, and the 'Recurso compartido:' field contains 'ImpASI'. The 'Presentar trabajos de impresión en equipos cliente' (Share print jobs with client computers) and 'Mostrar lista en el directorio' (Show list in directory) checkboxes are also checked. The 'Seguridad' (Security) tab is selected in the dialog title bar.
- Screenshot 3:** Shows the 'Propiedades de PDF24' dialog box again, but with the 'Seguridad' tab selected. It displays security settings for the printer, including a list of security groups and specific permissions for the 'Todos' (Everyone) group and the 'Grupo ASI1' (ASI1 Group) group. The 'Imprimir' (Print) permission is checked for both groups.

A continuación, facemos login nun cliente que pertenza ó Grupo ASI1, para agregar a impresora compartida. Un último cambio que deberemos facer dende o servidor é modificar o directorio de destino dos arquivos de impresión, para situala nun cartafol público e accesible para os clientes.

CLIENTE1018_Remoto (práctica 4) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Papelera de reciclaje

Más usados

- Introducción
- Descargar Skype
- Mapas
- Contactos
- Calculadora
- Alarma y reloj

La vida en un vistazo

- Calendario
- Correo
- Xbox
- Música
- Películas y TV
- Fotos
- Búsqueda
- Dinero
- Noticias
- El Tiempo
- Complementos
- OneNote
- Tienda
- Microsoft Solitaire Collection
- Get Office

Jugar y explorar

Explorador de archivos >

Configuración

Iniciar/Apagar

Todas las aplicaciones

Buscar en la web y en Windows

12:39 13/12/2019

CTRL DERECHA

CLIENTE1018_Remoto (práctica 4) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Dispositivos e impresoras

← → ↑ ↓ Panel de control > Hardware y sonido > Dispositivos e impresoras

Agregar dispositivo Agregar una impresora

Dispositivos (4)

- Monitor genérico que no es PnP
- CLIENTE1018
- Microfono (Dispositivo de High Definition Audio)
- USB Tablet

Impresoras (3)

- Fax
- Microsoft Print to PDF
- Microsoft XPS Document Writer

Agregar dispositivo

Elegir un dispositivo o una impresora para agregar a este equipo

PDF24 en SERVIDOR201918 Impresora

Siguiente Cancelar

SERVIDOR201918 (Rubén Oroña) [captura feita] [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Opciones PDF24 Creator - ADMIN

General

Asistente

Barra de Botones

Impresora virtual PDF24

Contexto del menú de la interfaz

Online PDF Converter

Interfaz de email

Actualizaciones

Características

PDF24

General

Los usuarios pueden modificar los ajustes en esta área

Herramienta de impresión PDF

Abrir el archivo PDF en el Asistente.

Abrir el archivo PDF en el Editor.

Guardar los documentos automáticamente después de imprimirlos

Cargar el archivo PDF en el Editor si éste ya está abierto.

Guardado automático

Directorio de destino: C:\Users\Public\Documents\Impresora ASI1

Nombre del archivo: %Y-%m-%d %H-%M-%S %file Name%

Calidad: Calidad Superior

Mostrar progreso mientras guarda

Abrir el directorio de destino después de guardar el archivo

Sobreescribir el fichero existente

Use un selector de nombre de archivo

Guardar con PDF24 Windows Service

Guardar como este usuario

Requerir un usuario autenticado en la instancia pdf24.exe

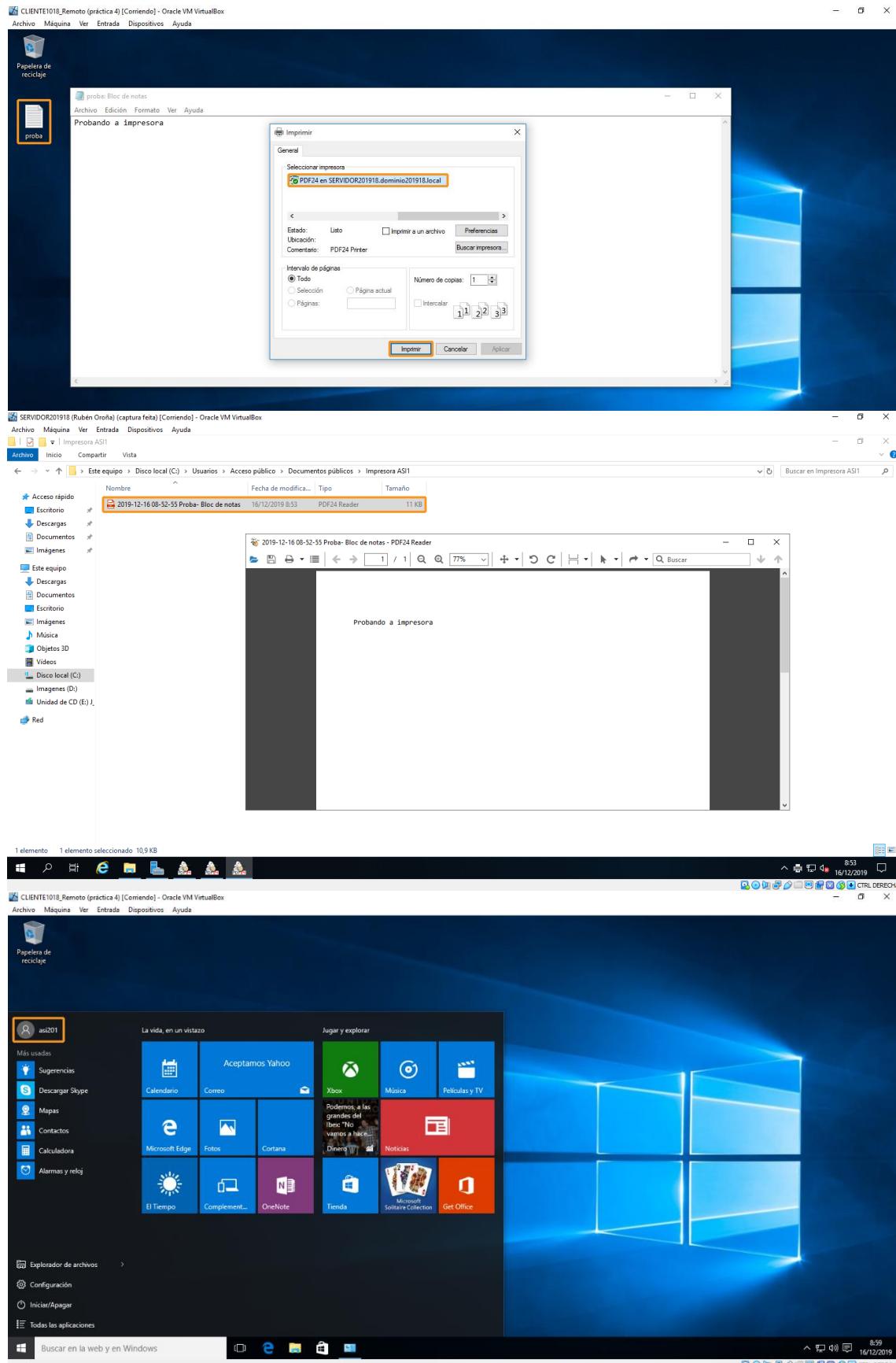
Ejecutar el siguiente comando después de guardar

