GRUPO DE TRABAJO

Practica sobre políticas de grupos de trabajo sobre Windows 10

Antonio Ferrer López

INDICE DE CONTENIDOS.

1. Introducción a la práctica.

a. Introducción

Con esta práctica se pretende explorar las posibilidades del editor de directivas de grupo local y la consola de administración de un sistema operativo Windows, así como, repasar los conceptos de grupos, usuarios y permisos.

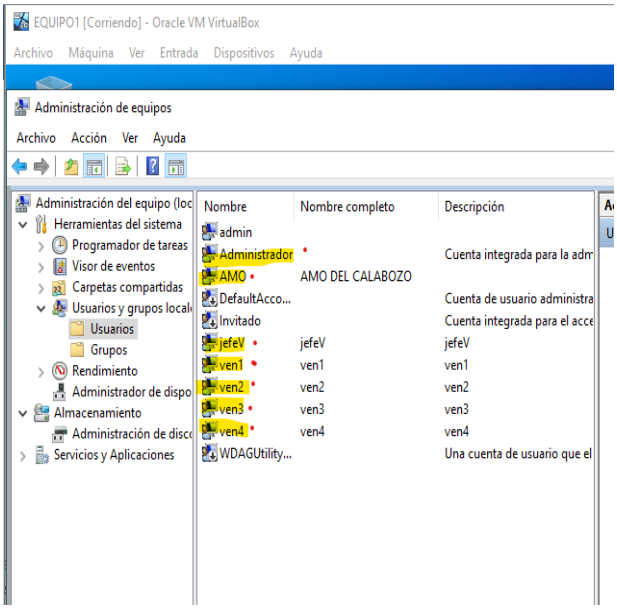
Para este caso se empleará la siguiente prueba de concepto:

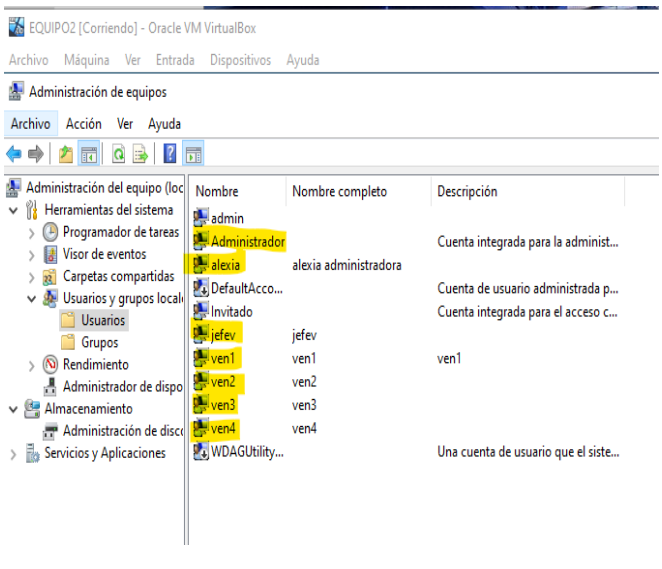
Se pretende implementar un plan de seguridad en una empresa la cual dispone de dos equipos EQUIPO 1 y EQUIPO 2, esta empresa está desarrollando dos proyectos y sus archivos se encuentran en la carpeta raíz proyectos ubicada el en EQUIPO 1.

Se pretenden establecer una serie de políticas de seguridad para dicha organización, las cuales serán exploradas a lo largo de la práctica.

b. Los usuarios.

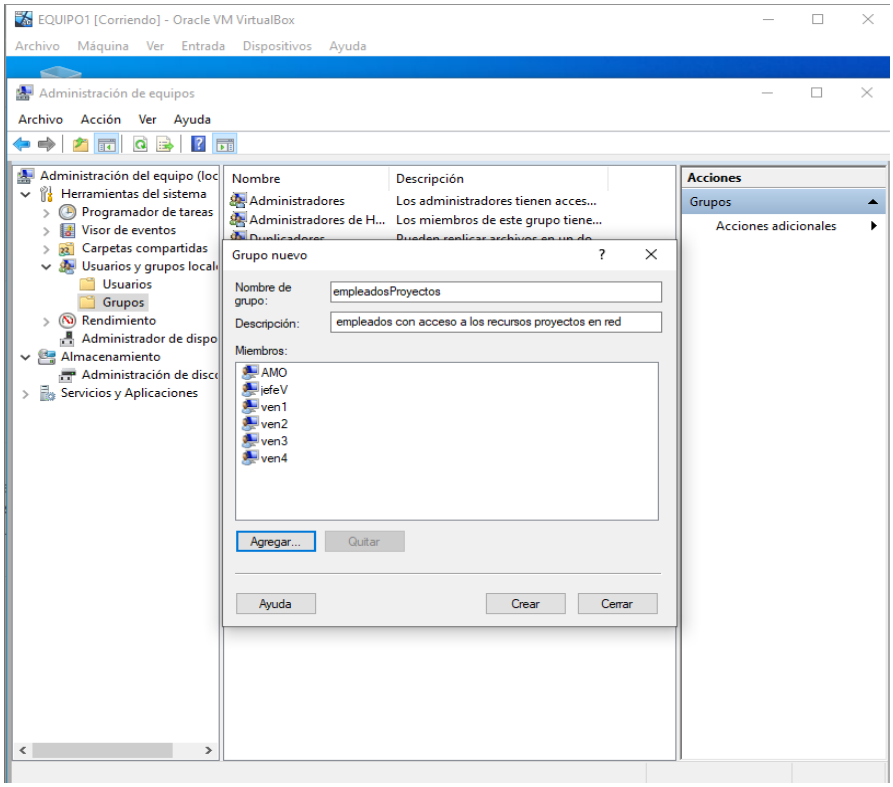
NOMBRE DE USUARIO	DESCRIPCIÓN	EQUIPO
administrador	Administrador del sistema.	1 y 2
AMO	Director de la empresa.	1
ven1	Vendedor 1 equipo de ventas del proyecto 1	1 y 2
Ven2	Vendedor 2 equipo de ventas del proyecto 1	1 y 2
Ven3	Vendedor 3 equipo de ventas del proyecto 2	1 y 2
Ven4	Vendedor 4 equipo de ventas del proyecto 2	1 y 2
Alexia	Administrativa de la empresa (No es administrador informático)	2
jefeV	Jefe del departamento de ventas	1 y 2





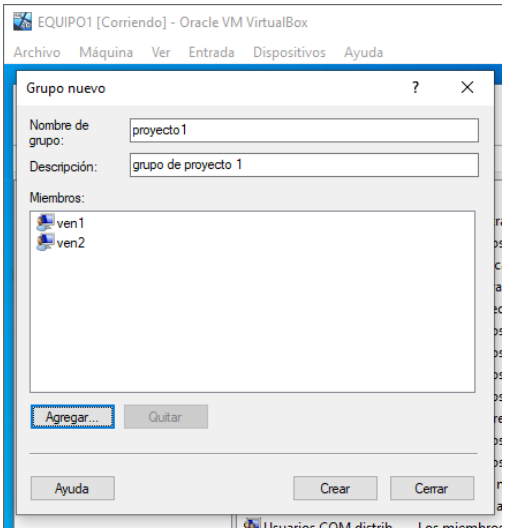
GRUPO	DESCRIPCIÓN	USUARIOS
empleadosProyectos	Grupo de empleados con acceso a la carpeta de proyectos por medio de la red local	Ven1, ven2, ven3, ven4, jefeV, AMO

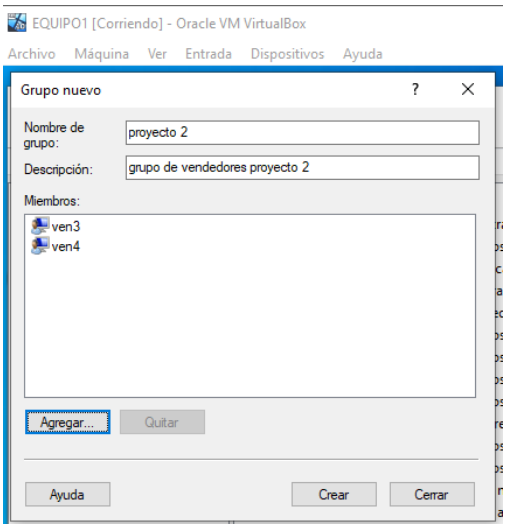
Para el acceso a los recursos compartidos en el equipo 1, se crea un grupo al que pertenecerán los usuarios que precisen del acceso a este recurso.



