

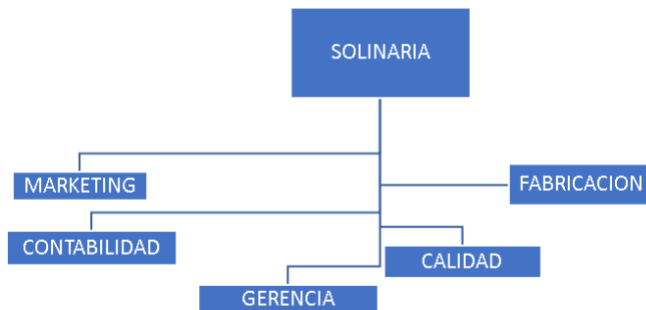
# Tarea para SI06.

## Detalles de la tarea de esta unidad.

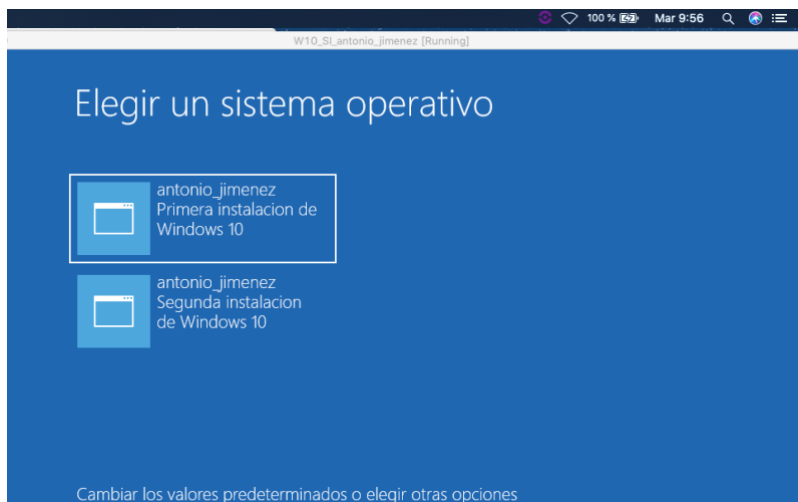
### Enunciado.

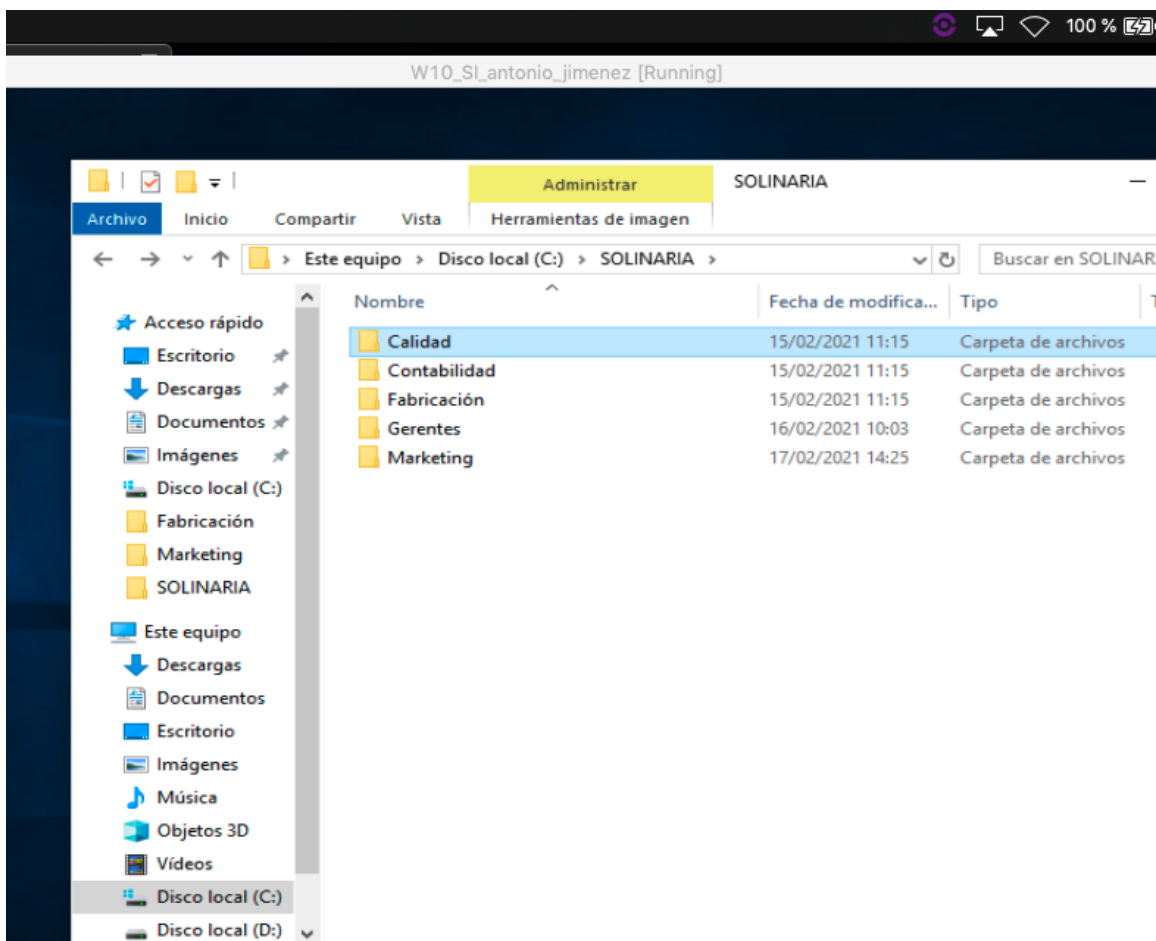
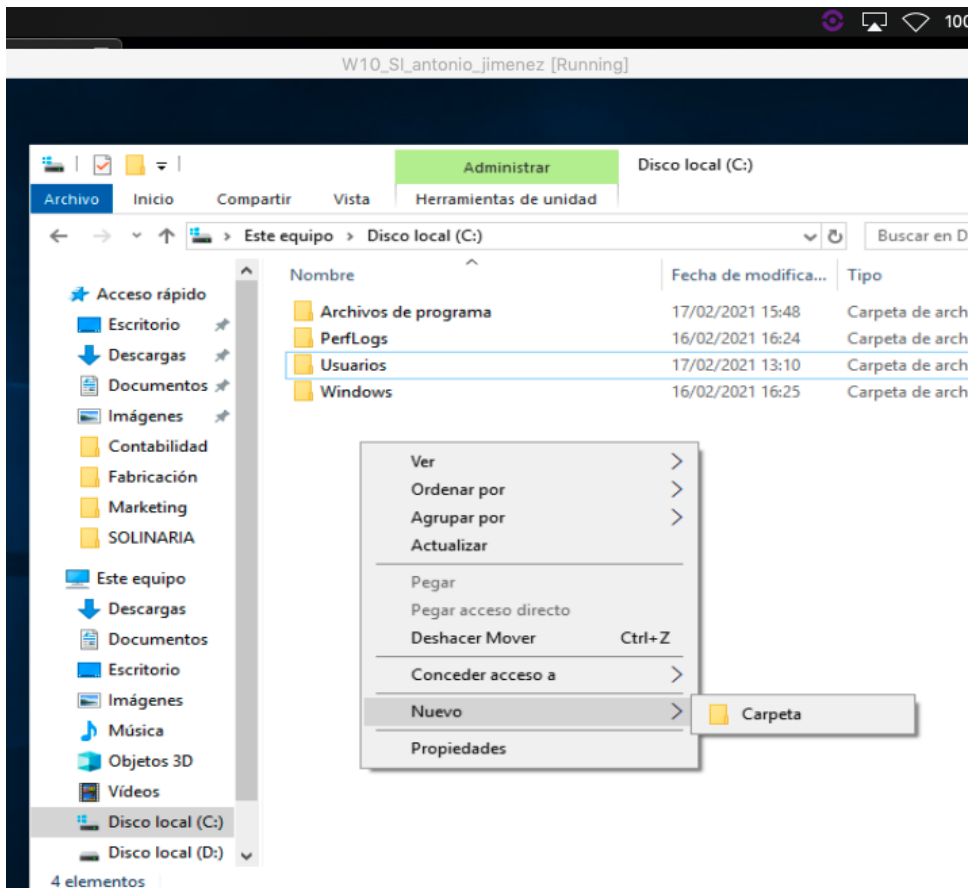
Utiliza la máquina virtual de Windows 10 profesional, creada en la tarea anterior para realizar los siguientes ejercicios. (Importante: Para la entrega de la tarea debes tomar capturas de pantalla claves en cada ejercicio y explicar los pasos realizados).

1. Crea la siguiente estructura departamental trasladándola a carpetas, es decir, crea una carpeta por cada departamento. Crea primero la carpeta 'SOLINARIA' y dentro de ésta las demás. Introduce algunos archivos, documentos, imágenes en cada carpeta. Sitúa la estructura de carpetas colgando directamente de una unidad de disco. (0,5 puntos)

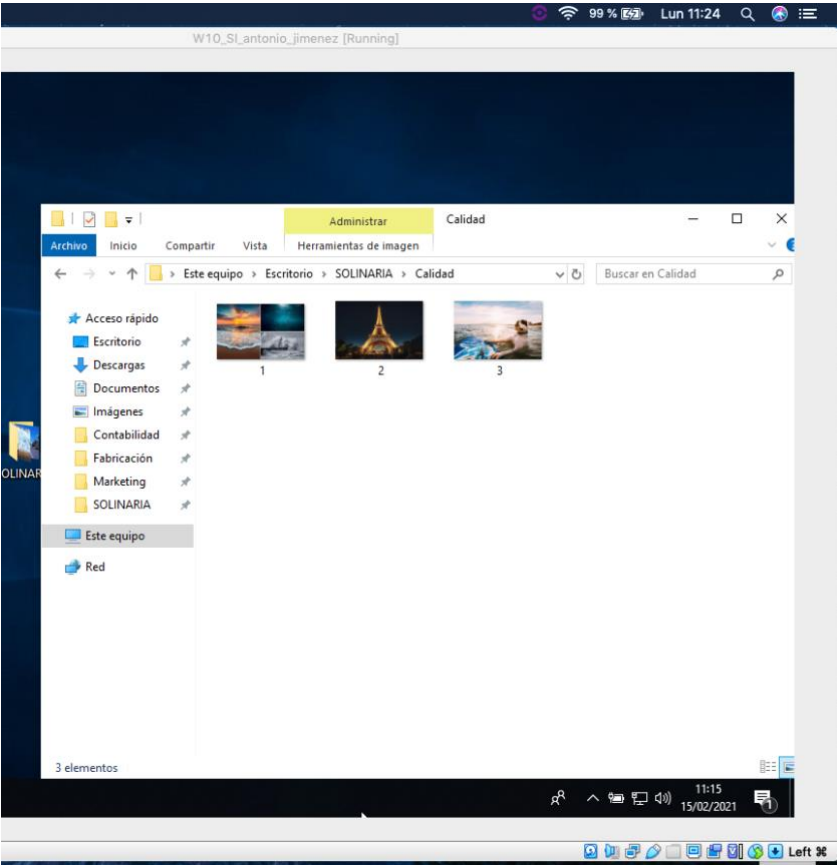


Lo primero abrimos virtual box y elegimos el usuario que queramos de la anterior práctica. Una vez dentro de Windows, creamos una carpeta en el escritorio, pulsando con el botón derecho del ratón , dándole a nuevo y luego carpeta. Escribimos el nombre “SOLINARIA” y dentro de la carpeta realizamos la misma operación, creando 4 carpetas con el nombre “MARKETING, CONTABILIDAD, FABRICACION, CALIDAD, GERENTES”. Metemos unas imágenes dentro de cada una de las carpetas.



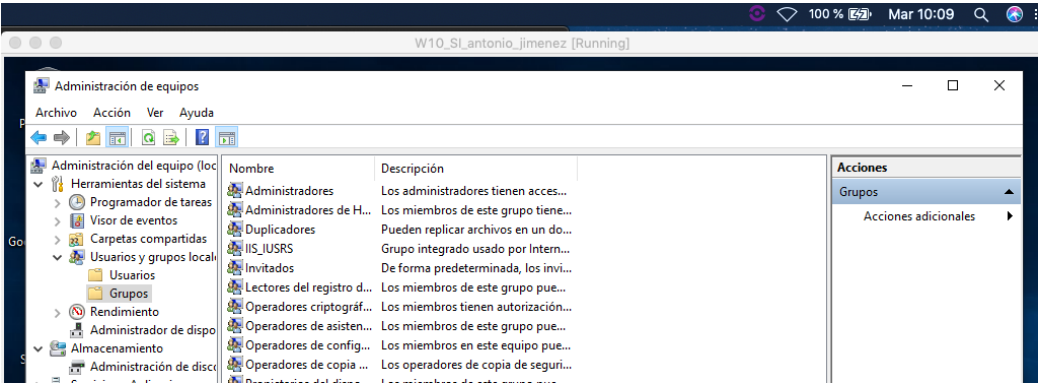


Dentro de las carpetas metemos imágenes.

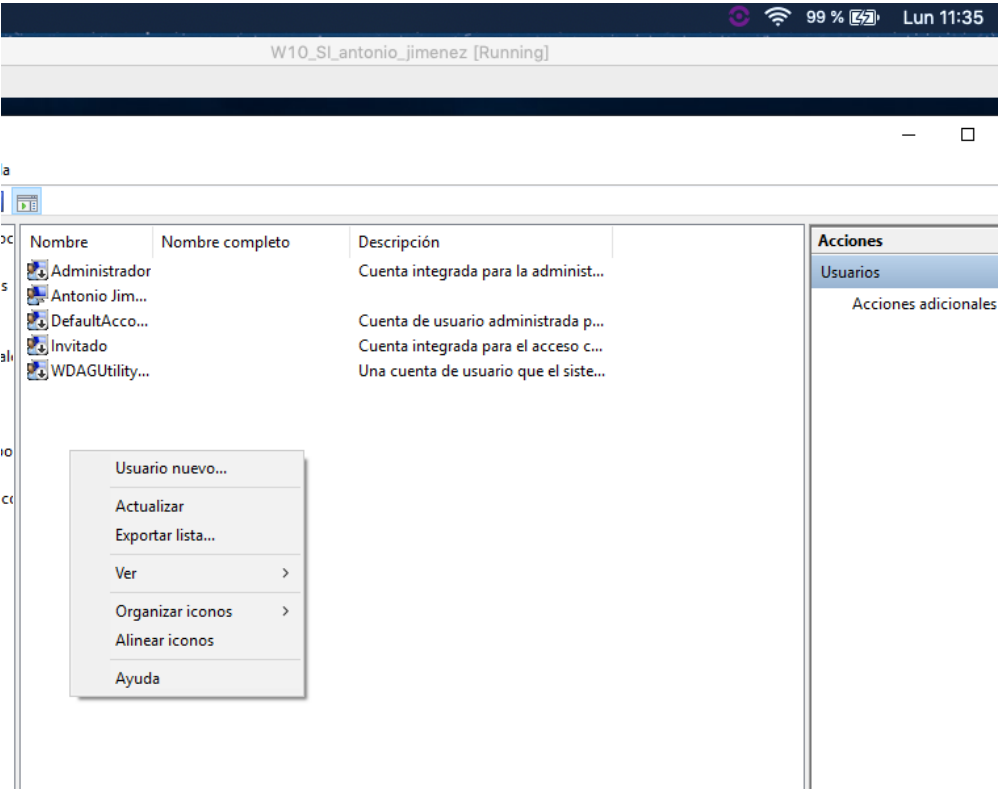


2. Después crea 2 usuarios para cada departamento (usuarios con privilegios limitados). Los usuarios aparecen al final de la tarea. Nómbralos, con la inicial del nombre y el primer apellido (por ejemplo: Ignacio Díaz sería idiaz). Guarda en la descripción de cada usuario el nombre y apellido completos. Crea un grupo de usuarios para cada departamento e incluye los dos usuarios en él. Un usuario sólo podrá pertenecer a un grupo únicamente. (2 puntos).