Aceptar Aplicar Cancelar

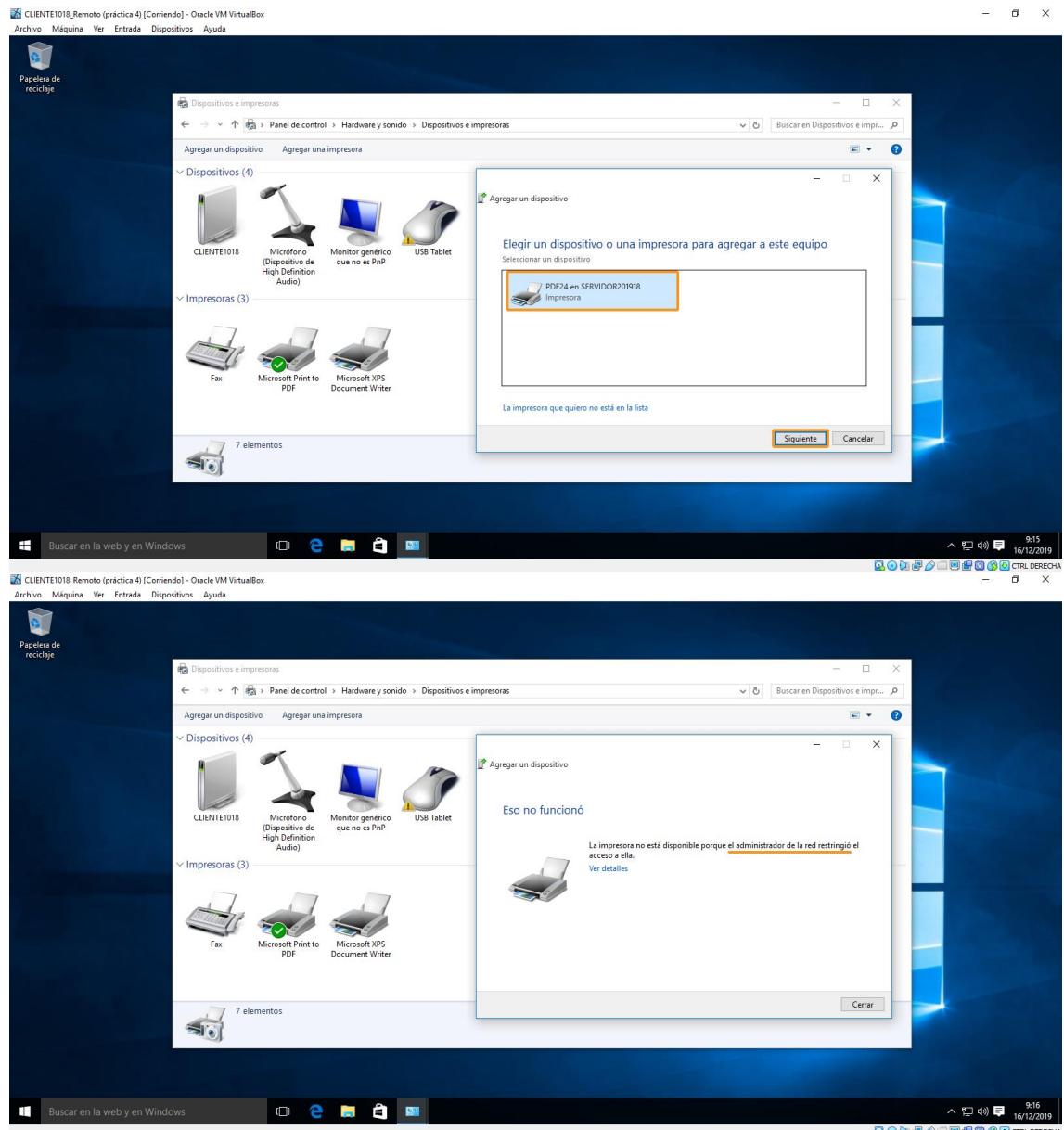
Todos los usuarios

CTRL DERECHA

Se facemos unha impresión de proba dende este cliente, poderemos comprobar que o arquivo .pdf aparece no cartafol configurado con anterioridade. A modo de contraposición, trataremos de instalar a impresora dende un usuario fóra do grupo compartido.



Como podemos observar, non somos capaces de agregar a impresora, pois temos o seu acceso restrinxido.



B. Copias de seguridad e recuperación

Para gardar as copias de seguridad, primeiro necesitamos crear un disco duro novo, que dedicaremos exclusivamente para as bakcups. Unha vez formateado, engadimos a característica para as copias de seguridad dende o administrador do servidor.

The screenshot shows the Windows Server 2019 Disk Management console. It lists three disks:

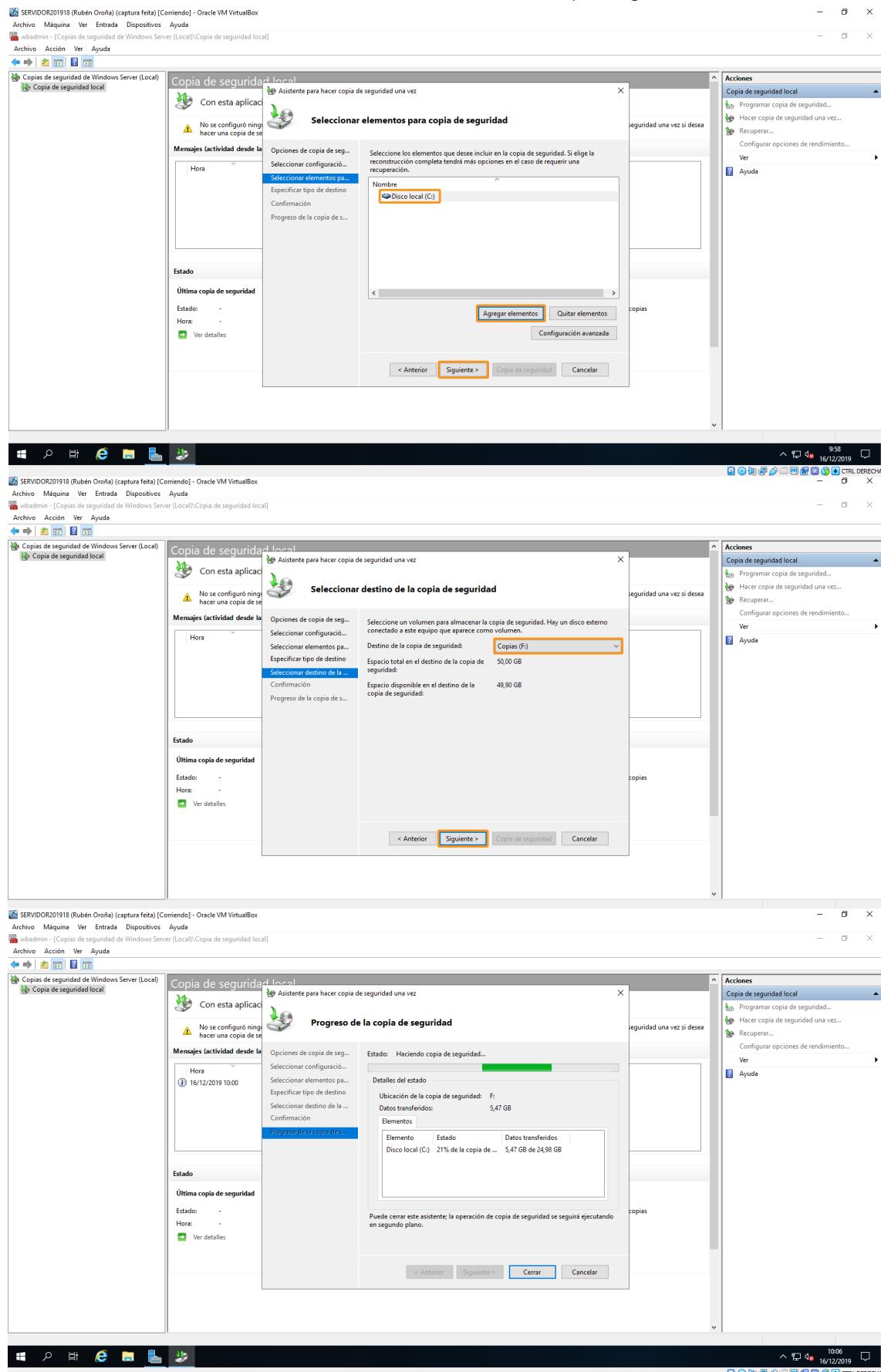
- Disk 0:** Basic, 50,00 GB, En pantalla. Contains partition (C): Sistema, Activo, Partición primaria.
- Disk 1:** Basic, 50,00 GB, En pantalla. Contains partition (D): Imagenes (D).
- Disk 2:** Basic, 50,00 GB, En pantalla. Contains partition (E): Copias (E:).