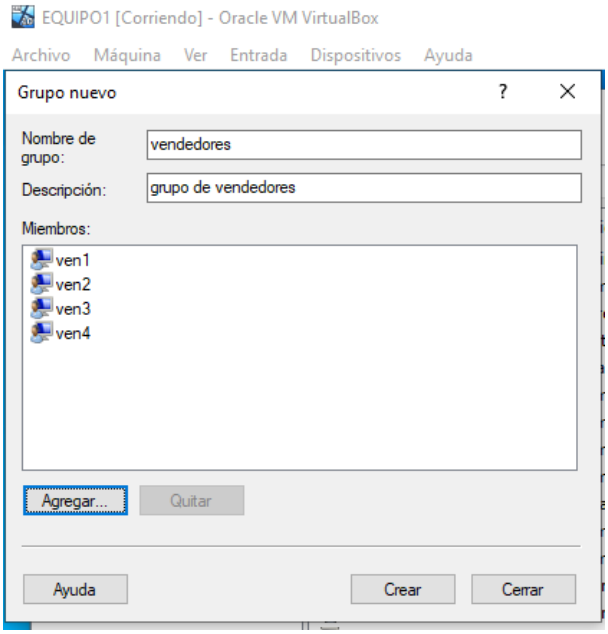
d. Grupos de usuarios

Con el fin de gestionar los permisos de los vendedores asignados a los proyectos, crearemos en EQUIPO 1 dos grupos para sendos proyectos en los que incluiremos a los vendedores que participaran en ellos.

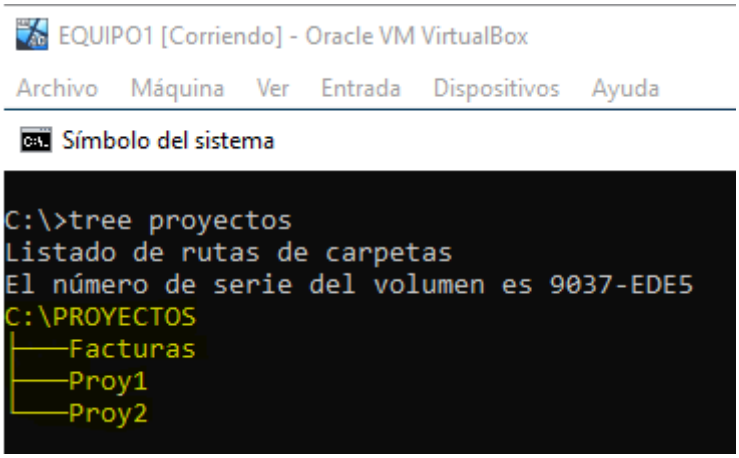




También crearemos un grupo para los vendedores, de esta forma podremos gestionar sus privilegios en conjunto.



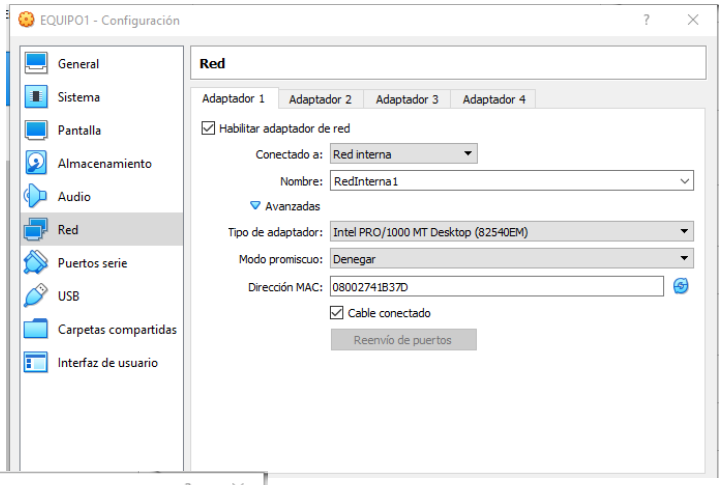
e. El árbol de archivos.

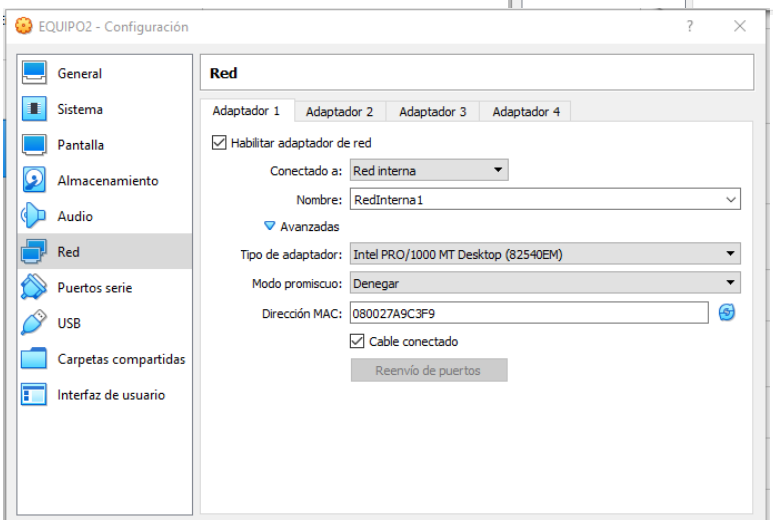


2. Compartiendo repositorio del proyecto en red.

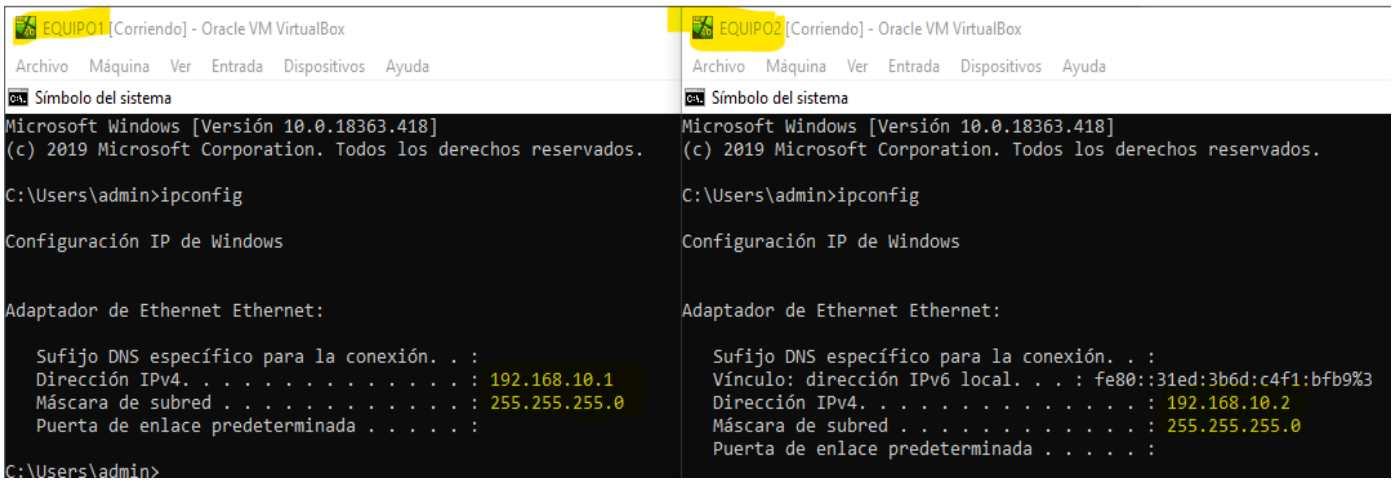
Antes de compartir el recurso vamos a comprobar la configuración de las máquinas virtuales para poder realizar este paso.

Configuraremos el tipo de red en ambas máquinas como *RED INTERNA* y comprobaremos que la *MAC* de cada uno de estos sea diferente.