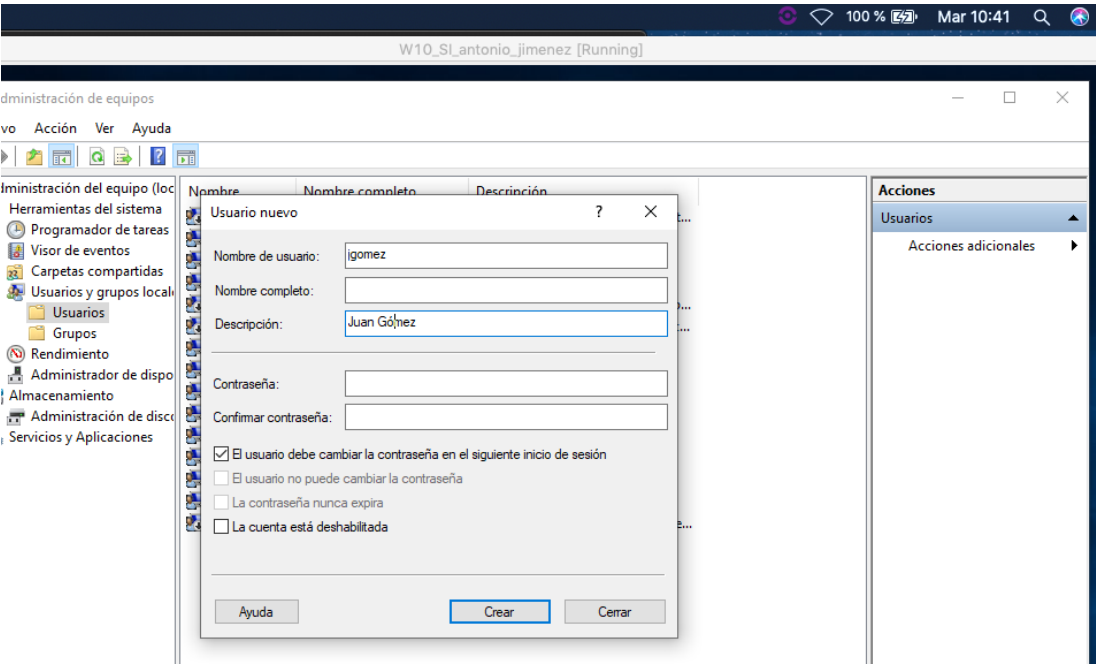
Nos dirigimos a Administrador de Equipos, y allí seleccionamos usuarios y grupos locales. Esta es una de las maneras de hacerlo pero se podría hacer dirigiéndonos a cuentas y usuarios.



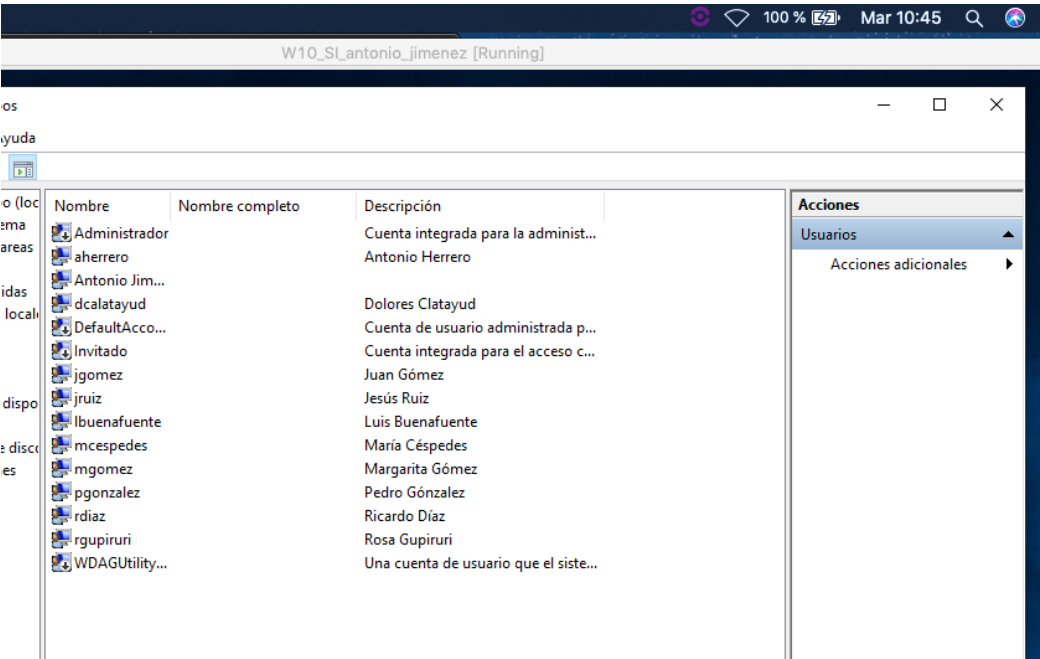
Clicamos sobre usuarios y con el botón derecho le damos a crear nuevo usuario.



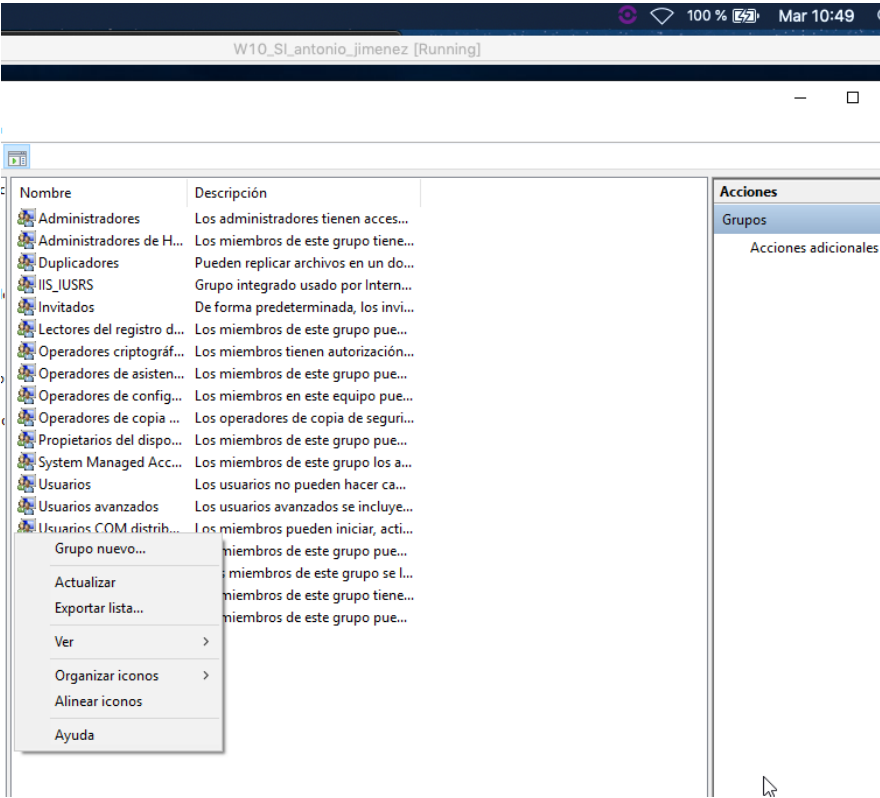
Escribimos el nombre de usuario primera letra del nombre y el apellido, en descripción escribimos luego el nombre y apellidos completo tal y como nos pide el enunciado. Realizamos el mismo paso para todos los usuarios.



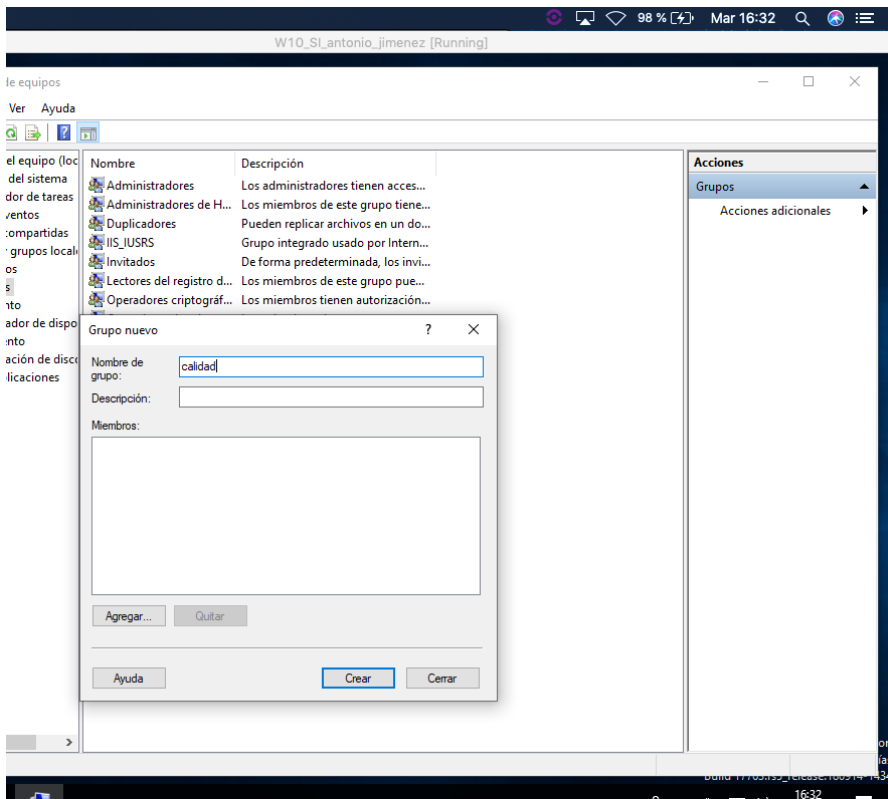
En la siguiente imagen vemos todos los usuarios creados.



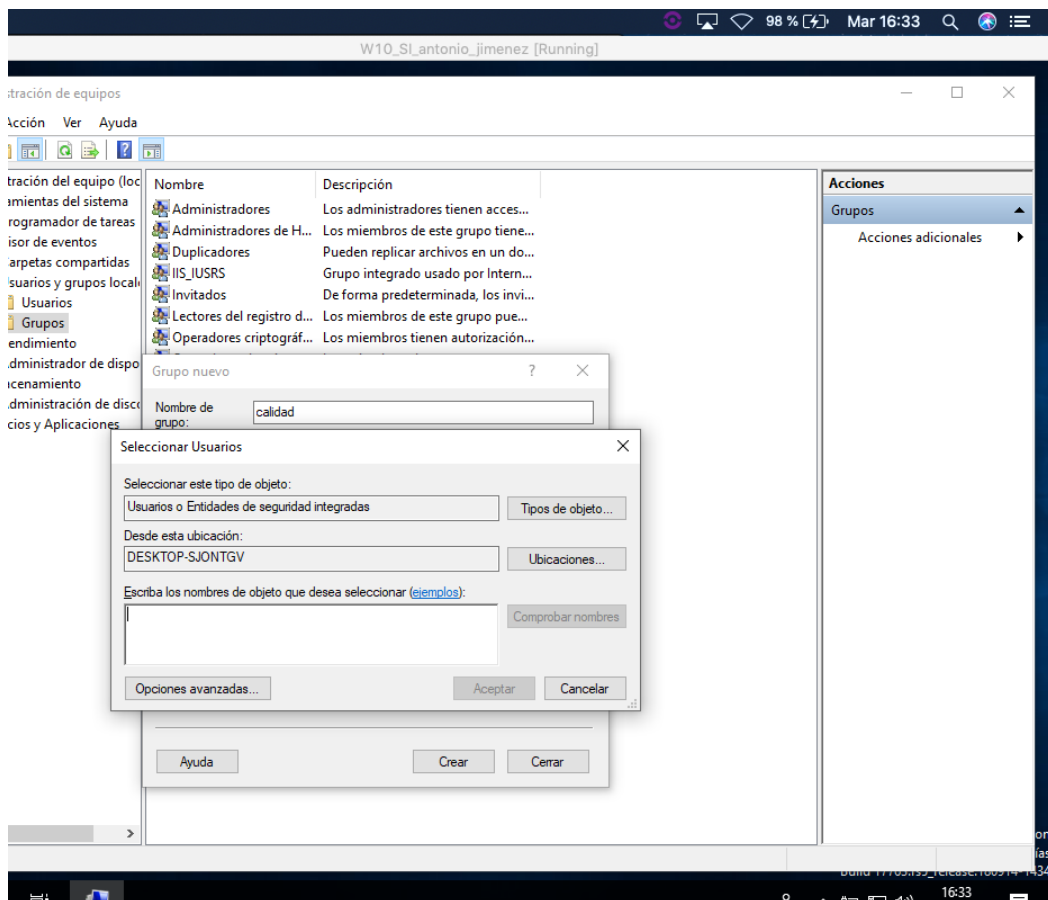
Ahora clicamos sobre grupos para poder crear un grupo para cada departamento, en los cuales incluiremos 2 usuarios por cada departamento.



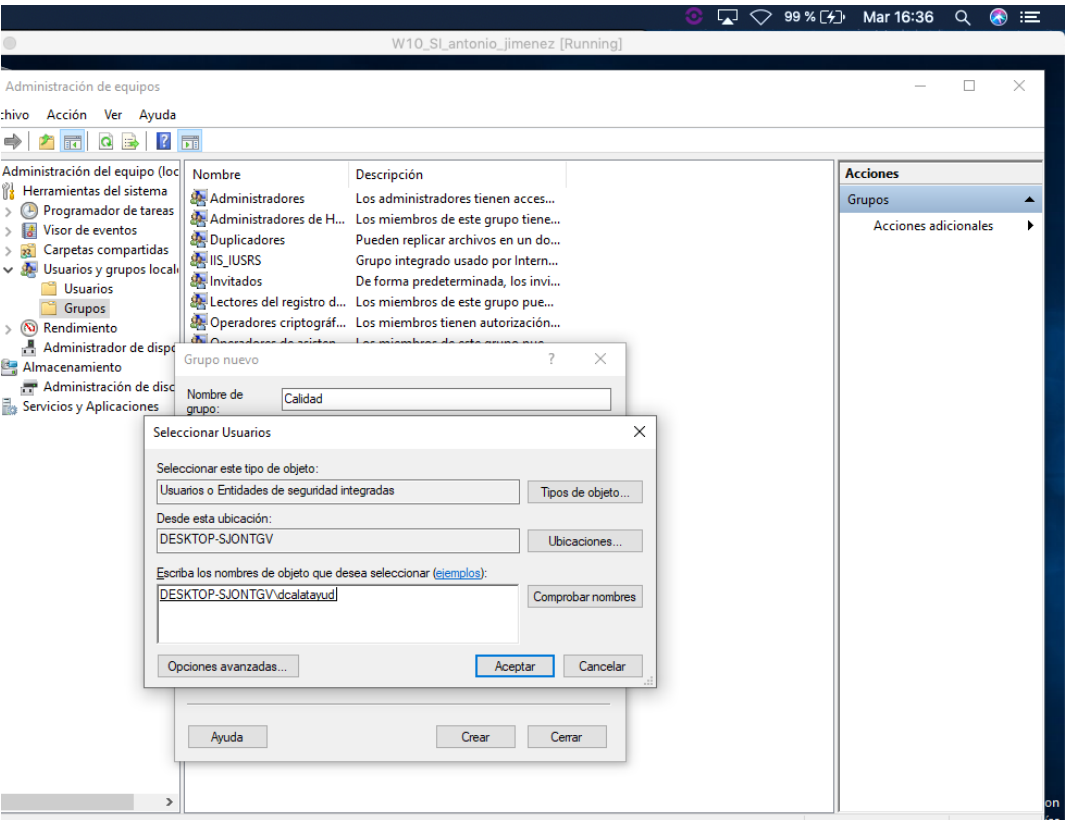
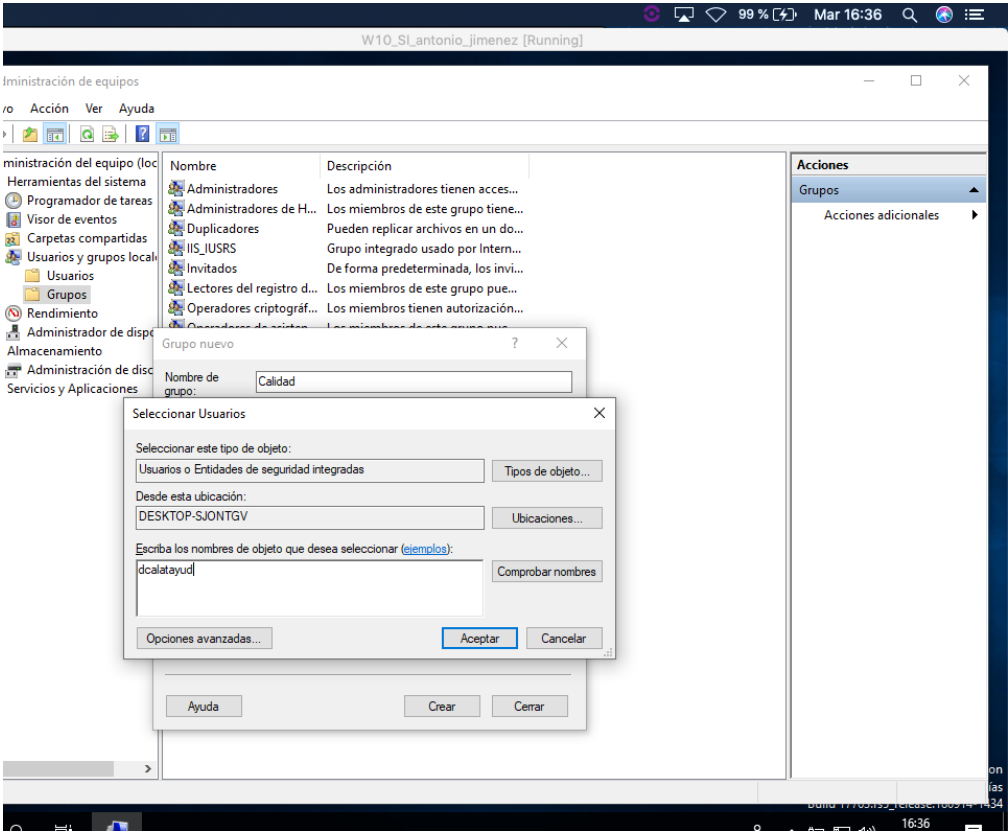
Introducimos el nombre del grupo