A context menu is open over Disk 2, with the option "Copias de seguridad de Windows Server" highlighted.

The screenshot shows the "Asistente para agregar roles y características" (Role and Feature Wizard) in the "Características" (Features) step. The "Copias de seguridad de Windows Server" checkbox is selected. Other options like "Administración de almacenamiento basada en est..." and "Administración de directivas de grupo (Instalado)" are also listed.

The screenshot shows the "Copia de seguridad local" (Local Backup) wizard in the "Seleccionar configuración de copia de seguridad" (Select backup configuration) step. The "Personalizada" (Custom) radio button is selected. Other options like "Servidor completo (recomendado)" and "Seleccionar elementos pa..." are available.

A continuación, prememos en crear copia de seguridad unha vez para realizar un backup do disco (C:) Como destino do mesmo escollemos o disco que engadimos antes.

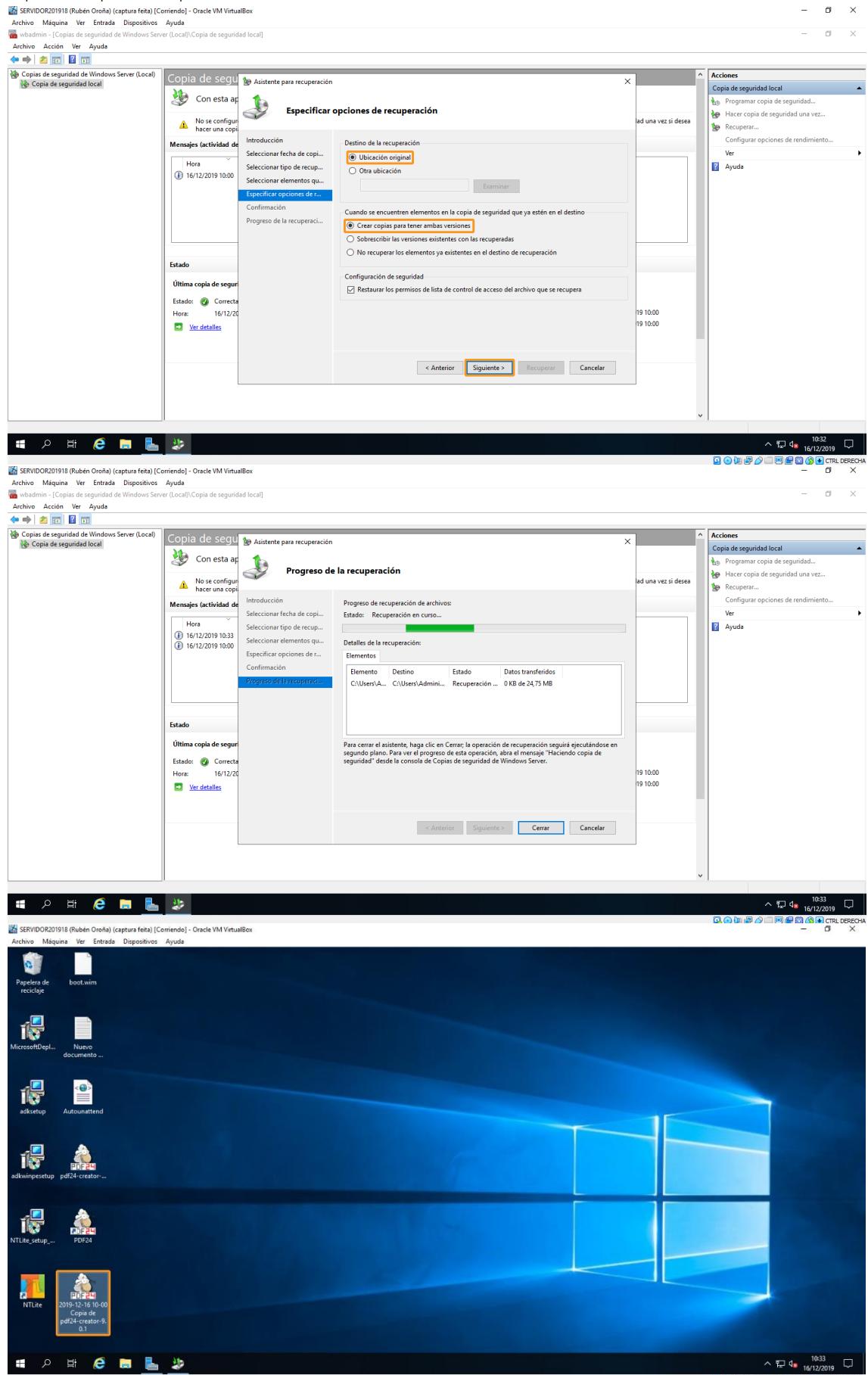


Agora trataremos de recuperar un arquivo específico da copia anterior, neste caso collemos o executable do pdf24 como exemplo.

The screenshots illustrate the process of recovering the `pdf24-creator-9.0.1.exe` file using the Windows Server 2019 Recovery Wizard:

- Step 1: Introducción (Introduction)**
Shows the initial screen of the Recovery Wizard. The "Este servidor (SERVIDOR201918)" radio button is selected under "Donde está la copia de seguridad almacenada que desea usar para la recuperación?". The "Siguiente >" (Next) button is highlighted.
- Step 2: Seleccionar tipo de recuperación (Select recovery type)**
Shows the selection screen. The "Archivos y carpetas" radio button is selected under "¿Qué desea recuperar?". The "Siguiente >" (Next) button is highlighted.
- Step 3: Seleccionar elementos que se van a recuperar (Select items to recover)**
Shows the file selection screen. The `pdf24-creator-9.0.1.exe` file is selected in the "Elementos disponibles" (Available items) tree view under "Desktop". The "Siguiente >" (Next) button is highlighted.

Optamos por recuperarlo na ubicación orixinal, sen substituílo.



C. Copia de seguridad programada

O seguinte paso da práctica consiste en configurar unha backup diaria. Escollemos a opción de programar copia de seguridade, e establecemos que se realice unha ó día.