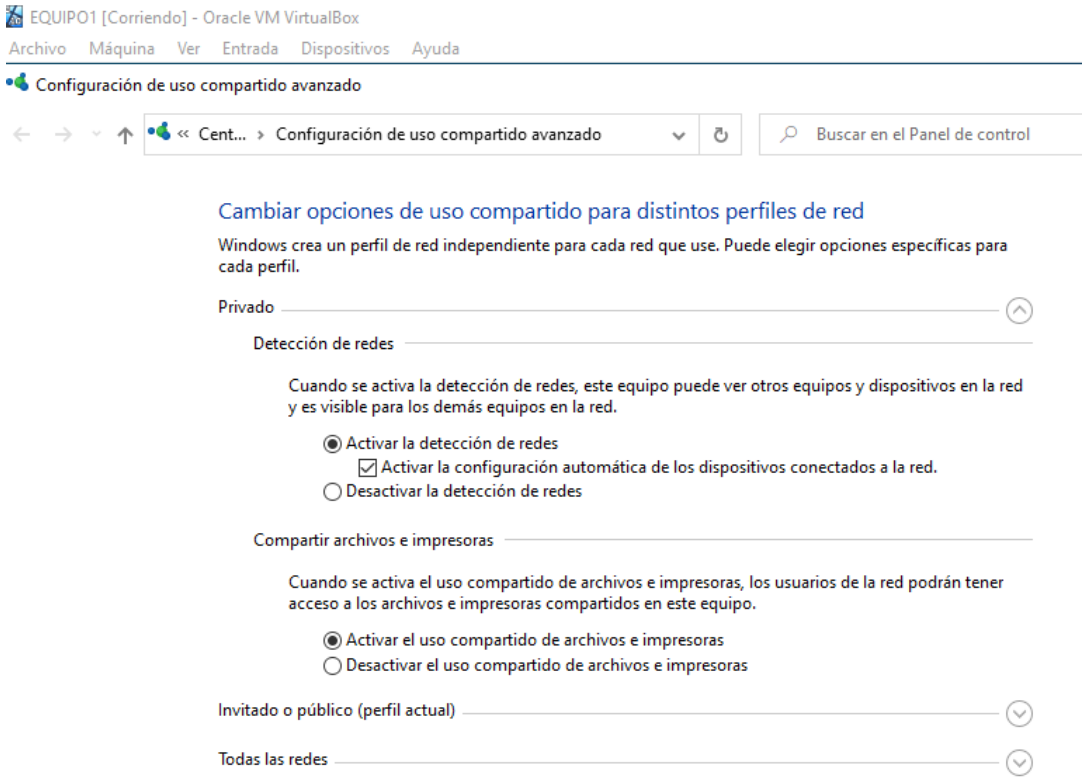




Posteriormente configuramos las direcciones IP de cada una de las máquinas para que estén en la misma red local tal y como podemos observar en las siguientes capturas:

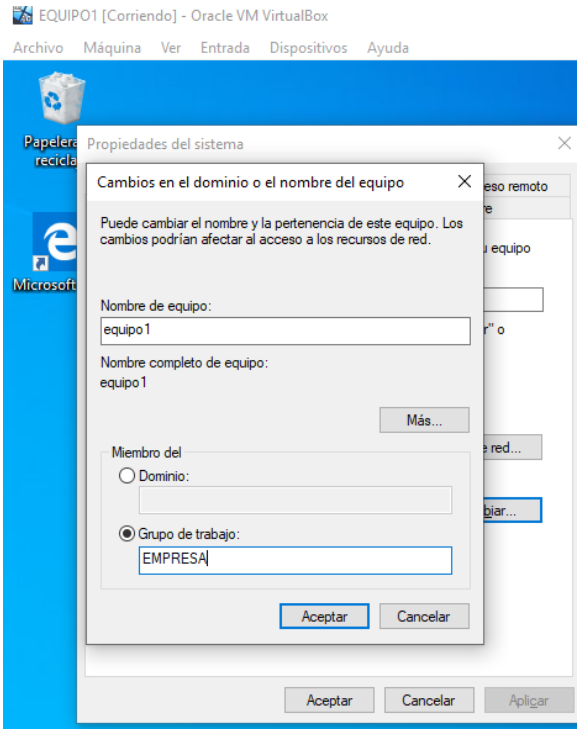


Una vez configurado, comprobaremos la configuración de uso compartido, en ambos equipos debe ser como se muestra a continuación:

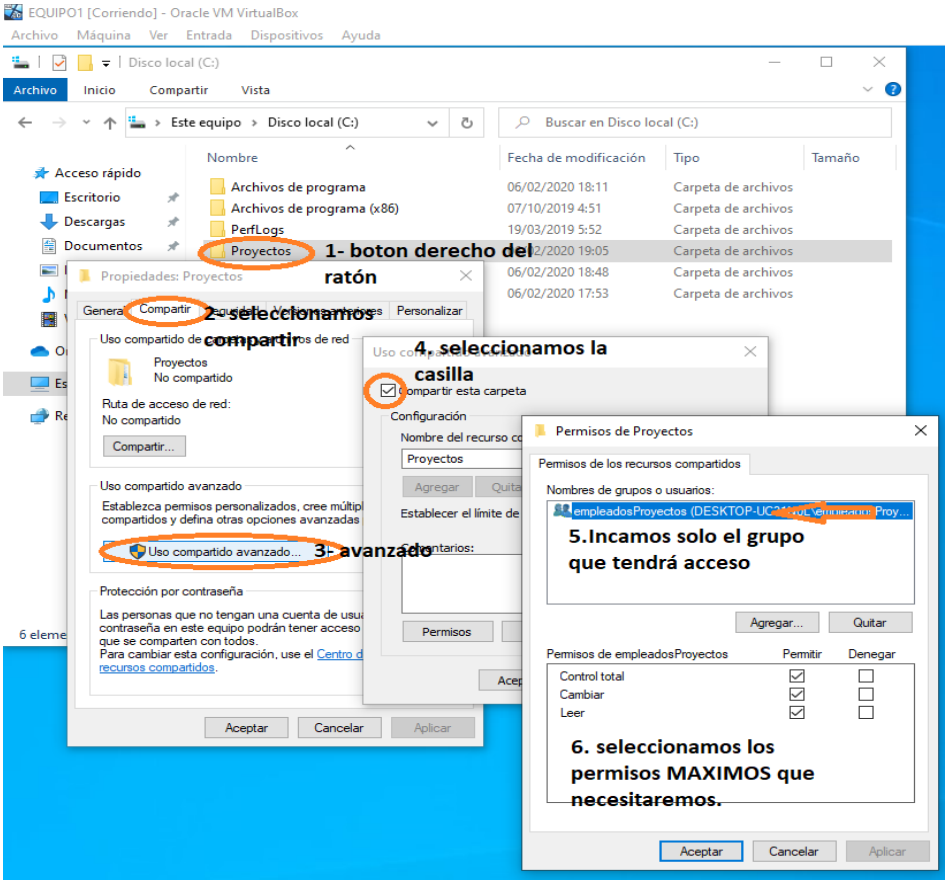


El siguiente paso es configurar el grupo de trabajo y los nombres de equipo de cada máquina, en este caso el grupo de trabajo (COMÚN A AMBOS EQUIPOS) es empresa y los nombres de equipo serán los propios (EQUIPO 1 y EQUIPO 2)

Como muestra, podemos ver la captura de la configuración del equipo 1



Finalmente, compartimos la carpeta configurando el grupo de usuarios que accederán a esta a través de la red y asignándole los permisos máximos que necesitemos, posteriormente limitaremos los permisos de cada uno de los usuarios según requisitos.



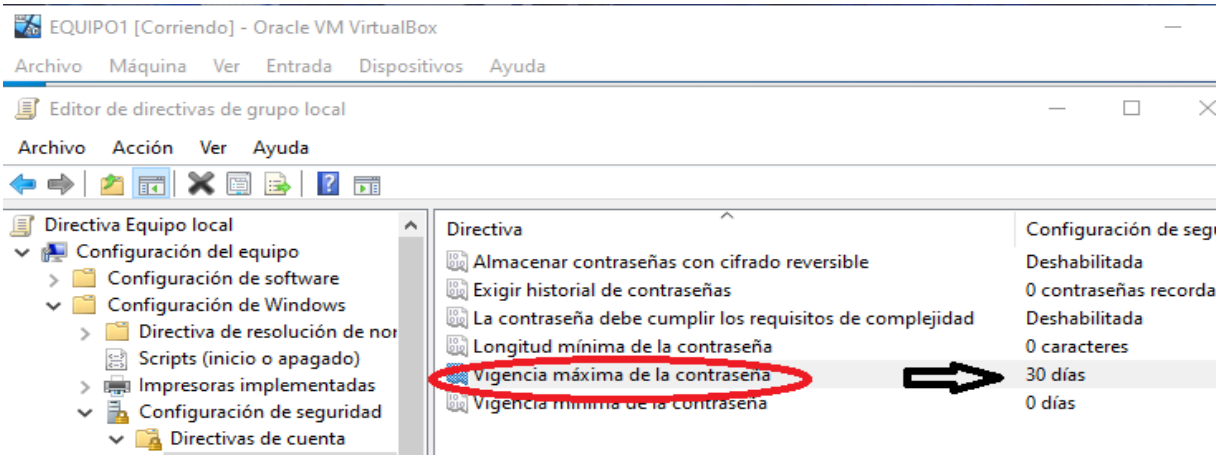
3. EL PLAN DE SEGURIDAD.

