

# GRUPOS, USUARIOS E PERMISOS EN CARTAFOLES COMPARTIDOS

**Índice** (empear a pestana de marcadores a modo de índice interactivo)

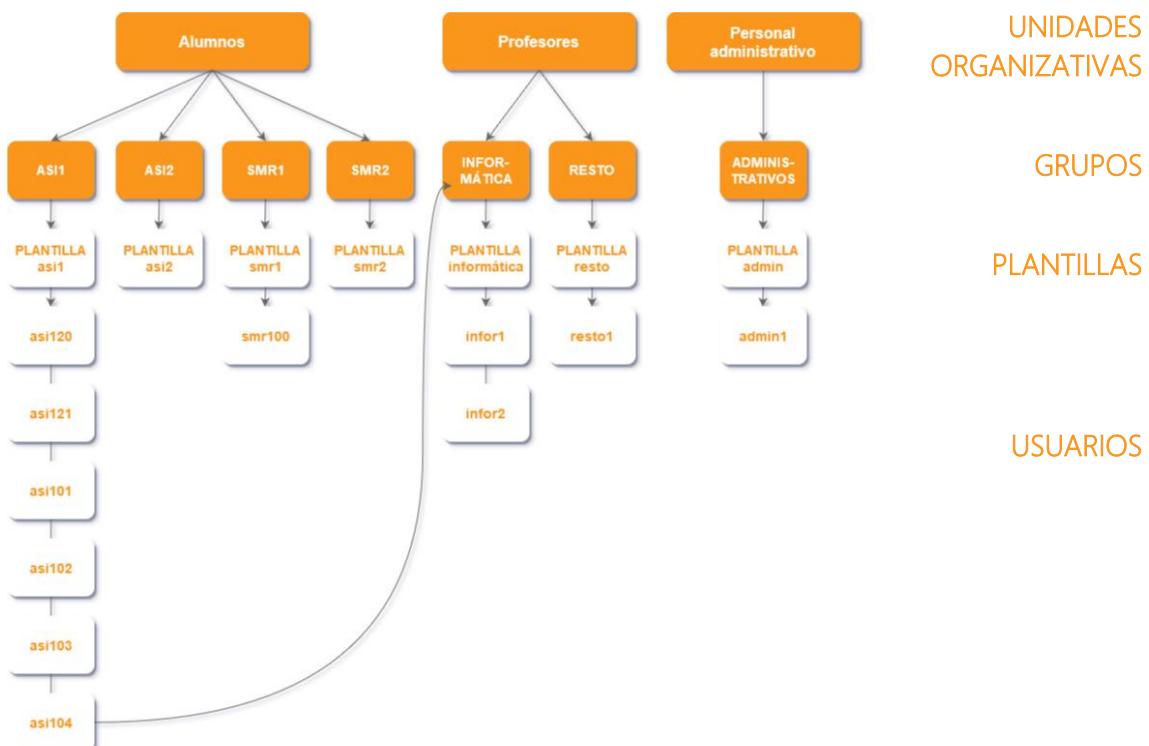
0. Consideracións previas	4
I. Nomenclatura e configuración IP do servidor	4
II. Árbore das unidades organizativas, grupos e usuarios	4
A. Creación das unidades organizativas, grupos e plantillas	5
I. Crear tres unidades organizativas	5
II. Crear os diferentes grupos	6
III. Crear unha plantilla para cada grupo	7
IV. Crear os usuarios asi120 e asi121	10
B. Cartafol PRÁCTICAS compartido para o grupo ASI1	11
I. Crear un cartafol chamado PRÁCTICAS	11
II. Outorgar acceso por rede a ASI1	11
III. Dar control total á identidade Creator Owner	11
IV. Deshabilitar a herdanza de permisos	12
V. Engadir o grupo ASI1	12
C. Comprobación dos usuarios smr100, asi120, asi121	14
D. Configuración dos usuarios asi101, asi102 e asi103	17
I. Crear os tres usuarios	17
II. Denegar permisos de escritura ó usuario asi101	18
III. Denegar a creación de archivos ó usuario asi102	18
IV. Agregar o usuario asi103	19
E. Comprobación dos usuarios smr100, asi120, asi121	20
I. Facer login con asi101	20
II. Facer login con asi102	21
III. Facer login con asi103	23

F. Cartafol COMÚN_PROFESORES compartido	<b>25</b>
I. Crear o cartafol COMÚN_PROFESORES	25
II. Outorgar acceso por rede a Informáticos e Resto	25
III. Deshabilitar a herdanza de permisos	25
IV. Engadir o grupo Resto	26
V. Outorgar control total ó grupo Informática	27
VI. Crear usuarios en ambos grupos	27
VII. Facer unha excepción co usuario infor1	28
G. Comprobación dos usuarios infor1, infor2 e resto1	<b>29</b>
I. Facer login co usuario infor2	29
II. Facer login co usuario infor1	29
III. Facer login co usuario resto1	32
H. Dar permisos de profesor a un alumno	<b>34</b>
I. Engadir o usuario asi104 ó grupo Informática	34
II. Acceder con asi104 no cartafol COMÚN_PROFESORES	35
III. Acceder con asi104 no cartafol PRÁCTICAS	36
I. Configuración por defecto de permisos na raíz do disco C:	<b>37</b>

## 0. Consideracións previas

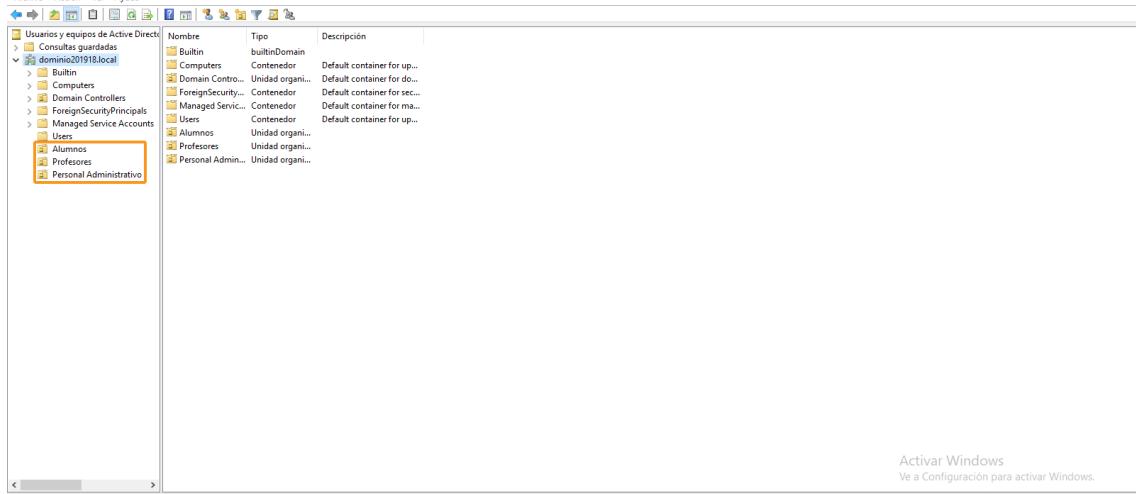
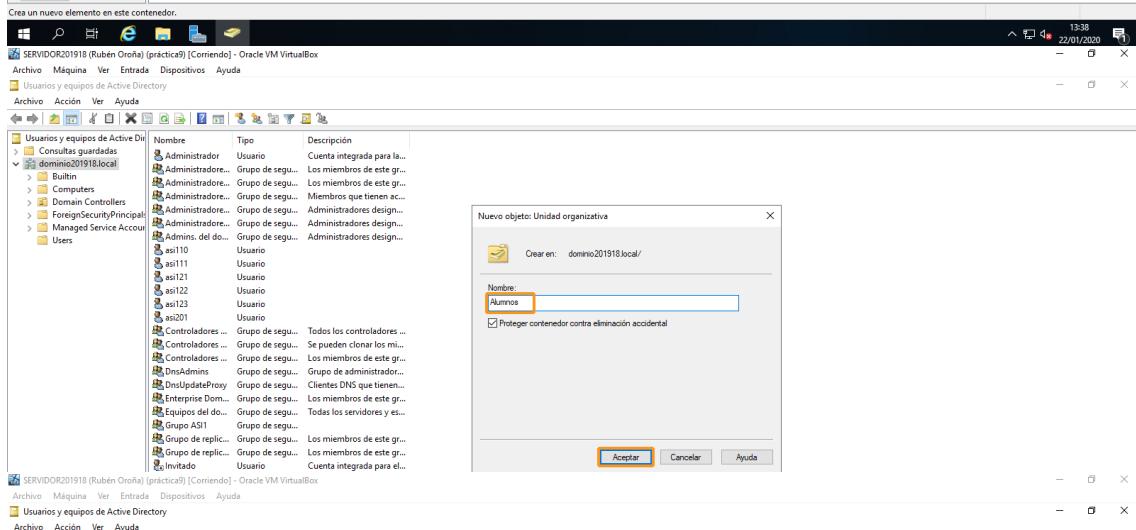
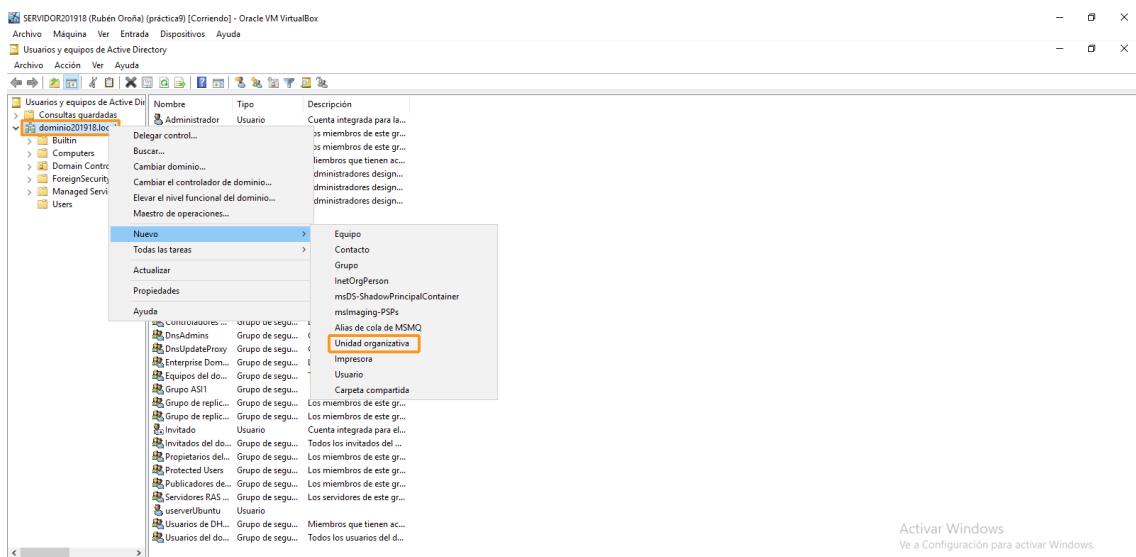
Para levar a cabo a xestión de cartafoles compartidos con diferentes permisos e restricións en función dos grupos e usuarios, empregaremos o servidor Windows Server 2019 creado en prácticas previas. Para elo imos usar o volume seccionado (l:) da tarefa anterior, no que crearemos dous cartafoles compartidos que contarán co acceso de varios grupos e usuarios con diferentes permisos. Tanto o servidor como o cliente vinculado ó dominio son creados como máquinas virtuais empregando o software Oracle VM VirtualBox (versión 6.0.16). A modo de resumo, amosamos unha táboa que recolle a [nomenclatura e configuración IP do servidor](#), ademais dunha [árbore das unidades organizativas, grupos e usuarios](#) empregados durante a práctica.

Sistema operativo:	Windows Server 2019
Nome do equipo:	SERVIDOR201918
Nome dominio:	<a href="#">dominio201918.local</a>
Dirección IP:	192.168.18.12
DHCP rango-inicio:	192.168.18.30
DHCP rango-final:	192.168.18.50
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. Creación das unidades organizativas, grupos e plantillas

Comezamos por acceder ó xestor de usuarios e equipos do administrador do servidor, co fin de **crear tres unidades organizativas**. Para elo, facemos clic dereito no dominio e prememos en nova unidade organizativa. Nomeámolas como Alumnos, Profesores e Personal Administrativo.



Se baixamos na xerarquía da árbore exposta ó comezo, agora toca **crear os diferentes grupos**. Para elo, entramos na unidade organizativa correspondente, e facendo clic dereito escollemos a opción adecuada. Serán grupos de seguridade de ámbito global. Na unidade Alumnos, os grupos chámense ASI1, ASI2, SMR1 e SMR2.

The screenshot shows the Windows Active Directory Users and Computers console. The left pane displays the organizational structure: 'Consultas guardadas', 'dominio201918.local' (selected), 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', 'Users', 'Alumnos' (selected), 'Profesores', and 'Personal Administrativo'. The right pane shows a table with columns 'Nombre', 'Tipo', and 'Descripción'. A context menu is open over the 'Alumnos' container, with 'Nuevo' expanded to show 'Equipo', 'Contacto', and 'Grupo'. The 'Grupo' option is highlighted. The status bar at the bottom right shows '13:59 22/01/2020' and 'CTRL DERECHA'.

The screenshot shows the 'Nuevo objeto: Grupo' dialog box. It has fields for 'Nombre de grupo:' containing 'ASI1' and 'Nombre de grupo (anterior a Windows 2000):' containing 'ASI1'. Under 'Ámbito de grupo', the 'Global' radio button is selected. Under 'Tipo de grupo', the 'Seguridad' radio button is selected. The 'Aceptar' button is highlighted. The status bar at the bottom right shows '13:59 22/01/2020' and 'CTRL DERECHA'.