Screenshot 1: Seleccionar configuración de copia de seguridad

Introducción: ¿Qué tipo de configuración desea programar?

- Servidor completo (recomendado)
- Personalizada

Deseo hacer una copia de seguridad de todos los datos del servidor, las aplicaciones y el estado del sistema.

Tamaño de copia de seguridad: 56,83 GB

Screenshot 2: Seleccionar elementos para copia de seguridad

Introducción: Seleccione los elementos que desea incluir en la copia de seguridad. Si elige la reconstrucción completa tendrá más opciones en el caso de requerir una recuperación.

Nombre: Imágenes (D:\)

Screenshot 3: Especificar hora de copia de seguridad

Introducción: Con qué frecuencia y cuándo desea ejecutar copias de seguridad?

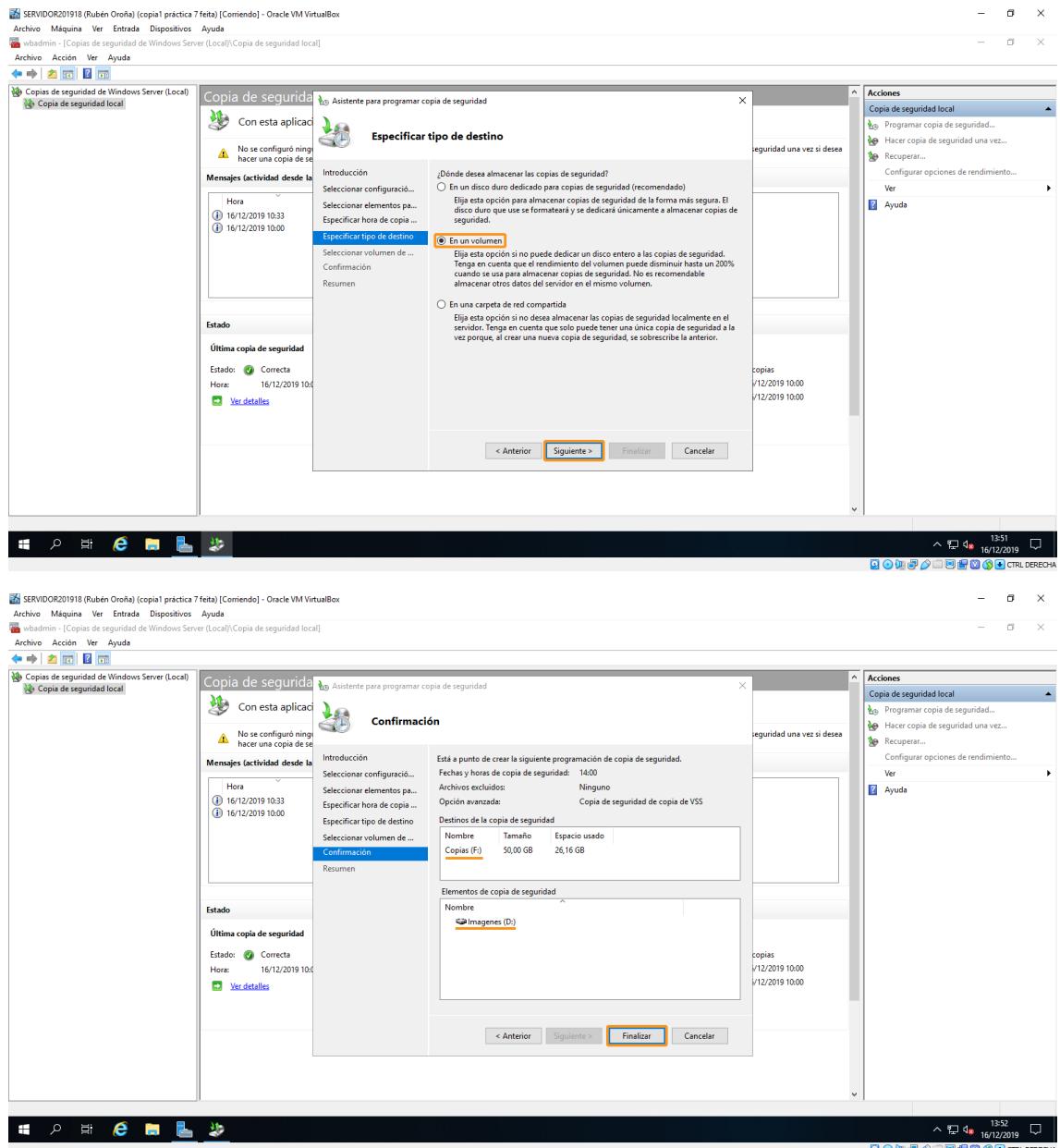
- Una vez al día
- Más de una vez al día