A efectos prácticos, en caso que se repitan las configuraciones en varios equipos, usuarios etc., y no suponga una falta de información, se mostrará una captura representativa de dicha configuración.

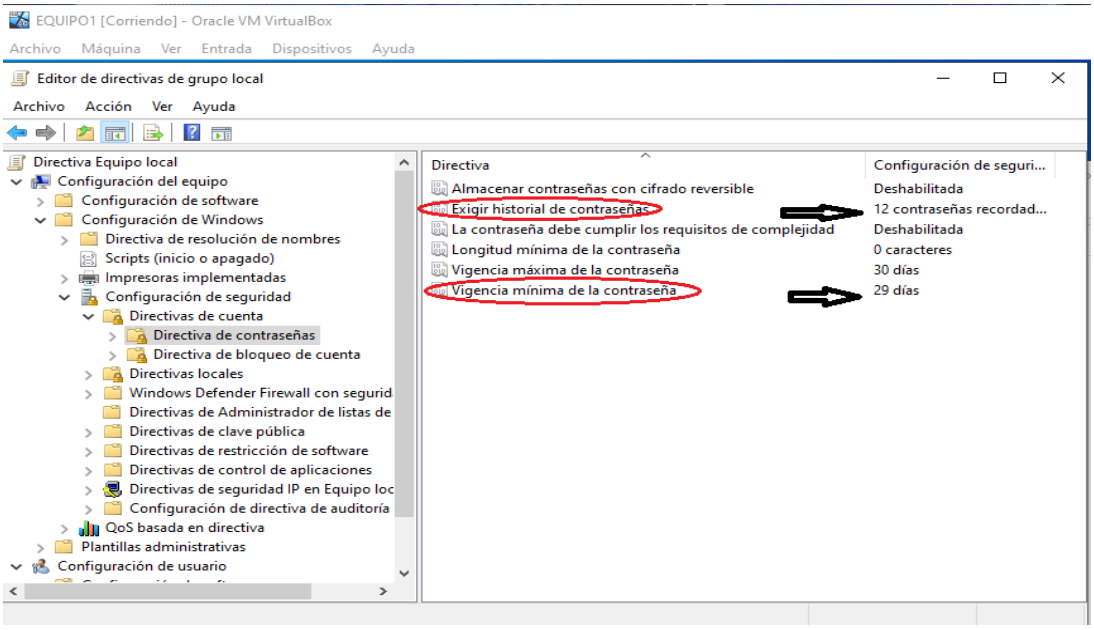
a. Sobre las contraseñas.

<u>Los usuarios deben cambiar su contraseña cada 30 días y sólo entonces, no pudiendo repetirse en un año.</u>

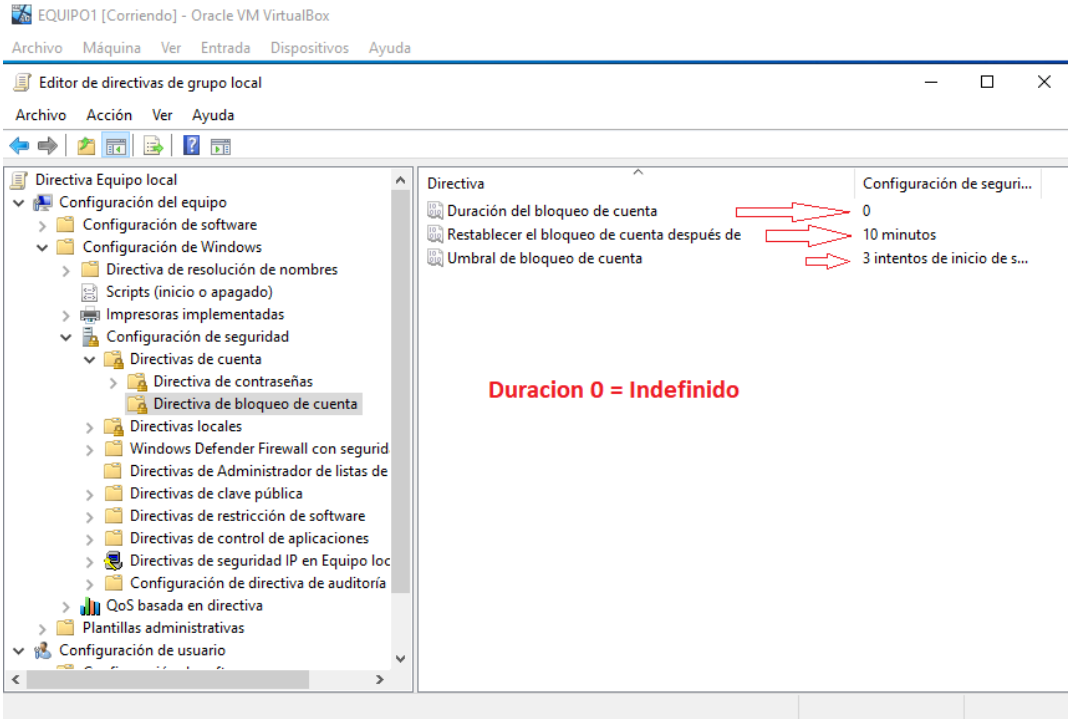
Primero estableceremos las vigencia MAXIMA de la contraseña que será en 30 días



Puesto que en 12 meses no se debe volver a repetir la contraseña , habilitaremos exigir historial de contraseñas en 12 y la vigencia mínima de contraseña en 29, de esta manera en las 12 veces que se cambie en un año no se podrán repetir las contraseñas .



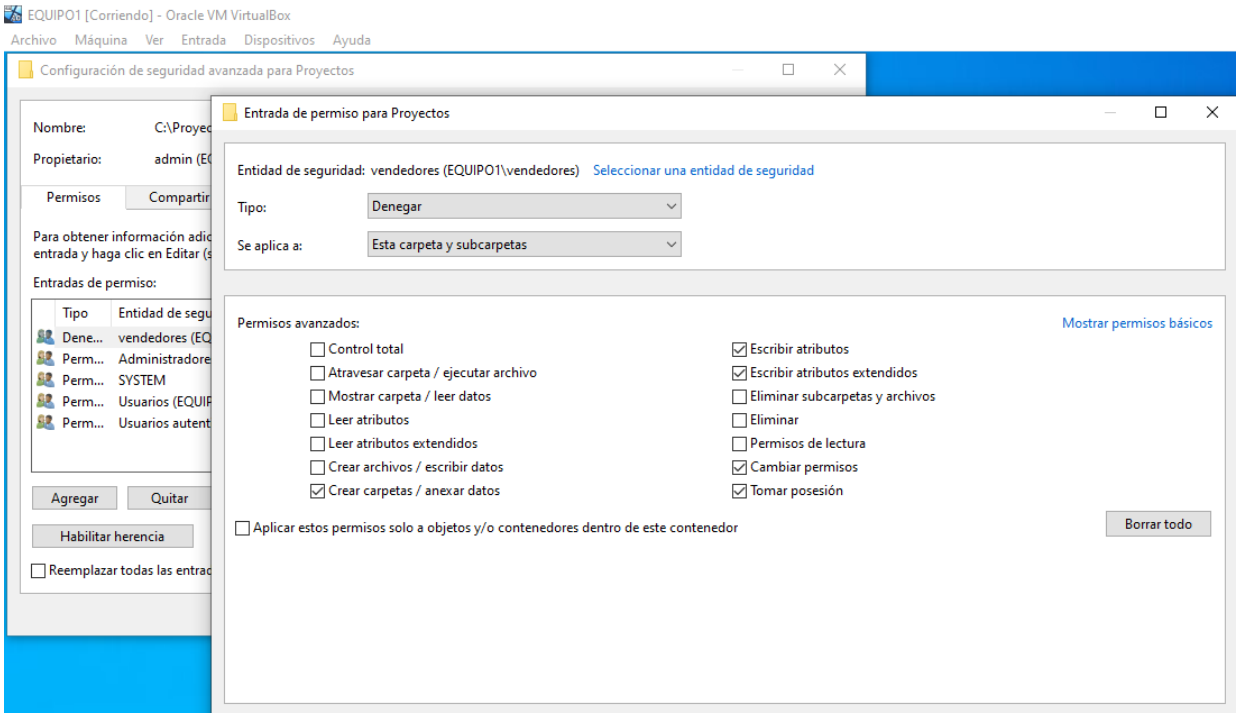
<u>Si se detectan tres acreditaciones fallidas, a lo largo de diez minutos a una cuenta de usuario, ésta debe quedar bloqueada indefinidamente.</u>



b. Sobre Proyectos.