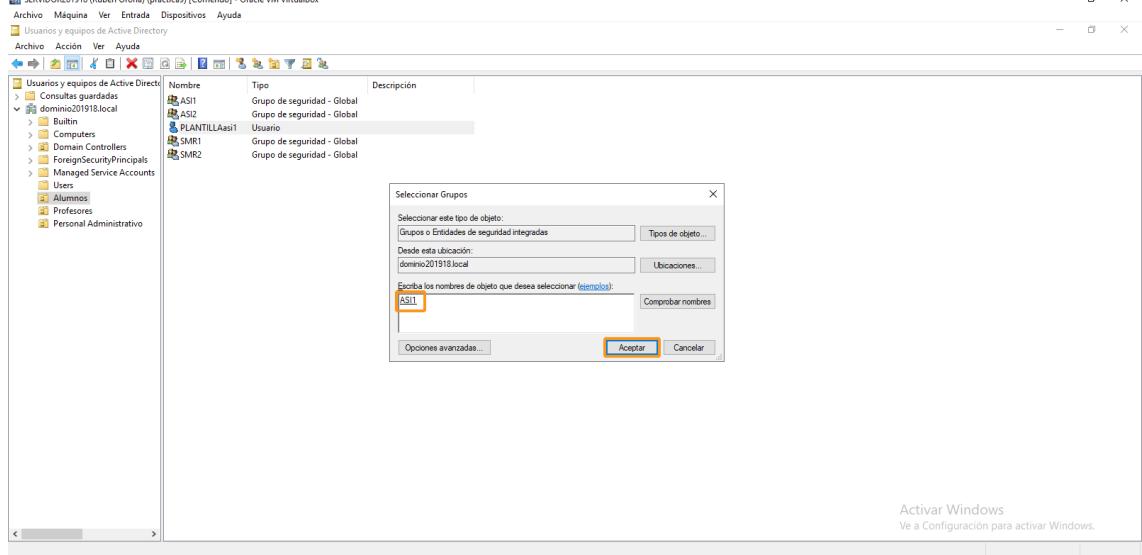
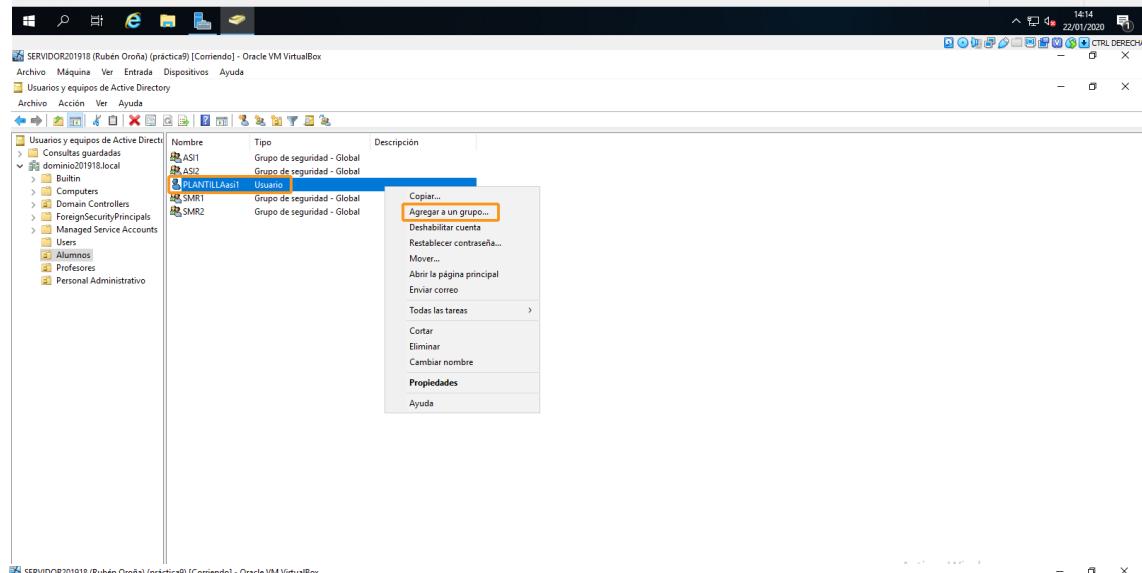
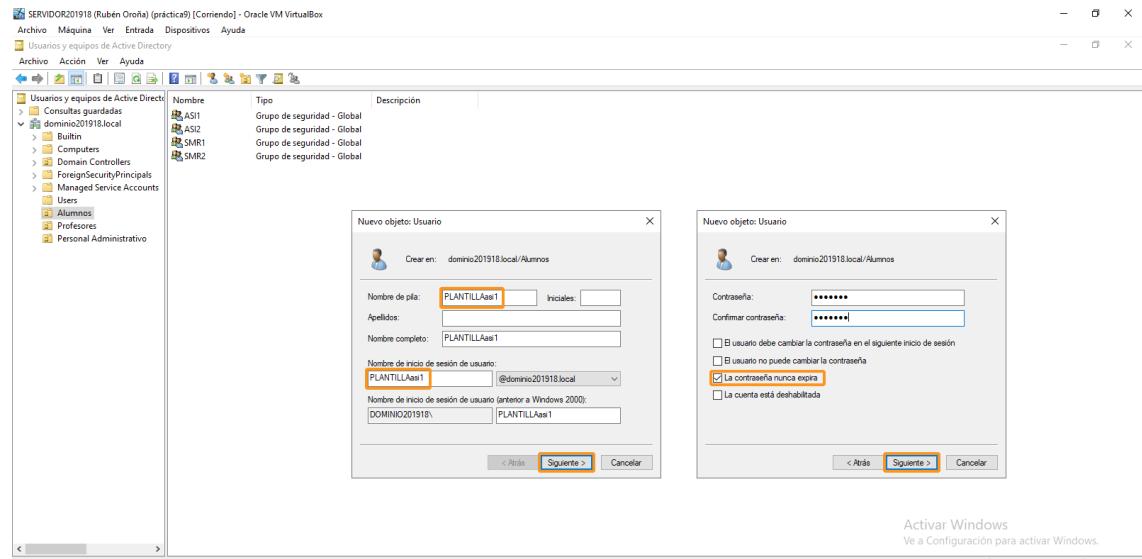
The screenshot shows the Active Directory Users and Computers console again. The 'Alumnos' container now contains four security groups: 'ASI1', 'ASI2', 'SMR1', and 'SMR2'. The status bar at the bottom right shows '13:59 22/01/2020' and 'CTRL DERECHA'.

Na unidade Profesores creamos os grupos INFORMÁTICOS e RESTO, mentres que dentro de Personal Administrativo xeramos só un, nomeado ADMINISTRATIVOS. A continuación, imos **crear unha plantilla para cada grupo**. En realidade trátase dunha conta de usuario ordinaria, pero que nos aforrará tempo en xerar posteriores usuarios, pois de cada modelo copiaremos a pertenza a un grupo específico.

The screenshots illustrate the process of creating security groups in Active Directory:

- Screenshot 1:** Shows the 'INFORMÁTICA' and 'RESTO' groups under the 'Profesores' container. Both groups are highlighted with orange boxes.
- Screenshot 2:** Shows the 'ADMINISTRATIVO' group under the 'Personal Administrativo' container. This group is also highlighted with an orange box.
- Screenshot 3:** Shows the context menu for a user account ('User') in the 'Alumnos' container. The 'Nuevo' option is selected, and a submenu is open, with 'Usuario' highlighted with an orange box.

Así pois, poñemos un nome xenérico a cada unha (PLANTILLAAnomegrupo), escollemos a opción de que o contrasinal nunca expire e engadimos cada modelo no seu grupo correspondente.



Una vez hecho esto, repétimolo para todos los grupos.

The screenshots illustrate the process of adding users to security groups in Active Directory:

- Screenshot 1:** Shows the 'Alumnos' group selected in the left pane. The right pane displays a list of security groups: ASI, AS2, PLANILLAAs1, PLANILLAAs2, PLANILLAAsm1, PLANILLAAsm2, SMR1, and SMR2. The 'ASI' group is highlighted with a red box.
- Screenshot 2:** Shows the 'Profesores' group selected in the left pane. The right pane displays a list of security groups: INFORMATICA, PLANILLAINFORMATICA, PLANILLARESTO, and RESTO. The 'INFORMATICA' group is highlighted with a red box.
- Screenshot 3:** Shows the 'Personal Administrativo' group selected in the left pane. The right pane displays a list of security groups: ADMINISTRATIVOS and PLANILLAAdministrativos. The 'ADMINISTRATIVOS' group is highlighted with a red box.

In all three cases, a confirmation dialog box is visible in the foreground, stating: "Se ha completado con éxito la operación Agregar a grupo." (The operation 'Add to group' was completed successfully.)

Agora imos empregar o modelo do grupo ASI1 para crear as dúas primeiras contas que imos usar no seguinte apartado. Polo tanto, facemos clic dereito na plantilla e prememos en copiar. Desta maneira, imos **crear os usuarios asi120 e asi121**. Ademais, faremos tamén unha conta smr100, para amosar que este non pode acceder ó cartafol compartido.

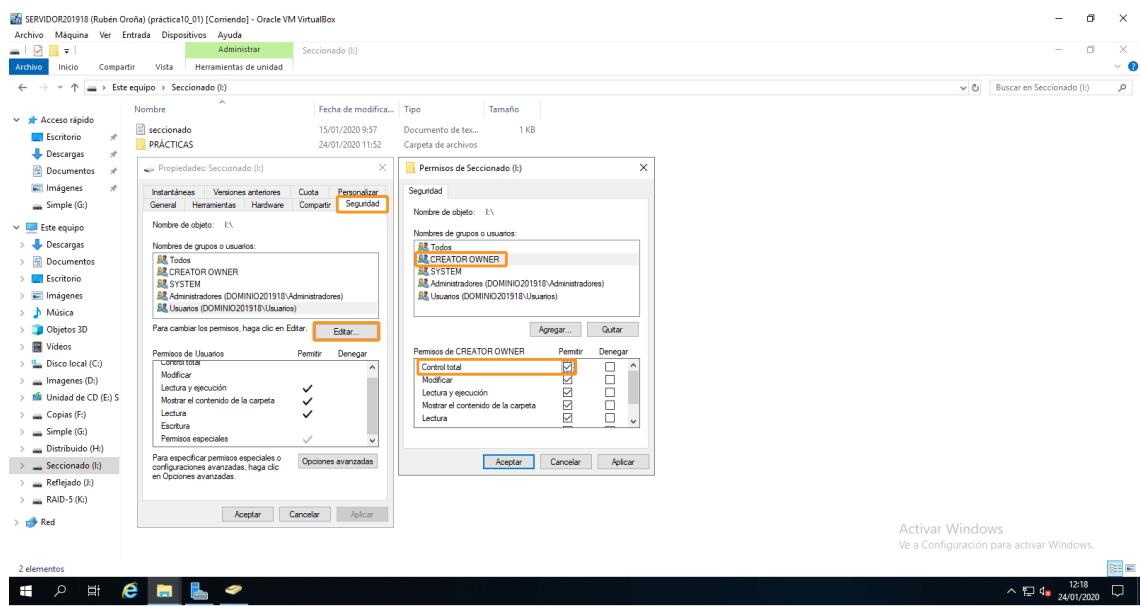
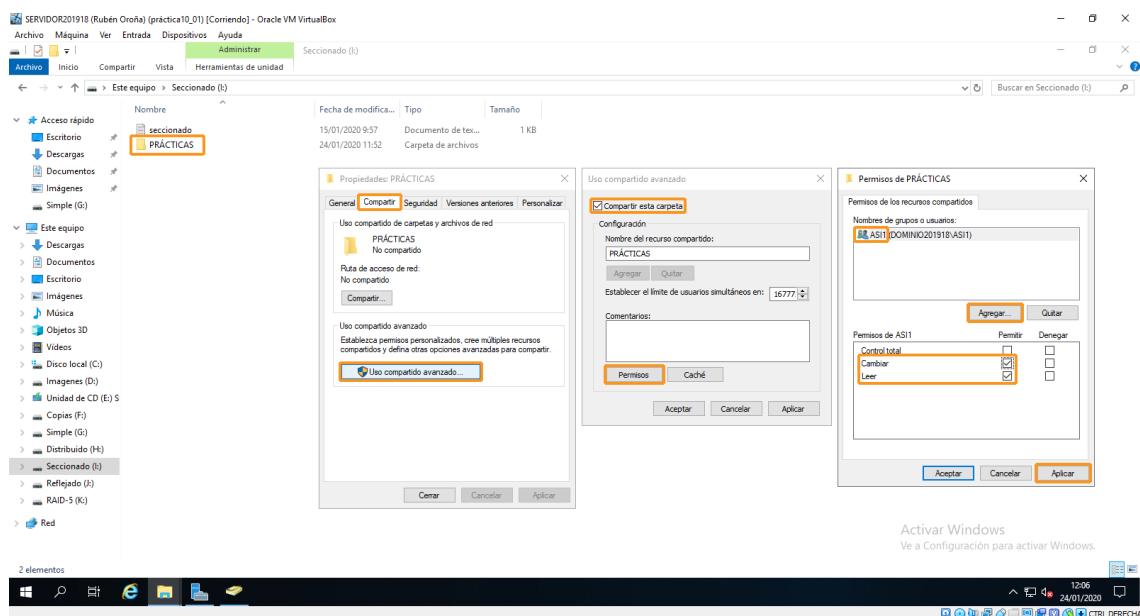
The screenshots illustrate the process of creating users from a template:

- Screenshot 1:** Shows the Active Directory Users and Computers interface. A context menu is open over the "PLANTILLAAsi1" object, with the "Copiar..." option highlighted.
- Screenshot 2:** Shows the "Copiar objeto: Usuario" dialog box. The "Nombre de pila:" field is set to "asi120". The "Nombre de inicio de sesión de usuario:" dropdown is set to "asi120 @dominio201918.local". The "Siguiente >" button is highlighted.
- Screenshot 3:** Shows the "Propiedades ASI1" dialog box for the "ASI1" group. The "Miembros" tab is selected, showing the users "asi120" and "asi121" listed under "Miembros".

## B. Cartafol PRÁCTICAS compartido para o grupo ASI1

No volume seccionado (l:), imos **crear un cartafol chamado PRÁCTICAS**, ó que só teñan acceso os usuarios pertenecentes ó grupo ASI1. Ademais, queremos que os alumnos poidan pegar, borrar, substituír ou ver as súas prácticas, pero non as dous seus compañeiros. A tenro destas condicións, temos que comezar por **outorgar acceso por rede a ASI1**. Para elo, entramos en propiedades/ uso compartido avanzado/ permisos, e engadimos o grupo ASI1, habilitándolle as xanelas de cambiar e ler.

Agora imos limitar os permisos por NTFS. En primeiro lugar, para controlar os privilexios dos alumnos en función de si as prácticas son deles ou non, debemos empregar a identidade especial Creator Owner, que ten en conta o propietario dos arquivos. Así pois, entramos na pestana seguridade e prememos en editar para **dar control total á identidade Creator Owner**.



A partir deste momento, temos que entrar nas opcións avanzadas de seguridade. Comezamos por deshabilitar a heranza de permisos, para así poder suprimir a entidade usuarios, aínda que en principio a carpeta non debería ser accesible ós alumnos de maneira local a través do servidor, máis alá do administrador. Por último, imos engadir o grupo ASI1.

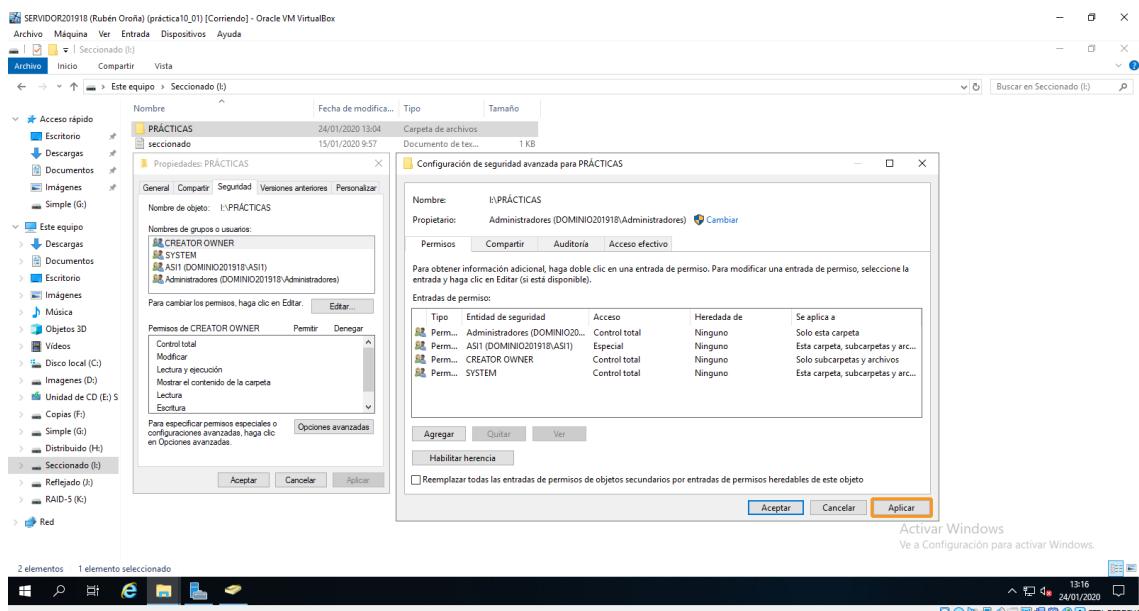
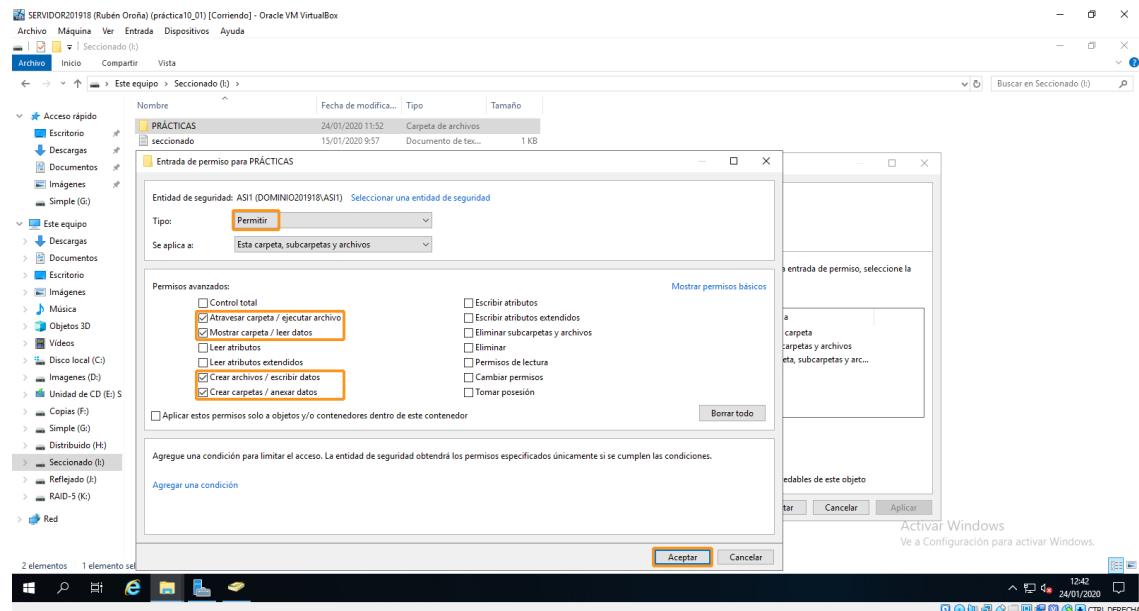
The screenshots illustrate the process of managing security inheritance for a folder named 'PRÁCTICAS' located at 'Este equipo > Seleccionado (l)'. The first screenshot shows the 'Seguridad' tab in the 'Propiedades de PRÁCTICAS' dialog, with a warning message about blocking inheritance. The second screenshot shows the 'Permisos' tab with inheritance disabled. The third screenshot shows the 'Seguridad' tab again, but this time with the 'ASI1' group added as a security principal.

