Davante

Gestión de usuarios y seguridad

Actividad 8

Título del índice

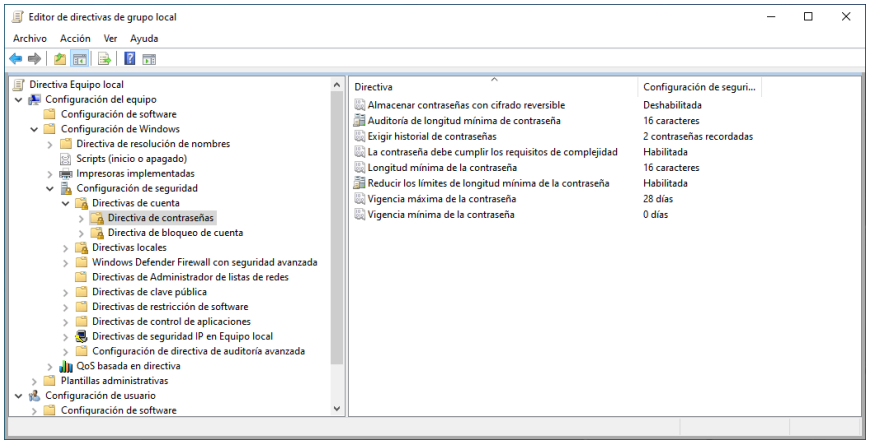
Introducción

La empresa ha encargado al departamento técnico crear y gestionar un sistema de grupos y permisos para organizar de forma segura y sencilla de mantener el acceso que tiene cada empleado a los recursos compartidos de la empresa. Para ello, vamos a tener que crear usuarios y grupos en múltiples sistemas operativos según las necesidades de cada departamento. Los departamentos de administración y dirección necesitan Windows y el equipo técnico utiliza Linux para sus equipos y servidores de la empresa.

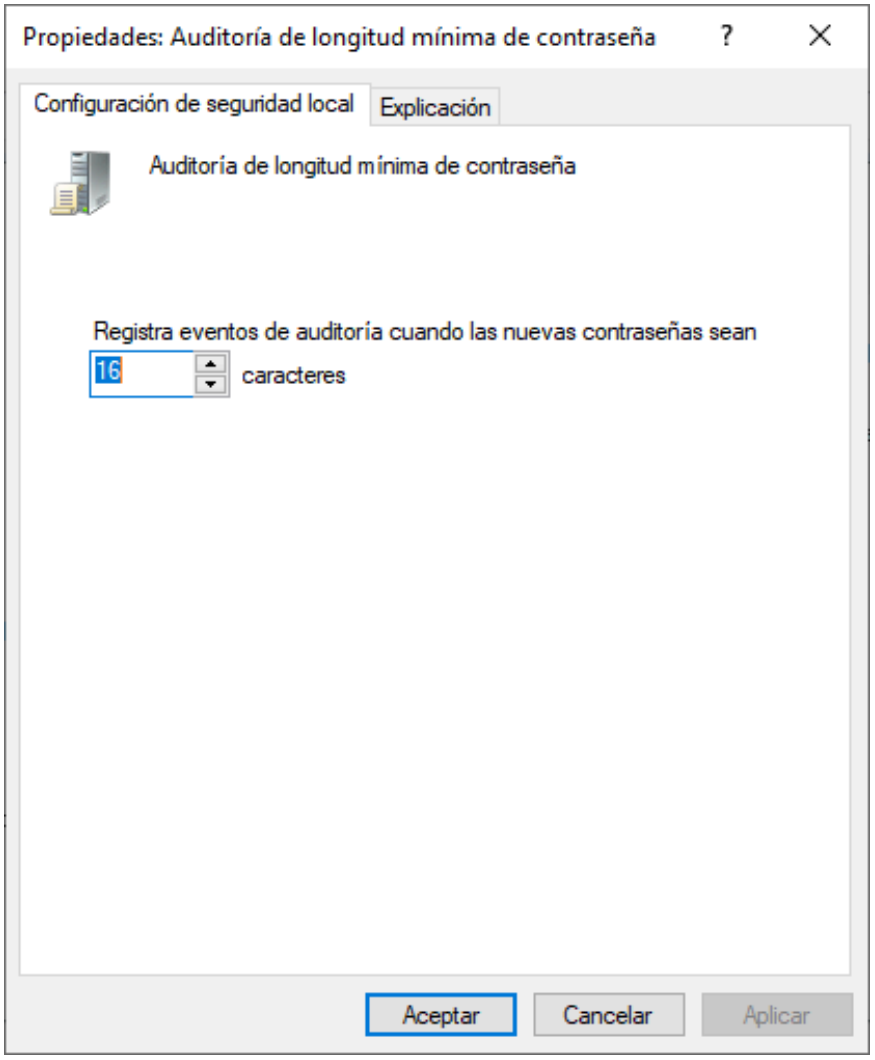
Creación y gestión de usuarios y grupos

Windows

1. Políticas de contraseñas seguras

a. 

Busca “Directivas de seguridad” y abre este programa. Dentro, navega por la columna lateral izquierda a través de “Configuración de equipo”, “Configuración de Windows”, “Configuración de seguridad”, “Directivas de cuenta”, hasta “Directiva de contraseñas”.

b. 

Para editar una directiva haz clic derecho sobre ella y pulsa en “Propiedades”. Te aparecerá un menú similar a este. Puedes encontrar una explicación arriba a la derecha y, en el centro, el ajuste a modificar. Una vez terminado, pulsa “Aceptar” para guardar los cambios.

c. Hemos decidido aplicar las siguientes directivas:

   i. **Almacenar contraseñas con cifrado reversible:** Desactivado.
   Era la opción por defecto y la hemos considerado innecesaria por ahora ya que no tenemos planeado utilizar ningún protocolo que lo requiera.

   ii. **Auditoría de longitud mínima de contraseña:** 16 caracteres
   La he definido con la misma cantidad que la longitud mínima de contraseña; lo que tiene un efecto similar a no establecer ningún valor.

iii. **Exigir historial de contraseñas:** 2
Permite al sistema recordar las últimas 2 contraseñas. Esto mejora la seguridad, al no permitir que se repitan las contraseñas más recientes.

iv. **La contraseña debe cumplir los requisitos de complejidad:** Habilitada
Al habilitar esta opción, el sistema obligará al usuario a establecer una contraseña segura, en lugar de mostrar una advertencia y permitir la contraseña insegura igualmente, como hace por defecto. Además, también obliga a introducir, como mínimo, un carácter especial, un número, una letra mayúscula, y una minúscula.

v. **Longitud mínima de contraseña:** 16 caracteres
Exige al usuario a establecer una contraseña de un mínimo de 16 caracteres. Hemos considerado esta longitud como suficiente, pero cuanto más larga mejor.