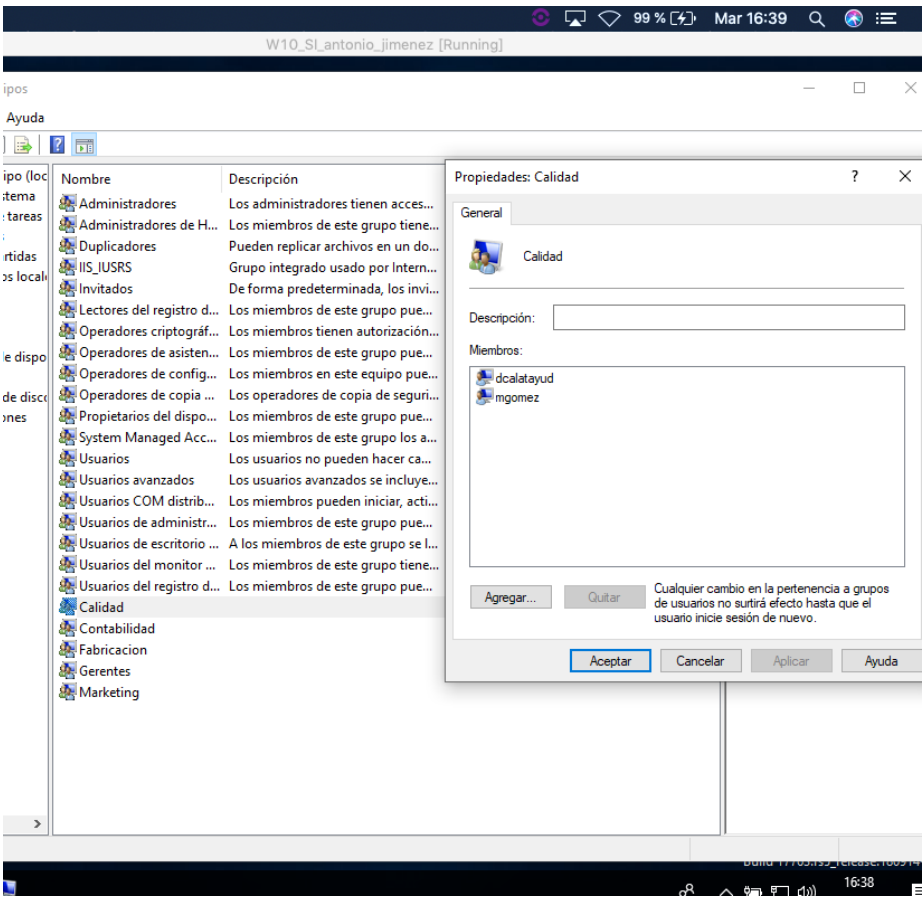
Introducimos los miembros y agregamos los nombres pinchando en agregar



Escribimos los nombres y comprobamos.



Para no repetir las capturas, en la imagen siguiente vemos como están agregados los usuarios en el departamento de Calidad, pero se puede ver los grupos creados (dentro de los grupos están los usuarios).



MARKETING

Juan Gómez, María Céspedes.

CONTABILIDAD

Jesús Ruiz, Pedro González.

FABRICACIÓN

Rosa Gupiruri, Antonio Herrero.

CALIDAD

Dolores Calatayud, Margarita Gómez.

GERENTES

Ricardo Díaz, Luis Buenafuente.



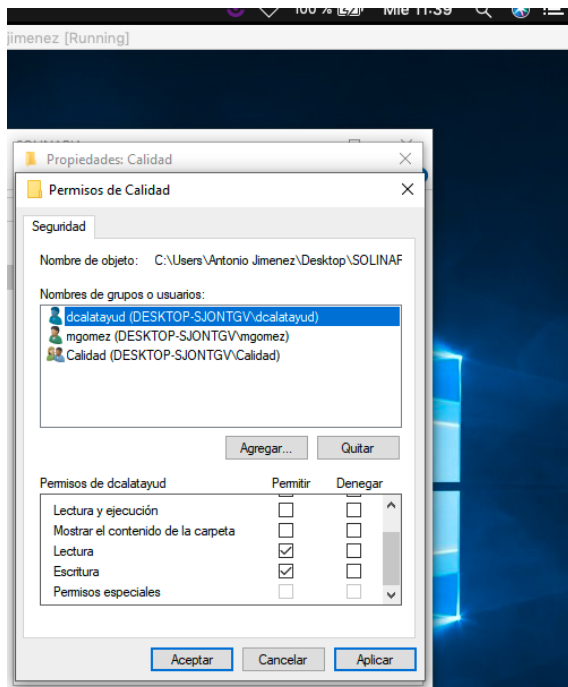
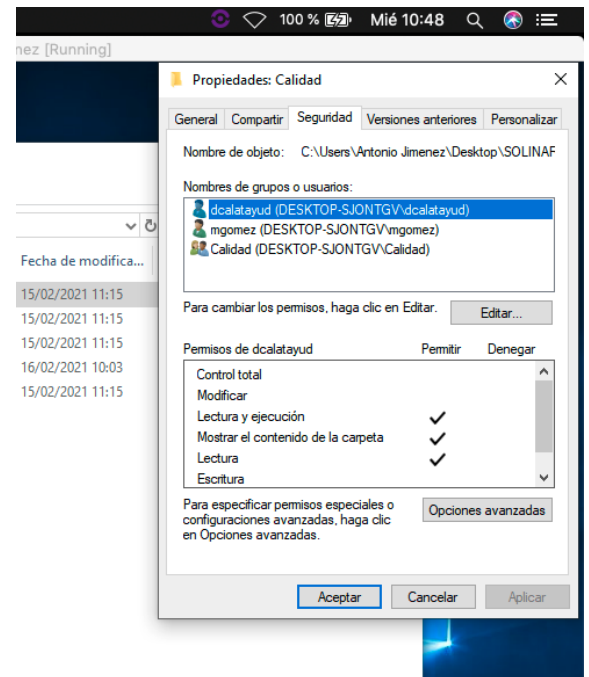
### 3. Configura los permisos de cada carpeta para que los grupos de usuarios de cada departamento tengan permisos de lectura y escritura sobre su carpeta del departamento. El resto de usuarios no tendrá acceso a carpetas de otros departamentos distintos del suyo. (2 puntos)

Cuando un usuario intenta acceder a un recurso, pide autorización al recurso para hacerlo. El recurso comprobará entonces si en su ACL aparece el SID del usuario, y en caso contrario, comprobará si en su ACL aparece el SID de algún grupo al que pertenezca el usuario.

Si no aparece en la ACL ningún SID del usuario, el recurso niega el acceso al usuario.

Si aparece en la ACL algún SID del usuario, el recurso comprueba si la acción que quiere realizar el usuario (leer, borrar, escribir, etc.) está permitida para ese SID en su ACL, si lo está, le autoriza para hacerlo, en caso contrario se lo impide.

Podemos ver como en la parte superior tenemos las SID a las que concedemos permisos (usuarios y grupos) y en la parte inferior tenemos los permisos concretos que le concedemos a dicha SID. Si ves las dos columnas por cada permiso, podemos tanto **Permitir** como **Denegar un permiso**. La denegación de un permiso es la que más pesa, y se aplica inmediatamente. De hecho, se aconseja no denegar permisos, a menos que sea absolutamente necesario.

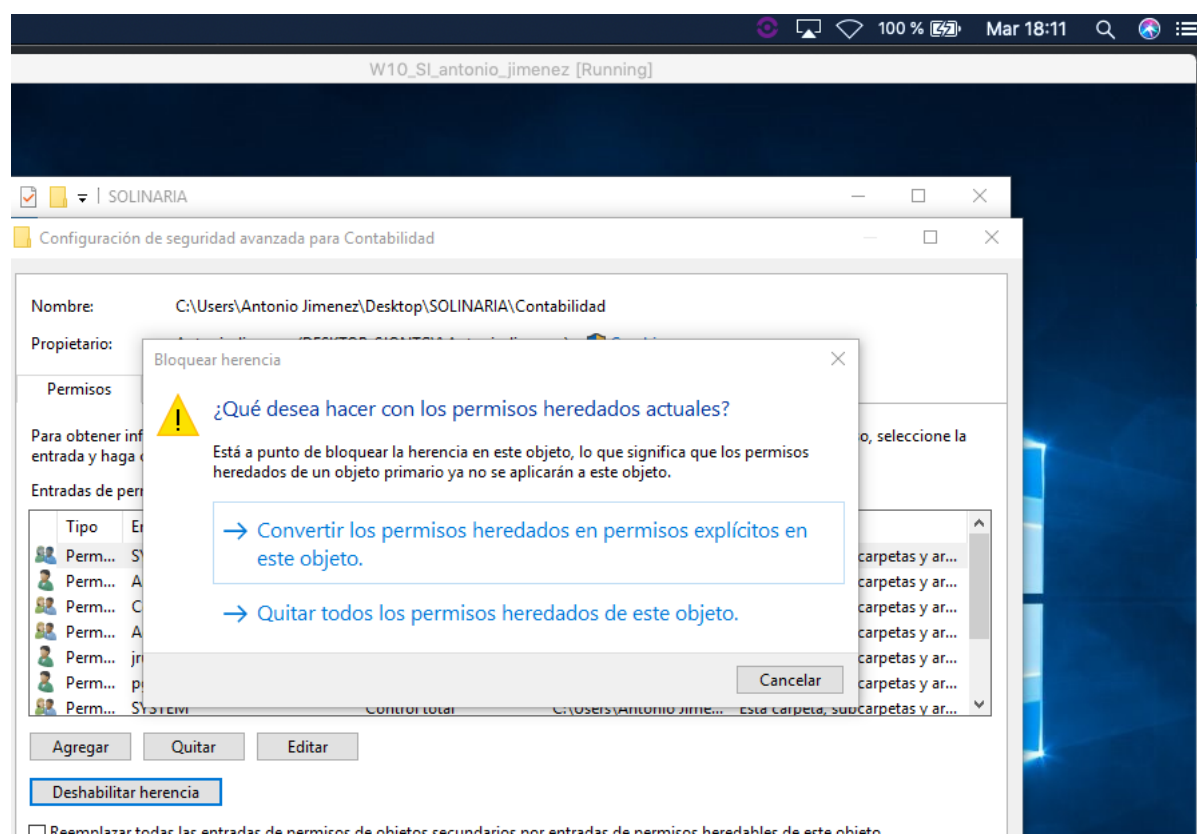
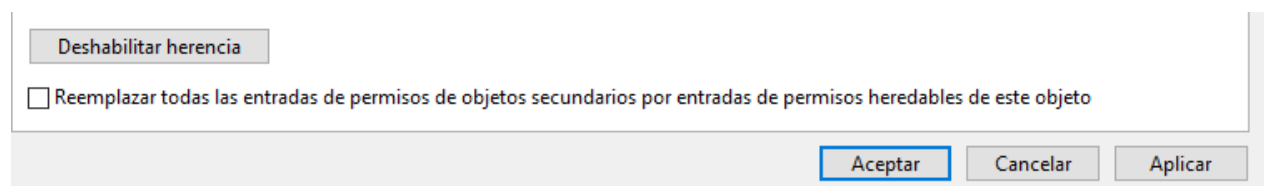


Con el botón **Editar** se nos abre una nueva pantalla donde aparecen los botones **Agregar** y **Quitar**. Con ellos podemos añadir o quitar usuarios o grupos de la ACL. En la parte inferior podemos pulsar en las casillas de **Permitir** y **Denegar** para dar y quitar **permisos**.

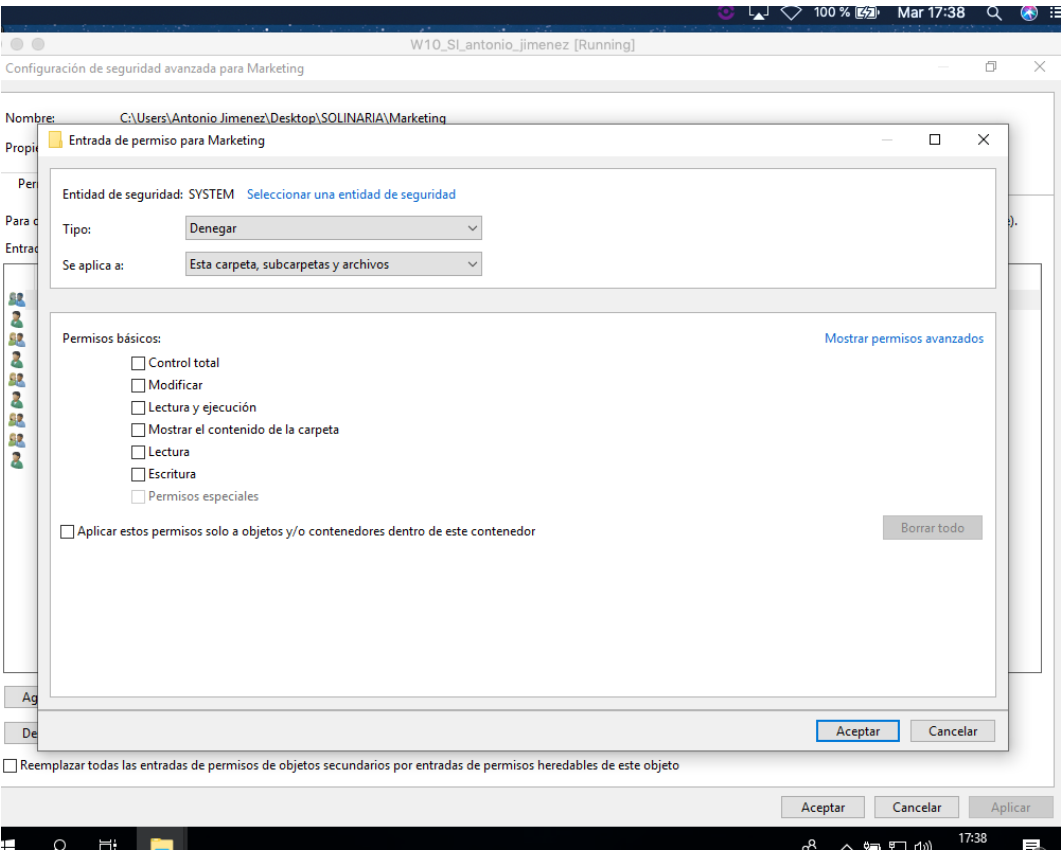
Una vez realizado esto, hemos preparado la carpeta para que cada usuario de cada departamento tenga los permisos de escritura y lectura, nos encontramos que existe un herencia entre carpetas.