Seleccionar hora del día: 14:00

Hora disponible: 0:00, 0:30, 1:00, 1:30, 2:00, 2:30, 3:00, 3:30, 4:00, 4:30

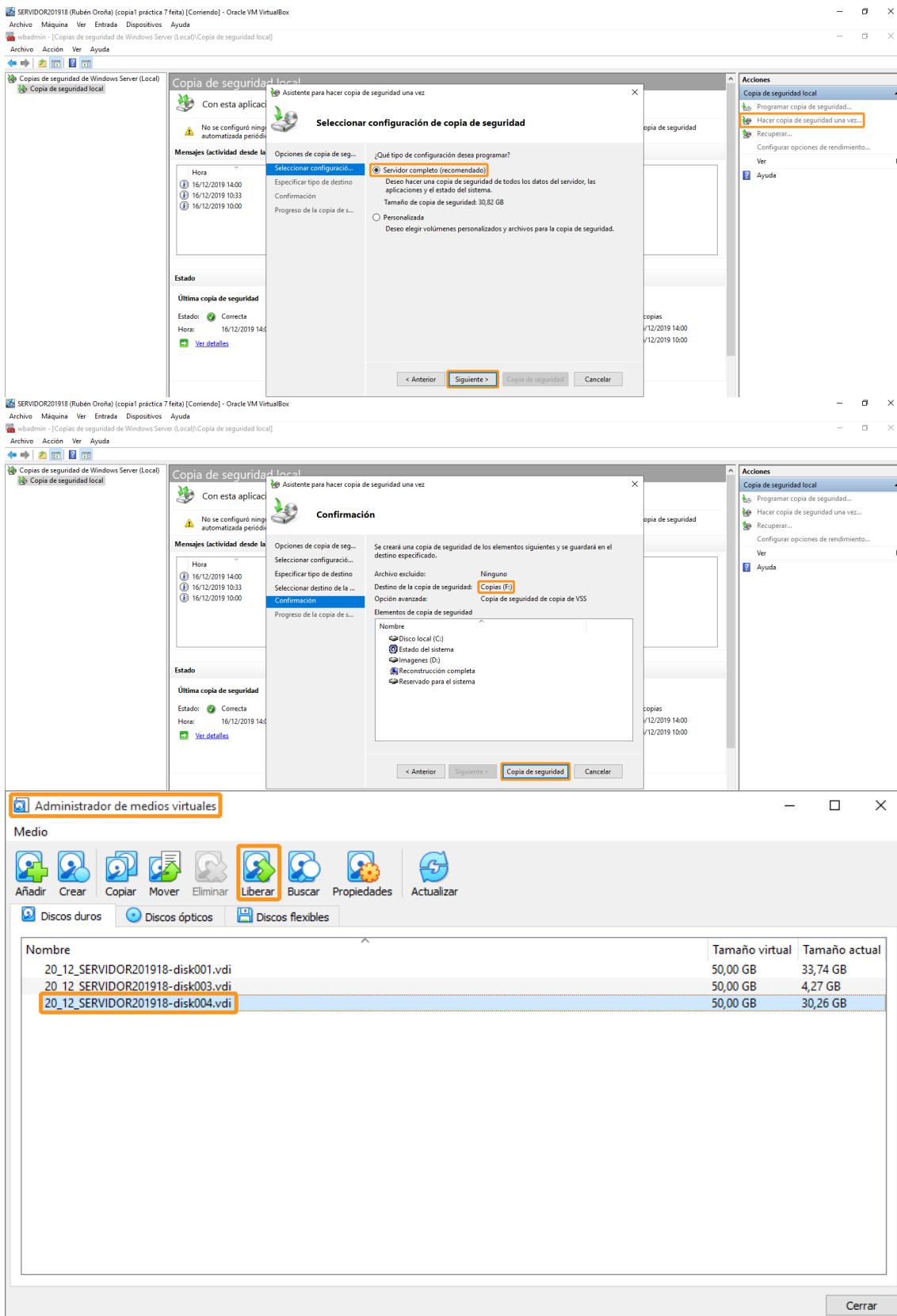
Hora programada: 21:00

O destino final da copia de segurança será o disco de cópias empregado anteriormente.

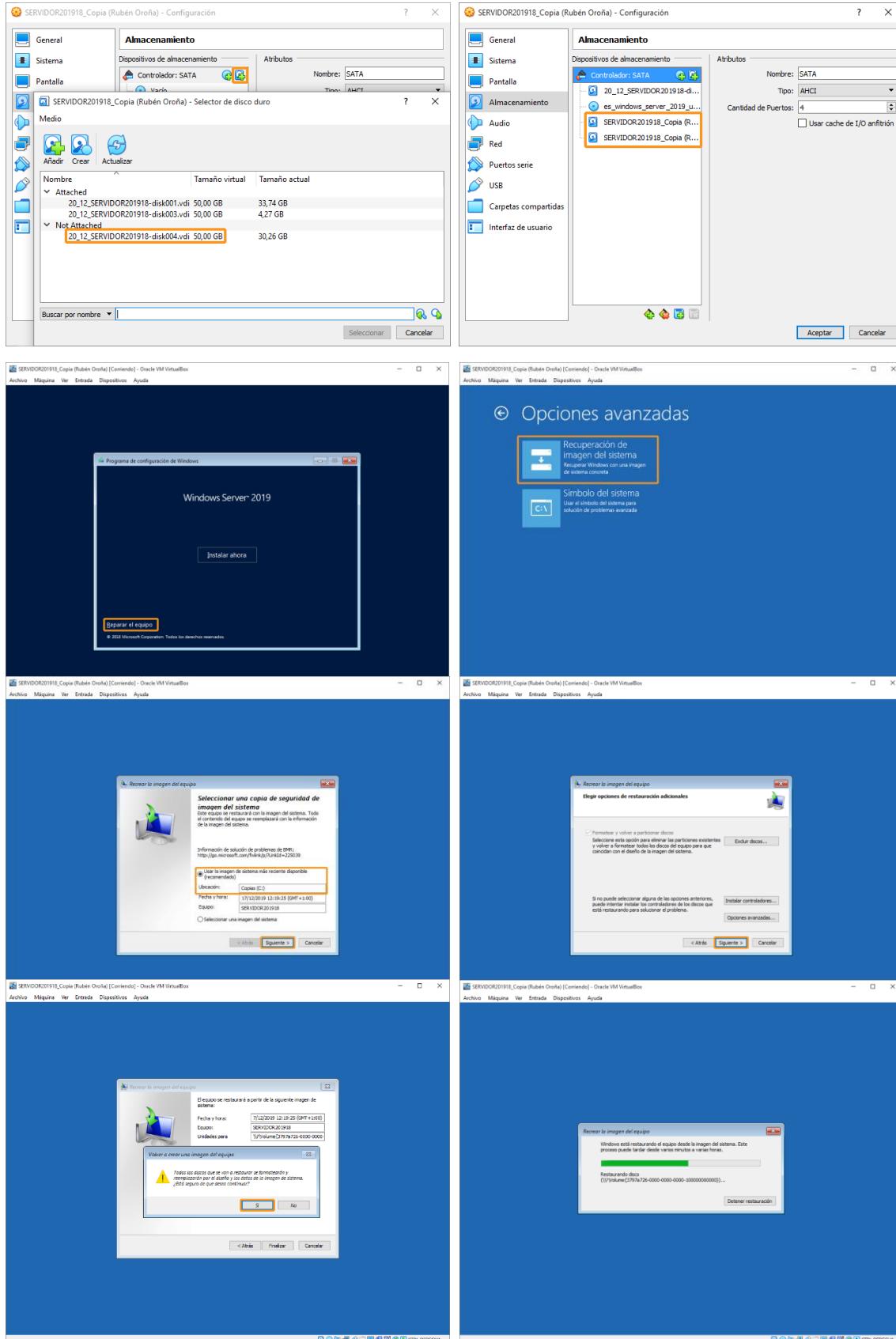


D. Recuperación completa do sistema dende unha copia de respaldo

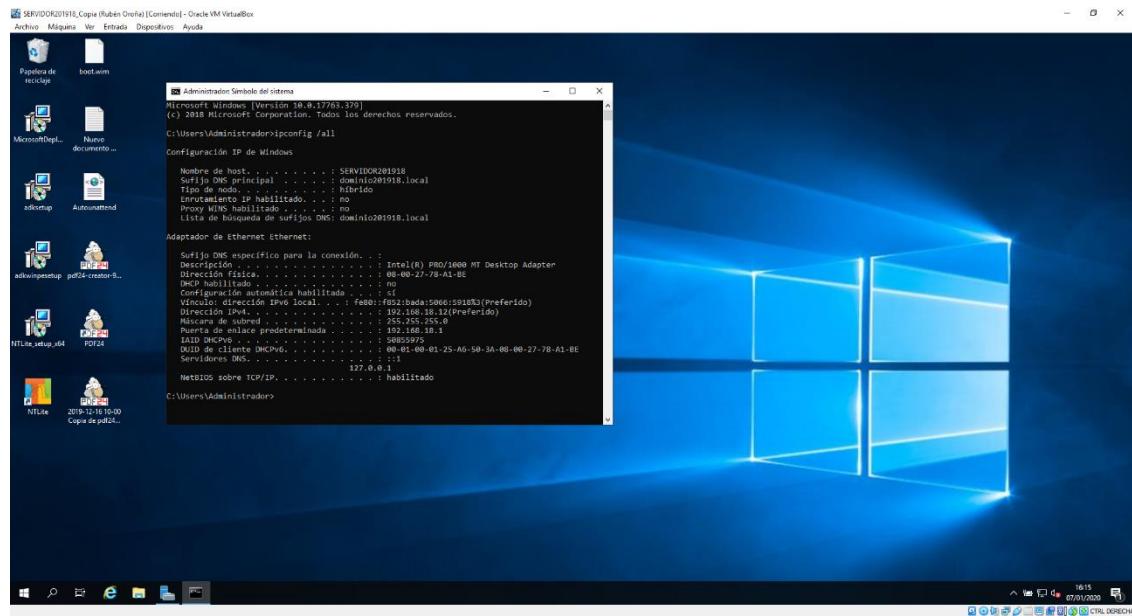
Imos realizar unha copia completa de todo o servidor, para poder empregala posteriormente nunha máquina baleira e recuperar o servidor. Unha vez realizado o backup, debemos ir ó administrador de medios virtuais de VirtualBox, onde liberamos este disco do servidor.