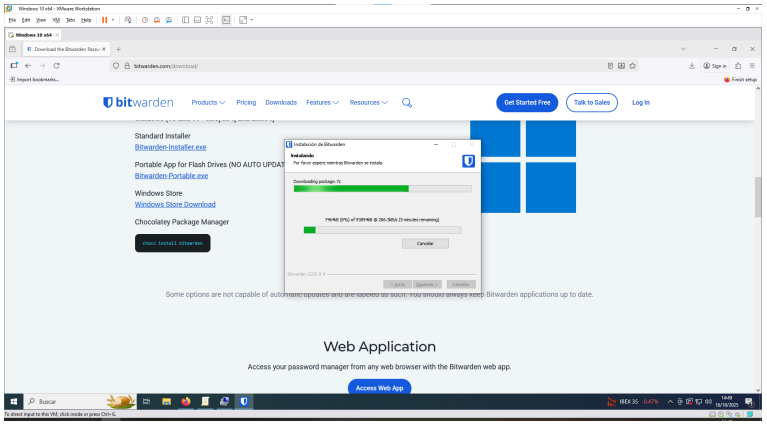
vi. **Reducir los límites de longitud mínima de la contraseña:** Habilitada
Esto era necesario para establecer una longitud mínima mayor a 14 caracteres.

vii. **Vigencia máxima de la contraseña:** 28 días
Establece una fecha de caducidad a la contraseña, para mayor seguridad. Hemos decidido cambiar la contraseña cada 4 semanas.

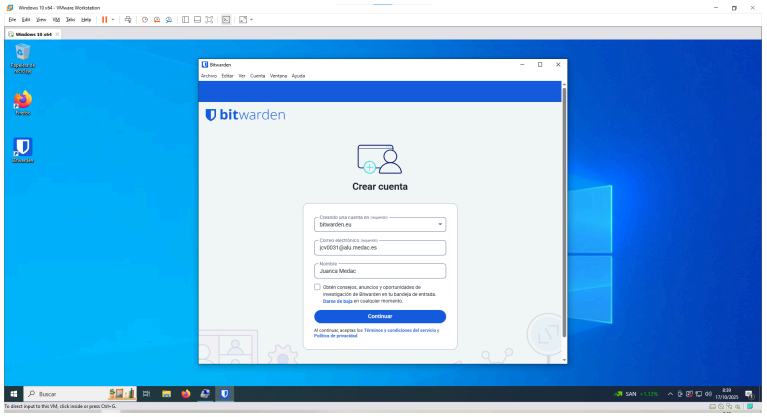
viii. **Vigencia mínima de la contraseña:** 0 días
Establece un tiempo mínimo que tiene que tener la contraseña antes de cambiarla. En este caso no lo vamos a tocar, ya que no nos interesa.

2. Gestión de contraseñas de forma segura

Para mayor seguridad, anteriormente establecimos unos requisitos mínimos de complejidad y caducidad de las contraseñas de los empleados; pero generar y almacenar de forma segura las contraseñas es complicado y sale mal. Para eso, lo mejor es usar un gestor de contraseñas como puede ser Bitwarden o Keepass, que genere contraseñas fuertes y las almacene encriptadas para que la empresa y nadie más pueda recuperarlas. En este caso, he elegido Bitwarden por familiaridad, pero ambos programas tienen características similares y nos permiten alojar nuestro propio servidor más adelante de ser necesario.

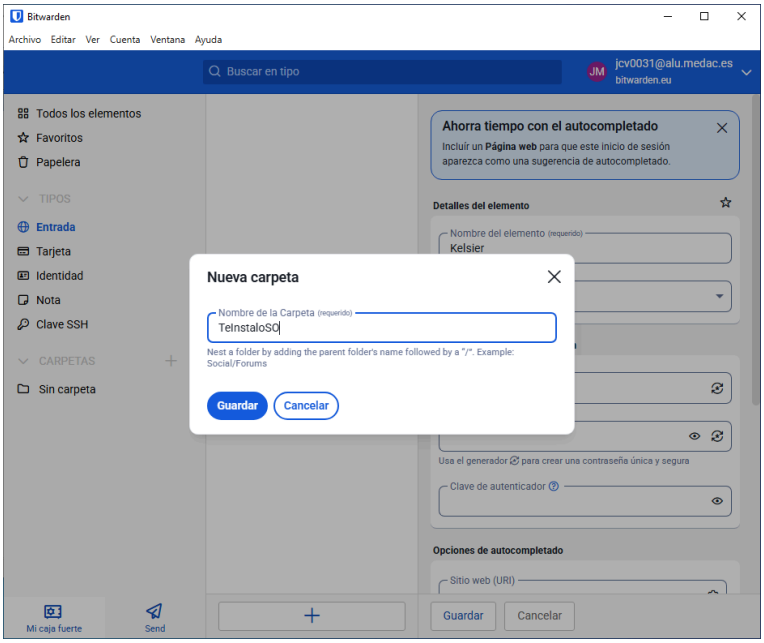
a. 

Descargamos Bitwarden en la página oficial.

b. 