Cualquier recurso que creemos, heredará automáticamente la ACL de su recurso padre si es que existe.

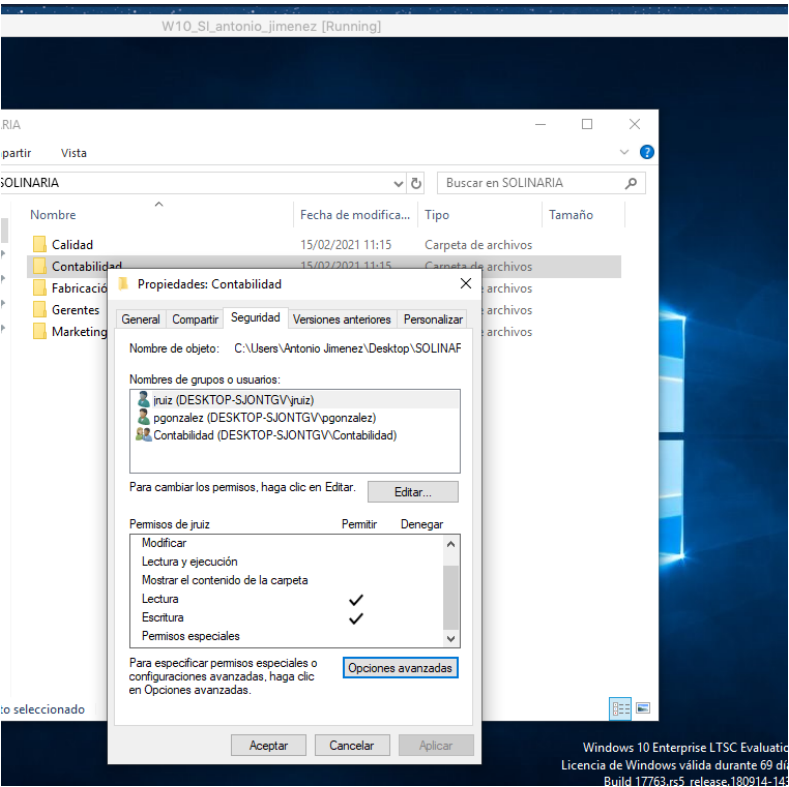
Para realizar cambios de herencia en la ACL de nuestra carpeta, ya que han heredado la ACL de su carpeta padre SOLINARIA debemos indicarle que rompa la herencia. Para ello accedemos al botón de opciones avanzadas en la pestaña de seguridad y nos quedaremos en la pestaña de permisos. En la parte inferior vemos que hay una pestaña que pone deshabilitar herencia, al pinchar nos salen dos opciones, **“Convertir los permisos heredados en permisos explícitos en este objeto.”** Y **“Quitar todos los permisos heredados de este objeto”**. Pinchamos en la segunda.



En la siguiente imagen denegaremos todos los permisos básicos, para que no tengan acceso los demás usuarios

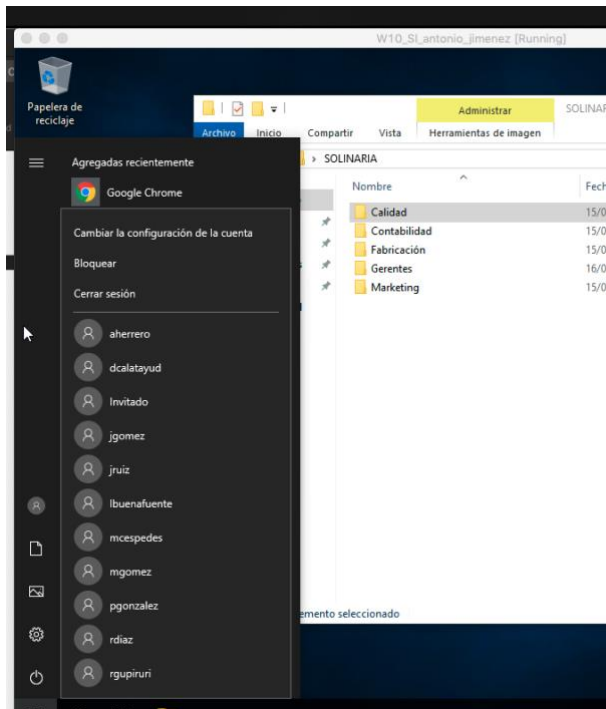


En la siguiente imagen vemos que los usuarios tienen los permisos de lectura y escritura

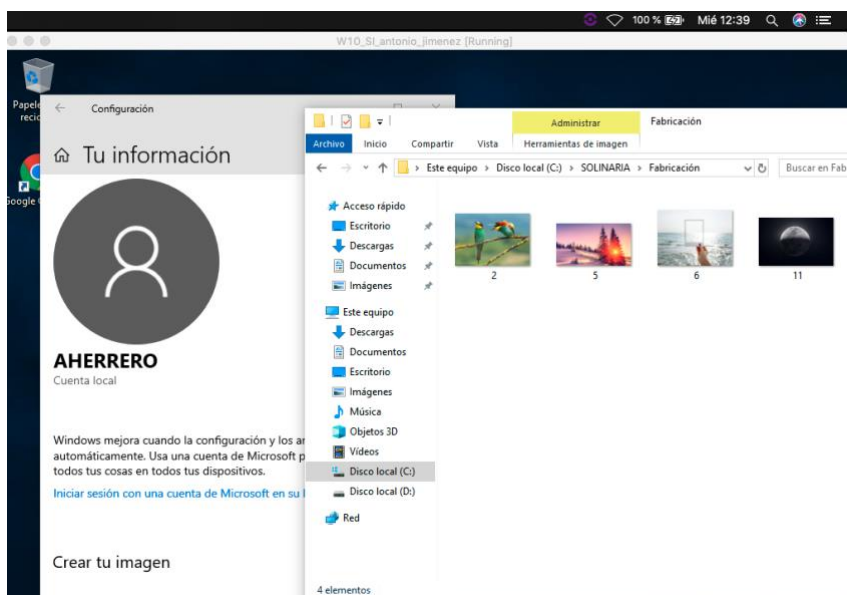


4. Inicia sesión con diferentes usuarios y comprueba que los permisos sobre las carpetas son correctos y que un usuario de un departamento sólo puede acceder a la carpeta común de su departamento. Intenta acceder a otras carpetas a las que el usuario no debería tener acceso. (0,5 puntos).

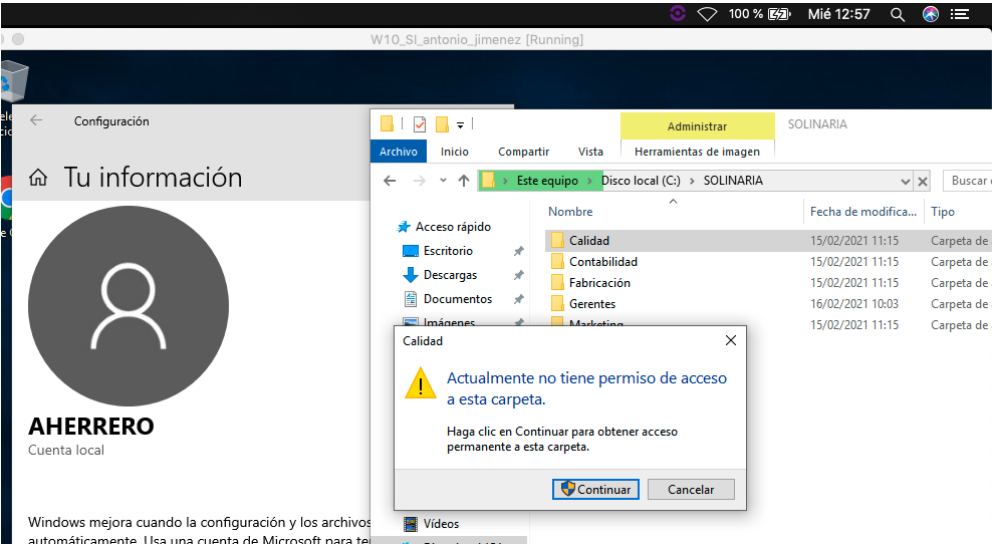
Iniciamos sesión con el usuario aherrero que pertenece FABRICACION.



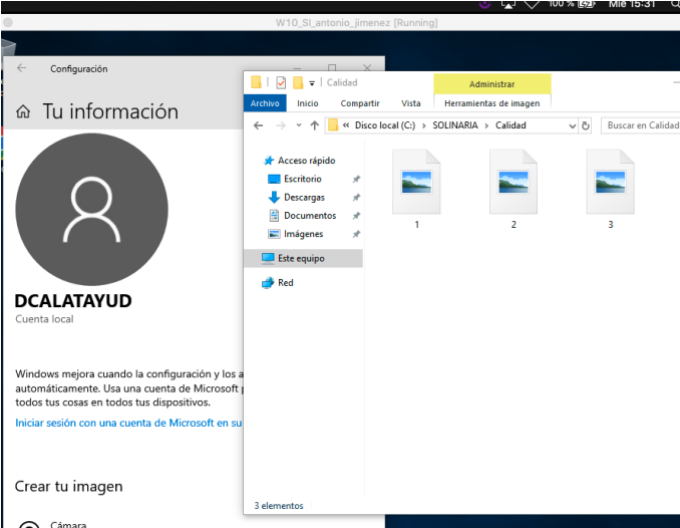
Accedemos a la carpeta FABRICACION sin problemas.



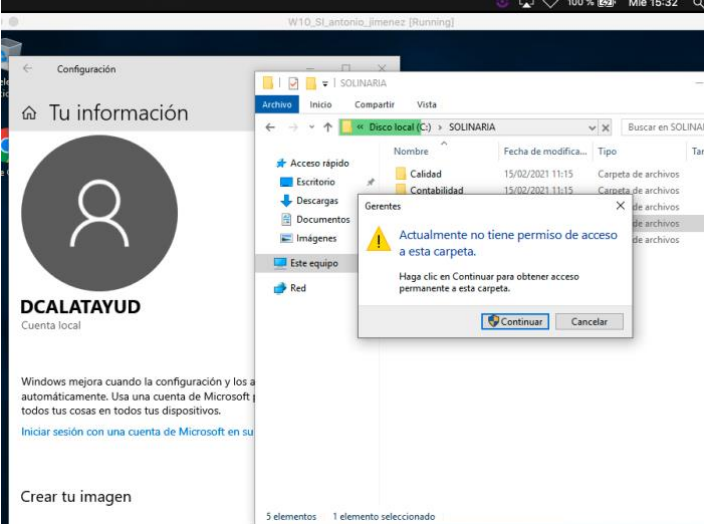
Intentamos acceder a la carpeta de Calidad y no tenemos permiso.



Inicio sesión con dcalatayud en la carpeta de calidad y me deja entrar sin problemas

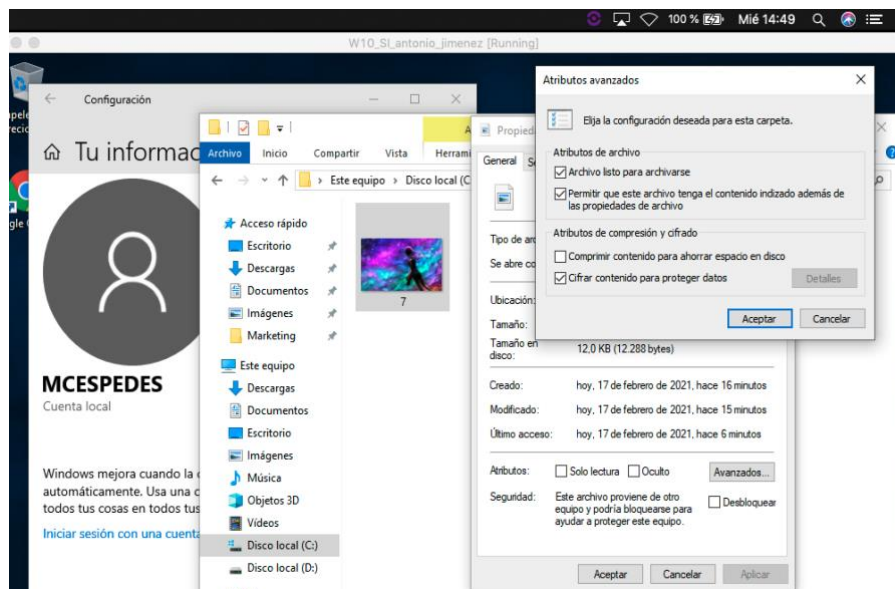


Intento abrir la carpeta de gerentes y no me deja.



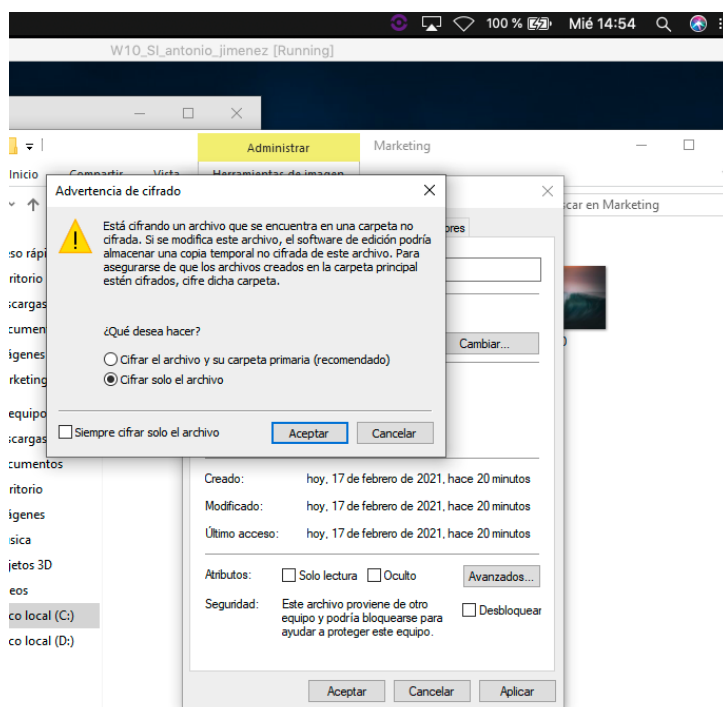
5. Inicia sesión con un usuario del primer departamento. En la carpeta del departamento cifra uno de los documentos que hay dentro. Haz una copia de seguridad del certificado de cifrado con la contraseña 123. Intenta entrar con el otro usuario del departamento y acceder al archivo cifrado e indica qué ocurre. (1,5 puntos).

Inicio sesión con mcespedes que pertenece al departamento de marketing que es el primero que aparece en la imagen de la tarea.



Para **cifrar archivos o carpetas con EFS**, abre el explorador de Windows y haz click con el botón secundario en el archivo o la carpeta que quieres cifrar. Haz click en Propiedades.

