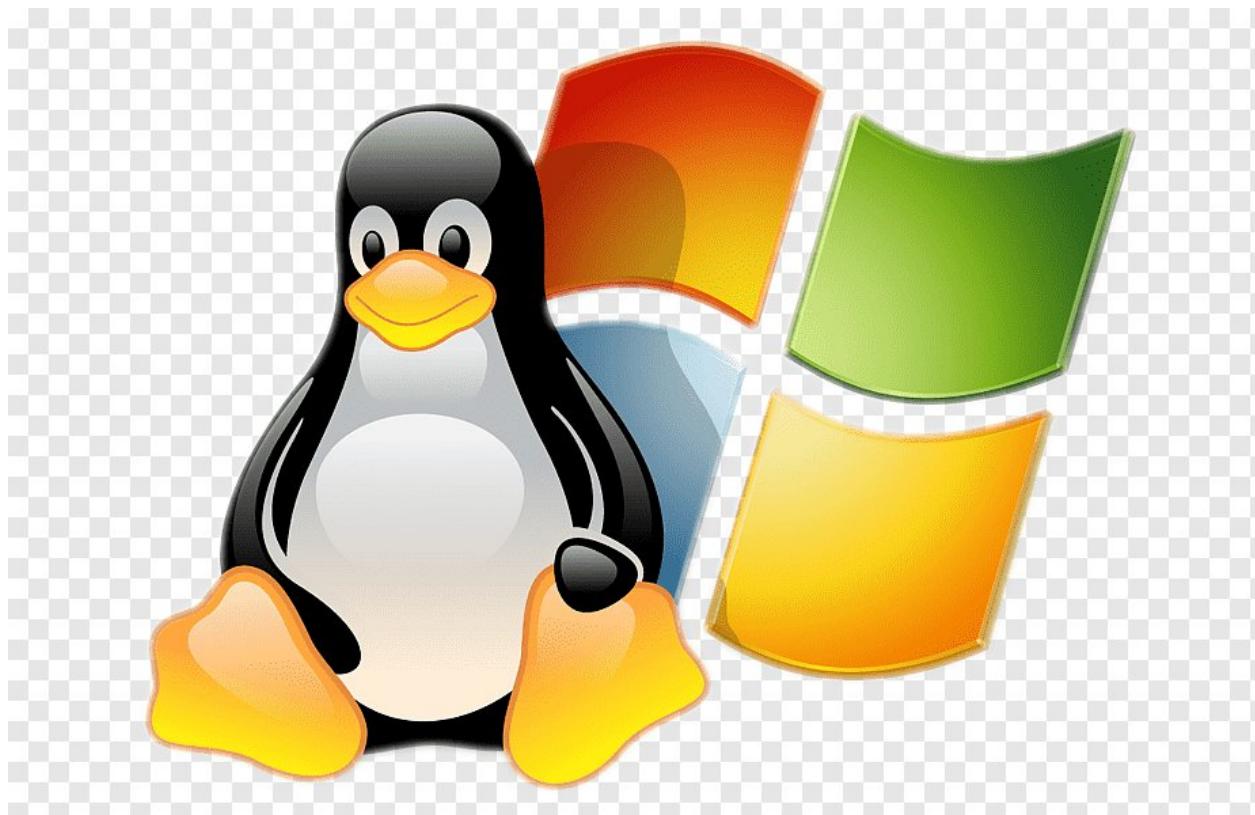


# IMPLANTACIÓN DE SISTEMAS OPERATIVOS

## TAREA 9

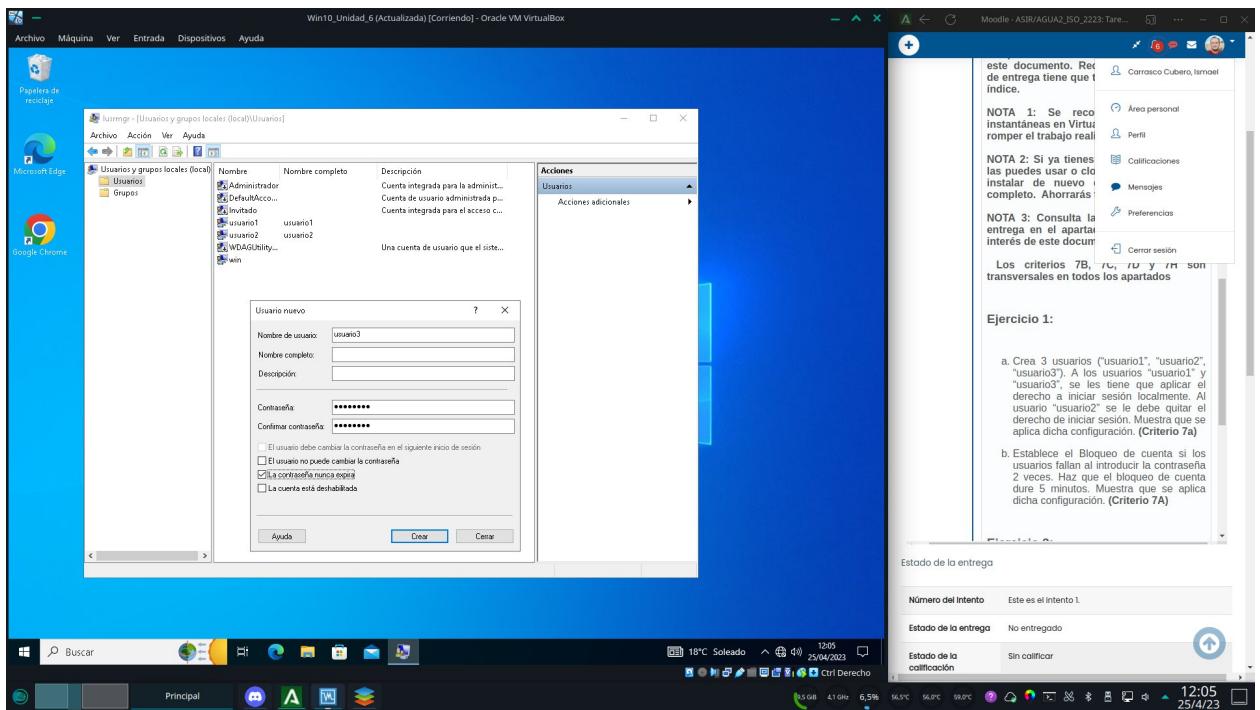