Agora, creamos a máquina nova co disco de backups xa liberado. Ademais, como no servidor orixinal tiñamos un disco principal mais o de imaxes, deberemos crear dous baleiros a maiores para unha correcta recuperación do sistema. Por último, engadimos o disco de instalación na unidade óptica.

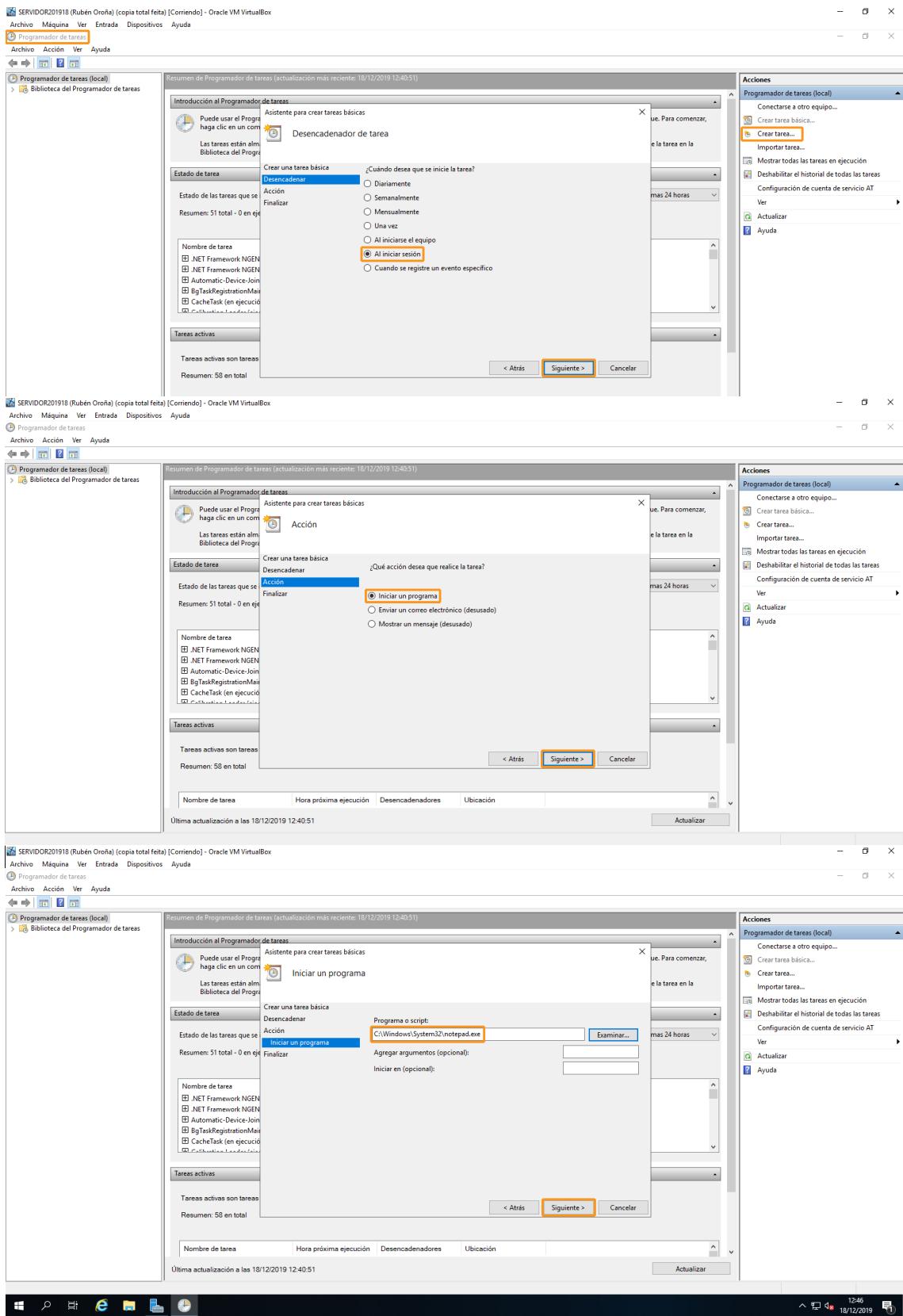


Mediante o arranque por CD, prememos en reparar equipo e recuperar imaxe do sistema. Vemos como se detecta de maneira automática o disco das copias de seguridade, dando comezo a unha instalación que se dilata no tempo uns corenta minutos. Tras iso, vemos que recuperamos o servidor tal e como o deixáramos.