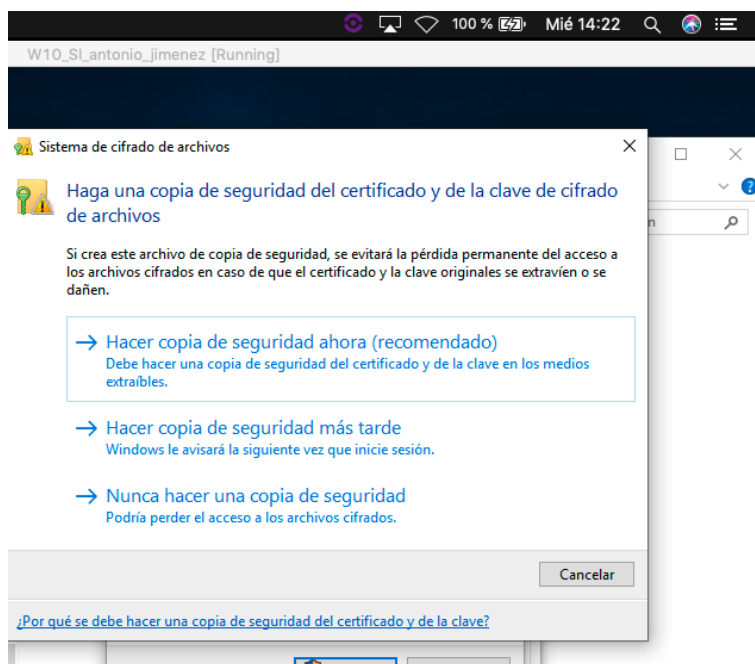
En la ficha General > Avanzadas y activamos la casilla **Cifrar contenido para proteger datos** y Aceptar. Hay disponibles opciones de cifrado adicionales. Le damos a aceptar, luego aplicamos y nos aparece en pantalla distintas opciones de cifrado elegimos solo el archivo. Podemos ver en la imagen un candado que nos dice que está cifrado.



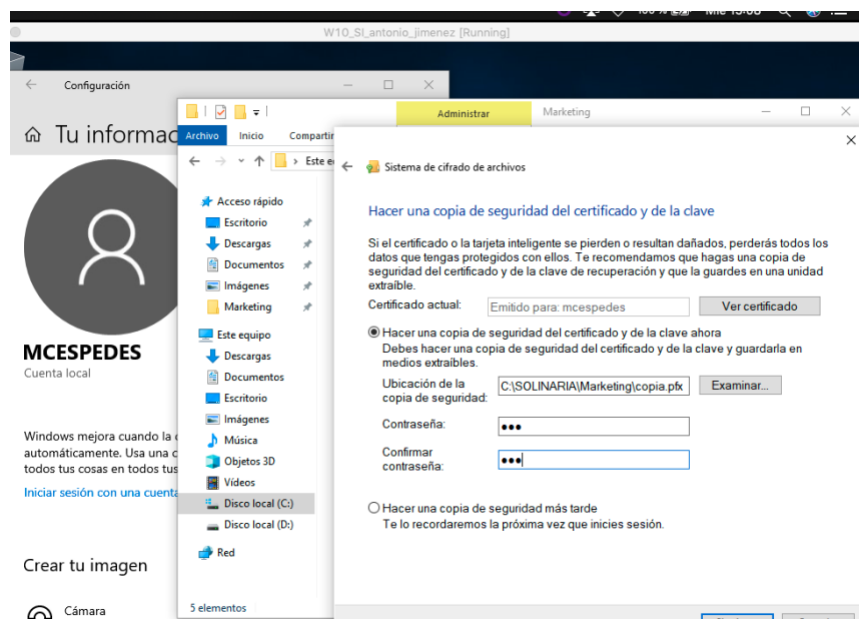
A continuación, se solicita que se haga copia de seguridad de la clave de cifrado:

Si cifras datos en el equipo, necesitas un método para recuperar esos datos en caso de que surja algún problema con la clave de cifrado. Si la clave de cifrado se pierde o queda dañada y no tienes ningún medio de recuperar los datos, éstos se perderán. También perderás datos si almacenas la clave de cifrado en una tarjeta inteligente y ésta se daña o se pierde. Para asegurarse de que siempre puede tener acceso a los datos cifrados, debes hacer una copia de seguridad de la clave y del certificado de cifrado. Si hay más de una persona que usa tu equipo, o si usas una tarjeta inteligente para cifrar archivos, debes crear un certificado de recuperación de archivos.

Finalmente, se genera un certificado del que deberemos hacer copia de seguridad, preferiblemente en un medio extraíble.

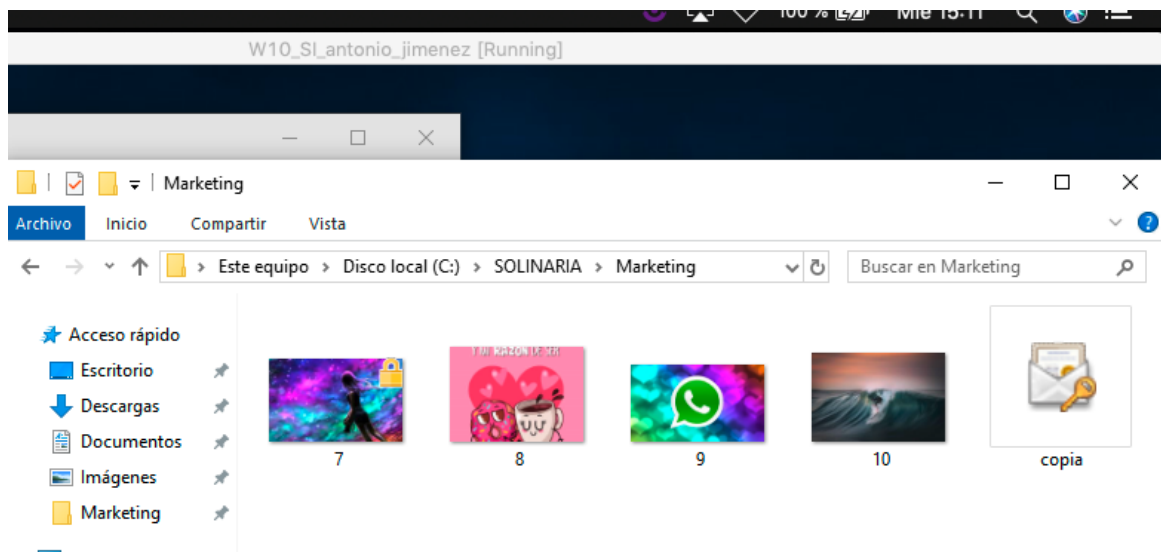


Le decimos donde queremos guardar la copia y la contraseña 123.

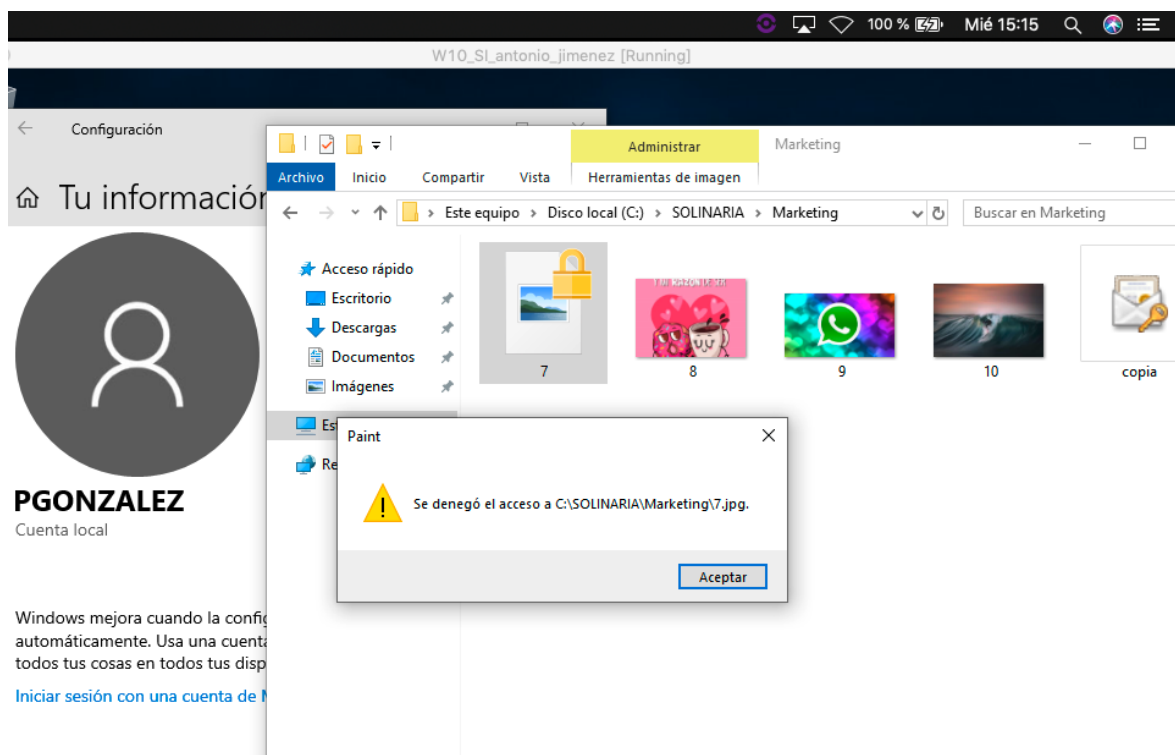




Vemos en la carpeta que la imagen tiene un candado (que significa que está cifrada) y la copia de seguridad.



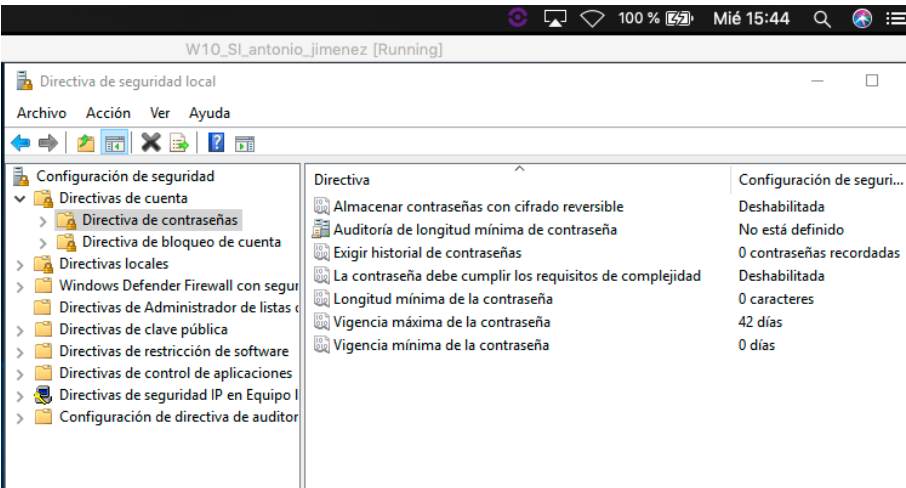
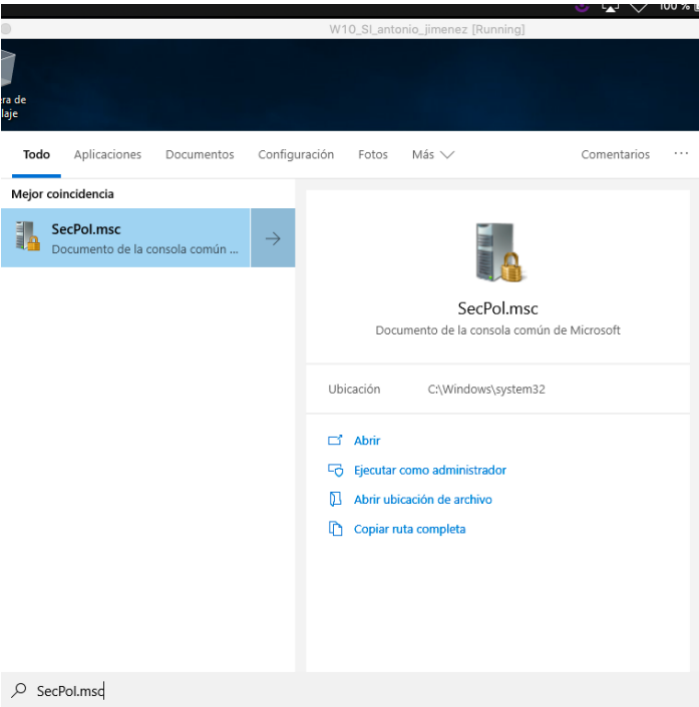
Entramos con el otro usuario de marketing pgomez, y al intentar entrar en la imagen no nos deja.



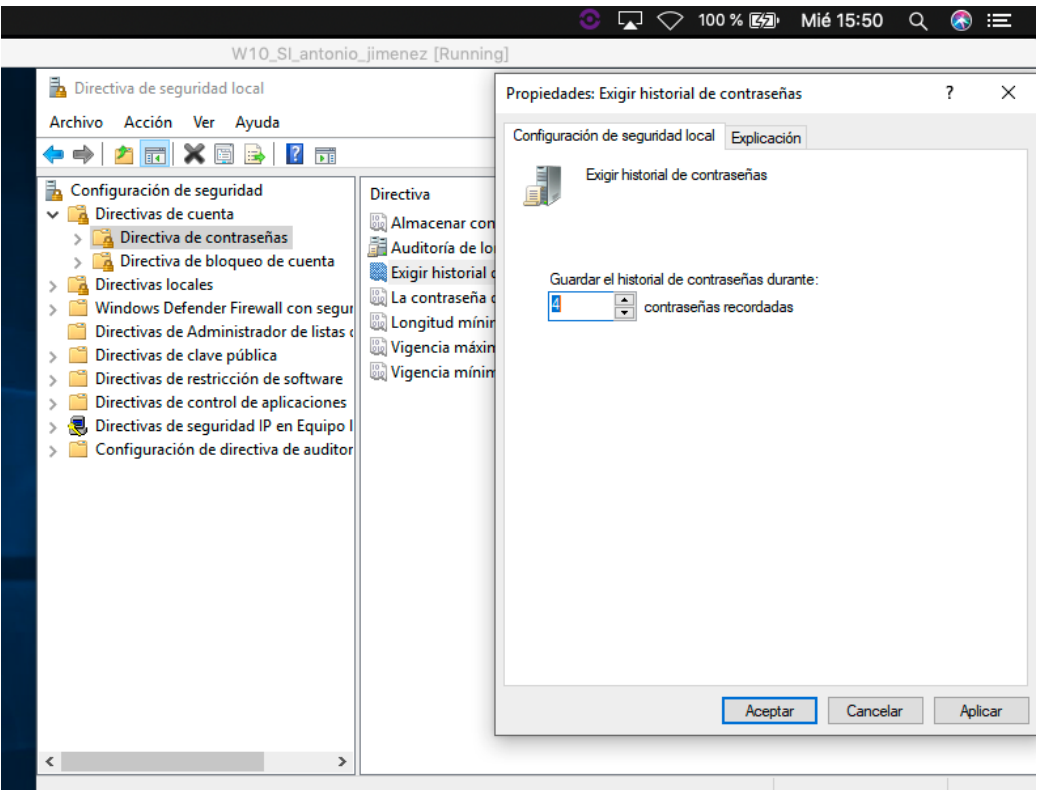


6. **Habilita las directivas de contraseña correspondientes para que el sistema guarde registro de las 4 últimas contraseñas de usuario, éstas deben ser complejas, tener una vigencia máxima de 1 mes, una longitud mínima de 10 caracteres y que permita hasta 3 equivocaciones del usuario al iniciar sesión. (1,5 puntos).**

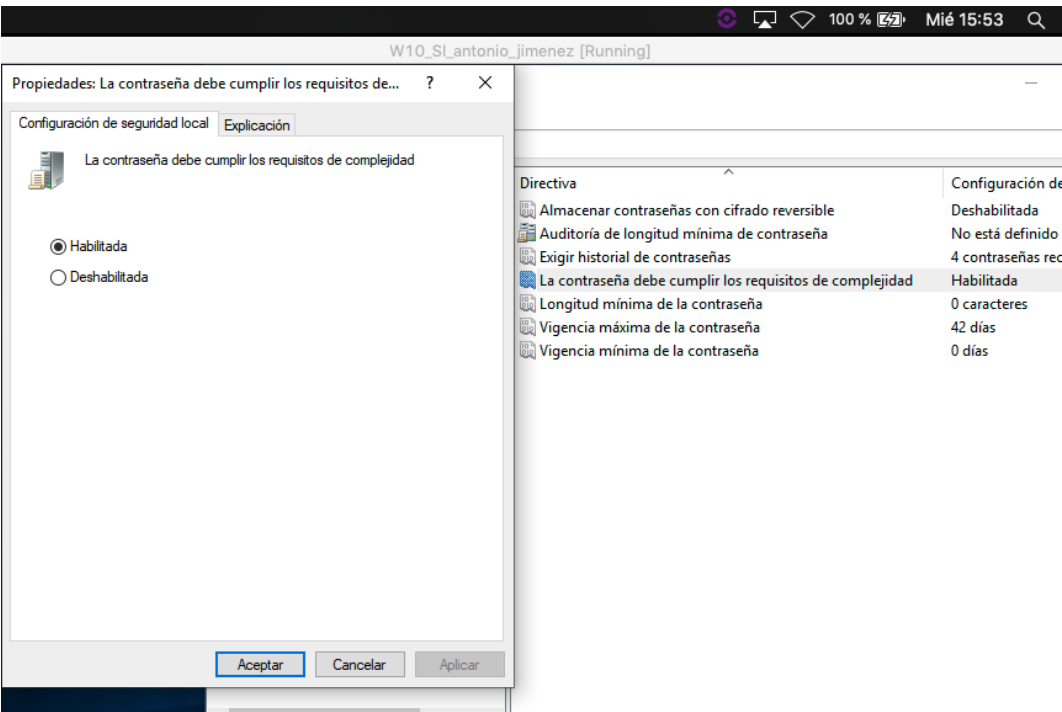
Para acceder a la consola Directivas de Seguridad haremos: **Inicio - Ejecutar - SecPol.msc** Una vez dentro podemos acceder a: **Configuración de Seguridad - Directivas de Cuenta - Directivas de Contraseñas** o también se puede acceder a través de **Inicio - Panel de Control - Sistema y Seguridad - Herramientas administrativas - Directiva de seguridad local**.