**Screenshot 1: Deshabilitar herencia**

**Screenshot 2: Seguridad sin herencia**

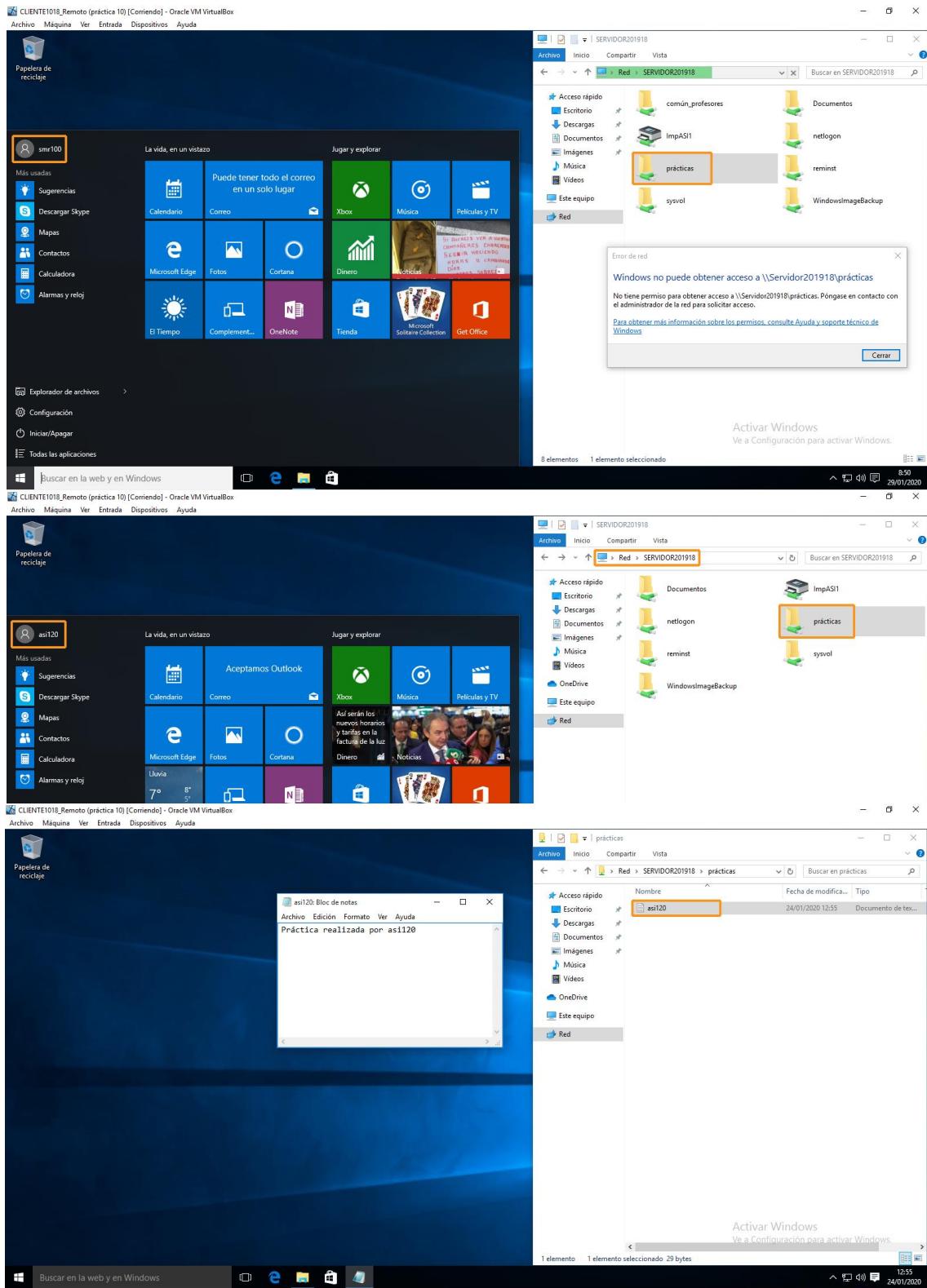
**Screenshot 3: Agregar el grupo ASI1**

Como contrapunto ó control total que lle outorgamos ó propietario, limitamos os privilexios dos alumnos ASI1 ós catro amosados na captura. Mediante eles os usuarios poden acceder ós diferentes cartafoles e pegar as prácticas (converténdose nos seus propietarios). Habilitamos ademais a creación de cartafoles, pois non se especifica como sería a organización de PRÁCTICAS, e semella raro que todas as tarefas dos alumnos fiquen na raíz do cartafol.

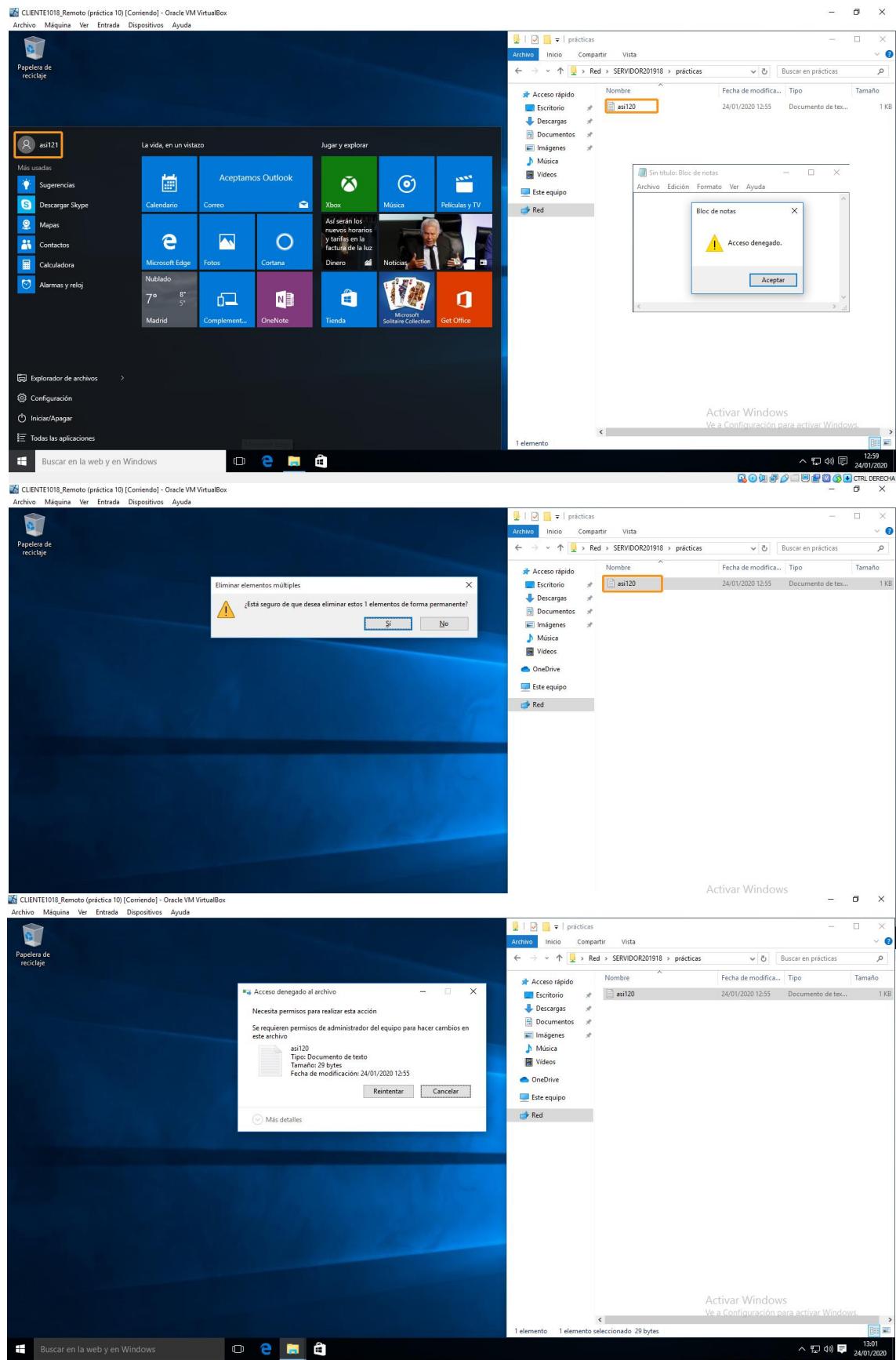


## C. Comprobación dos usuarios smr100, asi120, asi121

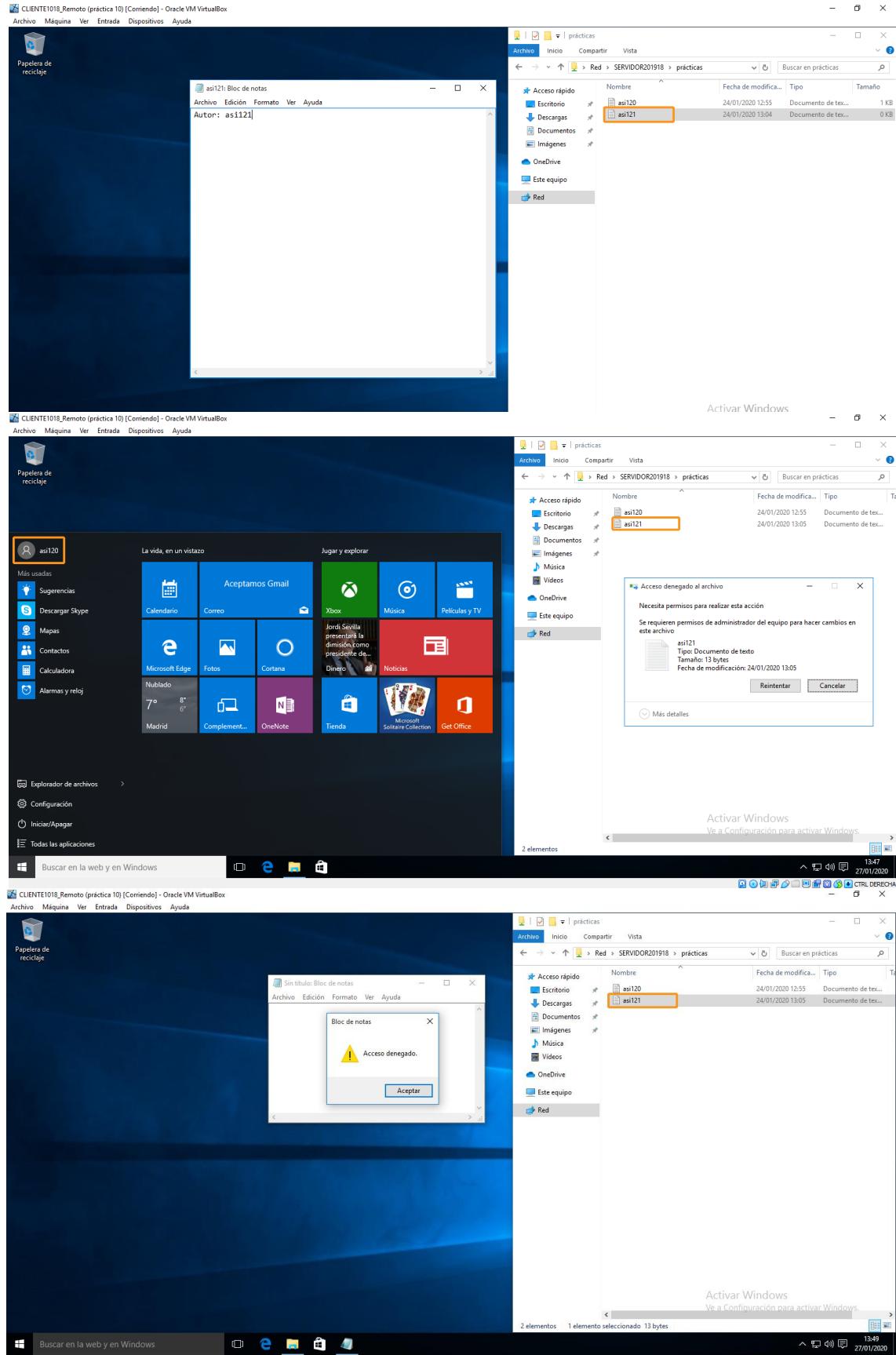
Accedemos coas seguintes contas de usuario ó cartafol compartido, para comprobar o funcionamento da configuración de permisos. Comezamos por tratar de entrar con smr100, e vemos que o acceso está restrinxido, pois o cartafol non foi compartido nin ó usuario nin ó seu grupo. Agora facemos o mesmo coa conta asi120, e constatamos tanto o acceso como o dereito de escritura.



A continuación, vemos que a identidade especial Creator Owner funciona satisfactoriamente, pois dende o usuario asi121 non podemos ler nin eliminar o arquivo creado anteriormente con asi120.



Agora, creamos un arquivo con asi121, e voltamos para facer as mesmas comprobacións co seu homólogo asi120. Por suposto, tampouco ten dereito a ver nin eliminar arquivos dos que non é propietario.



## D. Configuración dos usuarios asi101, asi102 e asi103

Agora, queremos modificar os permisos duns usuarios específicos dentro do grupo compartido. Así pois, queremos que asi101 non teña dereitos de escritura, que asi102 non poida crear arquivos e que asi103 só poida eliminar arquivos e cartafoles. Polo tanto, comezamos por **crear os tres usuarios**. Posteriormente, entramos na pestana seguridade das propiedades de PRÁCTICAS, e en opcións avanzadas imos engadindo os diferentes usuarios.

The screenshot shows the Windows Control Panel interface. In the center, a 'Propiedades de ASI1' (Properties of ASI1) dialog box is open, specifically the 'Membres' (Members) tab. It lists several users under 'Nombre' (Name), including 'asi101', 'asi102', and 'asi103'. These three users are highlighted with red boxes. The 'Aceptar' (Accept) button at the bottom right is also highlighted.

The screenshot shows the Windows File Explorer interface. A new folder named 'seccionado' has been created within the 'PRÁCTICAS' folder. The 'Propiedades' (Properties) dialog box for 'seccionado' is open, showing the 'Seguridad' (Security) tab. Under 'Permisos de ASI1', the 'Modificar' (Modify) permission is checked. The 'Opciones avanzadas...' (Advanced options...) button is highlighted with a red box. The 'Aceptar' (Accept) button at the bottom right is also highlighted.