ISMAEL CARRASCO CUBERO

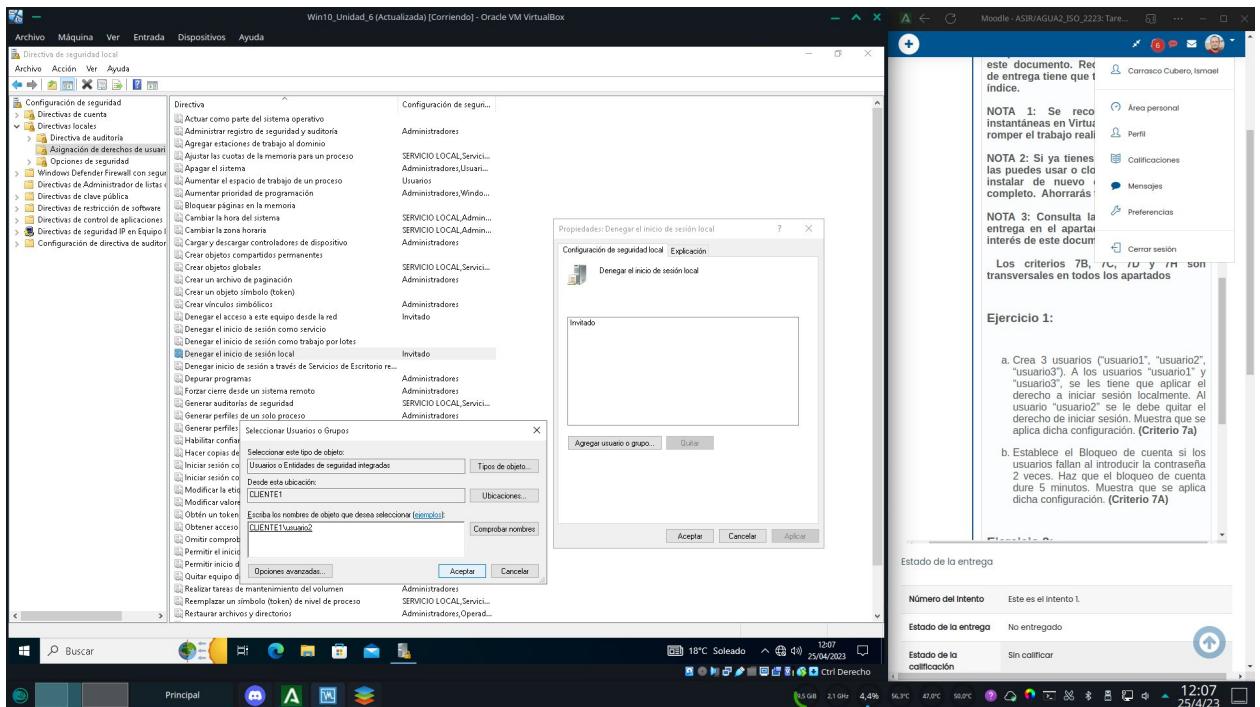
# Contenidos

Contenidos .....	2
Ejercicio 1: .....	3
<b>Ejercicio 2:</b> .....	8