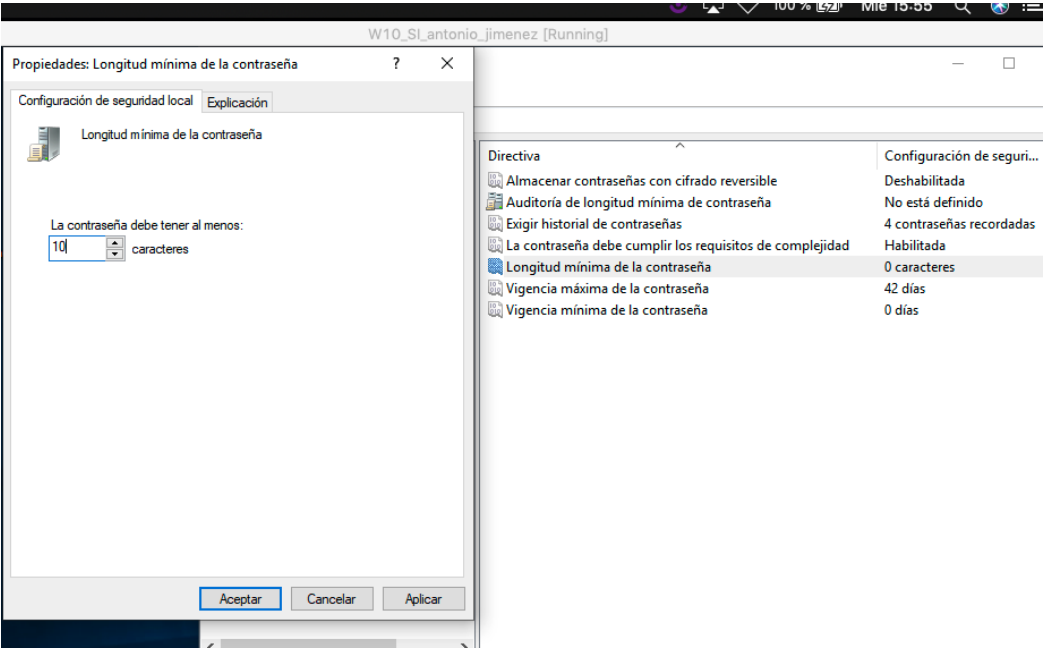
Primero vamos a guardar registro las 4 ultimas contraseñas, hacemos click en exigir historial de contraseñas y le indicamos que nos recuerde 4 contraseñas.



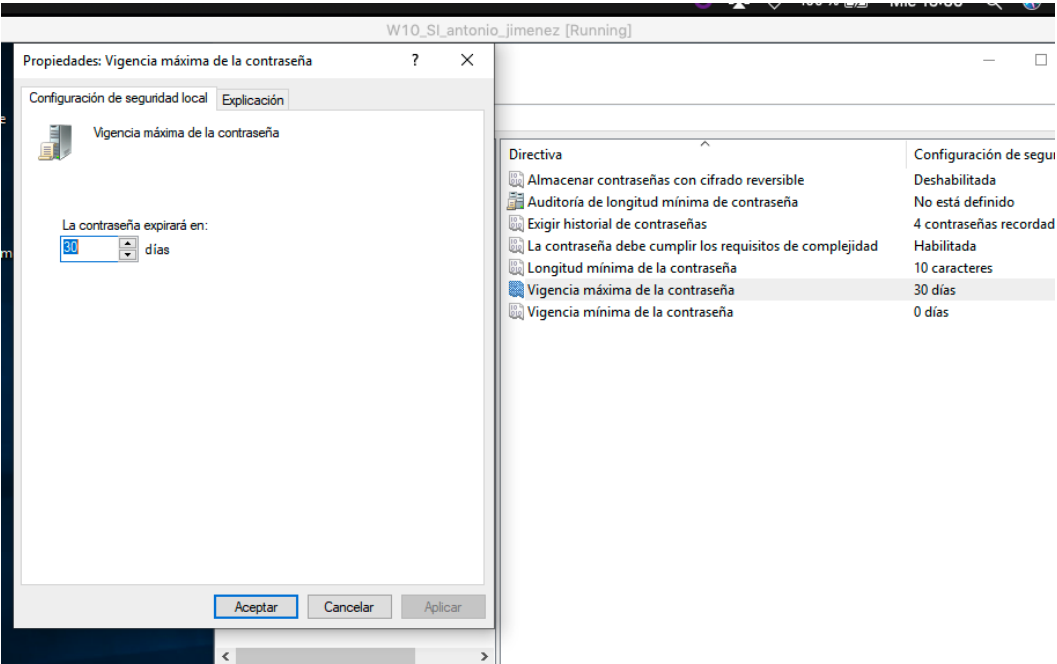
Acto seguido habilitamos los requisitos de complejidad clicando dos veces.



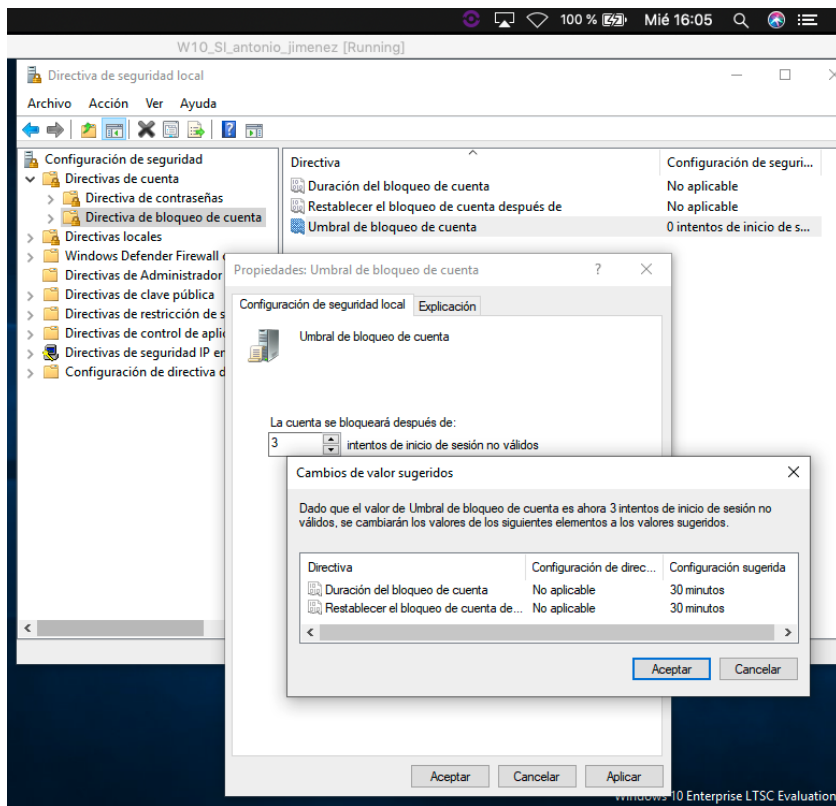
Ahora clicamos en longitud mínima de la contraseña y le indicamos que sea 10.



Clicamos en vigencia máxima, para indicarle que la queremos de 1 mes.

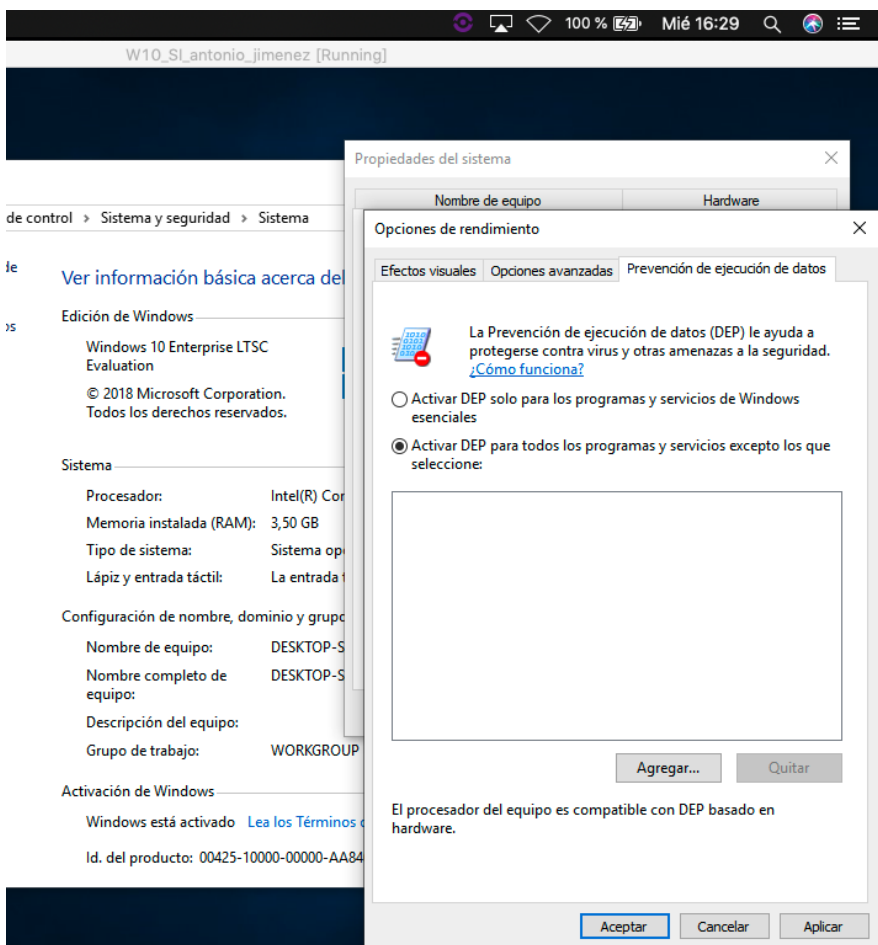
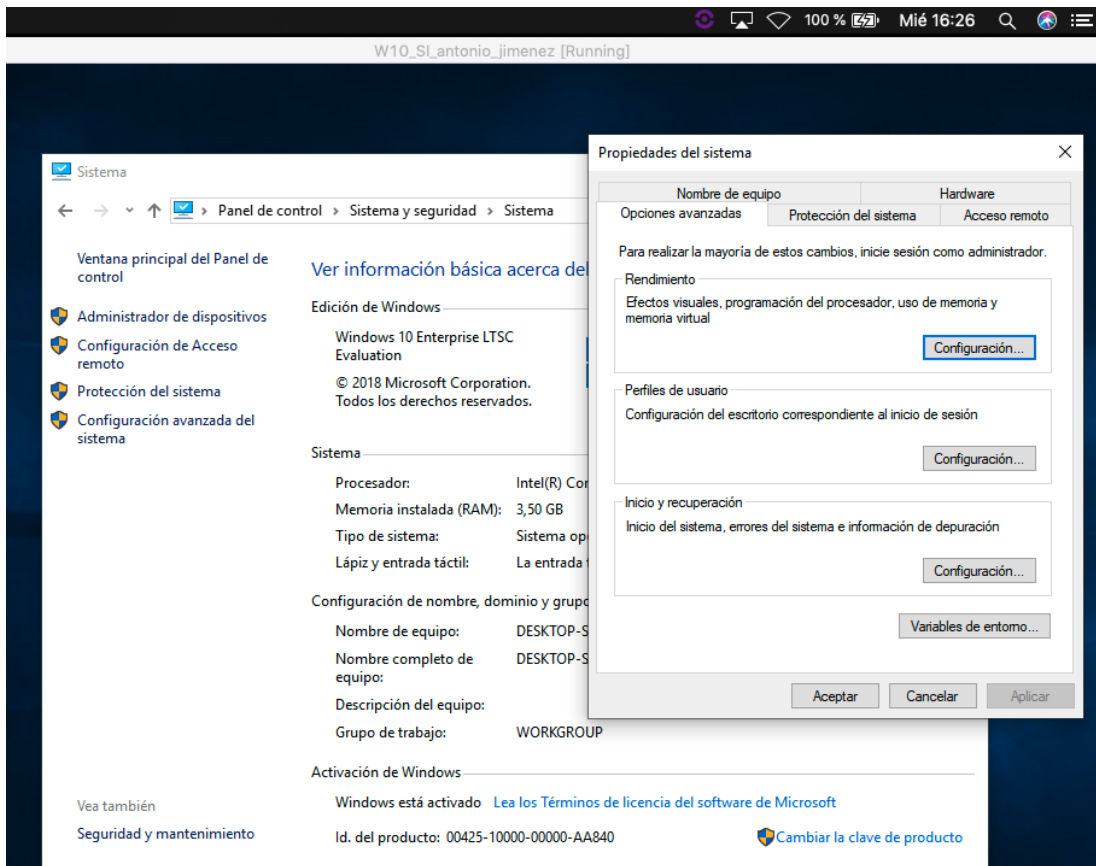