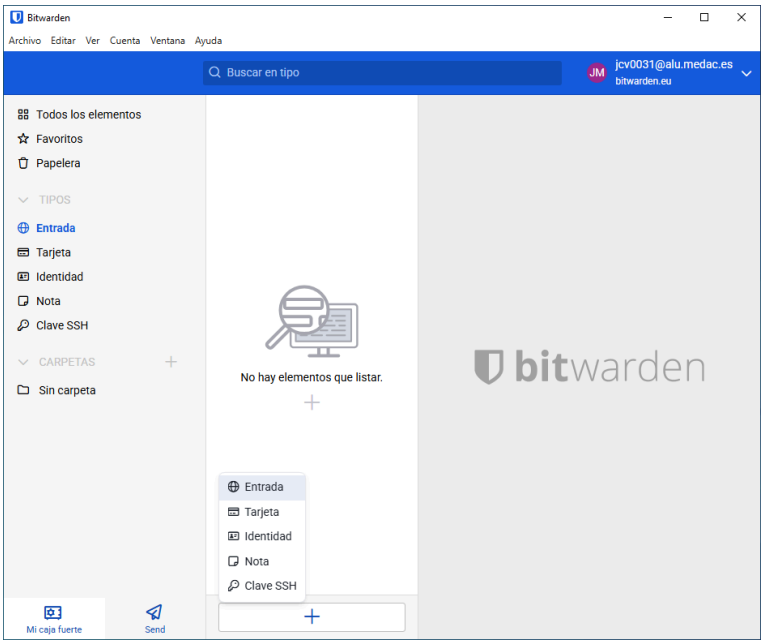
Una vez instalado, le damos a “Crear cuenta”; seleccionando servidor, un correo

c. Iniciar sesión
d. Crear carpetas

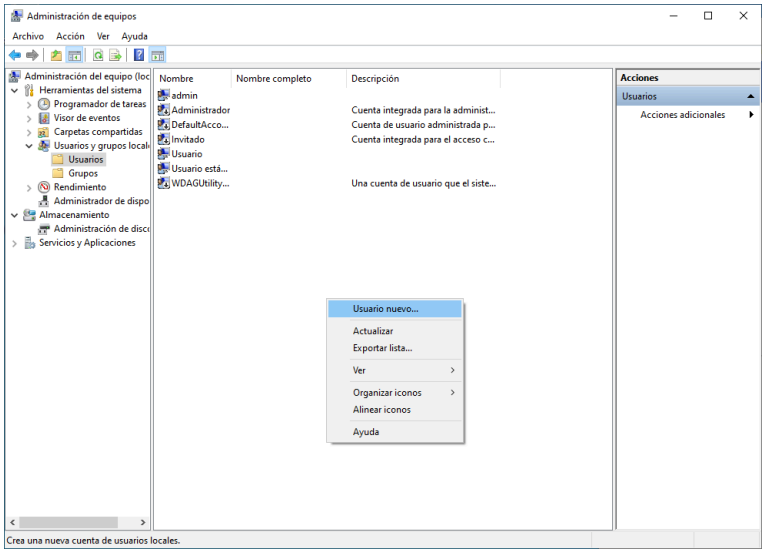


e. Generar y almacenar contraseña

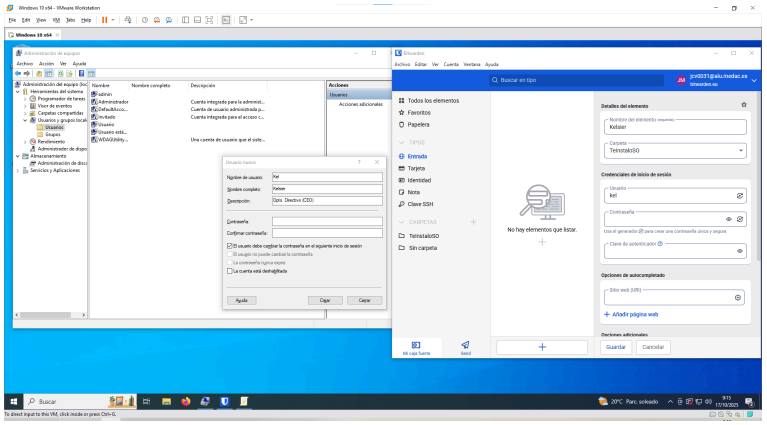
Esta parte se verá en el punto 3, creación de usuarios.



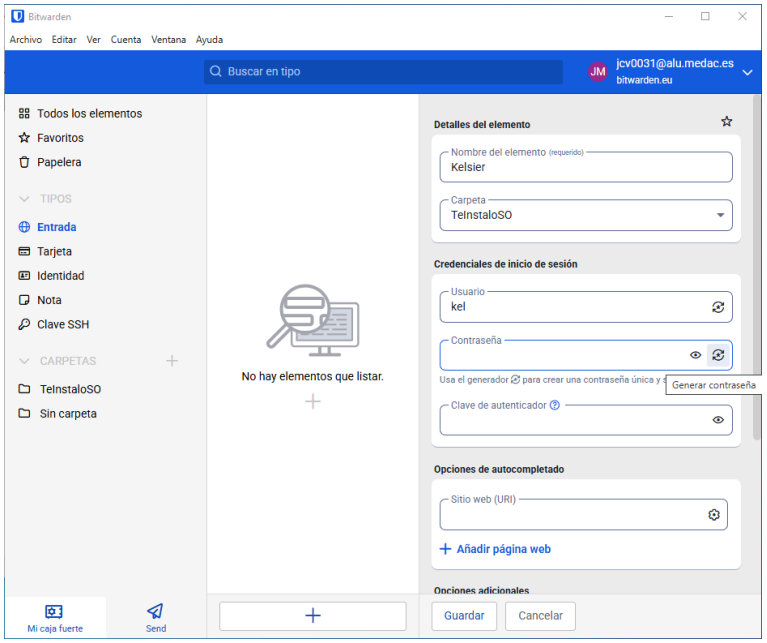
3. Creación de usuarios

a. 