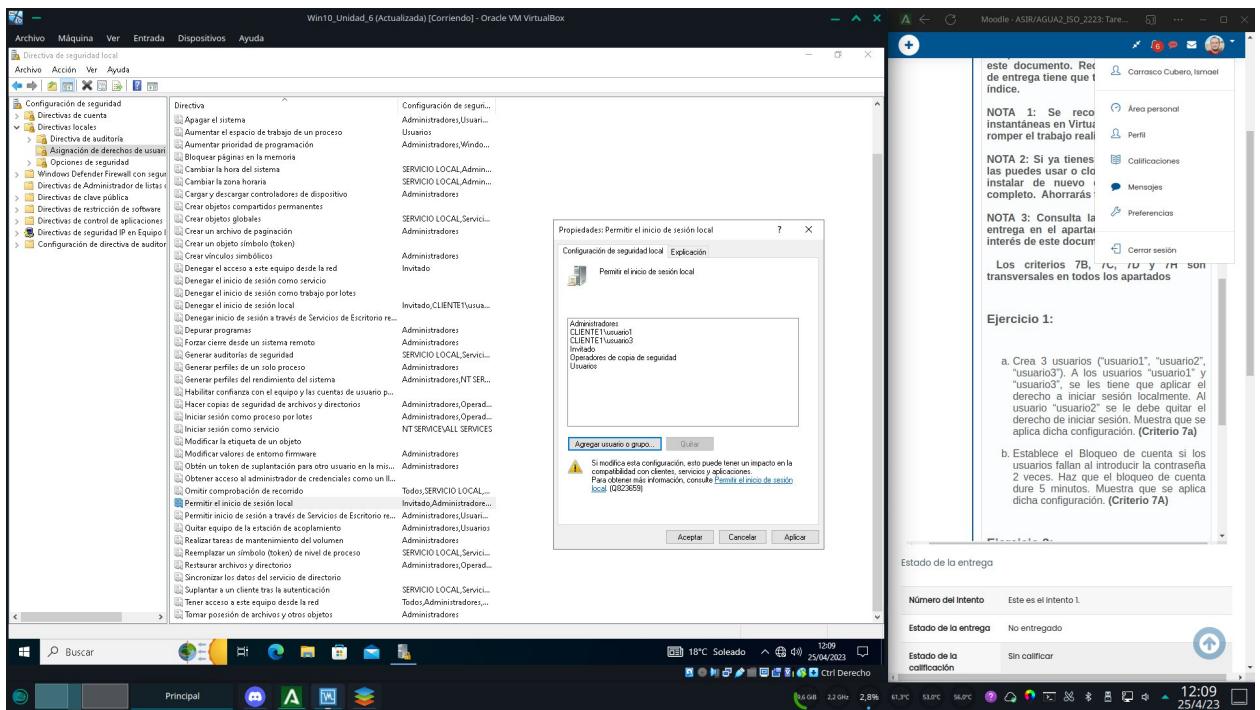
# Ejercicio 1:



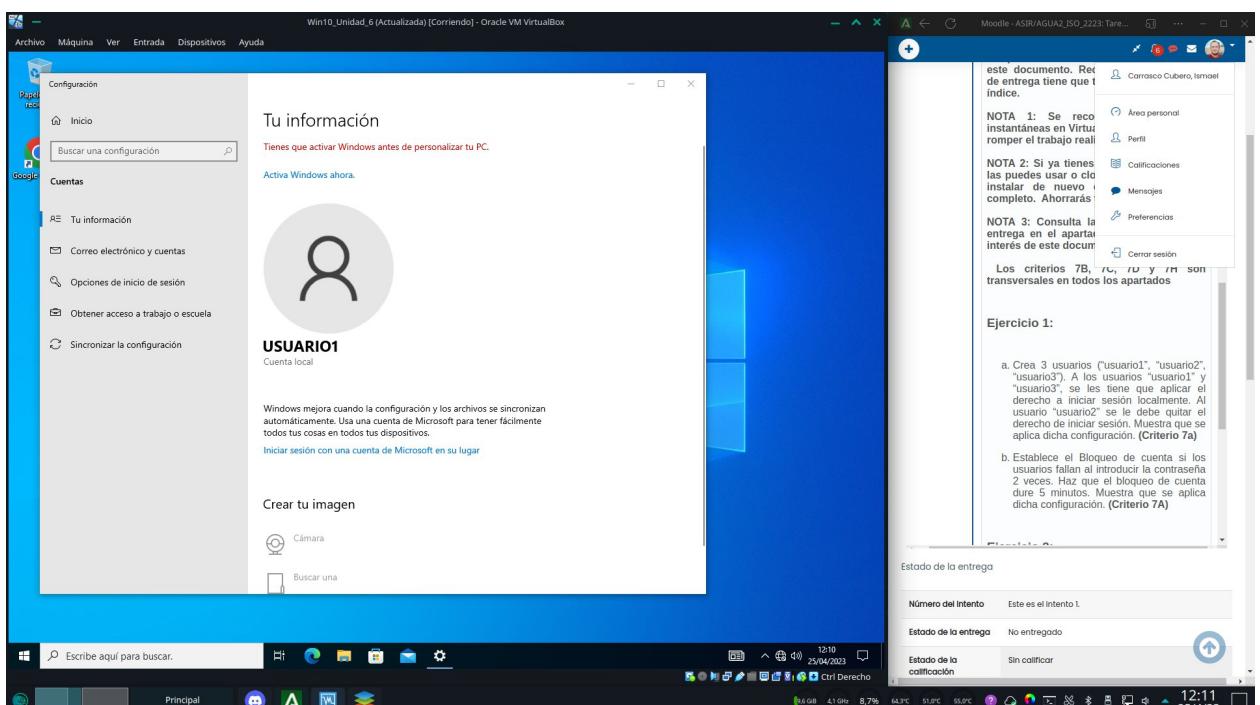
Comenzamos creando los 3 usuarios locales en windows 10