The screenshot shows the 'Configuración de seguridad avanzada para PRÁCTICAS' (Advanced security configuration for PRÁCTICAS) dialog box. It displays a table of permissions for the 'ASI1' security entity. The 'Modificar' (Modify) permission is checked for 'ASI1 (DOMINIO201918\ASI1)'. The 'Aceptar' (Accept) button at the bottom right is highlighted.

The screenshot shows the 'Entrada de permiso para PRÁCTICAS' (Permission entry for PRÁCTICAS) dialog box. It is used to add a new permission for user 'asi101'. The 'Tipo' (Type) dropdown is set to 'Permitir' (Allow). The 'Nombre' (Name) dropdown shows 'Está carpeta, subcarpetas y archivos' (This folder, subfolders and files). The 'Permisos básicos' (Basic permissions) section shows the 'Modificar' (Modify) checkbox checked. The 'Nombre' (Name) field in the 'Seleccionar Usuario, Equipo, Cuenta de servicio o Grupo' (Select User, Computer, Service Account or Group) dialog box is highlighted with a red box, containing the value 'asi101\asi101@domino201918.local'. The 'Aceptar' (Accept) button at the bottom right is also highlighted.

Comezamos por denegar permisos de escritura ó usuario asi101. Dos catros permisos concedidos ó grupo, restrinximos os dous últimos. Continuamos por denegar a creación de arquivos ó usuario asi102, e mantemos a posibilidade de crear cartafoles.

**Entrada de permiso para PRÁCTICAS**

Entidad de seguridad: asi101 (asi101@dominio201918.local) Seleccionar una entidad de seguridad

Tipo: Denegar

Se aplica a: Esta carpeta, subcarpetas y archivos

Nombre:

Propietario:

Permisos:

Para obtener info entrada y haga clic

Entradas de permiso

Tipo	Entid
Denegar	Permi...
Permitir	Permi...

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Permisos avanzados:

- Control total
- Modificar
- Leer y ejecución
- Mostrar el contenido de la carpeta
- Lectura
- Escritura
- Leer atributos
- Leer atributos extendidos
- Crear archivos / escribir datos
- Crear carpetas / anexar datos

Aplicar estos permisos solo a objetos y/o contendores dentro de este contendedor

Mostrar permisos básicos

Agregue una condición para limitar el acceso. La entidad de seguridad obtendrá los permisos especificados únicamente si se cumplen las condiciones.

Activar Windows: Ve a Configuración para activar Windows.

Activar Windows

2 elementos 1 elemento seleccionado

SERVIDOR201918 (Rubén Oroña) (práctica10\_01) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Inicio Compartir Vista

Este equipo > Seccionado (l)

PRÁCTICAS

Nombre Fecha de modificación Tipo

seccionado 24/01/2020 13:04 Carpeta de archivos Documento de texto

Propiedades: PRÁCTICAS

General Compartir Seguridad Versiones anteriores Personalizar

Nombre de objeto: I:\PRÁCTICAS

Nombres de grupos o usuarios:

- CREATOR OWNER
- SYSTEM
- ASI1 (DOMINIO201918\ASI1)
- Administradores (DOMINIO201918\Administradores)

Para cambiar los permisos, haga clic en Editar... Editar...

Permisos de ASI1 Permitir Denegar

Control total Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Aplicar Cancelar Aceptar

Entidad de seguridad: Seleccionar una entidad de seguridad

Tipo: Permitir

Se aplica a: Esta carpeta, subcarpetas y archivos

Nombre:

Propietario:

Permisos:

Para obtener info entrada y haga clic

Entradas de permiso

Tipo	Entid
Denegar	Permi...
Permitir	Permi...

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Permisos básicos:

- Control total
- Modificar
- Lectura y ejecución
- Mostrar el contenido de la carpeta
- Lectura
- Escritura
- Permisos especiales

Aplicar estos permisos solo a objetos y/o contendores dentro de este contendedor

Seleccionar una entidad de seguridad

Seleccionar este tipo de objeto:

Usuario, Grupo, O entidad de seguridad integrada PRÁCTICAS

Desde esta ubicación: dominio201918.local

Escriba el número de objeto para seleccionar (ejemplo): asi102 (asi102@dominio201918.local)

Opciones avanzadas...

Activar Windows

Activar Windows

2 elementos 1 elemento seleccionado

SERVIDOR201918 (Rubén Oroña) (práctica10\_01) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Inicio Compartir Vista

Este equipo > Seccionado (l)

PRÁCTICAS

Nombre Fecha de modificación Tipo

seccionado 15/01/2020 9:57 Carpeta de archivos Documento de texto

Propiedades: PRÁCTICAS

General Compartir Seguridad Versiones anteriores Personalizar

Nombre de objeto: I:\PRÁCTICAS

Nombres de grupos o usuarios:

- CREATOR OWNER
- SYSTEM
- ASI1 (DOMINIO201918\ASI1)
- Administradores (DOMINIO201918\Administradores)

Para cambiar los permisos, haga clic en Editar... Editar...

Permisos de ASI1 Permitir Denegar

Control total Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Aplicar Cancelar Aceptar

Entidad de seguridad: asi102 (asi102@dominio201918.local) Seleccionar una entidad de seguridad

Tipo: Denegar

Se aplica a: Esta carpeta, subcarpetas y archivos

Nombre:

Propietario:

Permisos:

Para obtener info entrada y haga clic

Entradas de permiso

Tipo	Entid
Denegar	Permi...
Permitir	Permi...

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

Permisos avanzados:

- Control total
- Modificar
- Leer y ejecución
- Mostrar el contenido de la carpeta
- Lectura
- Escritura
- Leer atributos
- Leer atributos extendidos
- Crear archivos / escribir datos
- Crear carpetas / anexar datos

Aplicar estos permisos solo a objetos y/o contendores dentro de este contendedor

Activar Windows

Activar Windows

2 elementos 1 elemento seleccionado

SERVIDOR201918 (Rubén Oroña) (práctica10\_01) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Inicio Compartir Vista

Este equipo > Seccionado (l)

PRÁCTICAS

Nombre Fecha de modificación Tipo

seccionado 24/01/2020 13:04 Carpeta de archivos Documento de texto

Propiedades: PRÁCTICAS

General Compartir Seguridad Versiones anteriores Personalizar

Nombre de objeto: I:\PRÁCTICAS

Nombres de grupos o usuarios:

- CREATOR OWNER
- SYSTEM
- ASI1 (DOMINIO201918\ASI1)
- Administradores (DOMINIO201918\Administradores)

Para cambiar los permisos, haga clic en Editar... Editar...

Permisos de ASI1 Permitir Denegar

Control total Modificar Lectura y ejecución Mostrar el contenido de la carpeta Lectura Escritura

Para especificar permisos especiales o configuraciones avanzadas, haga clic en Opciones avanzadas.

Opciones avanzadas

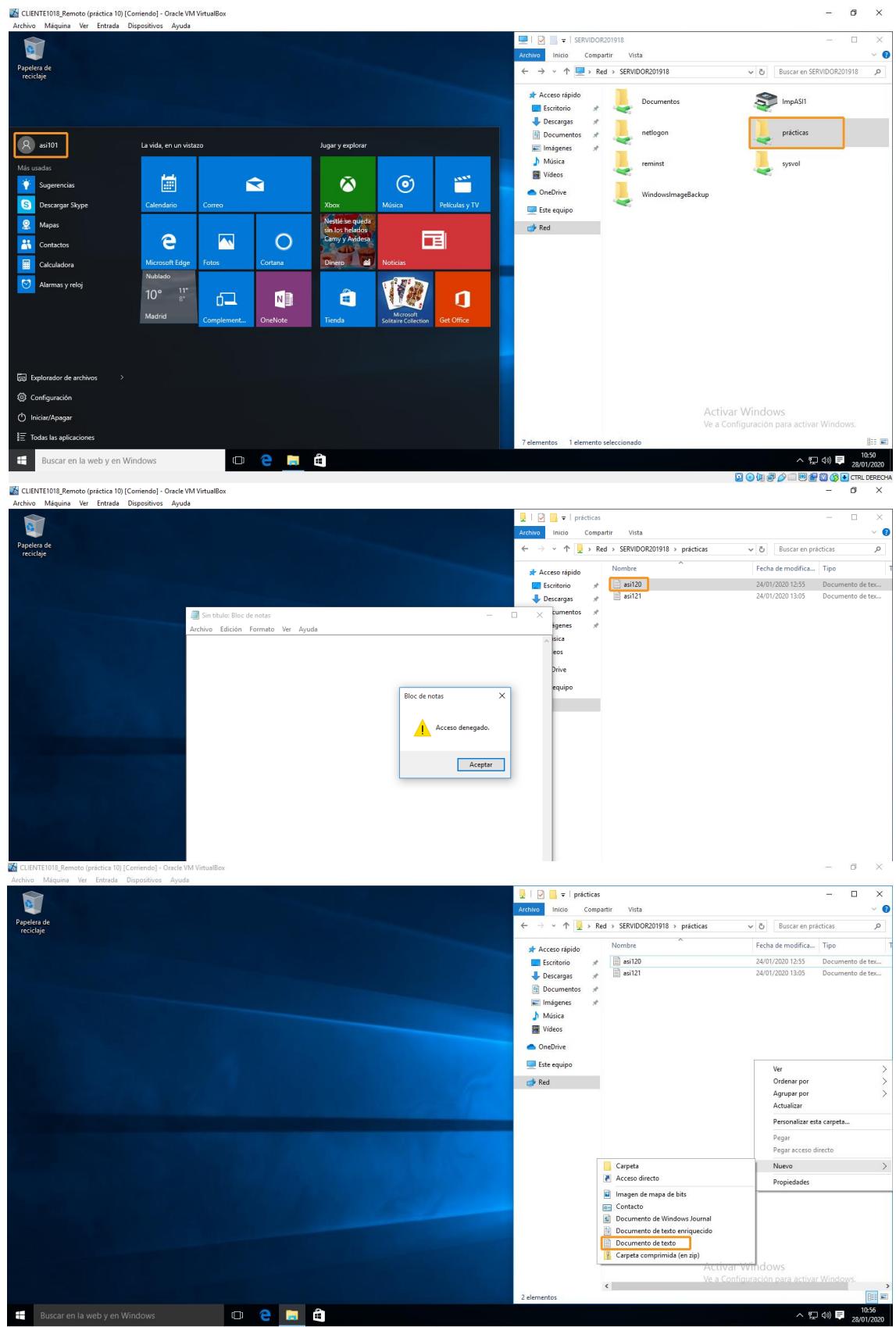
Aplicar Cancelar Aceptar

Por último, imos **agregar o usuario asi103**. Por unha banda, permitimos a eliminación de subcarpetas e arquivos. Por outro, denegamos os permisos de escritura.

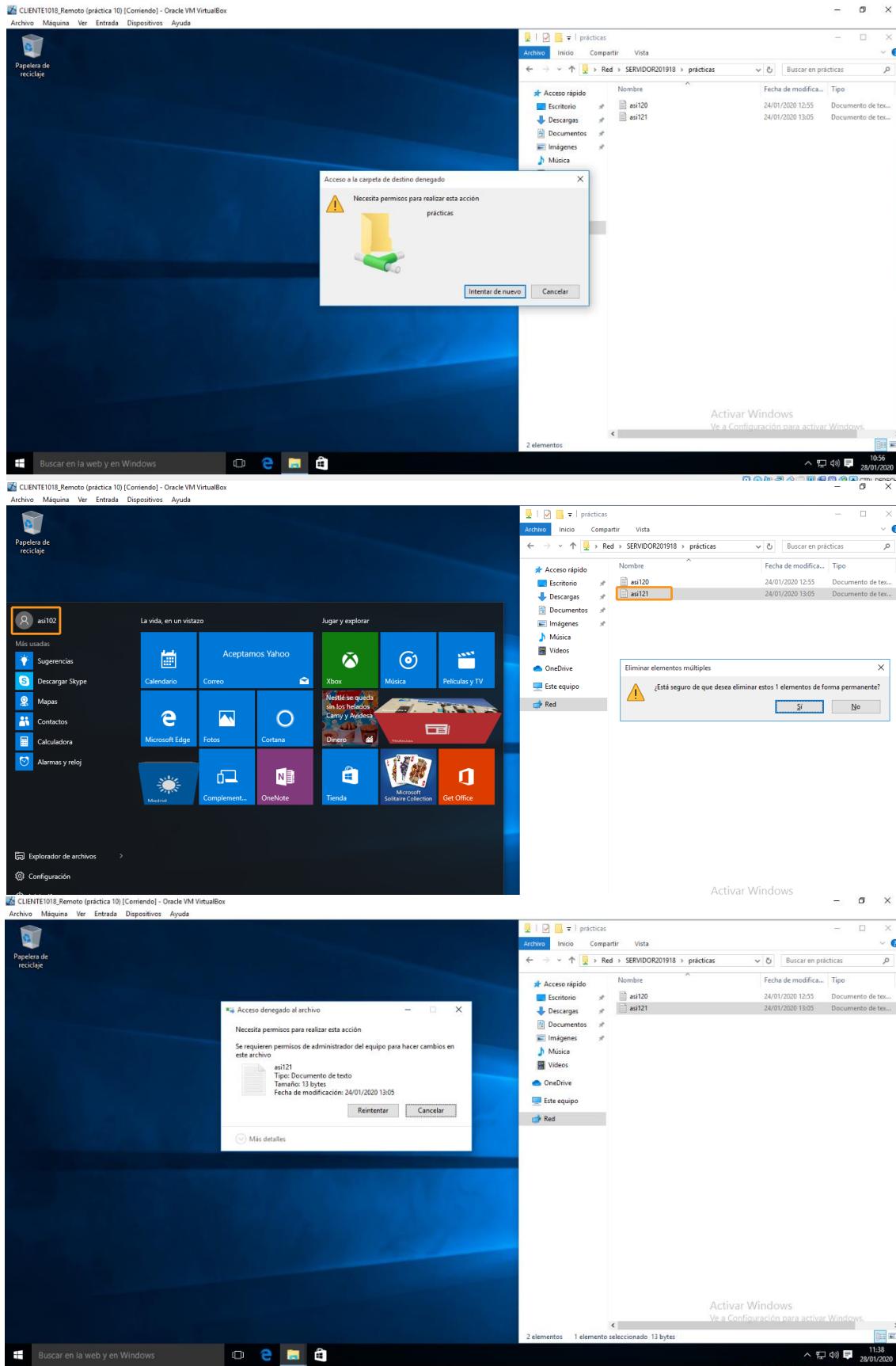
The screenshots illustrate the configuration of security permissions for a folder named 'PRÁCTICAS'. The process involves selecting the 'Seguridad' (Security) tab in the folder's properties dialog, choosing the 'Permitir' (Allow) or 'Denegar' (Deny) option for the 'asi103' user, and then checking the 'Eliminar subcarpetas y archivos' (Delete subfolders and files) checkbox under 'Permisos avanzados' (Advanced permissions). The screenshots also show the 'Activar Windows' (Activate Windows) button at the bottom right of the dialog.