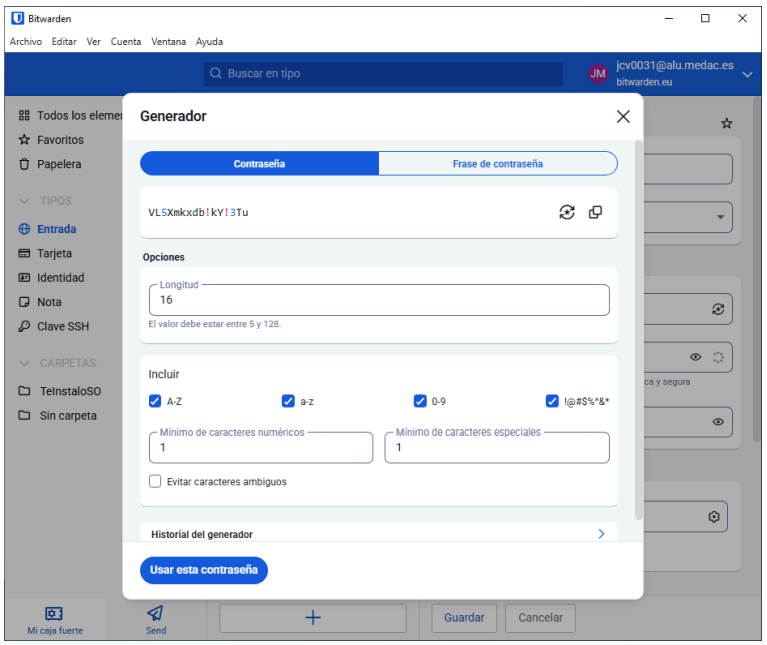
Buscando “Administración de equipos” en el buscador de Windows, podemos encontrar este programa. Navegamos por el menú lateral izquierdo a Herramientas del sistema > Usuarios y grupos locales > Usuarios, y hacemos clic derecho para entrar en “Usuario nuevo…”.

b. 

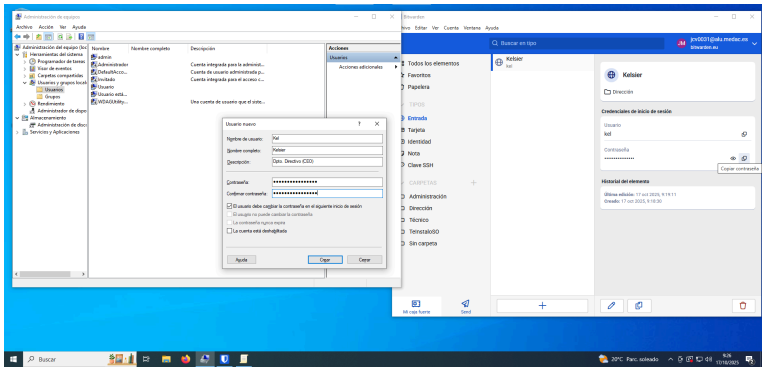
Ingresamos el nombre de usuario y el nombre real del usuario en ambos Bitwarden y la ventana de creación del usuario.

c. 

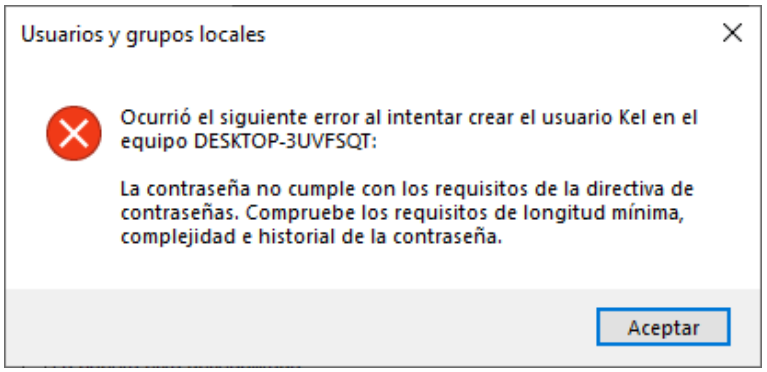
En Bitwarden, le damos al botón a la derecha de la caja de texto de “Contraseña”.

d. 

En este menú establecemos las normas que debe cumplir la contraseña y se generará de forma automática una contraseña aleatoria. Le damos a “Usar esta contraseña”.

e. 

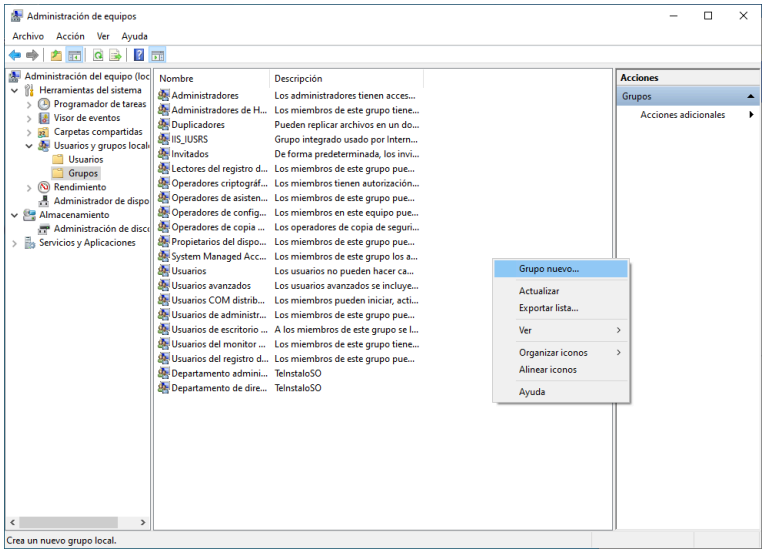
Copiamos la contraseña desde Bitwarden a la ventana de configuración y le damos a “Crear” para guardar al usuario.

f. 