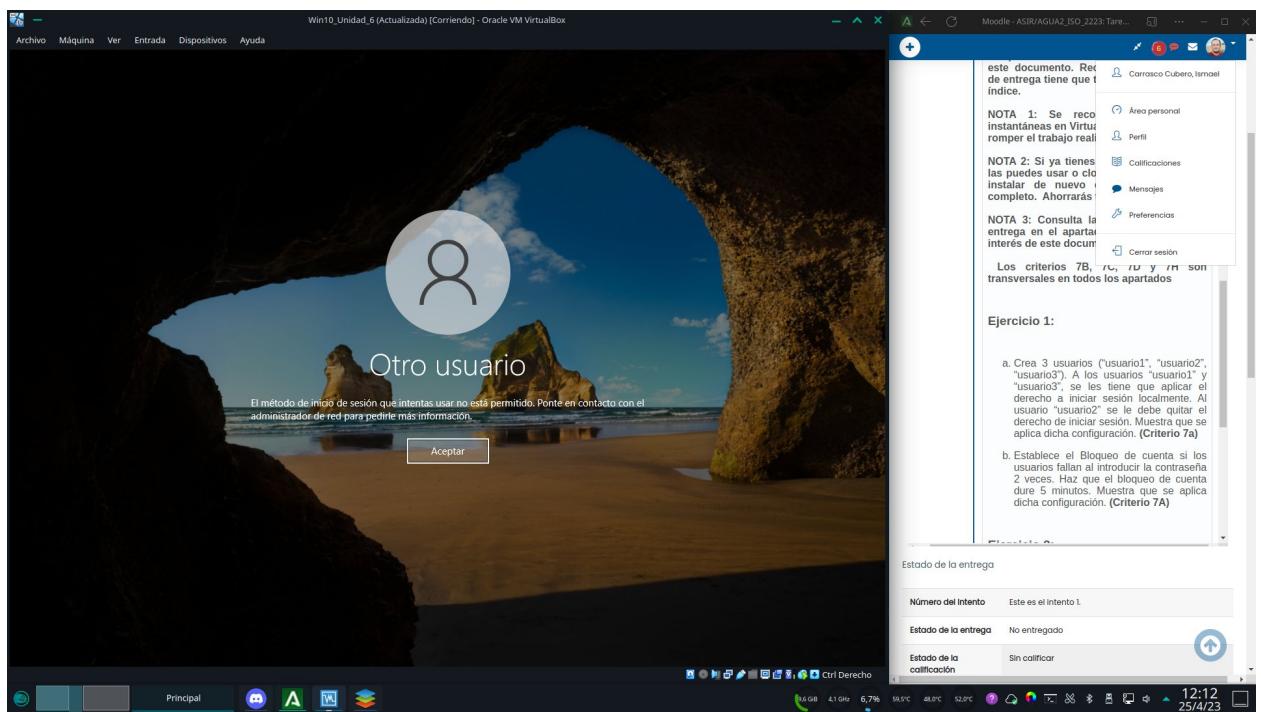
Vamos hasta el administrador de directivas locales, y ahí navegamos a directivas locales > asignación de derechos de usuario. Una vez en la lista, buscamos las dos directivas que nos interesan. Comenzamos por denegar el login local a usuario2