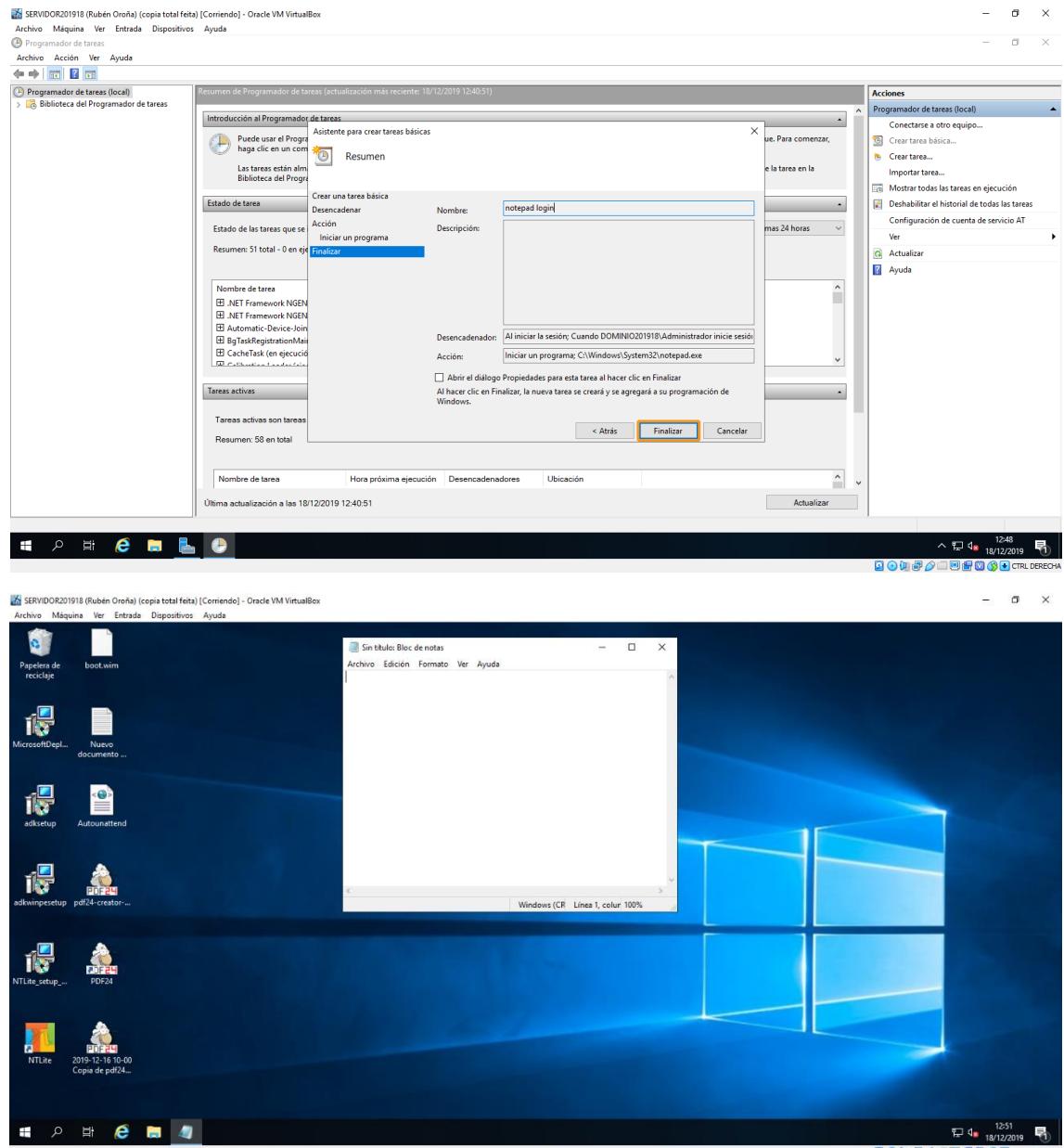


E. Tareas programadas

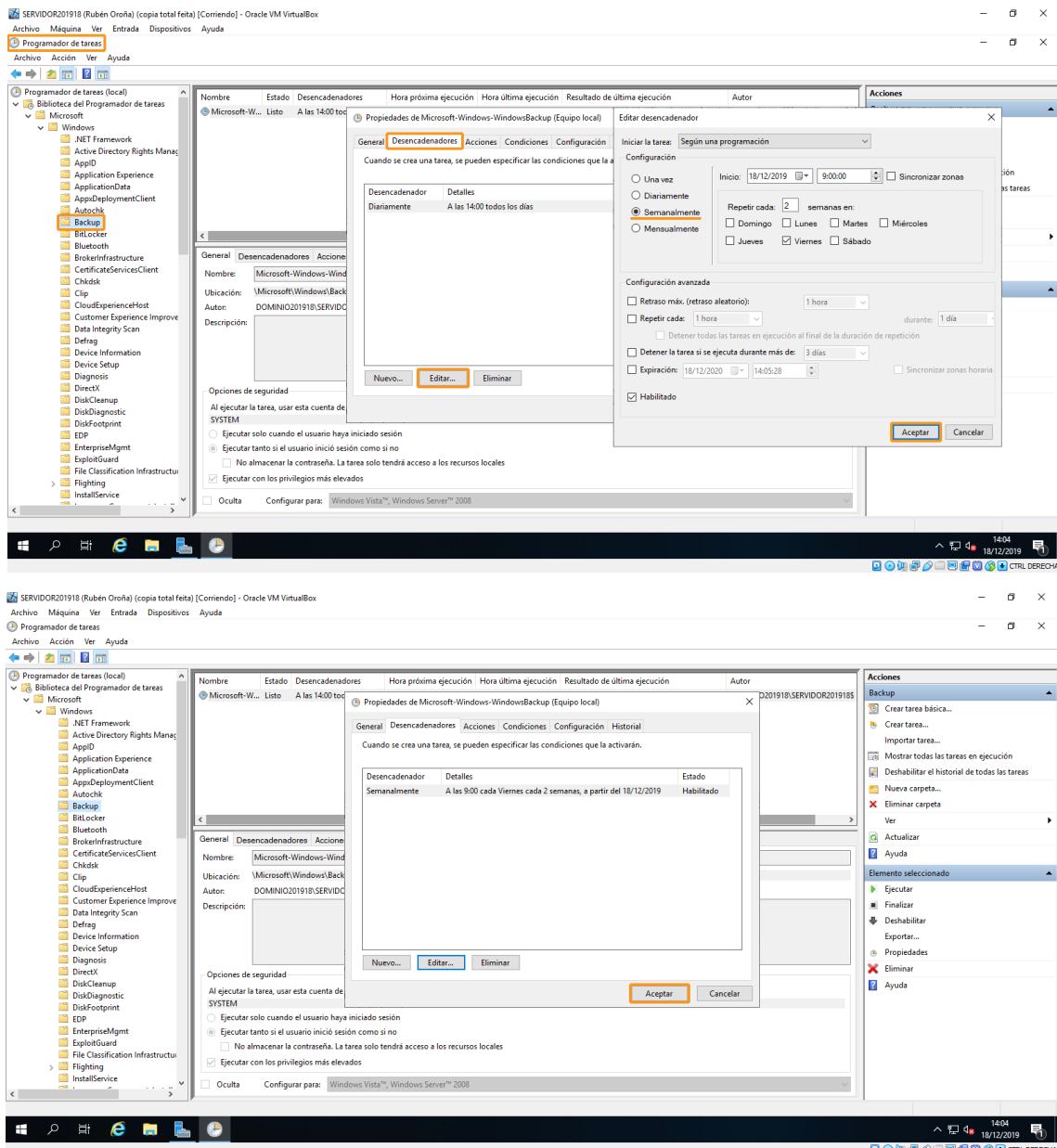
A tarea que desexamos configurar será a de abrir un bloc de notas cada vez que haxa un login correcto no servidor. Resulta moi sinxelo, pois basta con crear unha nova tarefa ó iniciar sesión, que execute un programa deseado. No noso caso, o notepad.



Unha vez configurada a tarefa, cerramos sesión e volvemos a facer login. Comprobamos desta maneira que o bloc de notas se executa correctamente..



A outra tarefa que realizaremos será a de modificar a cópia de segurança programada feita com anterioridade. Agora queremos que seja só todos os dias, em vez de diária. Usamos o menu da esquerda para atopar a tarefa referida a backups, e editamos os desencadeadores.



F. Visor de eventos

Imos comenzar por crear una vista personalizada que nos permita visualizar todos los login incorrectos en el servidor durante el último mes. Para ello, premos en crear vista personalizada e referímosla al error 4625. Agora imos crear un script que se execute cuando se produza este tipo de incidencia. No noso caso, será enviar un email que configuraremos desde o Powershell.

The screenshot shows the Windows Event Viewer interface. A context menu is open on the right side, with the option "Crear vista personalizada..." selected. This opens a dialog box titled "Crear vista personalizada" where the filter is set to "Últimos 30 días" and the event ID is set to "4625". The dialog also includes fields for "Categoría de la tarea:" (set to "4625"), "Palabras clave:", "Usuario:", and "Equipo(s:)". The "Aceptar" button is highlighted with a yellow box. Below this, the main Event Viewer window displays a list of events under the "ErrorLogin" view, which has 4 events. The details pane shows the first event, which is an information event from Microsoft Windows security auditing with the message "Error de una cuenta al iniciar sesión." The event ID is 4625, and the source is Logon. The bottom part of the screen shows a PowerShell window running on the server, with commands related to changing execution policies and creating a directory for scripts.

Creamos un mail de proba que será o que envíe os correos, sendo unha conta persoal a receptora dos mesmos. Empregaremos os servidores de google para o proceso. Comprobamos así que o script funciona correctamente facendo unha proba.

The screenshot shows a Windows desktop environment with two open PowerShell windows and a Gmail inbox window.