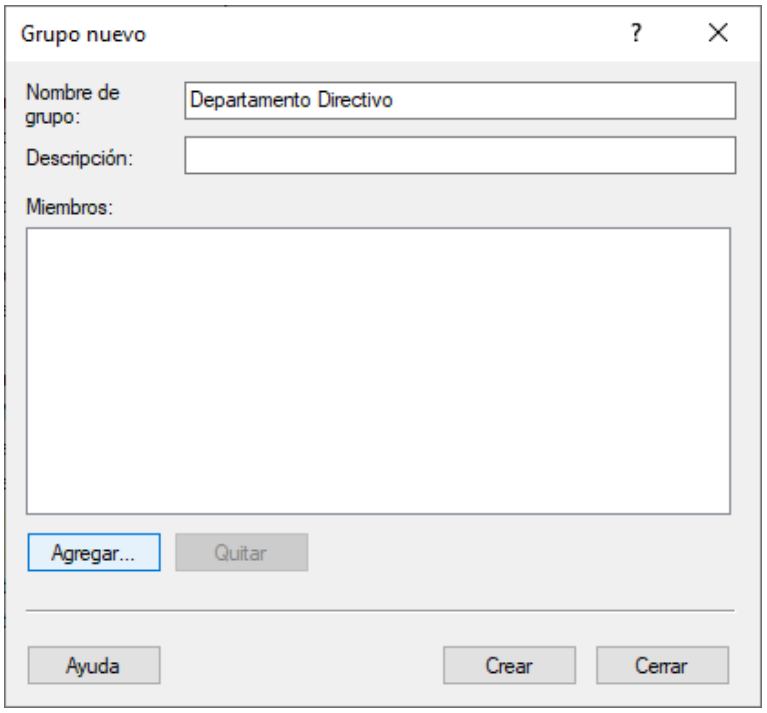
Este error aparecería si no ingresamos ninguna contraseña o si intentamos usar una contraseña que no cumpla con los requisitos de seguridad establecidos.

g. Repetimos el proceso con cada usuario, creando contraseñas distintas para cada uno.

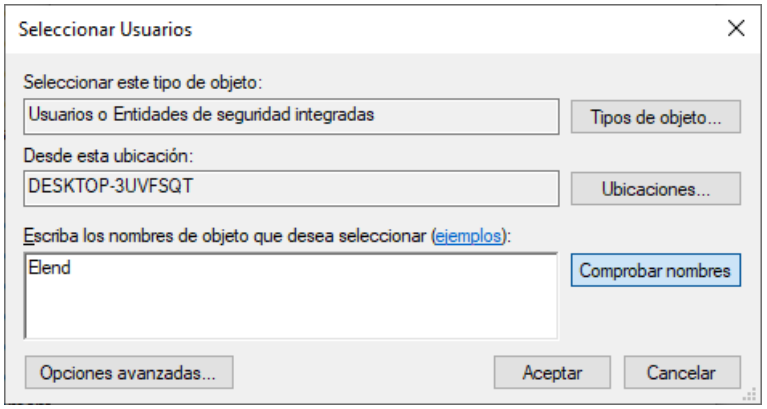
4. Creación de grupos

a. 

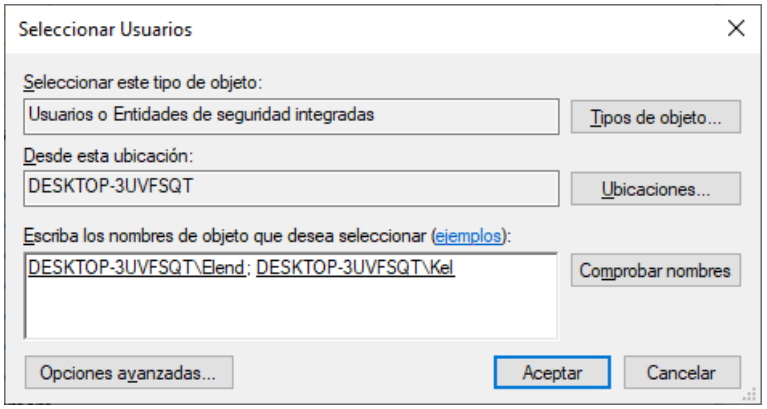
De nuevo, en el menú izquierdo, entramos en “”Grupos” y hacemos clic derecho para entrar en “Grupo nuevo…”.

b. 

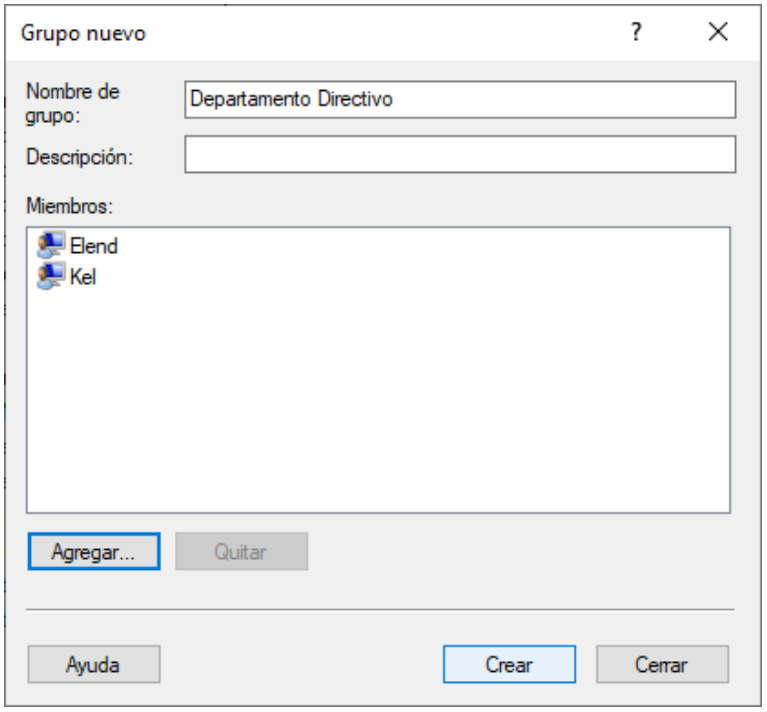
Le damos un nombre al grupo y le damos a “Agregar…”.

c. 

Escribimos el nombre de un usuario al que queramos añadir al grupo y pulsamos “Comprobar nombres” para que se introduzca el nombre del usuario en el formato adecuado.

d. 