Agregamos usuario1 y usuario3 a la lista de acceso para el login local en la directiva “permitir inicio de sesión local”

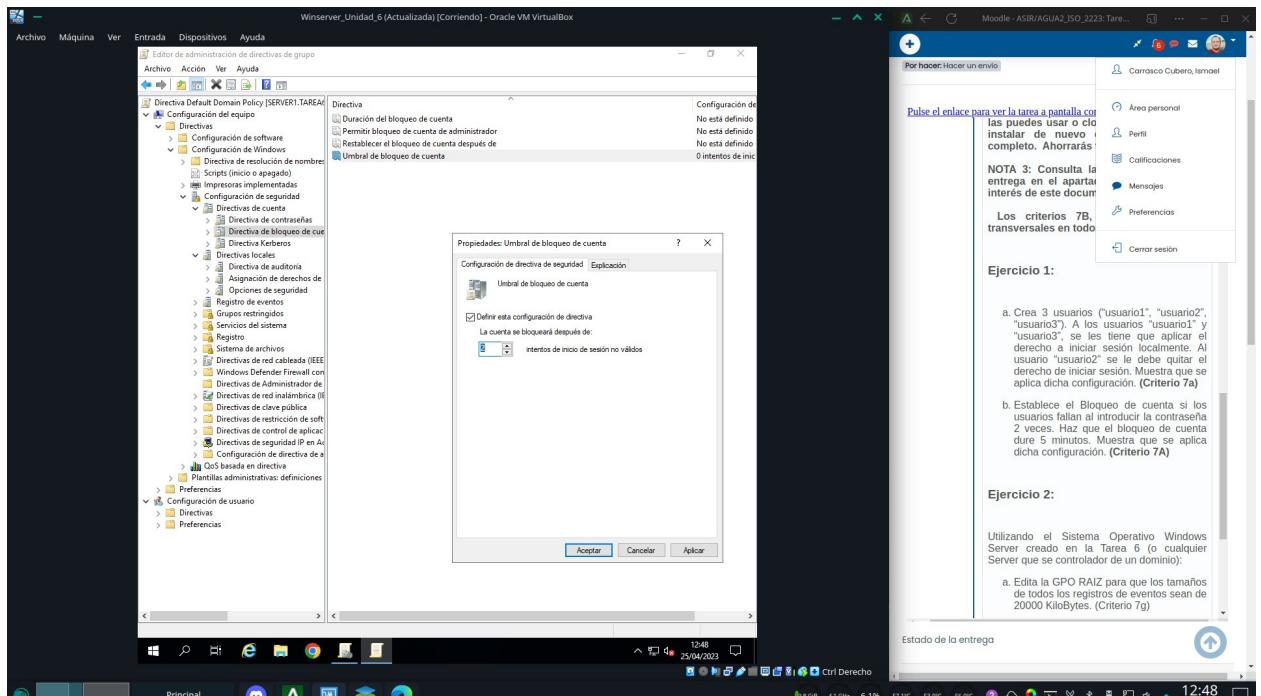


Comprobamos que usuario1 es capaz de loguearse sin problemas

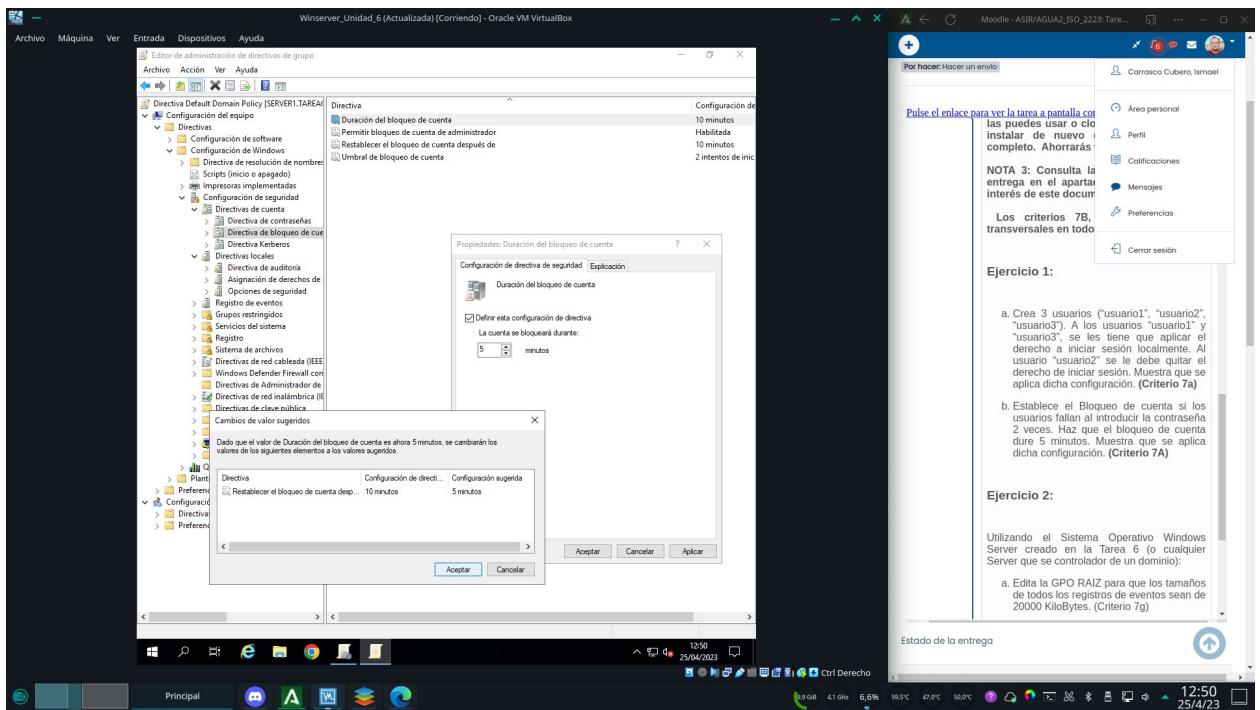


Sin embargo usuario2 no puede loguearse y se nos muestra un mensaje para que contactemos con el administrador.

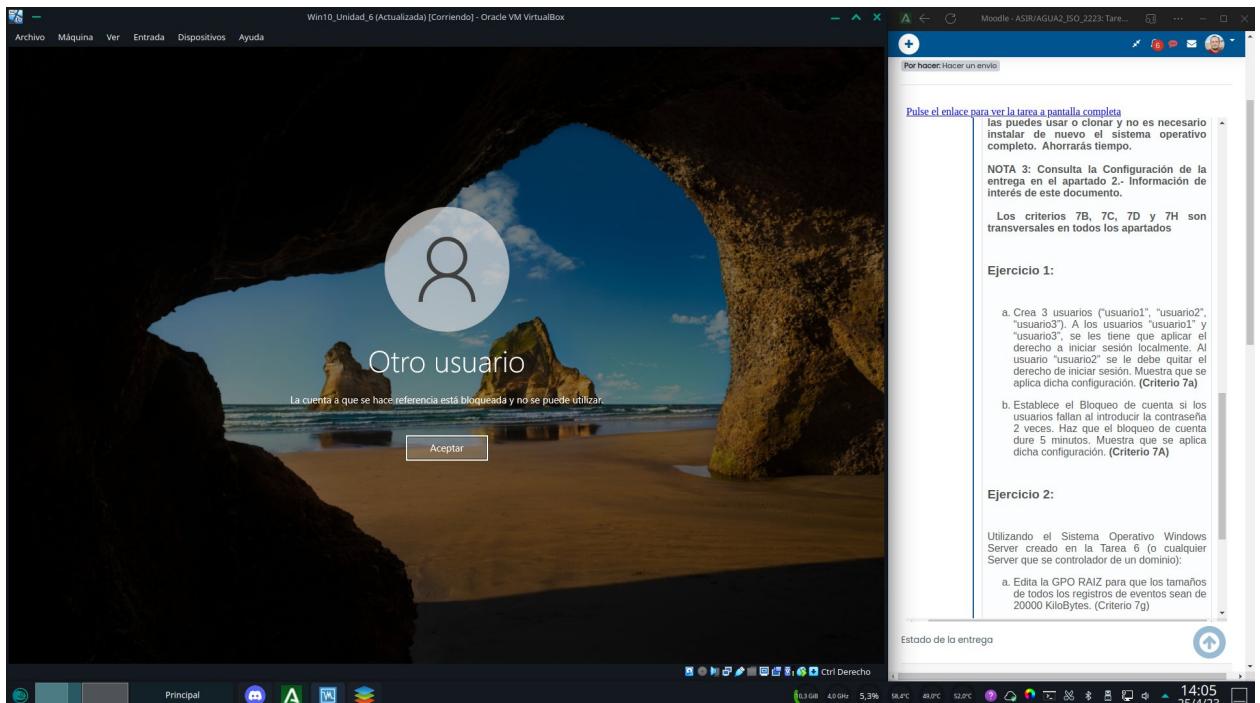
Para los bloqueos de cuenta por contraseña errónea:



Nos logueamos como administrador en el controlador de dominio y en el editor de directivas de grupo navegamos hasta configuración de equipo > directivas > configuración de windows > configuración de seguridad > directivas de cuenta > directiva de bloqueo de cuenta; y escogemos umbral de bloqueo de cuenta. En dicho apartado establecemos 2 intentos