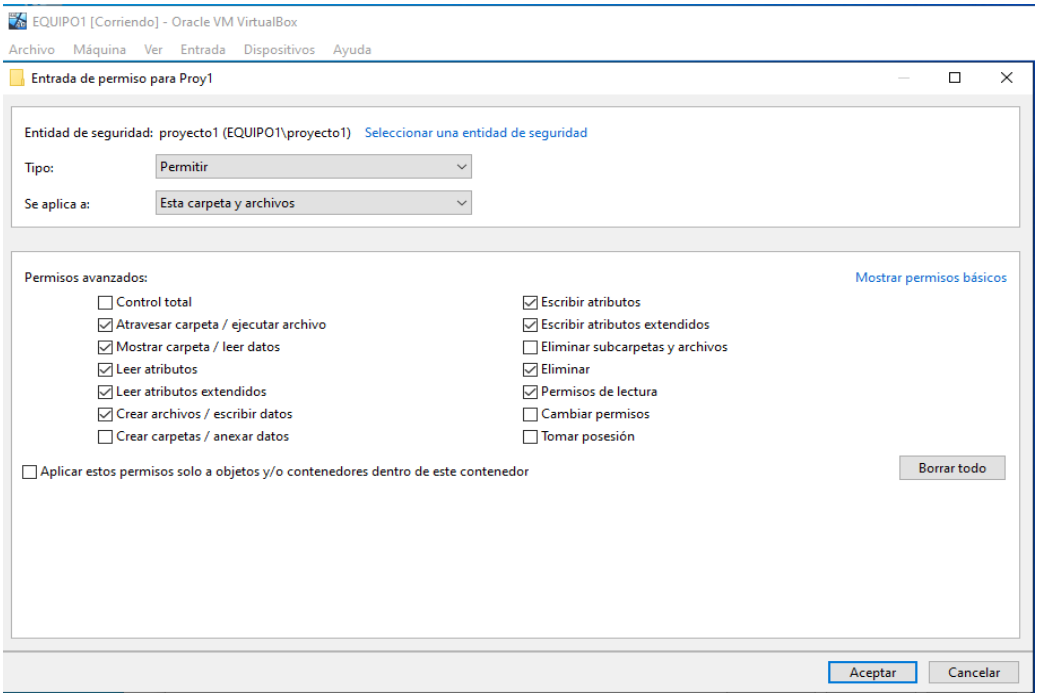
nota inicial: se deshabilita la en todas las configuraciones de seguridad

Cada proyecto tiene asociada una carpeta (proy1 y proy2, que están dentro de la carpeta C:\Proyectos, ubicada en equipo1), ningún vendedor puede modificar los nombres de las carpetas proy1 y proy2, sólo el jefe de ventas.

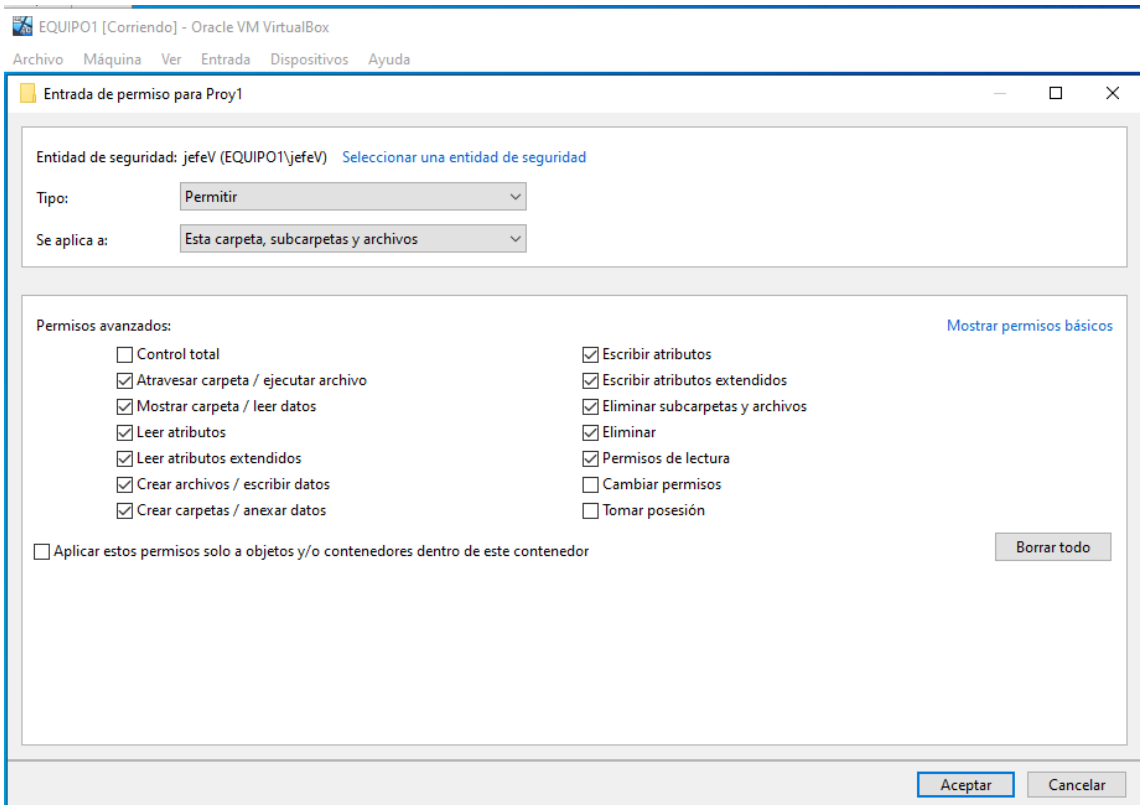


Cada vendedor puede leer el contenido de su carpeta, crear, modificar y eliminar archivos. No podrán crear ni eliminar ninguna carpeta adicional, eso será tarea del jefe de ventas.

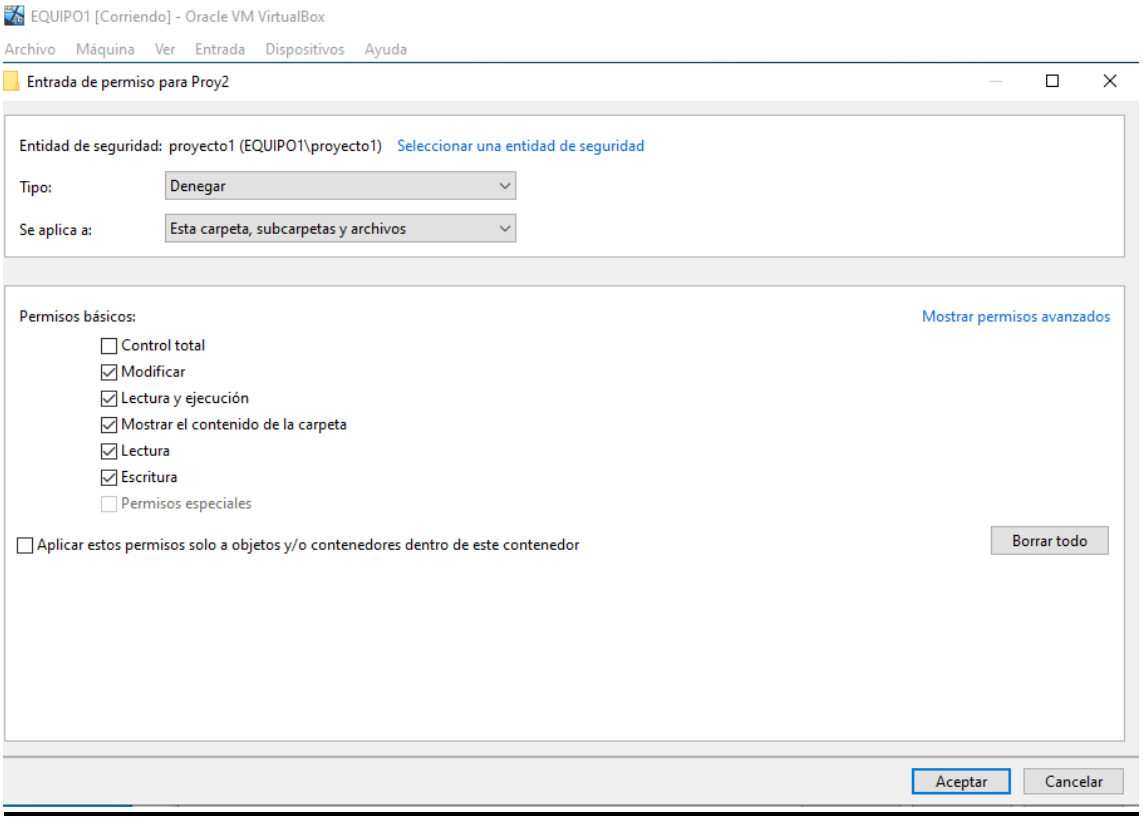
Vendedores:



Jefe de ventas:

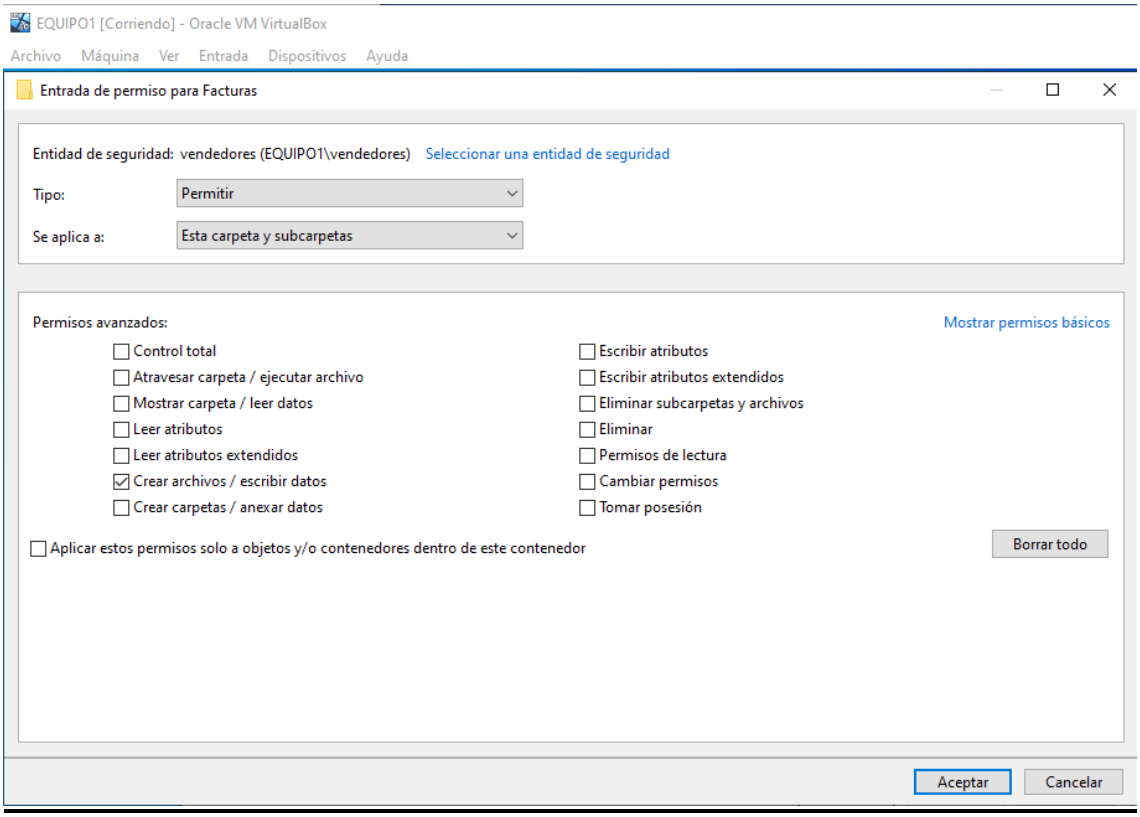


Los vendedores sólo podrán entrar en su carpeta.

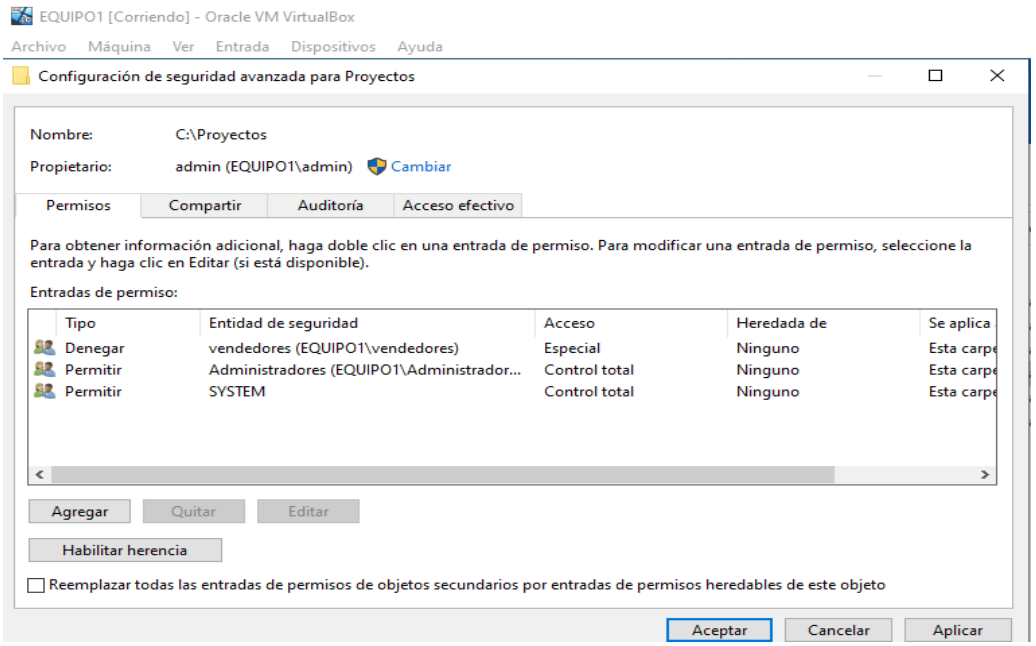


Eliminaríamos los permisos en el directorio proy1 del equipo de proyecto 2 y viceversa.

En la carpeta Proyectos, hay una carpeta llamada Facturas, donde los vendedores podrán dejar archivos, pero nunca ver su contenido.



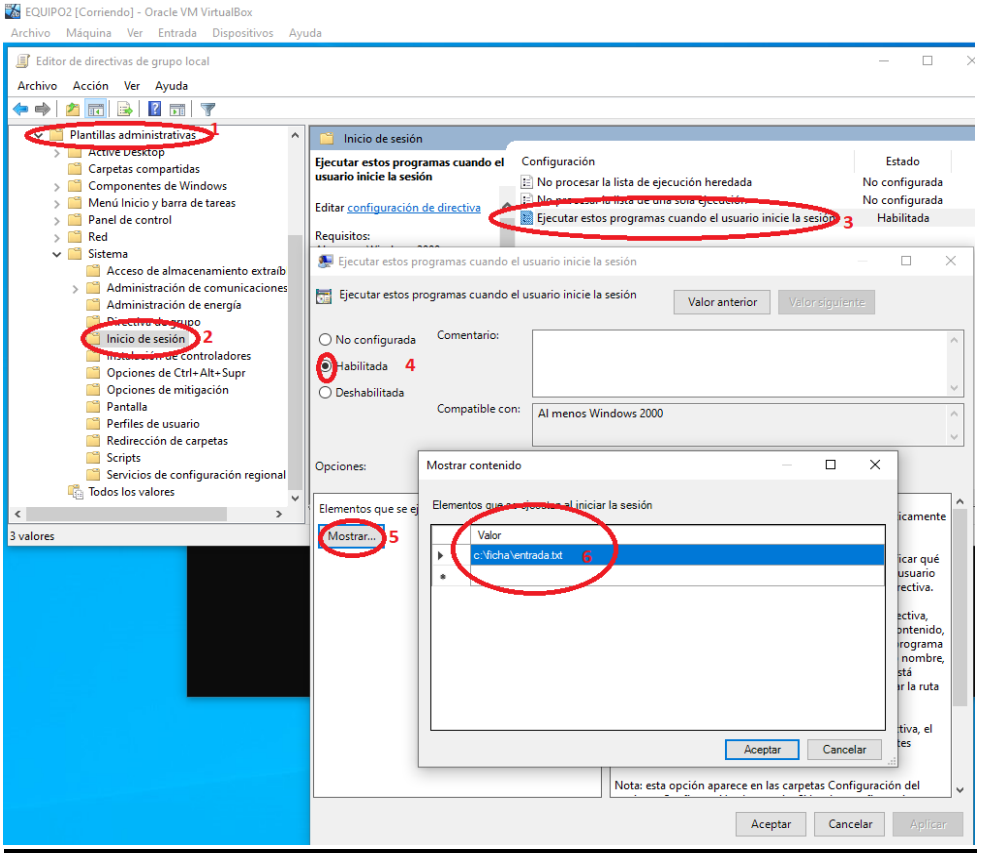
Sobre el resto de usuarios. En la organización pueden existir otros usuarios, actúales o futuros, no vinculados a ningún proyecto, los cuales no deben tener ningún permiso de acceso a la carpeta Proyectos.