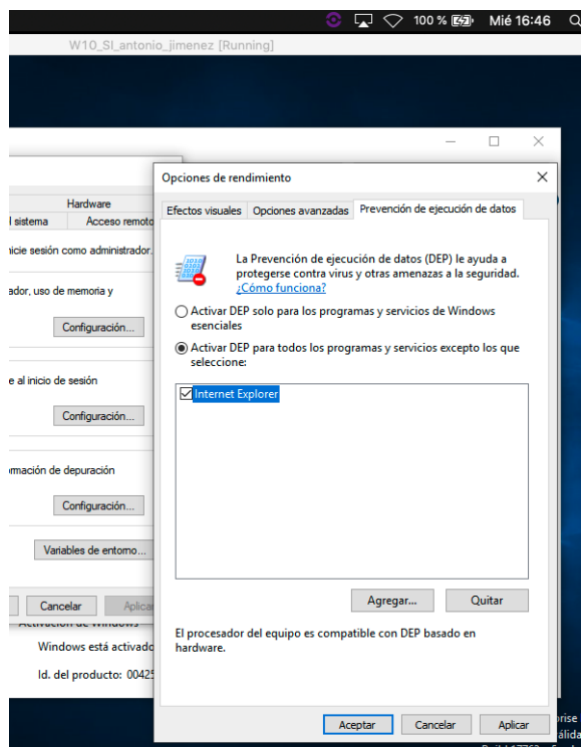
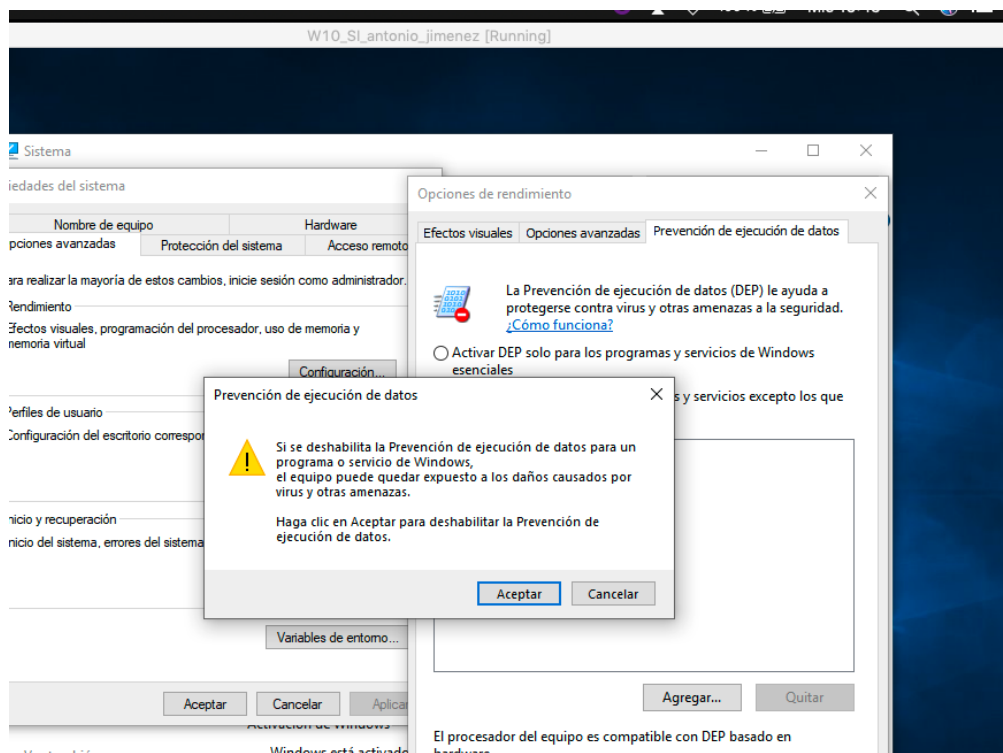
Ahora para cambiar el número de intentos que tenemos para bloquear la cuenta, nos dirigimos a **directiva de bloqueo de cuenta**, y clicamos en **Umbral del bloqueo de cuenta**, y le decimos que sean 3 los intentos de inicio de sesión válida, nos indica el tiempo de duración del bloqueo y el restablecimiento del bloqueo.



## 7. Desactiva la protección de datos en Windows para un programa concreto que tengas instalado. (0,5 puntos).

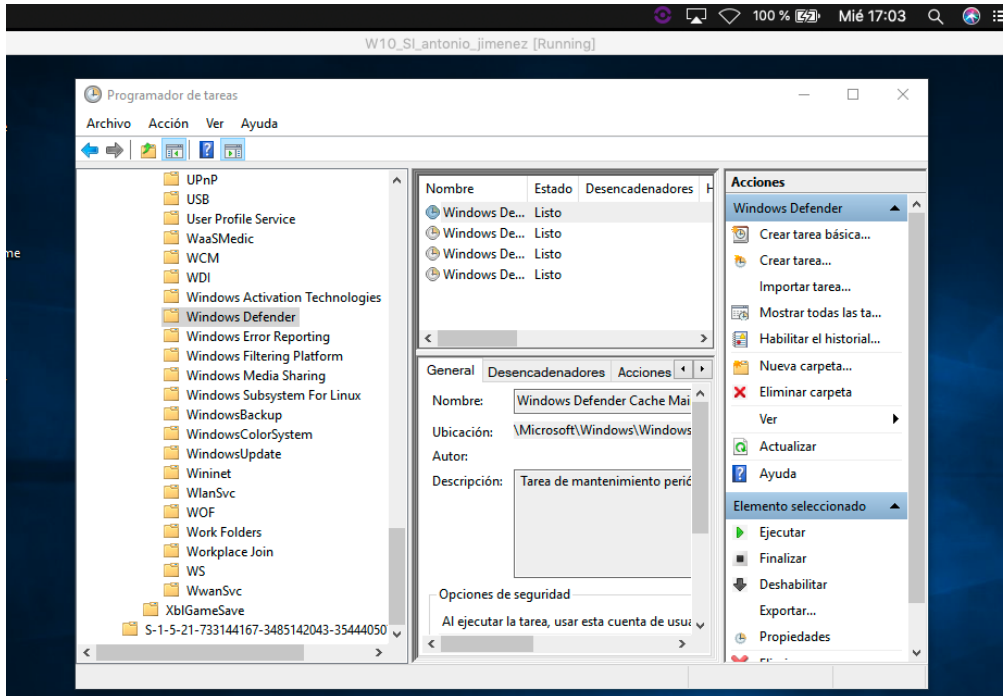
- Haz click en **Inicio Panel de control Sistema y seguridad Sistema**.
- Haz click en **Configuración avanzada del sistema** en el panel de tareas de la izquierda.
- Se obtiene la pantalla **Propiedades del sistema**.
- En **Rendimiento** de la ficha **Opciones avanzadas** de la pantalla Propiedades del sistema, haz click en **Configuración**. Se obtiene la pantalla **Opciones de rendimiento**.
- Haz click en la ficha **Prevención de ejecución de datos** y, a continuación, pulse en **Activar DEP** para todos los programas y servicios excepto los que selecciones. También se puede activar DEP sólo para los programas y servicios de Windows esenciales.
- Para **desactivar DEP** para un programa concreto selecciona la casilla del programa y acepta los cambios.
- Si el programa al desactivar DEP no aparece, elige **Agregar**, busca en la carpeta Archivos de programa, localiza el archivo ejecutable del programa, y, por último, click en **Abrir**.



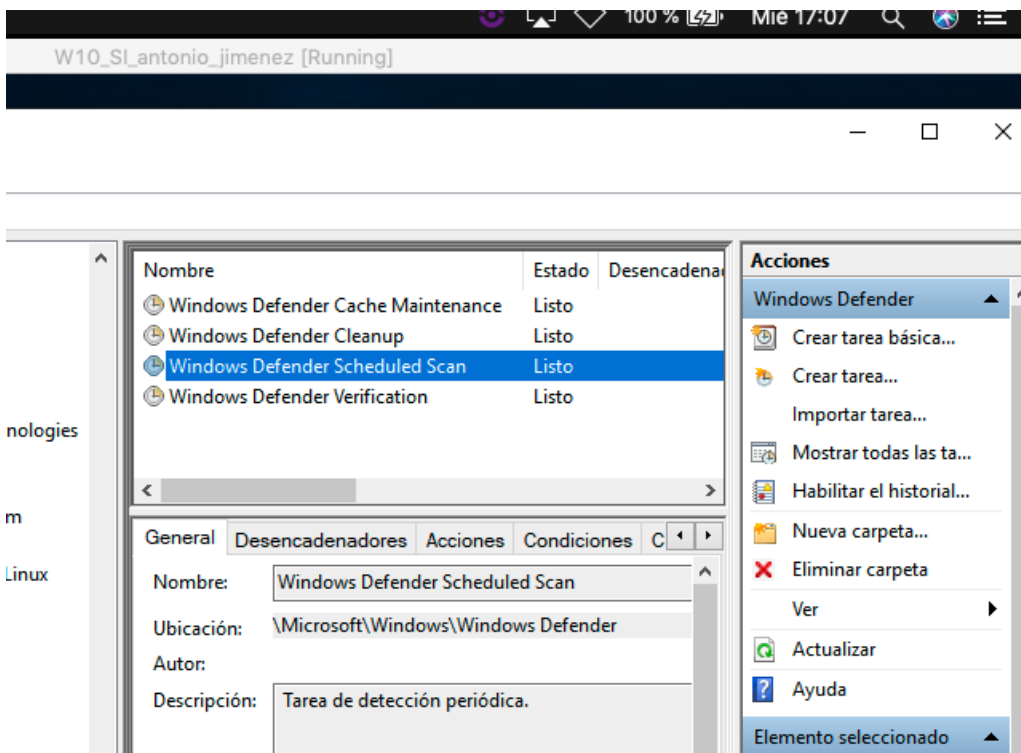


8. Configura un análisis rápido diario a las doce de la noche para detectar amenazas spyware. (0,5 puntos).

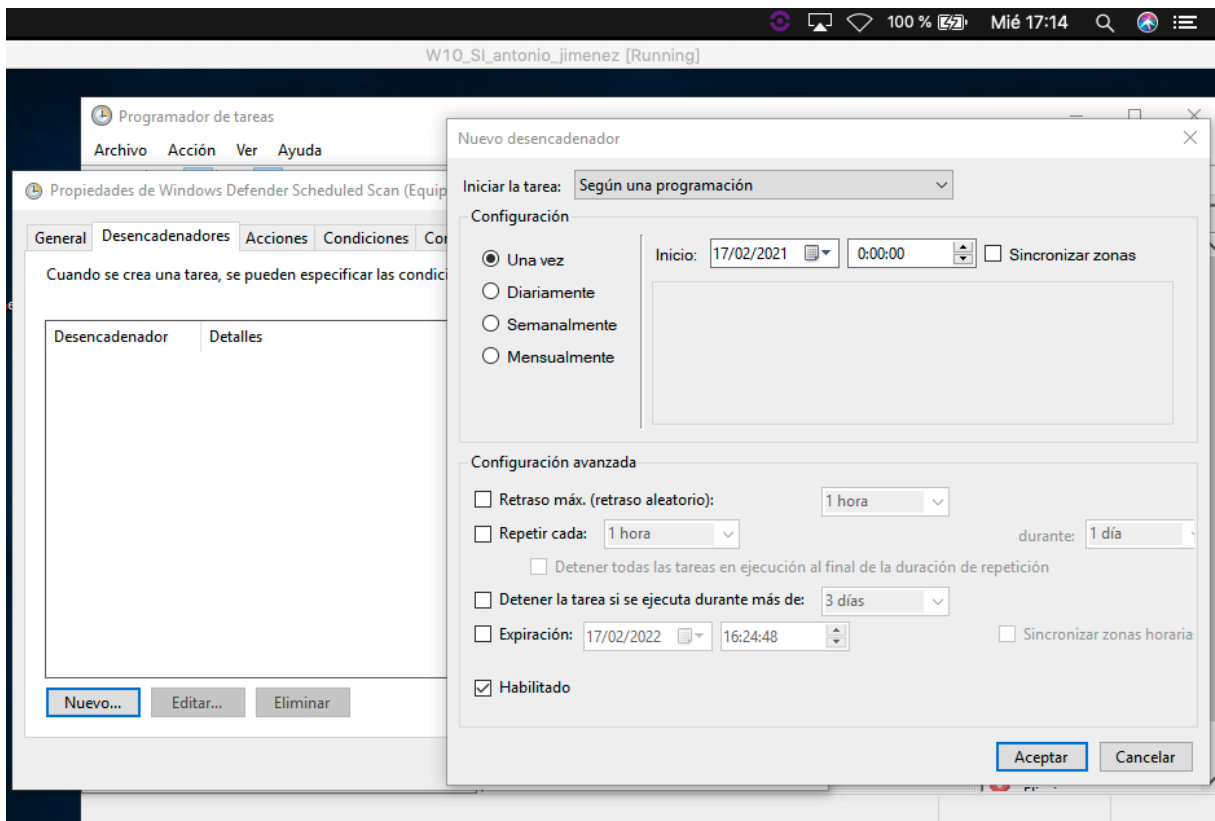
- Nos vamos al programador de Tareas.
- En el panel izquierdo, expande **Biblioteca del programador de tareas – Microsoft - Windows** – nos desplazamos hasta abajo para seleccionar la carpeta de **Windows Defender**.



- En el panel central superior, hacemos doble click en **Windows Defender Scheduled Scan** (análisis programado Windows defender)

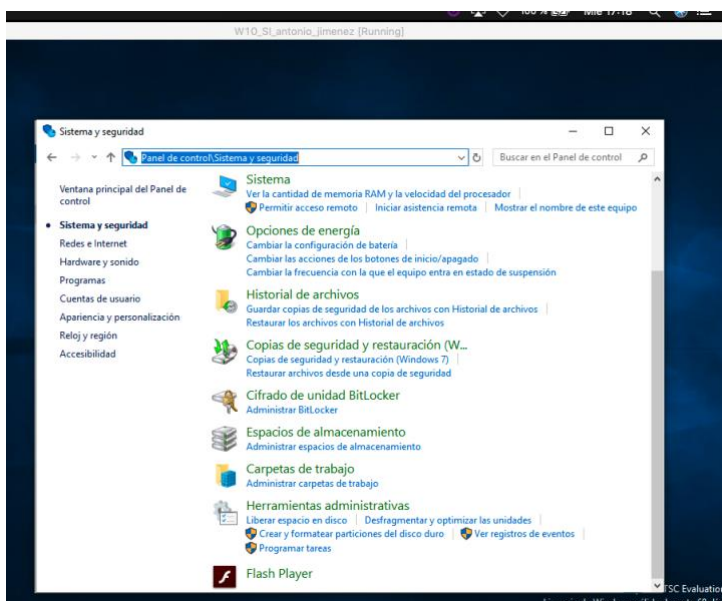


- Se nos abre una ventana que pone propiedades de **Windows Defender Scheduled Scan**(equipo local), seleccionamos la pestaña **desencadenadores**, pinchamos en **nuevo**, y seleccionamos **Una vez** y la hora a la que queremos.



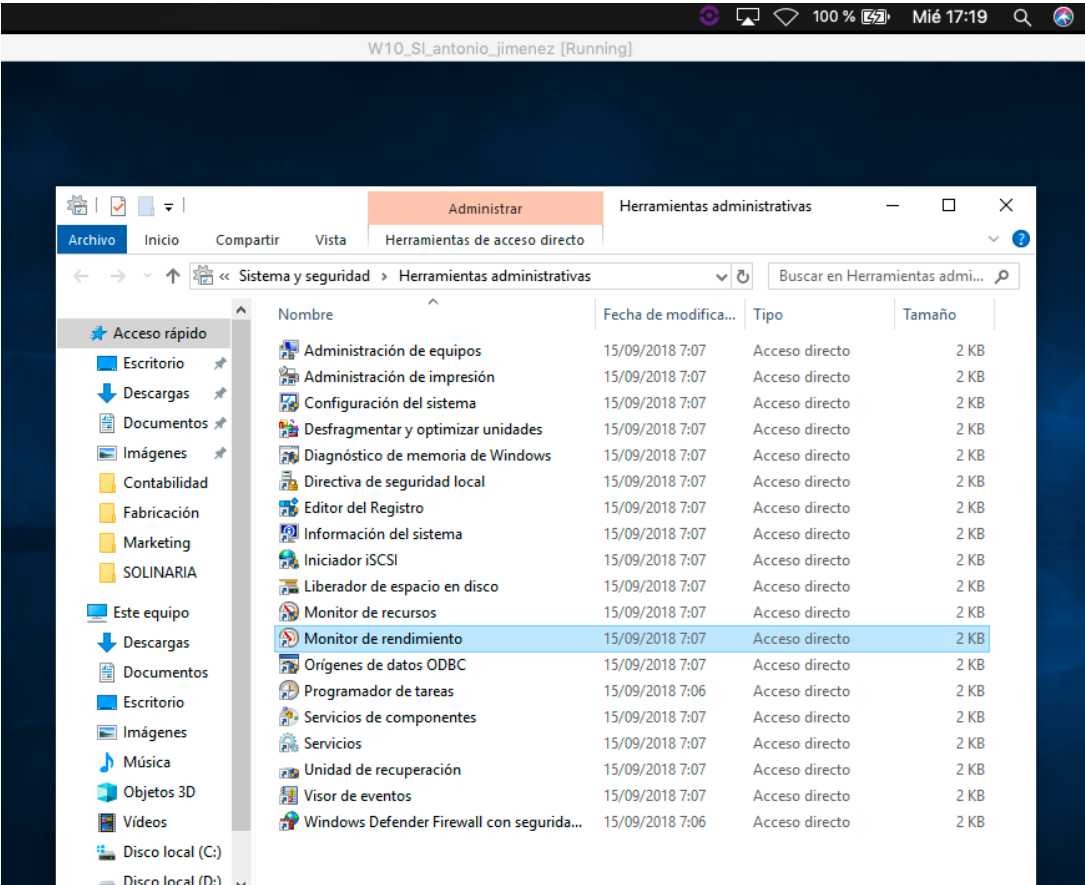
- Abre el monitor de rendimiento de Windows agrega los 3 componentes (procesador - % tiempo inactivo, sistema – procesos y operaciones de lectura de archivo/s) para realizar su seguimiento. Observa la gráfica. (0,5 puntos)

Dentro del grupo de primer nivel **Sistema y seguridad** se hallan las **Herramientas administrativas**. Otra forma de acceder a éstas es a través de Inicio Todos los programas Herramientas administrativas.