Top PowerShell Window:

```

$From      = "servidor201918@gmail.com"
$smtpServer = "smtp.gmail.com"
$To        = "rubenmoroandomiguez@gmail.com"
$Subject   = "Notificación de $($env:computername)"
$Event     = Get-EventLog -LogName "Security" -Newest 1
$Body      = $Event[0].Message
$EmailBody = "Evento a revisar en $($Event.MachineName)  
Identificador: $($Event.EntryId)  
Fuente: $($Event.Source)  
Tipo: $($Event.EntryType)  
Fecha / Hora: $($Event.TimeGenerated)  
Texto: $($Event.Message)  
"
$SmtpClient = New-Object System.Net.Mail.SmtpClient($smtpServer, 587)
$SmtpClient.EnableSsl = $true
$SmtpClient.Credentials = New-Object System.Net.NetworkCredential("servidor201918", "abc123.ABC")
$SmtpClient.Send($From, $To, $Subject, $Body)

```

Bottom PowerShell Window:

```

PS C:\Users\Administrador> $from      = "servidor201918@gmail.com"
$smtpServer = "smtp.gmail.com"
$To        = "rubenmoroandomiguez@gmail.com"
$Subject   = "Notificación de $($env:computername)"
$Event     = Get-EventLog -LogName "Security" -Newest 1
$Body      = $Event[0].Message
$EmailBody = "Evento a revisar en $($Event.MachineName)  
Identificador: $($Event.EntryId)  
Fuente: Microsoft-Windows-Security-Auditing  
Tipo: SuccessAudit  
Fecha / Hora: 12/19/2019 12:08:16  
Texto: Se cerró sesión en una cuenta.  
"
$SmtpClient = New-Object System.Net.Mail.SmtpClient($smtpServer, 587)
$SmtpClient.EnableSsl = $true
$SmtpClient.Credentials = New-Object System.Net.NetworkCredential("servidor201918", "abc123.ABC")
$SmtpClient.Send($From, $To, $Subject, $Body)

```

Gmail Inbox:

A message from "servidor201918@gmail.com" titled "Notificación de SERVER201918" is shown in the inbox. The message content is:

Evento a revisar en SERVER201918.dominio201918.local
Identificador: 4634
Fuente: Microsoft-Windows-Security-Auditing
Tipo: SuccessAudit
Fecha / Hora: 12/19/2019 12:08:16
Texto: Se cerró sesión en una cuenta.

Windows Event Viewer:

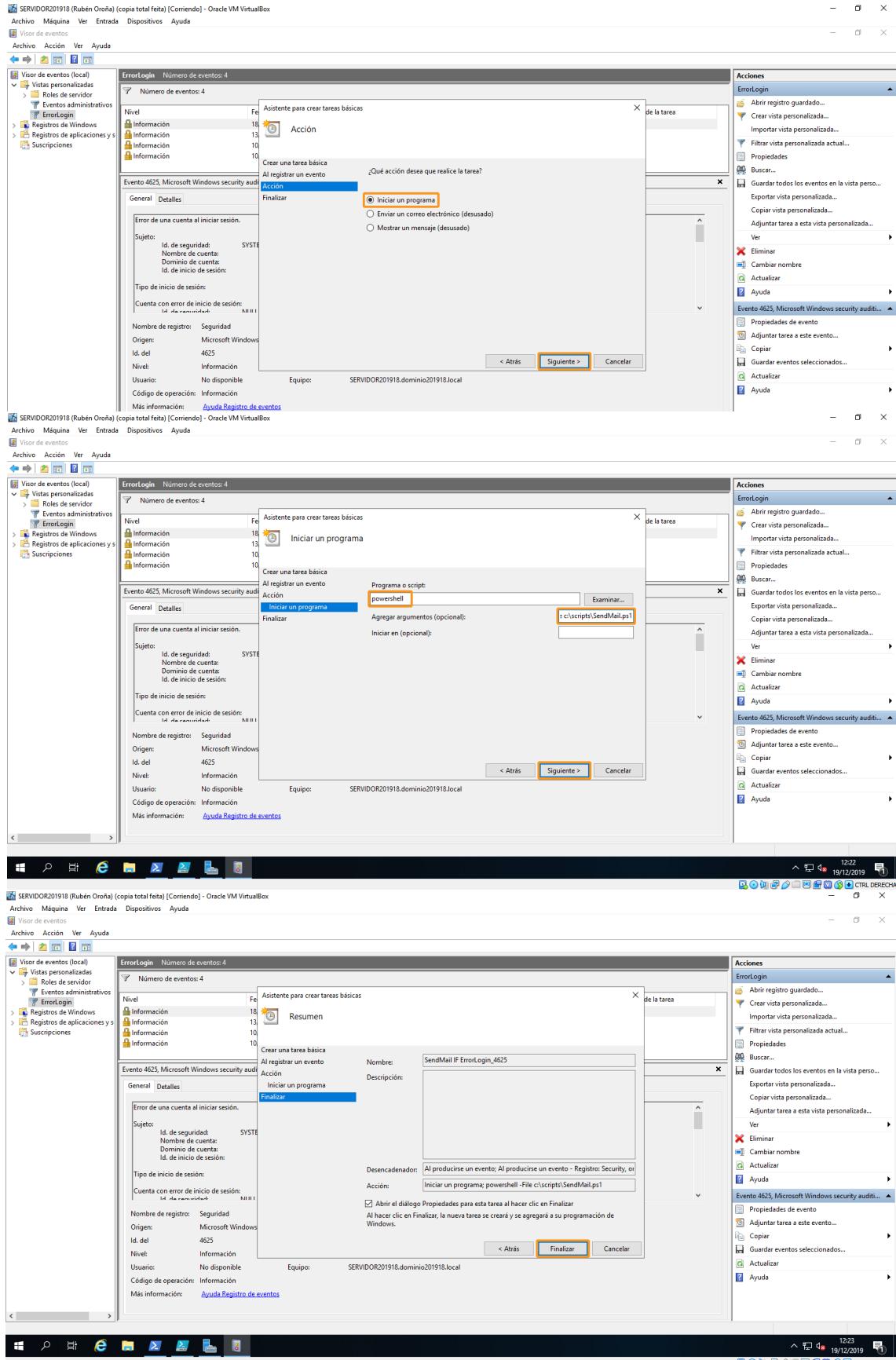
The Event Viewer shows an event titled "ErrorLogin" (Número de eventos: 4). The event details are:

Sujeto:
Id. de seguridad: S-1-5-18
Nombre de cuenta: SERVER201918\$
Dominio de cuenta: DOMINIO201918
Id. de inicio de sesión: 0x29946

General | Details

Nombre de registro: Seguridad
Origen: Microsoft Windows security audit... Registrado: 18/12/2019 13:57:48
Id. del evento: 4625 Categoría de tarea: Logon
Nivel: Información Palabras clave: Error de auditoría
Usuario: No disponible Equipo: SERVER201918.dominio201918.local
Código de operación: Información
Más información: Ayuda Registro de eventos

Agora imos a relacionar o script do mail co erro 4625, premendo en axustar tarefa a este evento. Escollemos que a tarefa sexa iniciar un programa, que será executado mediante o Powershell. Por último, deberemos indicar a ruta onde se atopa o noso script.



Para rematar, editamos as propiedades da tarefa creada, habilitando as xanelas para que se execute tanto si o usuario inicia sesión ou non, ademais de outorgarlle os privilexios de administrador. Como comprobación final, facemos un login erróneo, que provoca que recibamos o mail que da fin á práctica.