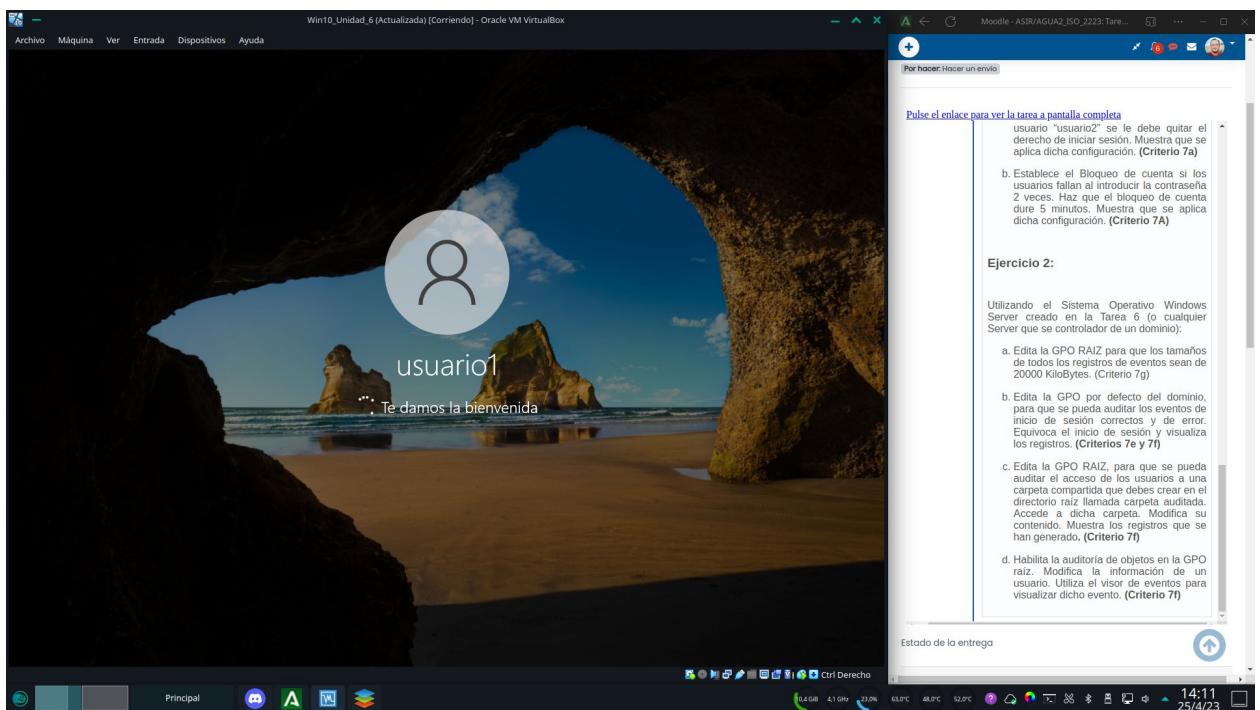


A continuación establecemos la duración del bloqueo de cuenta desde su correspondiente opción