## E. Comprobación dos usuarios asi101, asi102, asi103

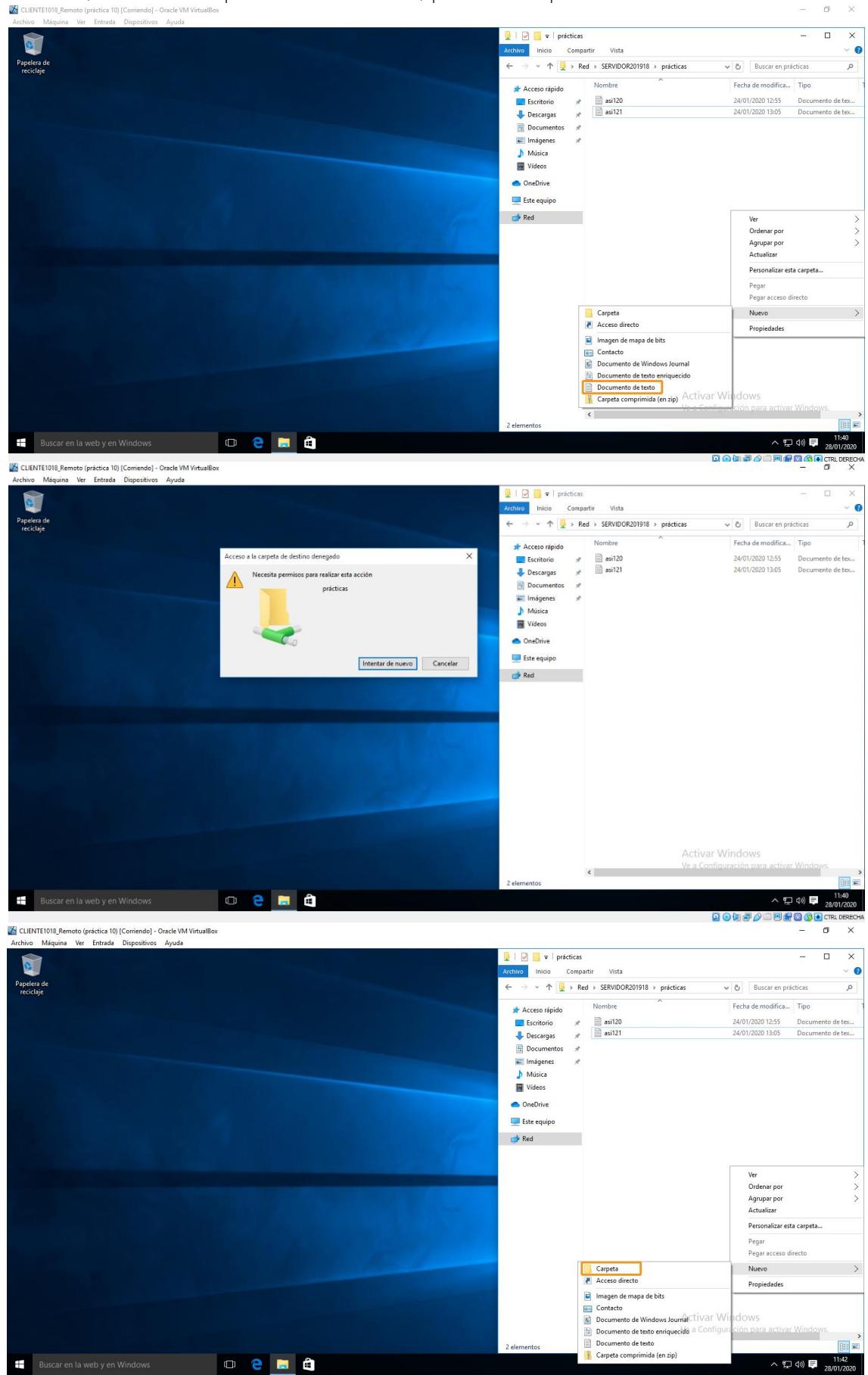
Comezamos por **facer login con asi101**. Por suposto, non podemos ver o contido de arquivos dos que non é propietario. Ademais, comprobamos que non ten dereitos de escritura.



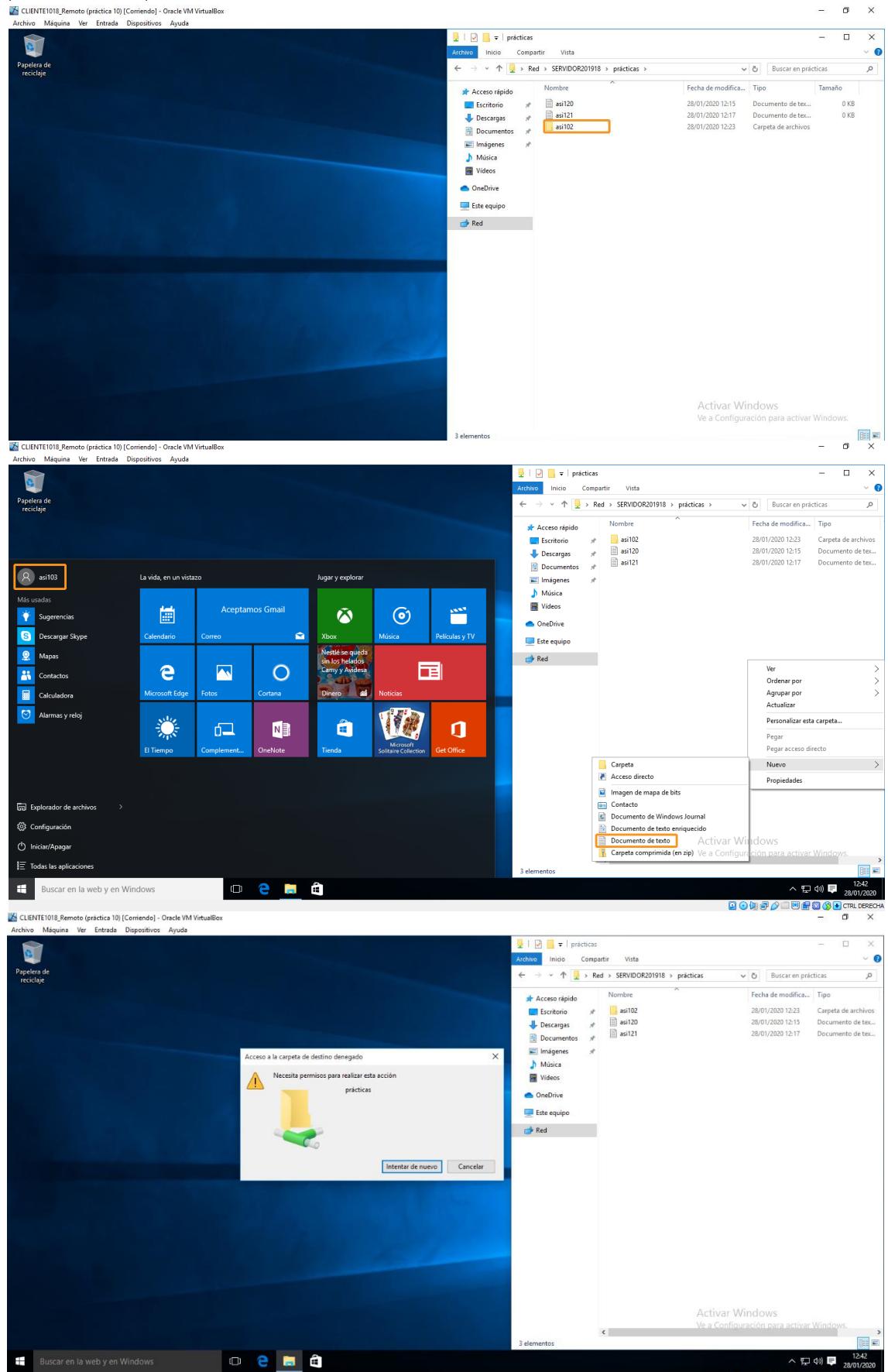
A continuación, imos **facer login con asi102**. Igual que no paso anterior, demostramos un permiso que deberían ter todos os ASI1 por defecto (neste caso, non poder suprimir un arquivo do que non é propietario, debido á configuración do Creator Owner).



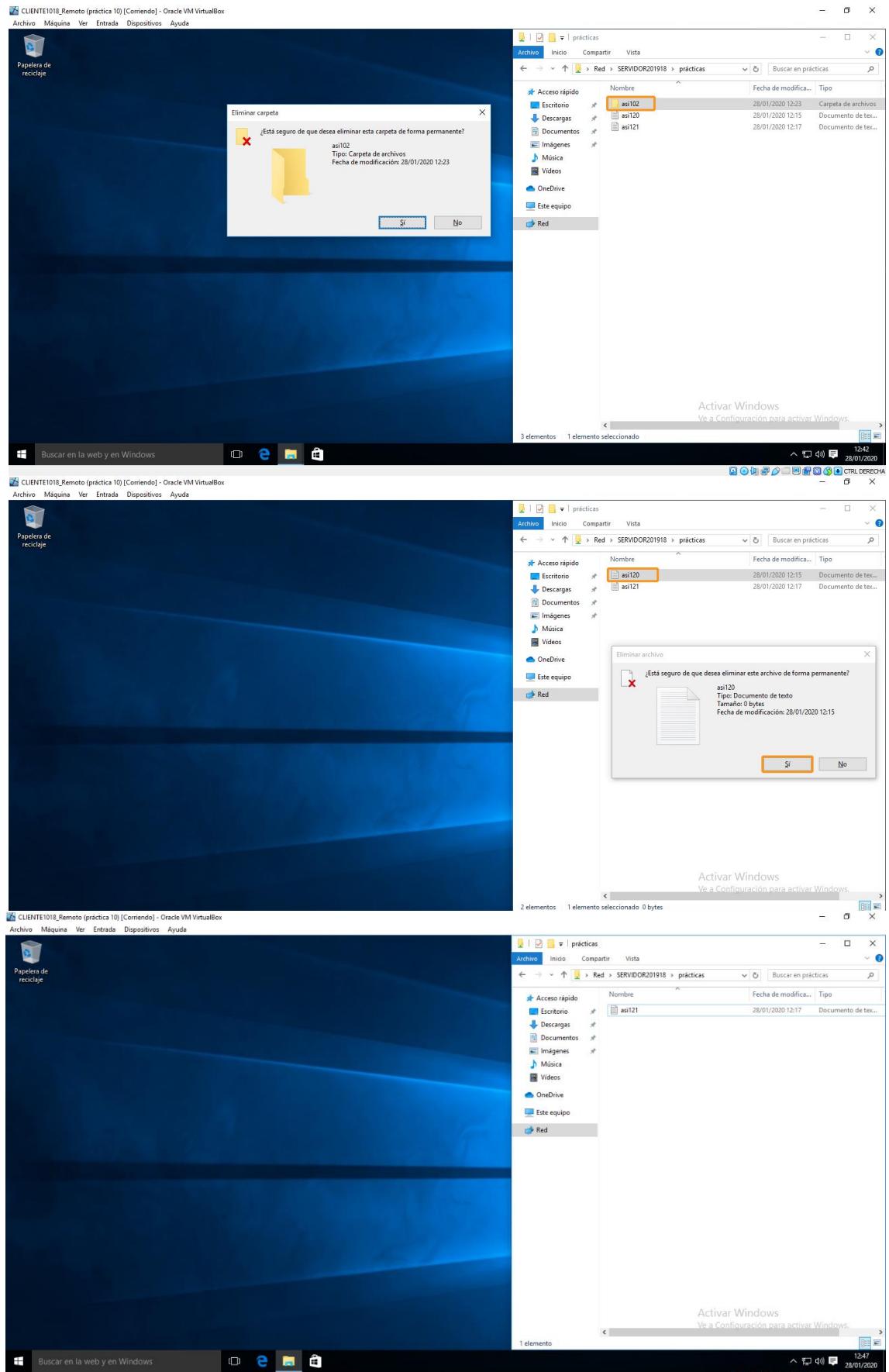
Ademais, vemos como pode crear cartafoles, pero non arquivos.



Por último, temos que **facer login con asi103**. A diferenza dos anteriores, este usuario non pode crear archivos nin cartafoles.



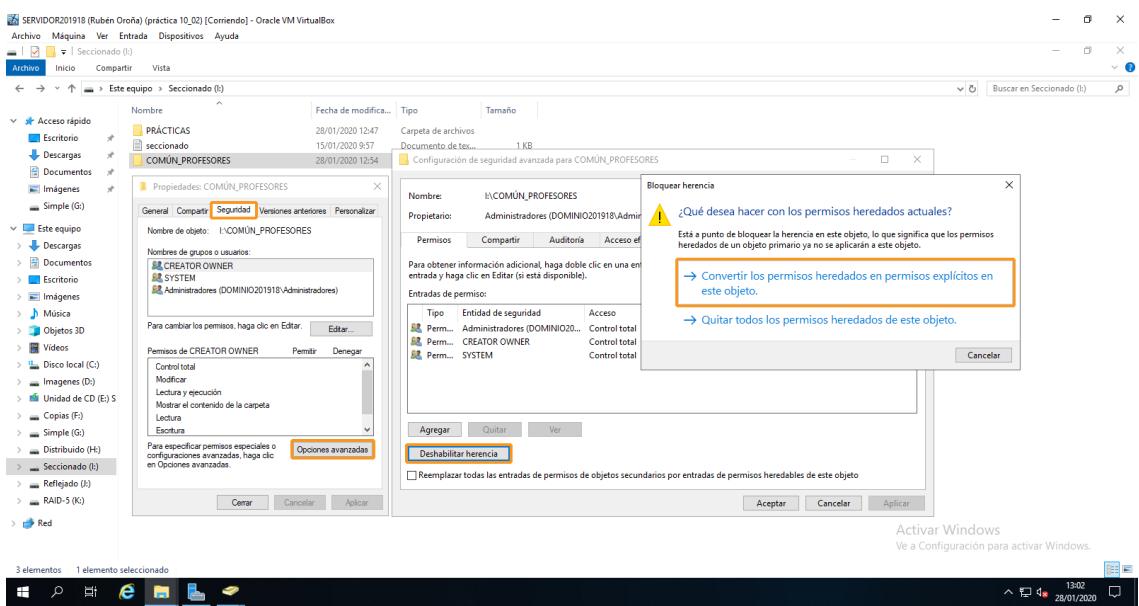
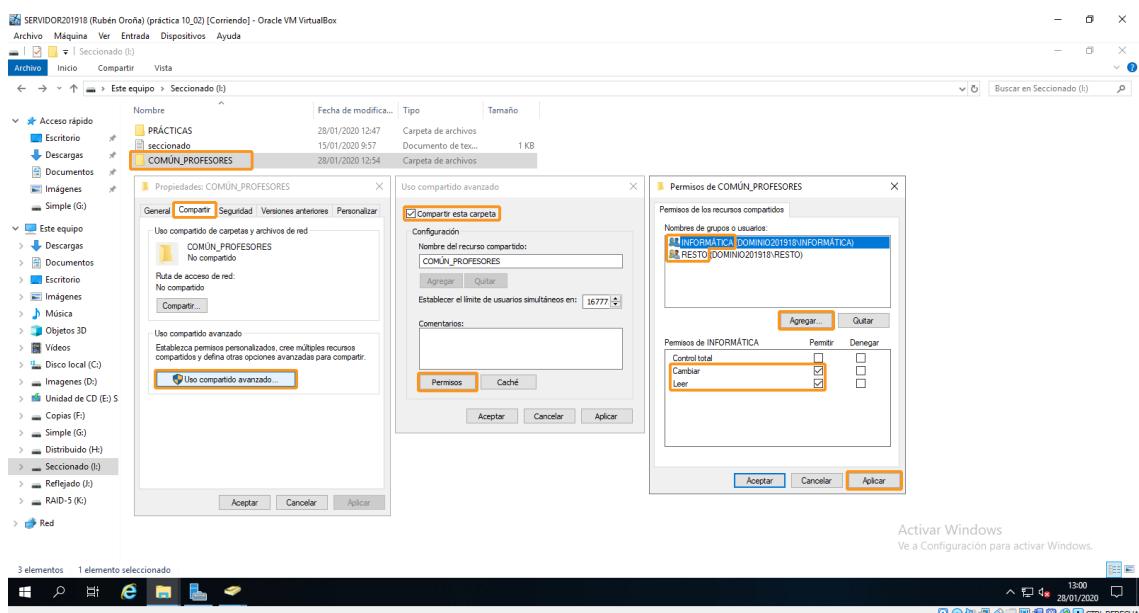
Sen embargo, vemos como si pode eliminar calquera tipo de arquivo, sexa ou non o propietario dos mesmos.