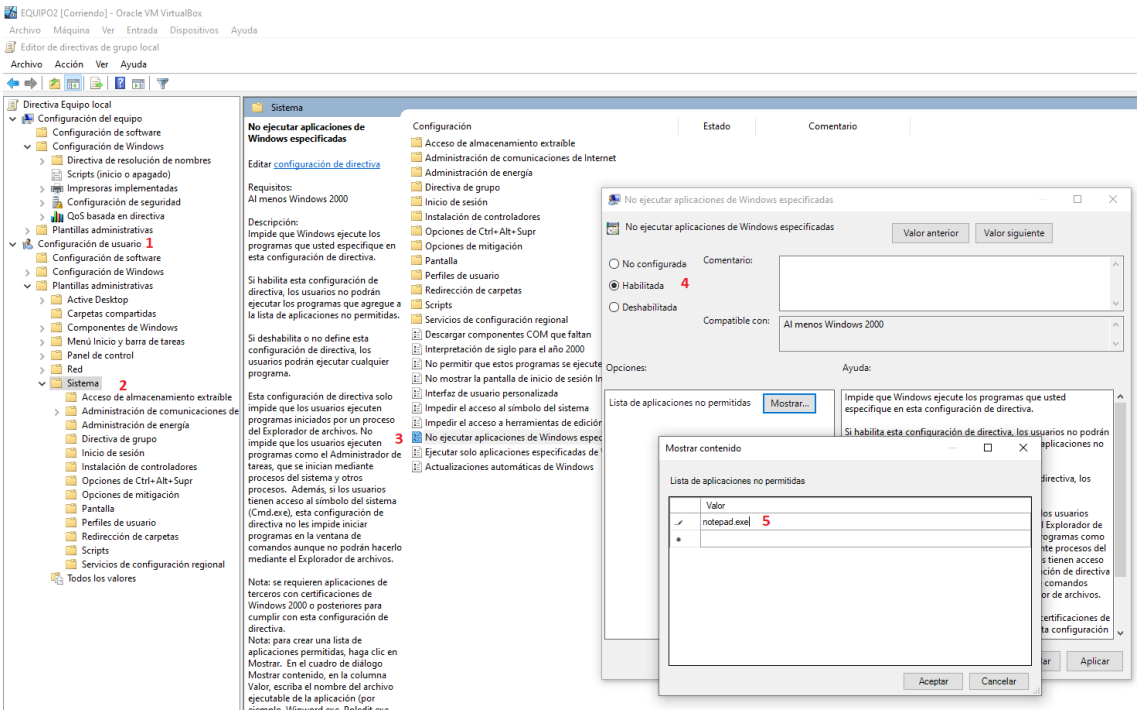
Solo mantenemos los grupos y usuarios que deseemos que accedan al repositorio.

c. Sobre EQUIPO 2

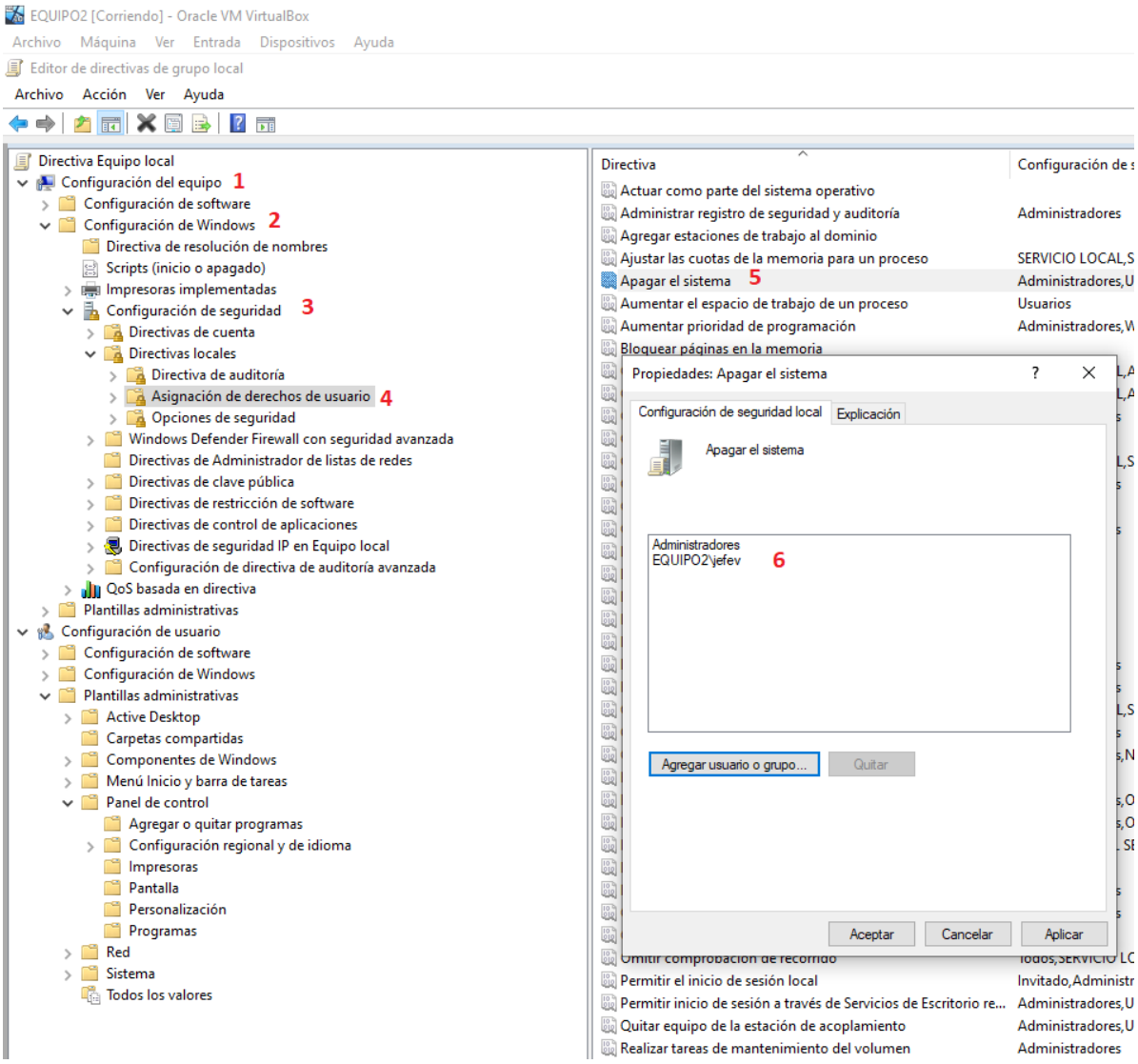
Al iniciar sesión queremos que a los usuarios se les abra automáticamente el archivo Entrada.txt (ubicado en C:\Ficha\).



Todos los usuarios del equipo tendrán imposibilitado el uso del Bloc de Notas.