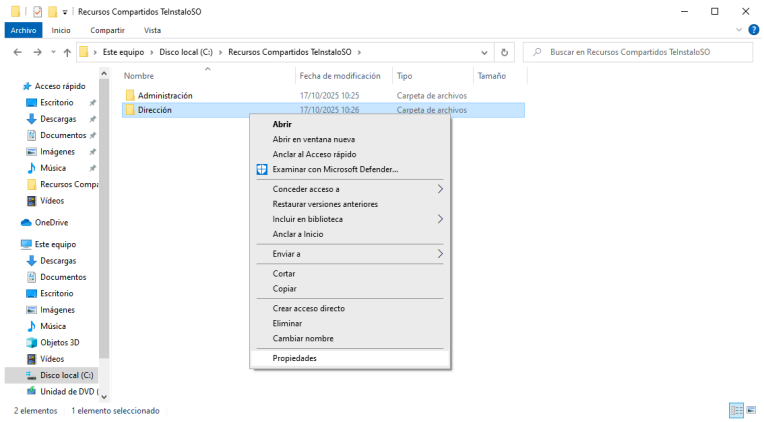
Repetimos el proceso con todos los usuarios del grupo y le damos a “Aceptar”.

e. 

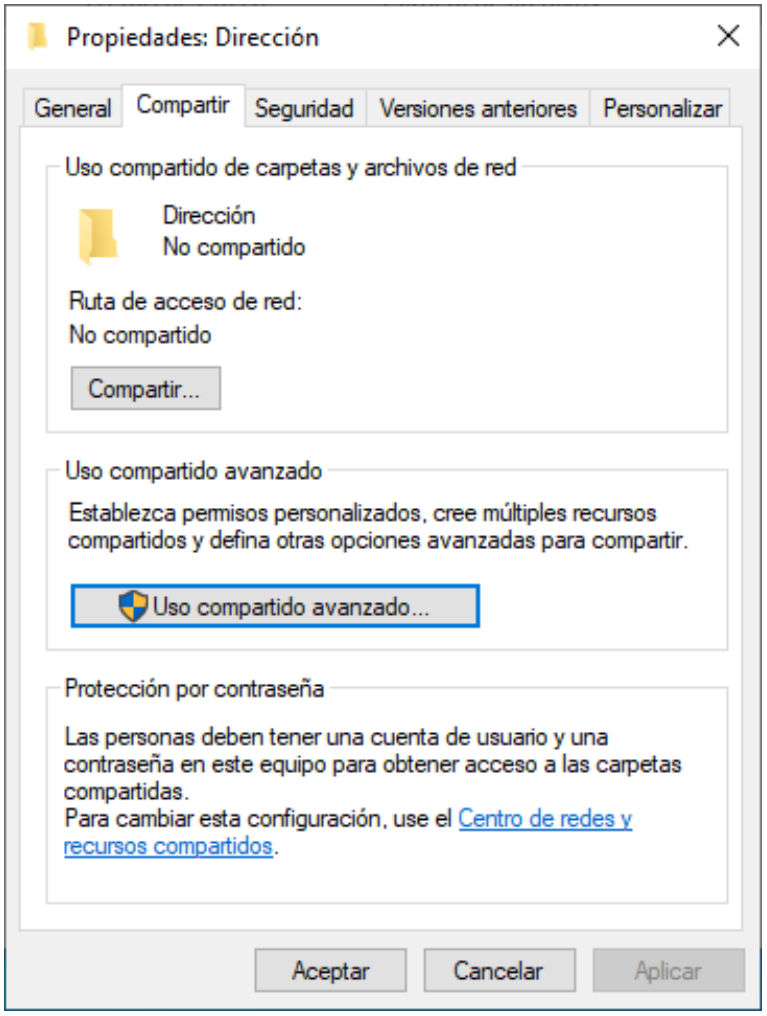
Ahora podemos ver a todos los usuarios dentro del grupo y darle a “Crear” para guardarlo.

f. Repetimos el proceso con el resto de grupos.

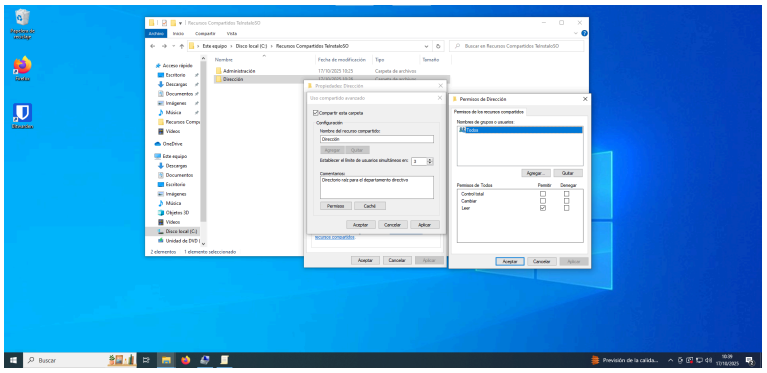
5. Creación y gestión de directorios compartidos

a. 

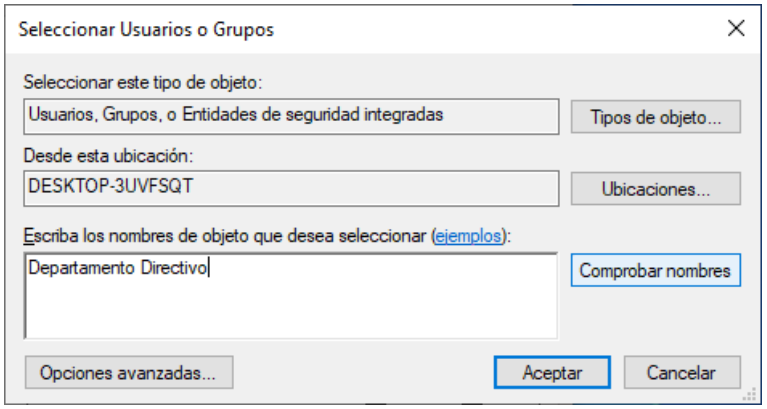
Creamos los directorios que queremos compartir en la estructura deseada. Seleccionamos un directorio a compartir con clic derecho y entramos en “Propiedades”.

b. 