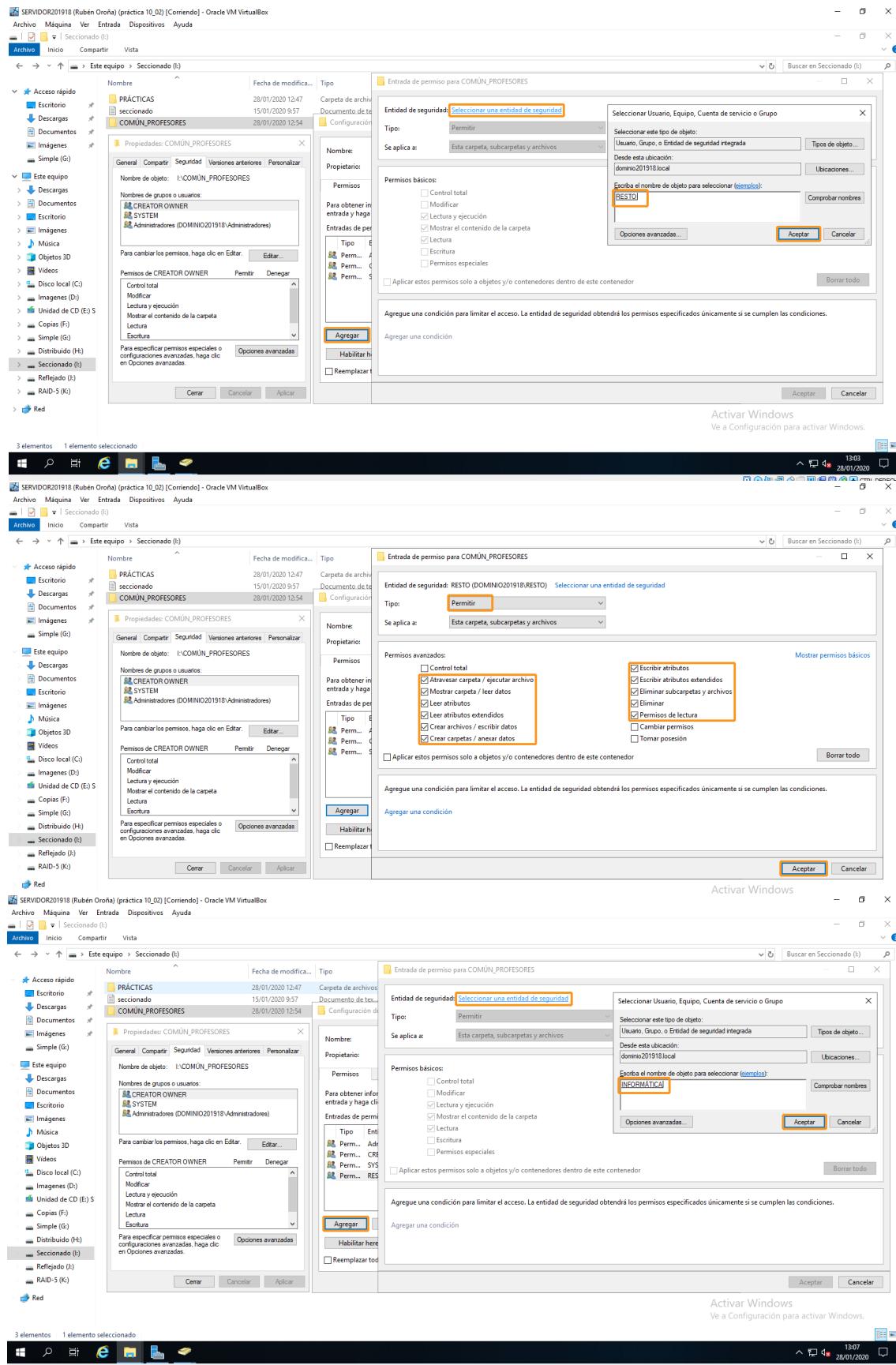
## F. Cartafol COMÚN\_PROFESORES compartido

O primeiro paso é **crear o cartafol COMÚN\_PROFESORES**, tamén no volume seccionado (l:). O obxectivo é dar control total ó grupo Informáticos, mentres que Restos non poida tomar posesión e cambiar permisos. Igual que no anterior caso, debemos comezar por **outorgar acceso por rede a Informáticos e Resto**. Para elo, entramos en propiedades/ uso compartido avanzado/ permisos, e engadimos ambos grupos, habilitándolles as xanelas de cambiar e ler.

Agora imos limitar os permisos por NTFS. A partir deste momento, temos que entrar nas opcións avanzadas de seguridade. Igual que na anterior tarefa, debemos **deshabilitar a herdanza de permisos**.



Comezamos por **engadir o grupo Resto**, que contará con todos os privilexios agás o cambio de permisos e toma de posesión.



Pola contra, imos **outorgar control total ó grupo Informática**. Posteriormente, temos que **crear usuarios en ambos grupos** para comprobar o funcionamento dos permisos. Estes serán infor1, infor2 e resto1.

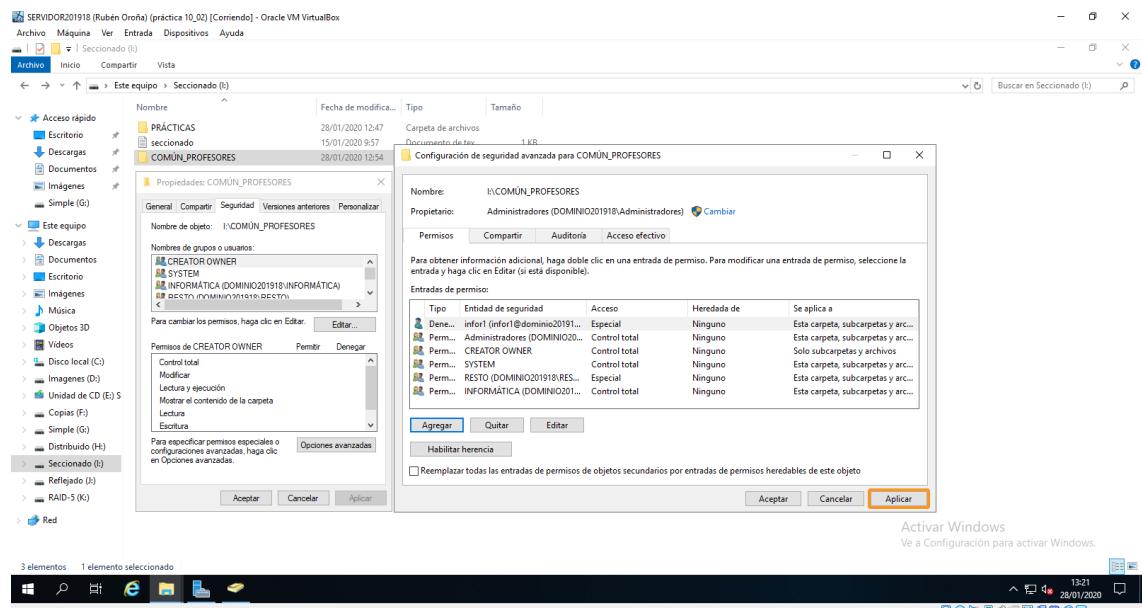
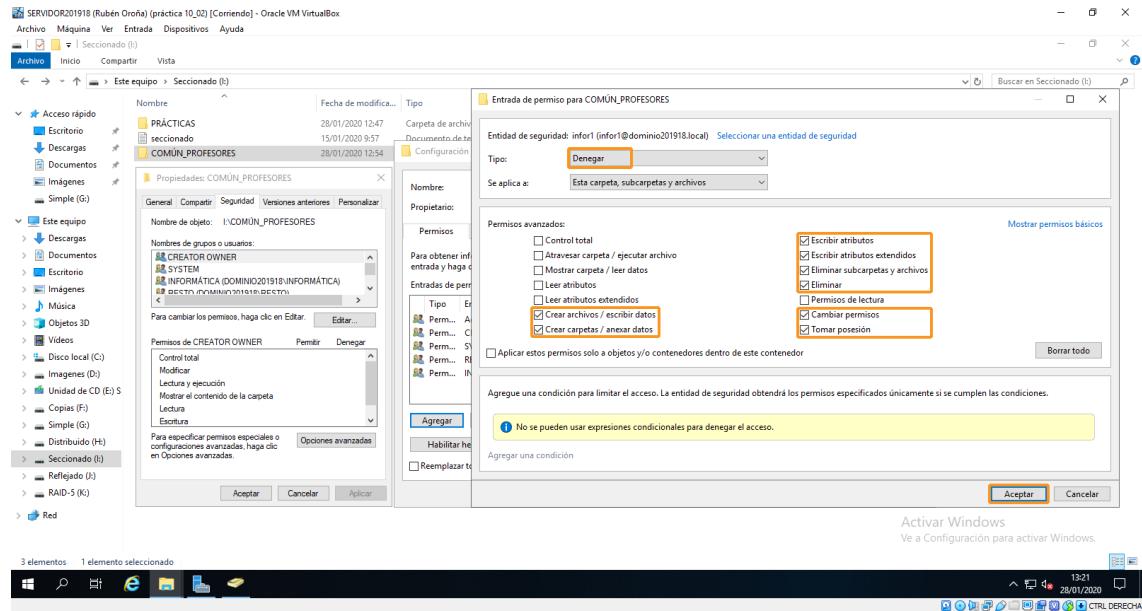
The figure consists of three vertically stacked screenshots from a Windows Server 2019 desktop environment. All screenshots have a title bar reading "SERVIDOR201918 (Rubén Oroña) (práctica 10\_02) [Corriendo] - Oracle VM VirtualBox".

**Screenshot 1:** Shows the "File Explorer" window with a folder structure. A context menu is open over a folder named "COMUN\_PROFESORES" in the "PRÁCTICAS" folder. The "Properties" dialog box is displayed, specifically the "Security" tab. It shows the "Propietario" (Owner) is "INFORMÁTICA (DOMINIO201918)\INFORMÁTICA". Under "Permisos de CREATOR OWNER", the "Control total" checkbox is checked. The "Entradas de permiso" section lists several permission types: Control total, Modificar, Lectura y ejecución, Mostrar el contenido de la carpeta, Lectura, Escritura, and Escribir atributos extendidos. The "Permisos avanzados" section has the "Control total" checkbox checked. The "Aplicar estos permisos solo a objetos y/o contenidos dentro de este contenedor" checkbox is checked. The "Aceptar" button is highlighted.

**Screenshot 2:** Shows the "Active Directory Users and Computers" window. The left navigation pane shows "Users and computers of Active Directory". The main pane displays a list of users and groups under the "dominio201918.local" domain. Several users are selected: "infor1", "infor2", "INFORMÁTICA", "PLANTILLAinformática", "PLANTILLARest0", and "resto1".

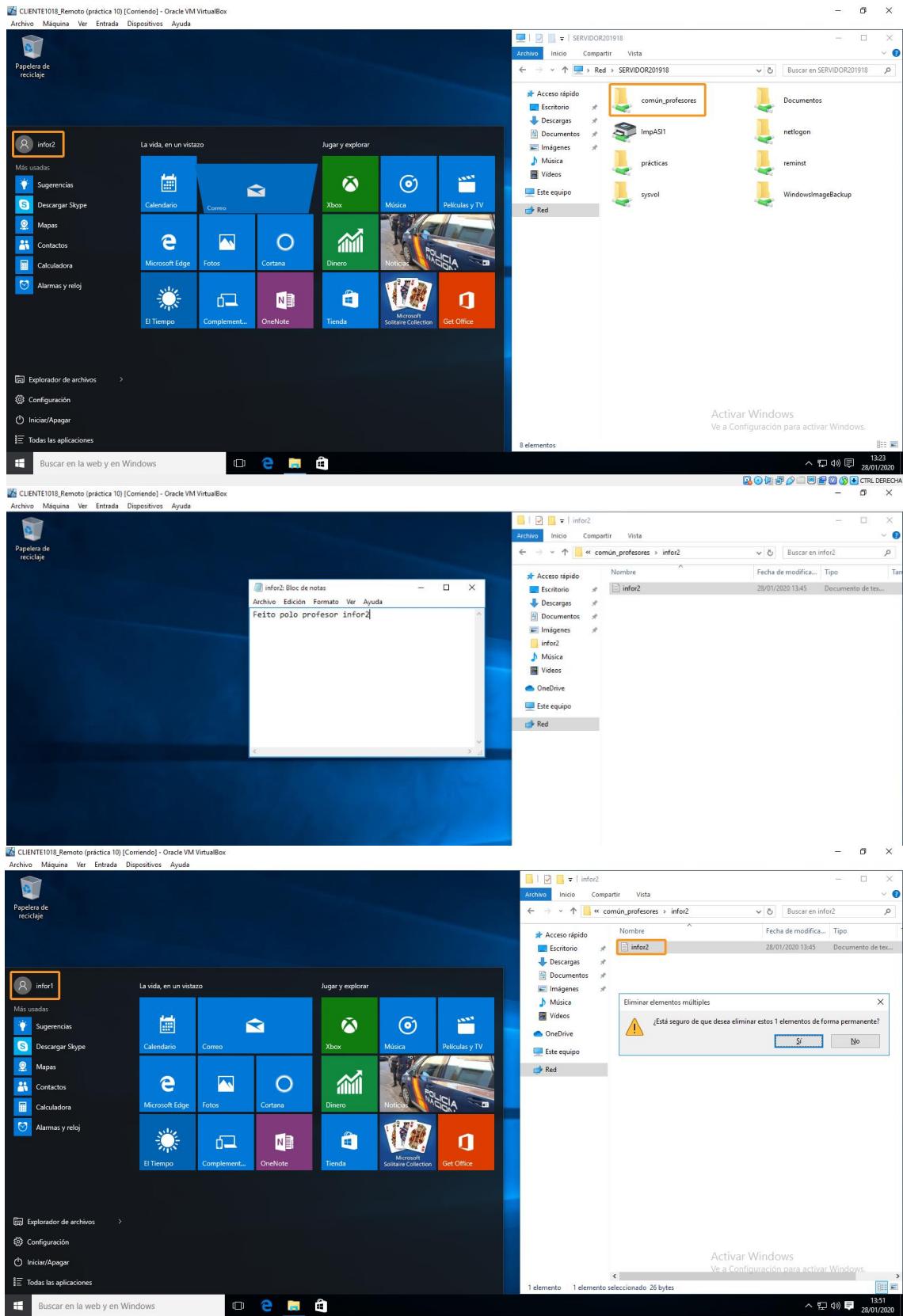
**Screenshot 3:** Similar to Screenshot 1, but the "File Explorer" window shows the "COMUN\_PROFESORES" folder again. The "Properties" dialog box is open, and the "Security" tab shows the "Propietario" as "INFORMÁTICA (DOMINIO201918)\INFORMÁTICA" and the "Control total" checkbox checked. The "Entradas de permiso" section lists the same permissions as in Screenshot 1. The "Permisos avanzados" section also has the "Control total" checkbox checked. The "Aplicar estos permisos solo a objetos y/o contenidos dentro de este contenedor" checkbox is checked. The "Aceptar" button is highlighted. Below the "File Explorer" window, the taskbar shows the date and time as "28/01/2020 13:19".

Antes de rematar, debemos **facer unha excepción co usuario infor1**, pois queremos que este profesor só teña permiso de lectura. Polo tanto, denegamos os permisos de creación, escritura, borrado e modificación de permisos/ propietario. Aplicamos os cambios realizados antes de saír.