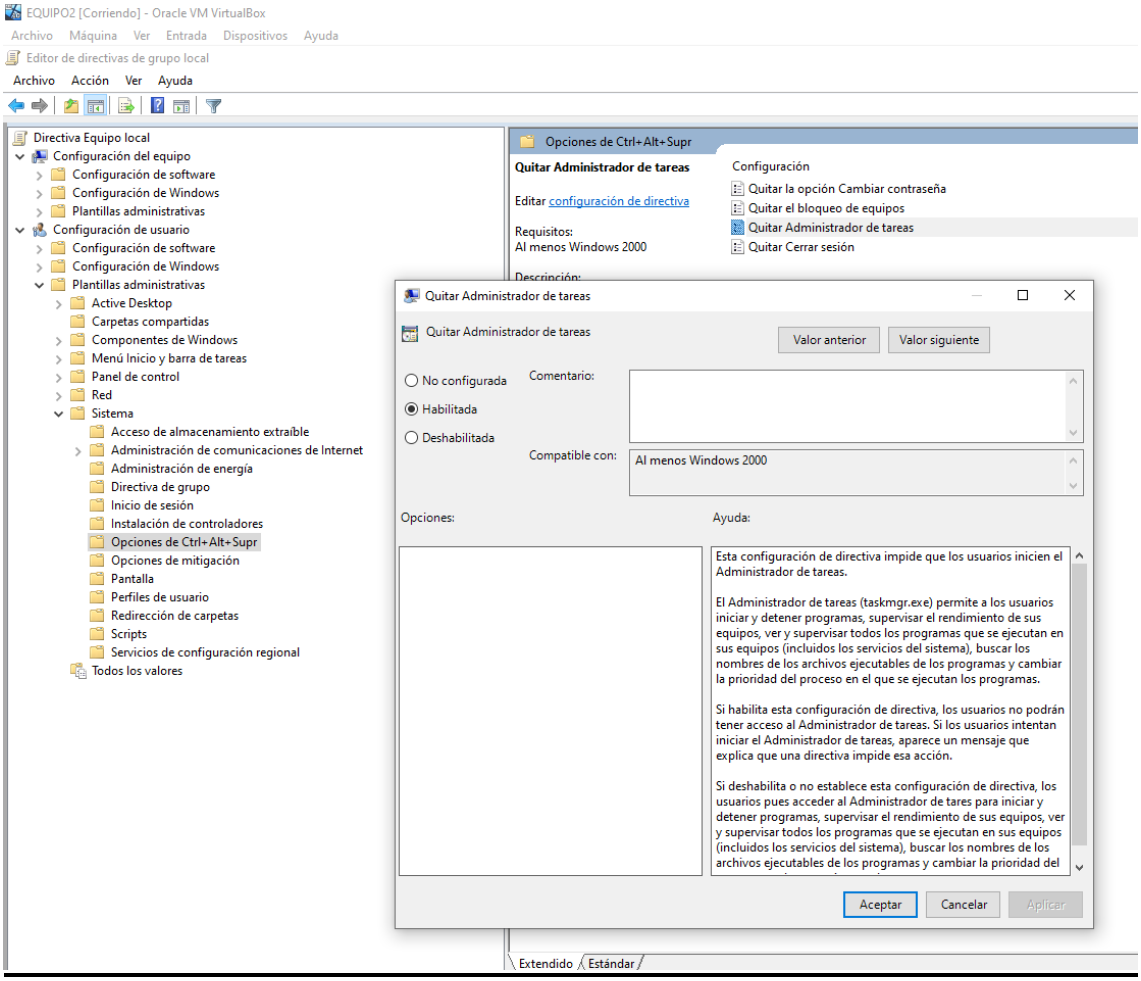


Sólo el jefe de Ventas y el Administrador podrán apagar el equipo.

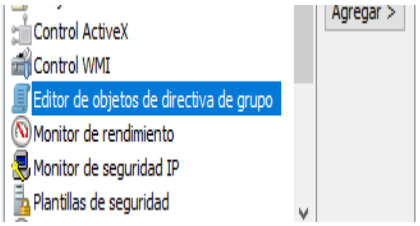


En la lista de usuarios o grupos que pueden apagar el sistema, debemos dejar los usuarios que se les va a permitir realizarlo.

No queremos que los usuarios no administradores, puedan entrar en el Administrador de tareas al pulsar Ctrl+Alt+Supr.

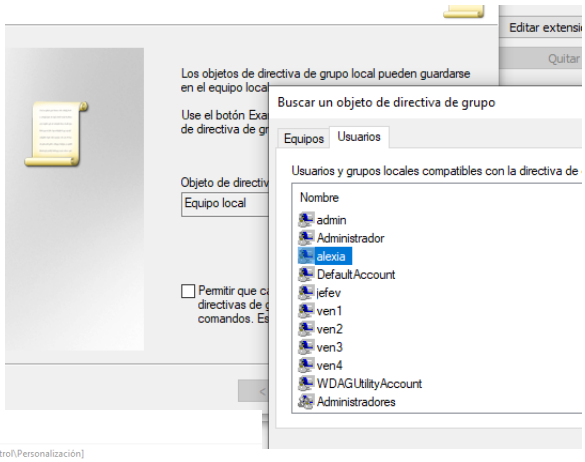


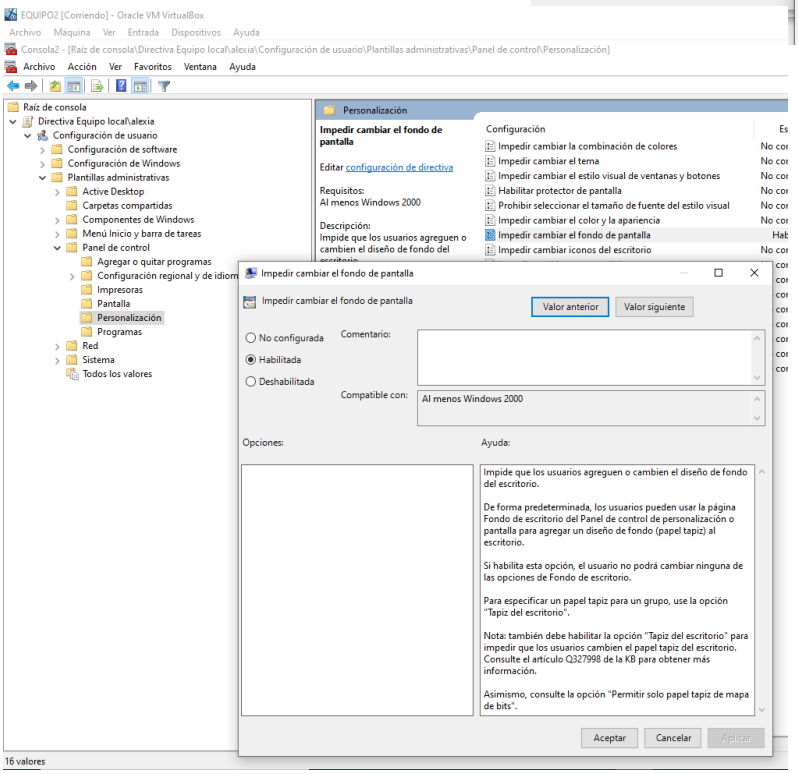
Alexia, no deseamos que pueda cambiar el fondo de la pantalla.



Creamos con MMC una nueva directiva de grupo.

Seleccionamos el usuario Alexa para aplicarle la restricción

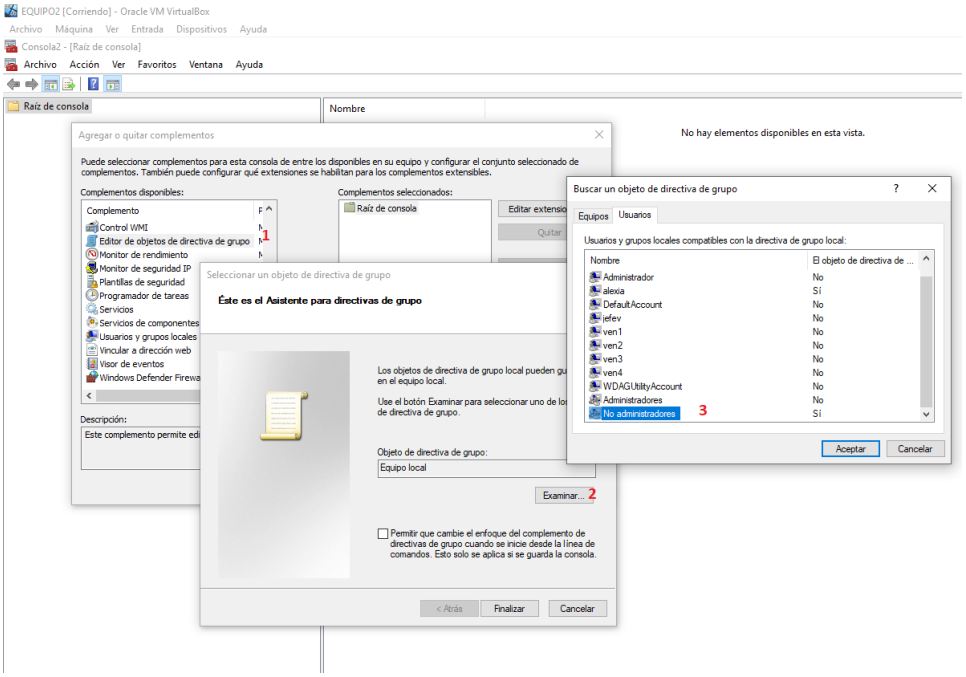




Aplicamos la restricción que corresponda, en este caso,

plantillas administrativas -> panel de control -> personalización -> Impedir cambiar fondo de pantalla

Para todos los usuarios, menos los administradores, deseamos que, al borrar un archivo en el explorador, se eliminen definitivamente sin ir a la Papelera de reciclaje.



Empleando MMC creamos un nuevo objeto de directiva de grupo, al crearlo, seleccionaremos todos los usuarios EXCEPTO administradores, de esta manera, esta política se aplicará a todos los usuarios que no sean administradores.