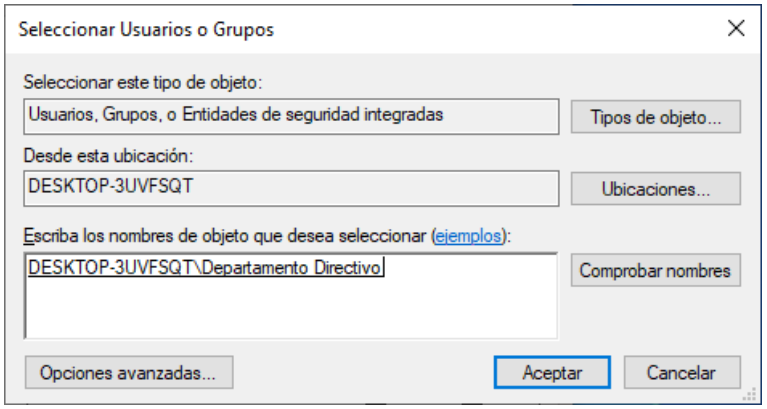
Entramos en “Uso compartido avanzado…”.

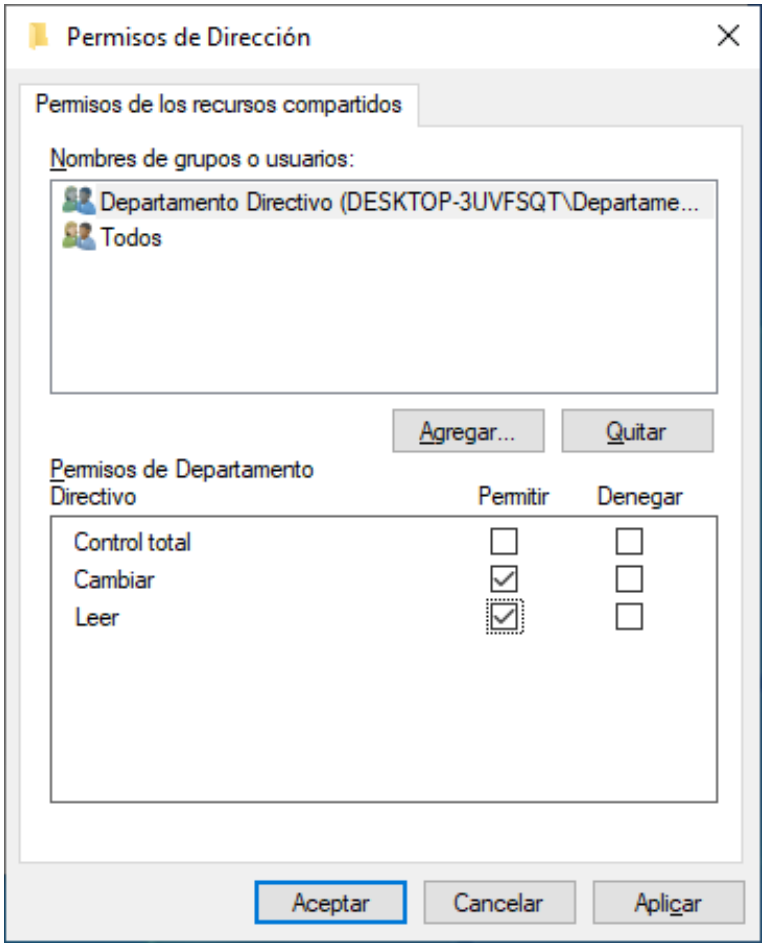
c. 

Entramos en “Permisos” y dentro de la nueva ventana le damos a “Agregar…”.

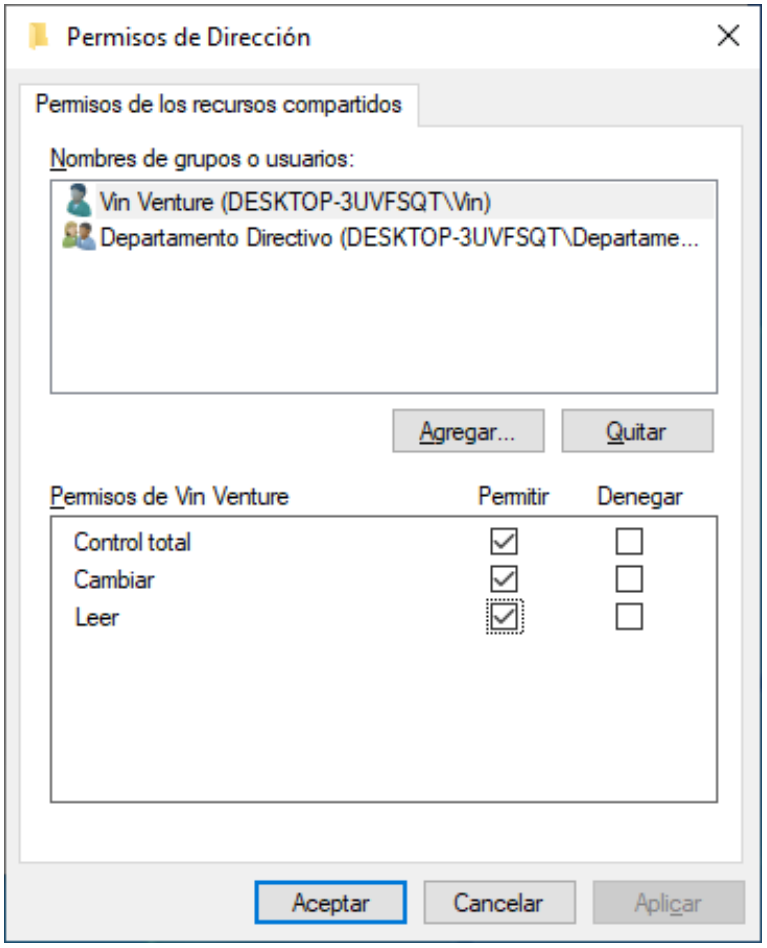
d. 

Veremos una interfaz similar a la de añadir usuarios a un grupo, solo que en este caso es añadir grupos y usuarios al directorio. Los añadiremos de la misma forma que vimos en la creación de grupos.

e. 

f. 