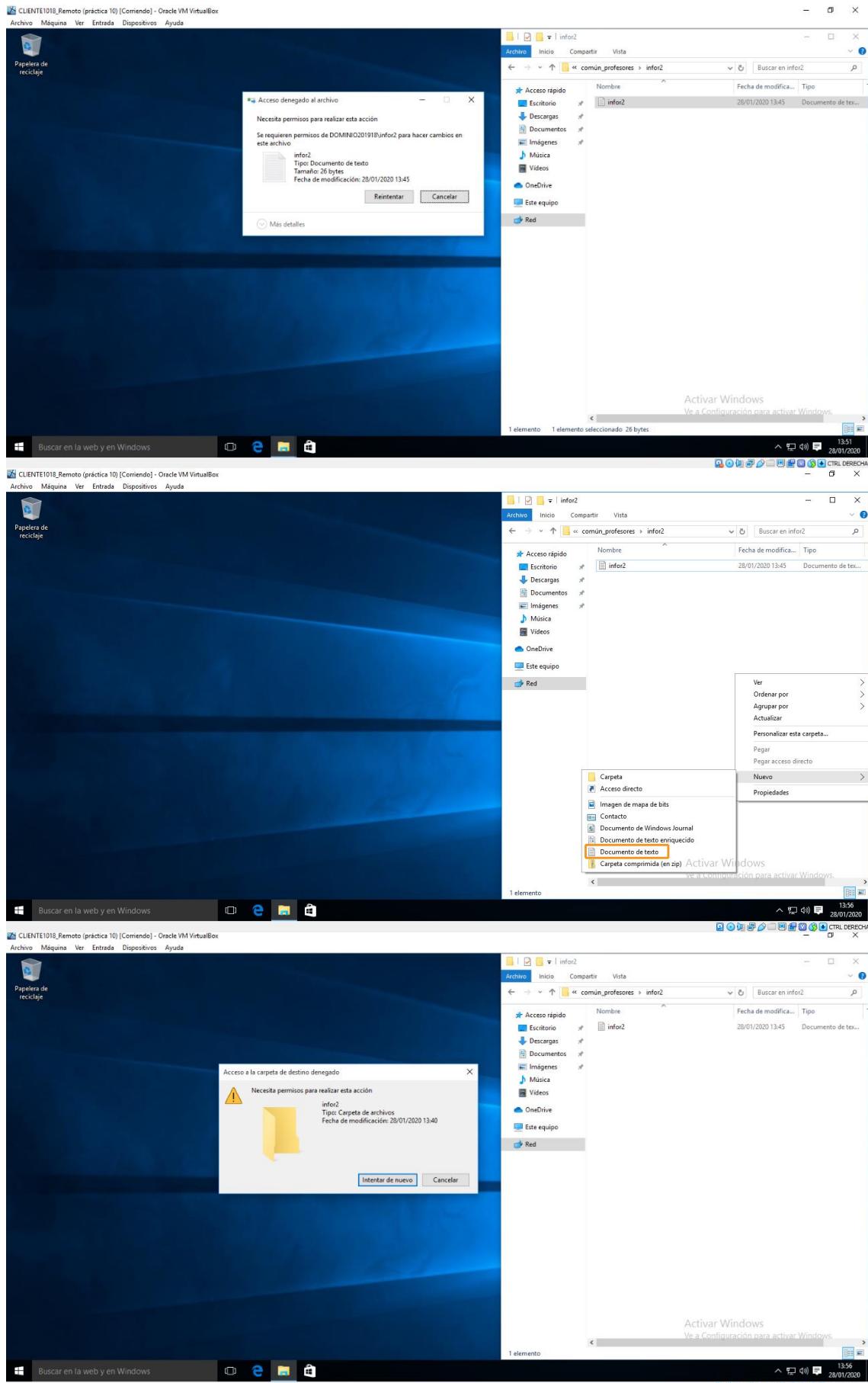


## G. Comprobación dos usuarios infor1, infor2 e resto1

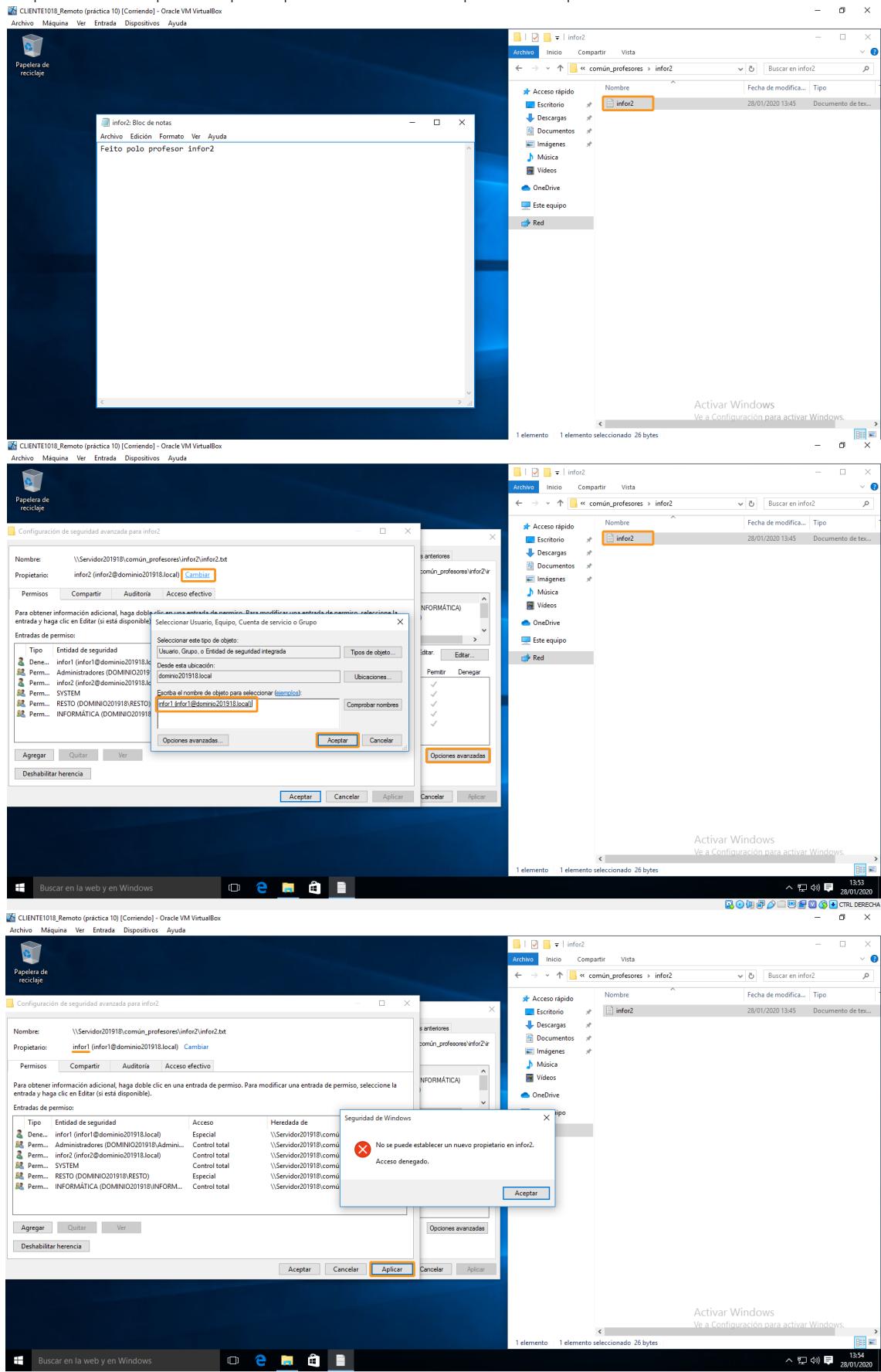
Comezamos por facer login co usuario **infor2**, que posúe control total. Como a raíz está baleira, creamos un cartafol e un arquivo de texto. Tras isto, cambiamos para **facer login co usuario infor1**. A este profesor limitámosselle os privilexios, polo que só pode ler arquivos.



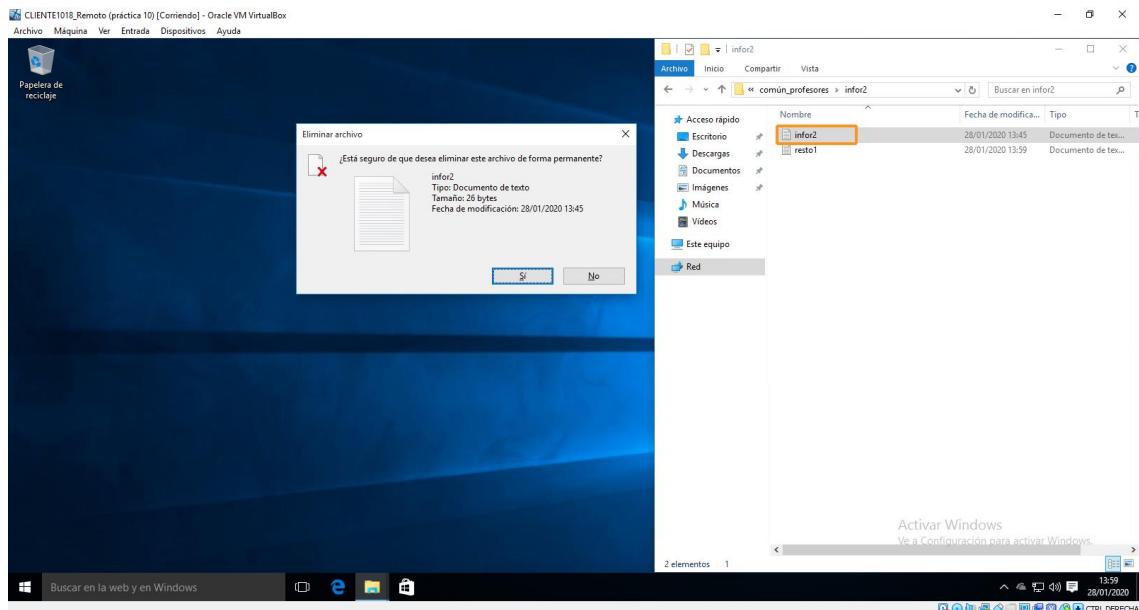
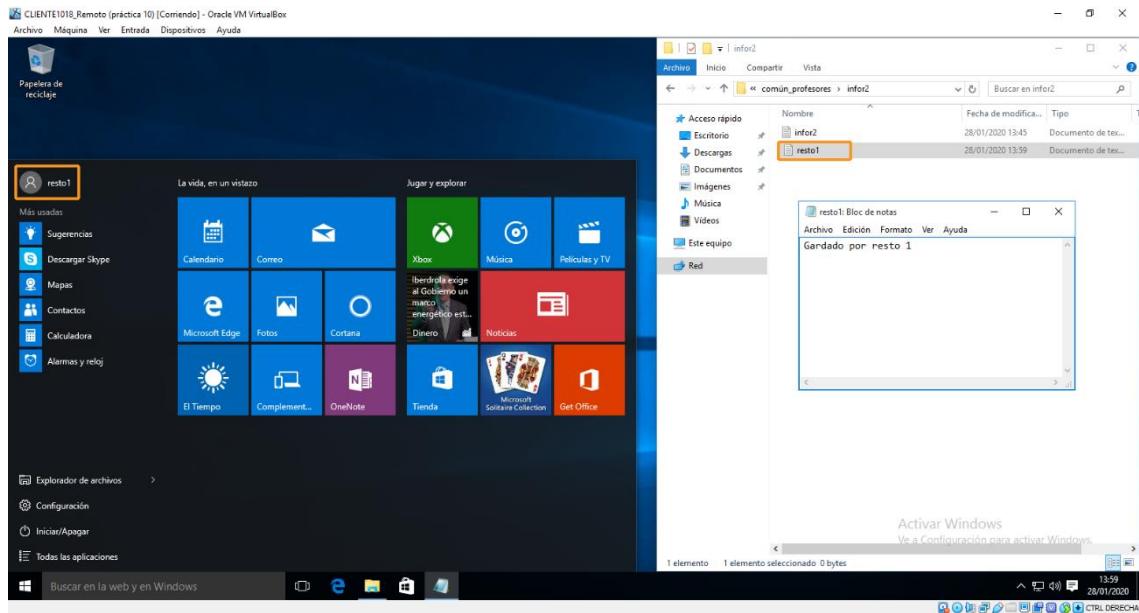
Como podemos comprobar, infor1 non pode eliminar nin crear arquivos.



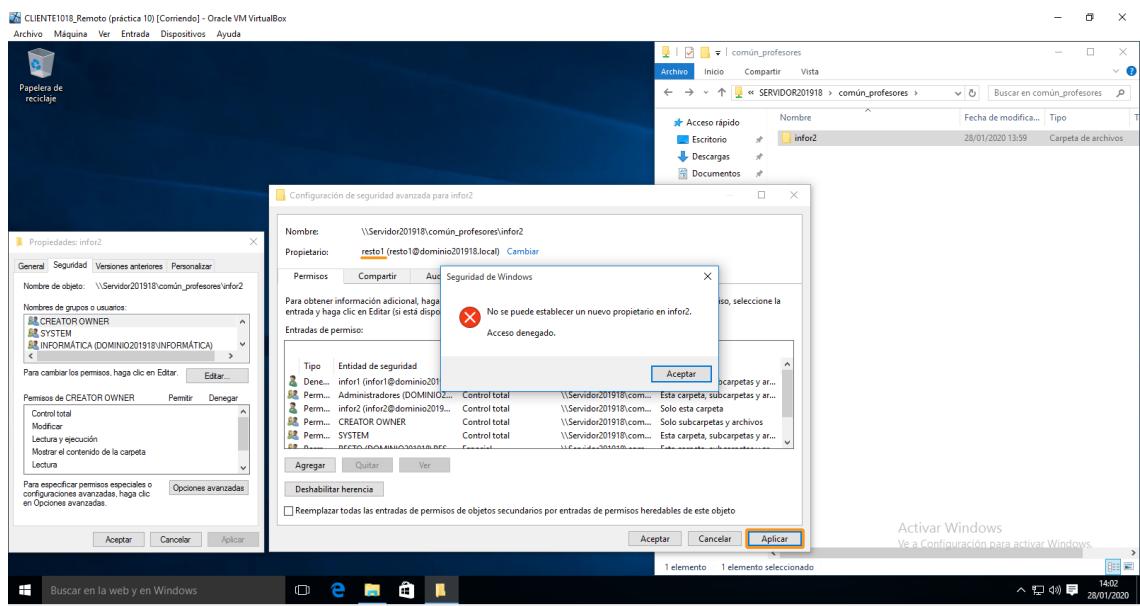
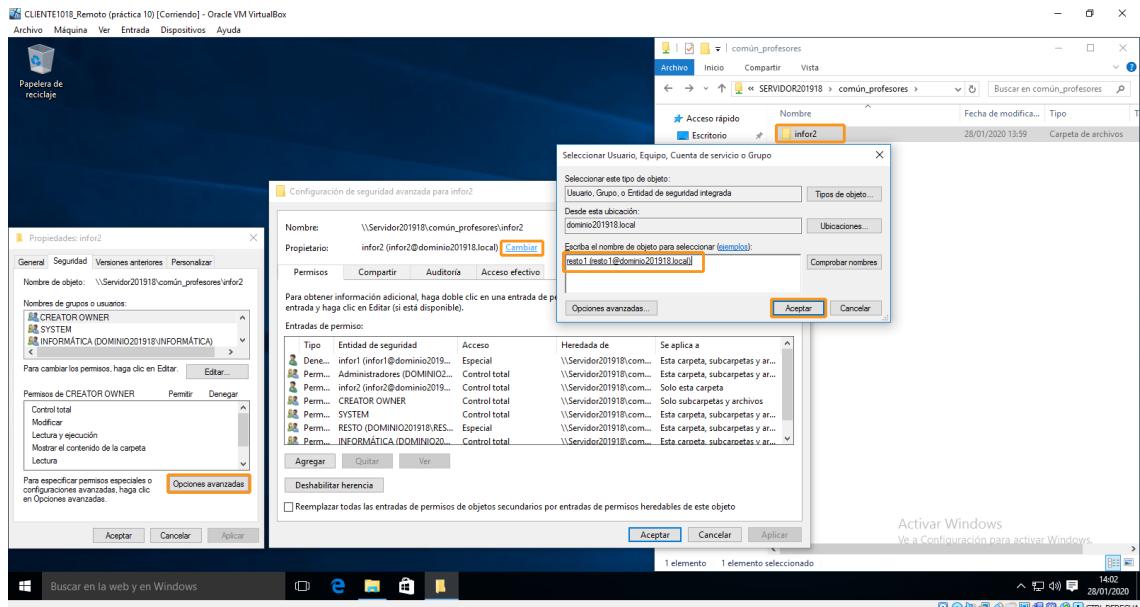
Pola contra, si que pode ler o seu contido. Por último, tratamos de tomar posesión do mesmo arquivo, acción para a que o profesor infor1 tampouco ten permisos.