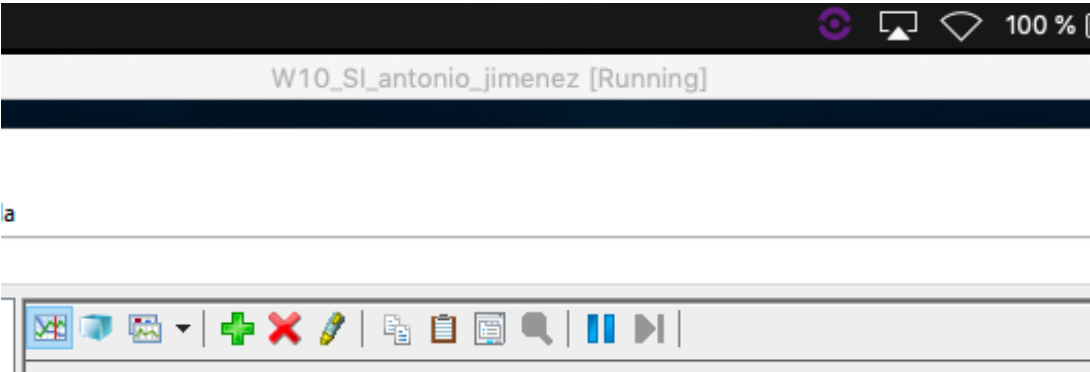




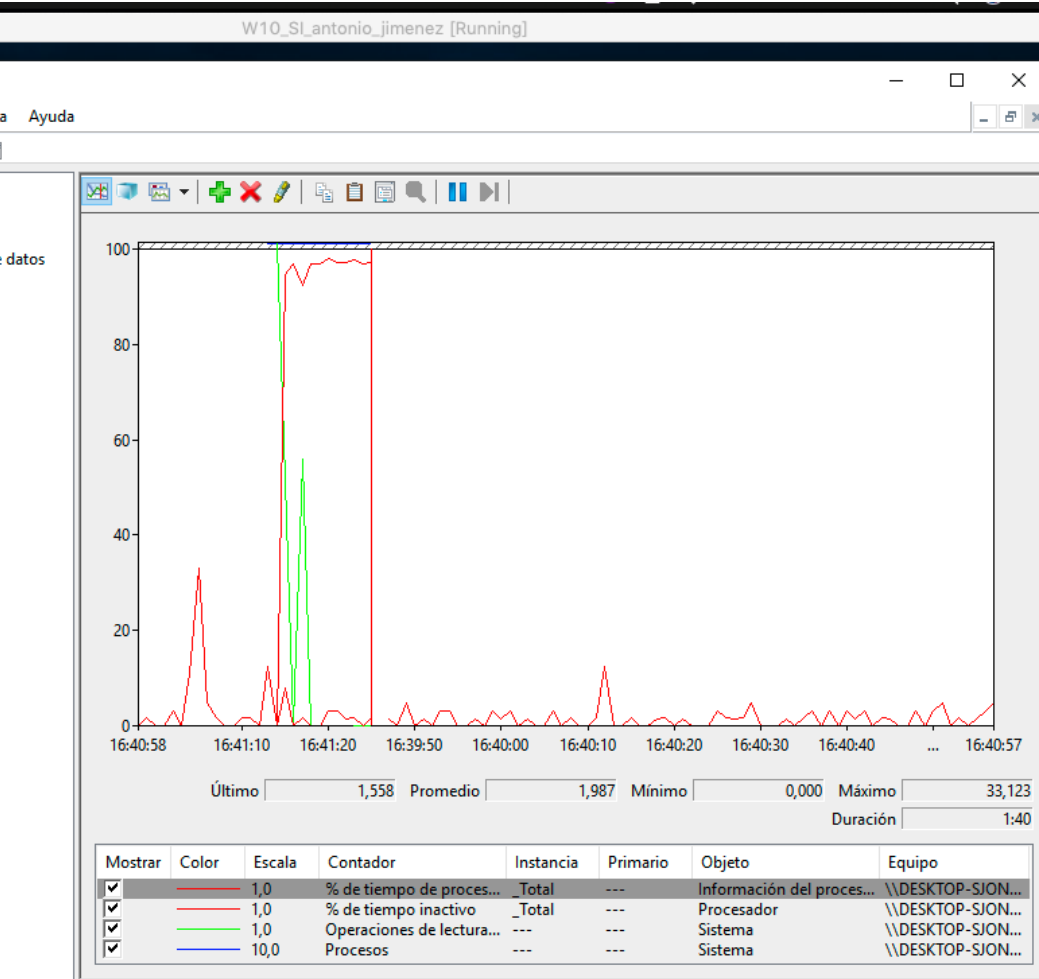
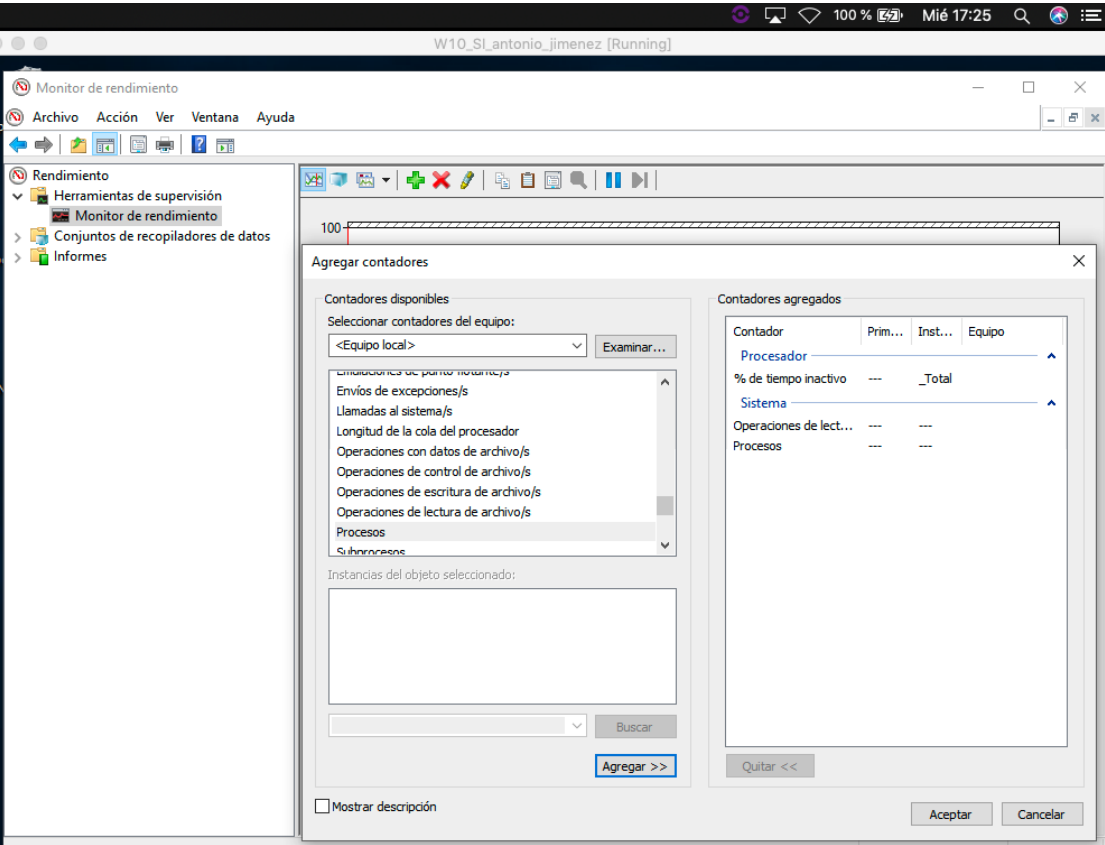
Abrimos el monitor de rendimiento.



Pinchamos en la cruz verde para agregar.

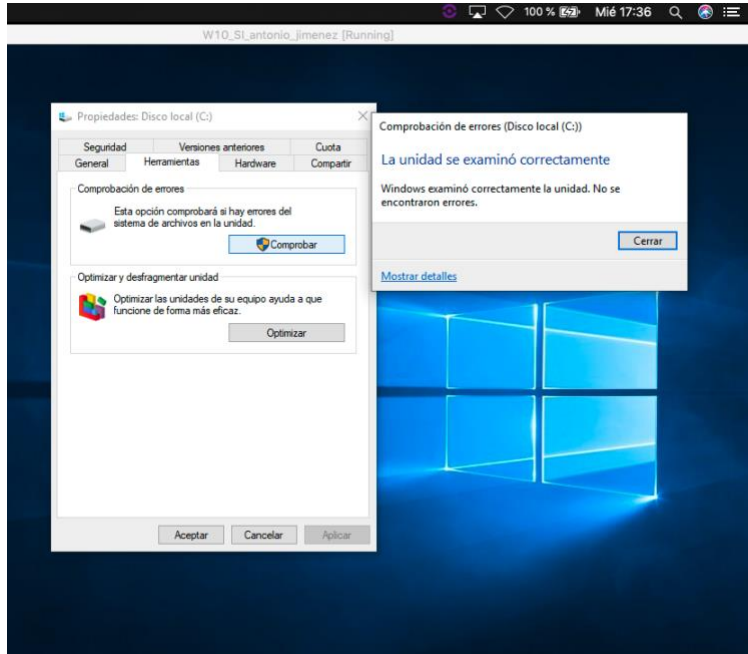


Agregamos contadores de la columna de la izquierda seleccionamos lo que nos pide la tarea, y los vamos a agregando a la columna de la derecha

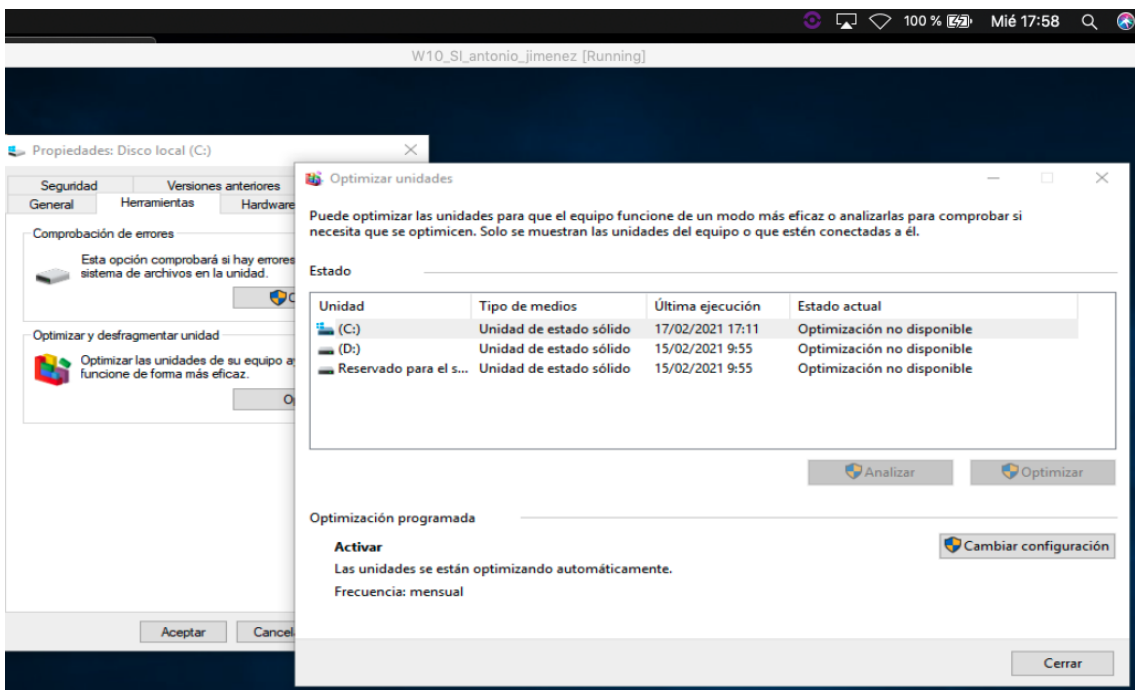


## 10. Desfragmenta y chequea la unidad donde tengas instalado Windows 10. (0,5 puntos)

En la unidad c: es donde tenemos nuestro Windows instalado pinchamos con el botón derecho propiedades en la carpeta de la unidad C: y en la pestaña de **herramientas** pinchamos en comprobar, para chequear la unidad.



Para desfragmentar la carpeta de Windows, nos dirigimos al equipo y en la carpeta C: clicamos con el botón derecho y damos en propiedades, en la pestaña herramientas tenemos la opción de desfragmentar, pero como se ve en la imagen no me deja.



Así que he ido a **Símbolo del Sistema** y he entrado como administrador, he escrito en la consola de comandos **defrag c:**, y ha comenzado la desfragmentación.

```
W10_SI_antonio_jimenez [Running]

Administrador: Símbolo del sistema

Invocando a desfragmentación en (C:)...

Informe de optimización previa:

Información de volumen:
    Tamaño del volumen           = 30,70 GB
    Espacio disponible           = 19,54 GB
    Espacio total fragmentado     = 11%
    Tamaño más grande de espacio disponible = 19,37 GB

Nota: los fragmentos de archivo con tamaño superior a 64 MB no se incluirán en las estadísticas de fragmentación.

La operación se completó correctamente.

Post Defragmentation Report:

Información de volumen:
    Tamaño del volumen           = 30,70 GB
    Espacio disponible           = 19,54 GB
    Espacio total fragmentado     = 0%
    Tamaño más grande de espacio disponible = 19,25 GB

Nota: los fragmentos de archivo con tamaño superior a 64 MB no se incluirán en las estadísticas de fragmentación.

C:\Windows\system32>
C:\Windows\system32>fdgdfgdfg
```

W10\_SI\_antonio\_jimenez [Running]

Propiedades: Disco local (C:)

Optimizar unidades

Puede optimizar las unidades para que el equipo funcione de un modo más eficaz o analizarlas para comprobar si necesita que se optimicen. Solo se muestran las unidades del equipo o que estén conectadas a él.

Estado

| Unidad                 | Tipo de medios          | Última ejecución | Estado actual              |
|------------------------|-------------------------|------------------|----------------------------|
| (C:)                   | Unidad de estado sólido | En ejecución...  | Paso 2: 0% consolidado     |
| (D:)                   | Unidad de estado sólido | 15/02/2021 9:55  | Optimización no disponible |
| Reservado para el s... | Unidad de estado sólido | 15/02/2021 9:55  | Optimización no disponible |

Detener

Optimización programada

**Activar**

Las unidades se están optimizando automáticamente.

Frecuencia: mensual

Cambiar configuración

Cerrar

Windows 10 Enterprise LTSC Evaluation  
Licencia de Windows válida durante 68 días