Si seleccionamos un grupo, podremos cambiar sus permisos con los cuadros de debajo. Le daremos al grupo directivo permisos de escritura y lectura, eliminaremos el grupo “Todos” para quitarle los permisos a los usuarios externos.

g. 

Añadimos a la usuaria Vin y le damos control total, ya que será la propietaria del directorio.

Linux

Políticas de contraseña

Al igual que con Windows, en Linux podemos establecer políticas de contraseña. Establecer las políticas de contraseña adecuadas mejorará considerablemente la seguridad de nuestro sistema. Como otras configuraciones que hemos visto en trabajos previos con Linux, podemos encontrar el archivo de configuración de políticas de contraseña dentro del directorio “etc”. En los sistemas basados en Debian, como Ubuntu, este fichero es `/etc/pam.d/common-password`. Podemos editarlo con `nano` o con cualquier otro editor de texto, gráfico o de consola, que queramos.

Dentro de este fichero, podemos encontrar una serie de líneas de texto. Podemos eliminar todo el contenido actual para establecer nuestras propias reglas. [1]

Requerir el cumplimiento de las reglas:

Para que las reglas se vuelvan obligatorias en lugar de tan solo mostrar un aviso, hay que empezar cada línea de la configuración con `password required`.

Historial de contraseñas:

Escribimos la siguiente línea, ingresando la cantidad de contraseñas recordadas que queramos tras "remember":
`password required pam_pwhistory.so remember=2 use_authok`

Requisitos mínimos:

Queremos que, como en Windows, la contraseña incluya como mínimo una letra minúscula, una mayúscula, un número, y un carácter especial. Para ello incluiremos en la siguiente línea, respectivamente, lcredit=-1, ucredit=-1, dcredit=-1, y ocredit=-1. Se vería así:

```
password required pam_pwquality.so lcredit=-1 ucredit=-1 dcredit=-1
ocredit=-1
```

Con estas dos líneas tendríamos los requisitos mínimos necesarios configurados. Sólo queda guardar el archivo y reiniciar el sistema para aplicar los cambios.

Creación de usuarios

Crear usuarios en sistemas operativos basados en Linux es realmente sencillo. Sólo hay que abrir un terminal y escribir el comando `sudo useradd nombre-usuario`. Después, para darle una contraseña, ejecutar el comando `sudo passwd nombre-usuario` y escribir la contraseña. Recuerda que, al igual que cuando utilizamos `sudo`, no veremos asteriscos (*) ni ningún otro tipo de feedback al escribir la contraseña. Al acabar, pulsamos intro y se habrá guardado la contraseña para nuestro nuevo usuario. [2]

Creación de grupos

Crear grupos también es muy simple. Ejecutamos en la línea de comandos `sudo groupadd grupo`. Para añadir un usuario al grupo usamos el comando `sudo usermod -a -G grupo nombre-usuario`. Con eso, el usuario "nombre-usuario" formaría parte del grupo "grupo". Un mismo usuario puede formar parte de todos los grupos que queramos.

Creación y gestión de directorios compartidos

Para crear un directorio compartido tendremos que hacer varias cosas. Los pasos a seguir serían:

Crear un directorio: `sudo mkdir /home/compartido`

Asignar un grupo propietario del directorio compartido: `sudo chgrp grupo /home/compartido`

Cambiamos los permisos: `sudo chmod +770 /home/compartido`

Especificar que todos los directorios hijos hereden el grupo y permisos del directorio compartido: `sudo chmod +s /home/compartido`

Prueba de funcionamiento:

Ejecutamos todos los comandos de antes, creando el usuario Vin y el grupo Actividad8:

```
jnk@lgo /v/h/jnk> sudo useradd vin
[sudo] contraseña para jnk:
jnk@lgo /v/h/jnk> sudo groupadd actividad8
jnk@lgo /v/h/jnk> sudo usermod -a -G actividad8 vin
jnk@lgo /v/h/jnk> sudo mkdir /home/compartido
jnk@lgo /v/h/jnk> sudo chgrp actividad8 /home/compartido/
jnk@lgo /v/h/jnk> sudo chmod +770 /home/compartido/
jnk@lgo /v/h/jnk> sudo chmod +s /home/compartido/
jnk@lgo /v/h/jnk> sudo mkdir /home/compartido/prueba-de-permisos
jnk@lgo /v/h/jnk> groups
jnk wheel libvirt
jnk@lgo /v/h/jnk> groups vin
vin : vin actividad8
jnk@lgo /v/h/jnk> ls -l /home/compartido/
total 0
drwxr-sr-x. 1 root actividad8 0 nov 29 20:02 prueba-de-permisos/
jnk@lgo /v/h/jnk>
```

Iniciamos sesión en el usuario Vin y probamos a leer y escribir:

```
vin@lgo:~$ cd /home/compartido/
vin@lgo:/home/compartido$ ls
```

```
prueba-de-permisos
vin@lgo:/home/compartido$ mkdir puedo-editar
vin@lgo:/home/compartido$ ls
prueba-de-permisos  puedo-editar
vin@lgo:/home/compartido$
```

Conclusiones

Ahora que hemos visto cómo crear usuarios, grupos, y directorios compartidos en ambos sistemas operativos; podemos comprobar las diferencias y similitudes.

Al igual que hemos visto en otras actividades, Windows tiende a ser configurado a través de distintas interfaces, mientras que Linux se configura con comandos y archivos de configuración almacenados en `/etc`. Esto hace que Windows sea más sencillo de configurar de primeras, pero Linux es más replicable y capaz de hacer tareas en lotes a través de scripts automatizados. Además, Linux ofrece un control más granular en general, por ejemplo para los requisitos de las contraseñas o el sistema de grupos y permisos. Windows también parece más orientado a redes con distintos equipos compartiéndose directorios entre ellos, y no tanto en ser utilizado por varios usuarios locales de forma simultánea.

Bibliografía

[1] Requisitos de contraseñas en Linux:
https://community.learnlinux.tv/t/etc-pam-d-common-password-example/2785/2

[2] Creación y gestión de usuarios y recursos compartidos en Linux:
https://www.geeksforgeeks.org/linux-unix/how-to-create-a-shared-folder-between-two-local-user-in-linux/