A continuación, imos **facer login co usuario resto1** para comprobar os permisos do seu grupo. Como podemos observar, pode crear e eliminar archivos. A única restrición que lle configuramos foi a imposibilidade de modificar atributos e tomar posesión.

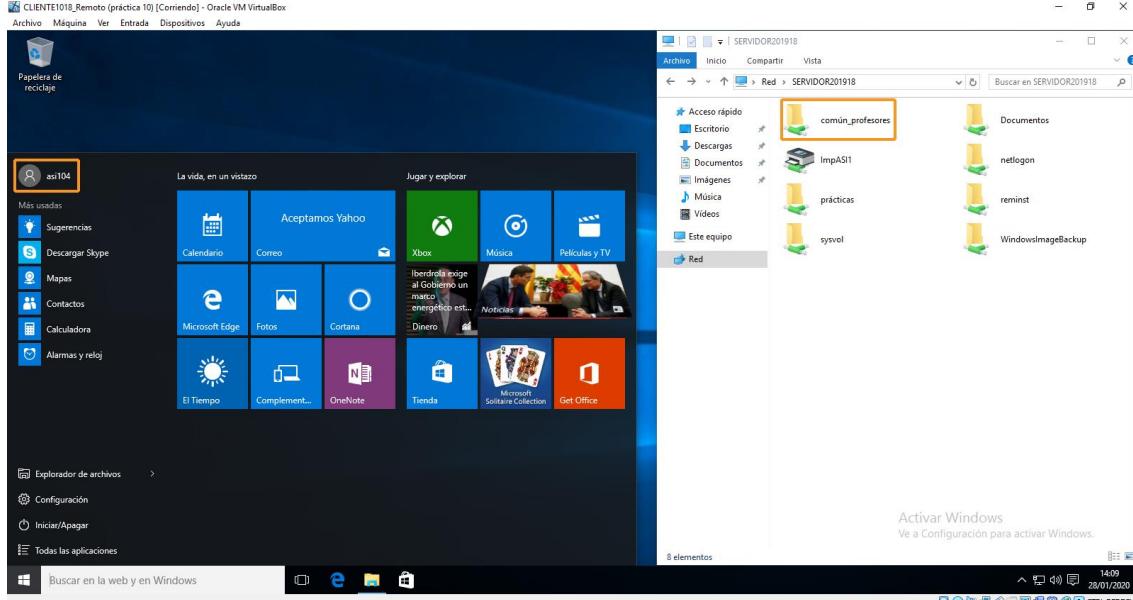
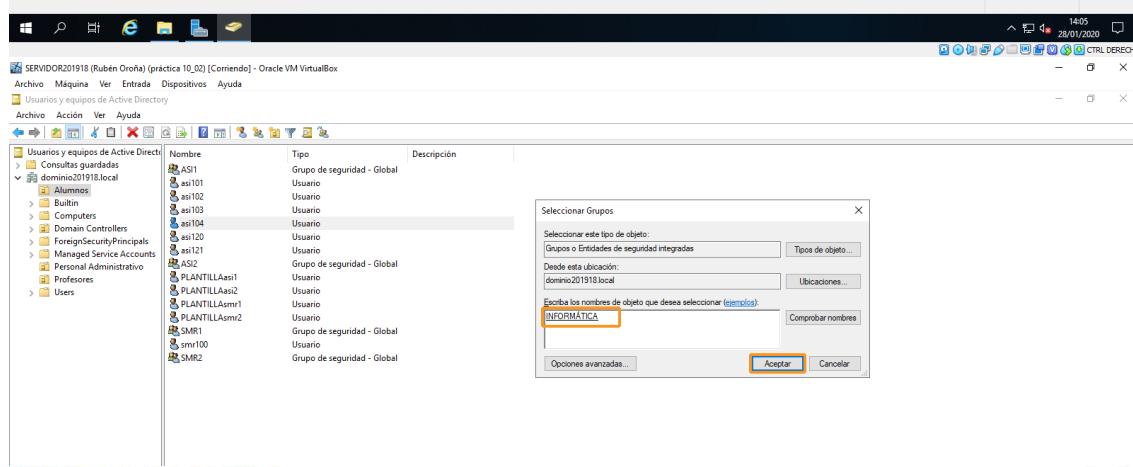
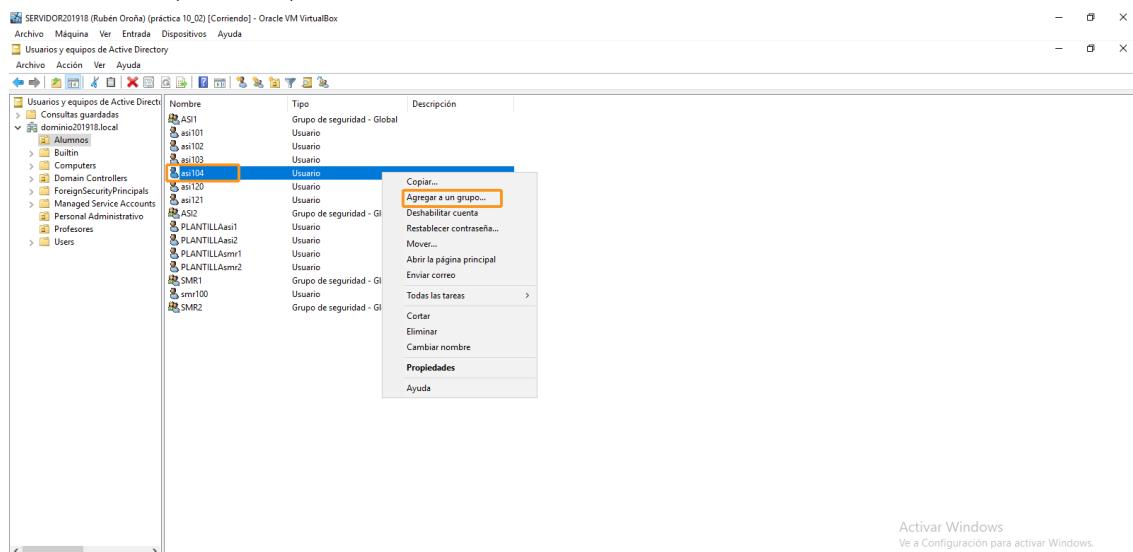


Polo tanto, para rematar tratamos de tomar posesión do cartafol creado antes por infor2, naturalmente sen éxito.

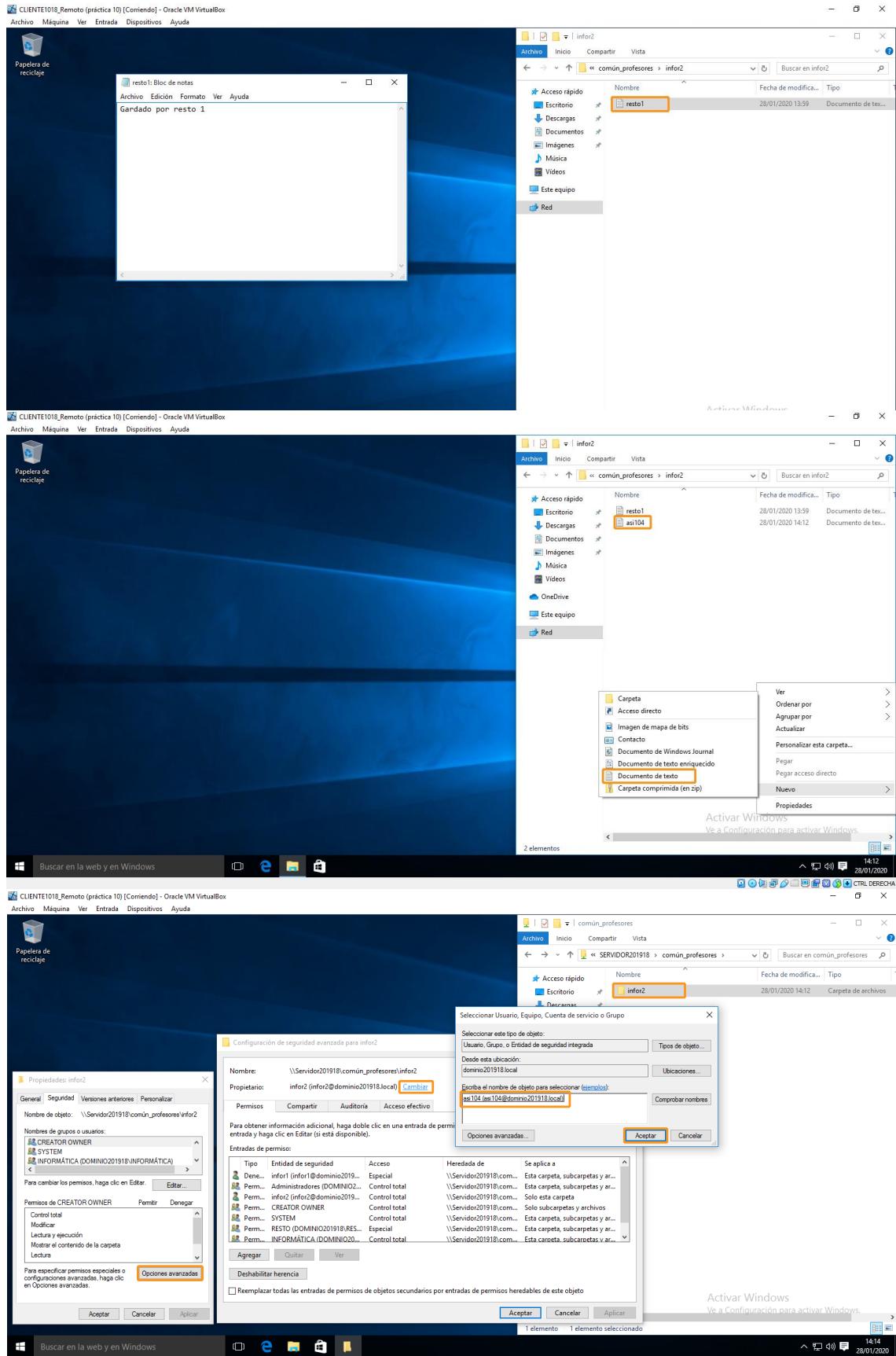


## H. Dar permisos de profesor a un alumno

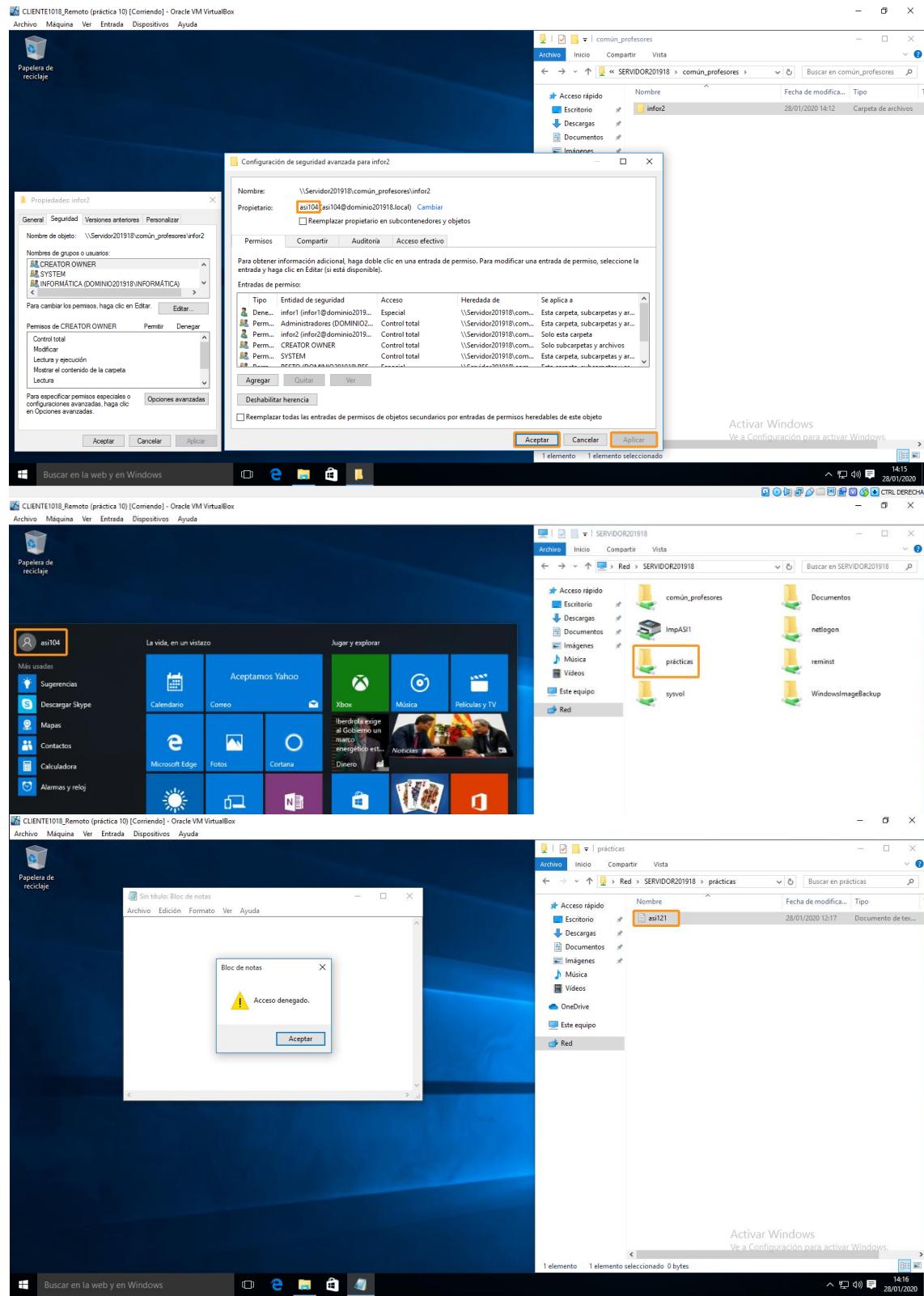
A premisa deste apartado é saber como poder outorgar permisos de profesor a un alumno específico, neste caso o asi104, de maneira puntual e sinxela. Tendo en conta isto, o mellor método é engadir o usuario asi104 ó grupo Informática, polo que herdará os privilexios de control total que estes posúen sobre o cartafol COMÚN\_PROFESORES.



Para comprobar o correcto funcionamiento dun usuario membro de dous grupos, imos comenzar por acceder con asi104 no cartafol COMÚN\_PROFESORES. Como podemos observar, este posúe control total, polo que pode crear archivos, ver o contido de outros...



A mostra máxima de control total é facerse coa propiedade dun arquivo creado por outro profesor, acción que podemos realizar de maneira satisfactoria. Para rematar, imos **acceder con asi104 no cartafol PRÁCTICAS**, para demostrar que os privilexios non se trasladan entre unidades compartidas áinda que o usuario pertenza a diferentes grupos do mesmo dominio. Como podemos comprobar, este alumno tampouco pode ver o contido dun arquivo creado por outro compañeiro.



## I. Configuración por defecto de permisos na raíz do disco C:

O obxectivo é comprender por que un usuario do dominio pode crear cartafoles pero non arquivos na raíz do volume principal (C:) Para elo, imos crear o usuario admin1 pertencente ó grupo Administrativos, que conta cos privilexios por defecto para calquera usuario do dominio. Se iniciamos sesión con esta conta dende o cliente Windows10 e consultamos os permisos de seguridade do disco principal, vemos como os usuarios por defecto teñen dereito a modificar subcarpetas e arquivos, ademais de a crear cartafoles só na raíz do volume (C:) Pola contra, vemos non existe o permiso para crear arquivos na mesma ubicación, o que explica que un usuario por defecto non posúa dereitos de escritura de arquivos pero si de cartafoles na raíz do disco principal.