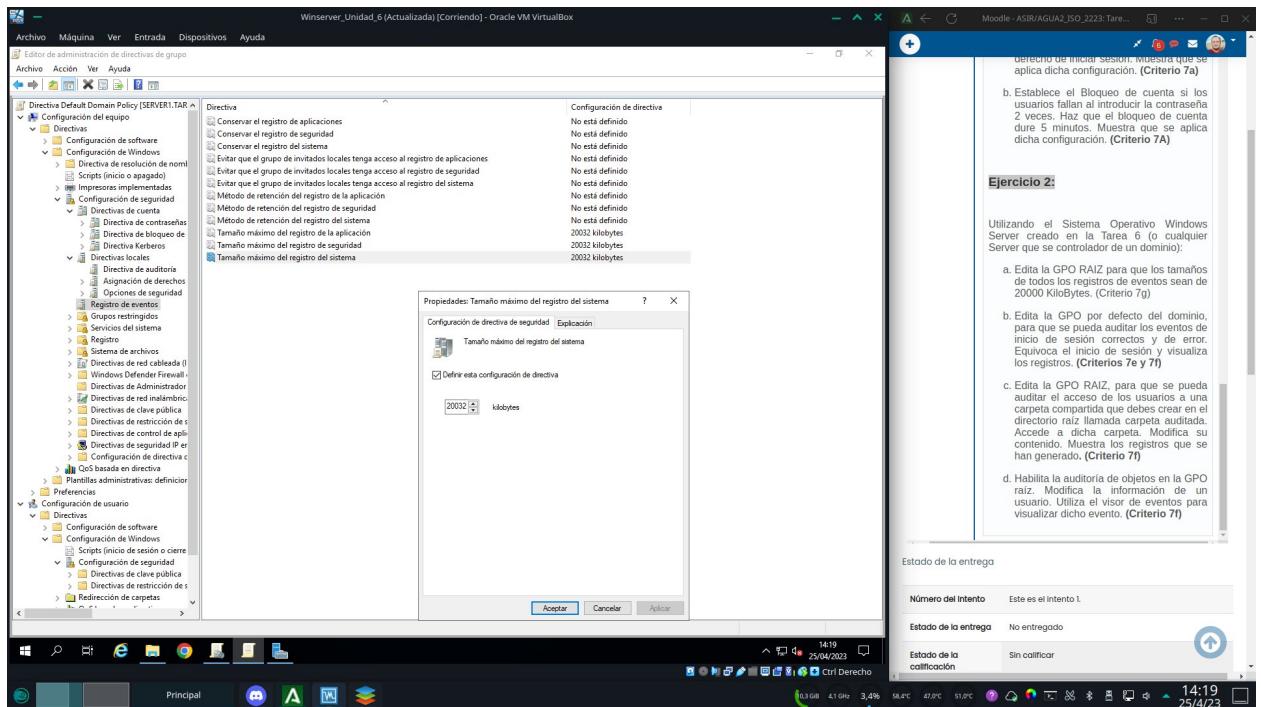
Tras introducir la contraseña de forma errónea varias veces, queda bloqueada a las 14:05, veamos a las 14:10

# Ismael Carrasco Cubero

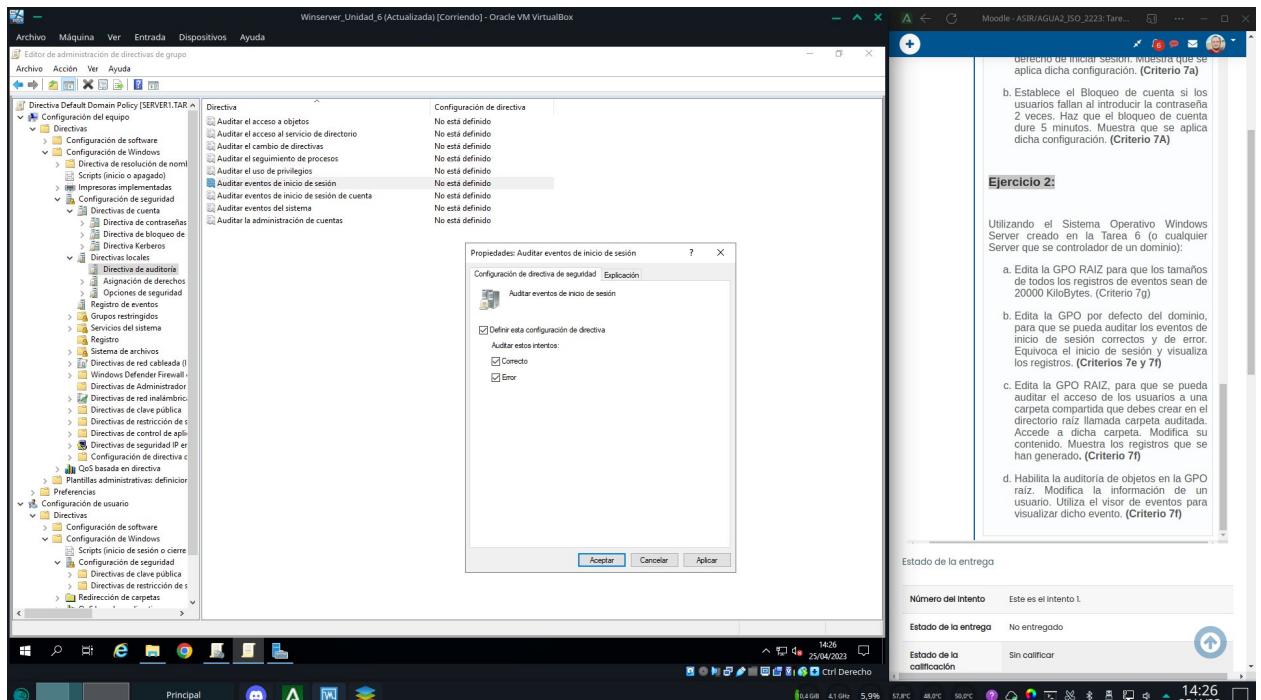


Unos minutos después, el bloqueo queda anulado y el usuario puede volver a loguear

## Ejercicio 2:

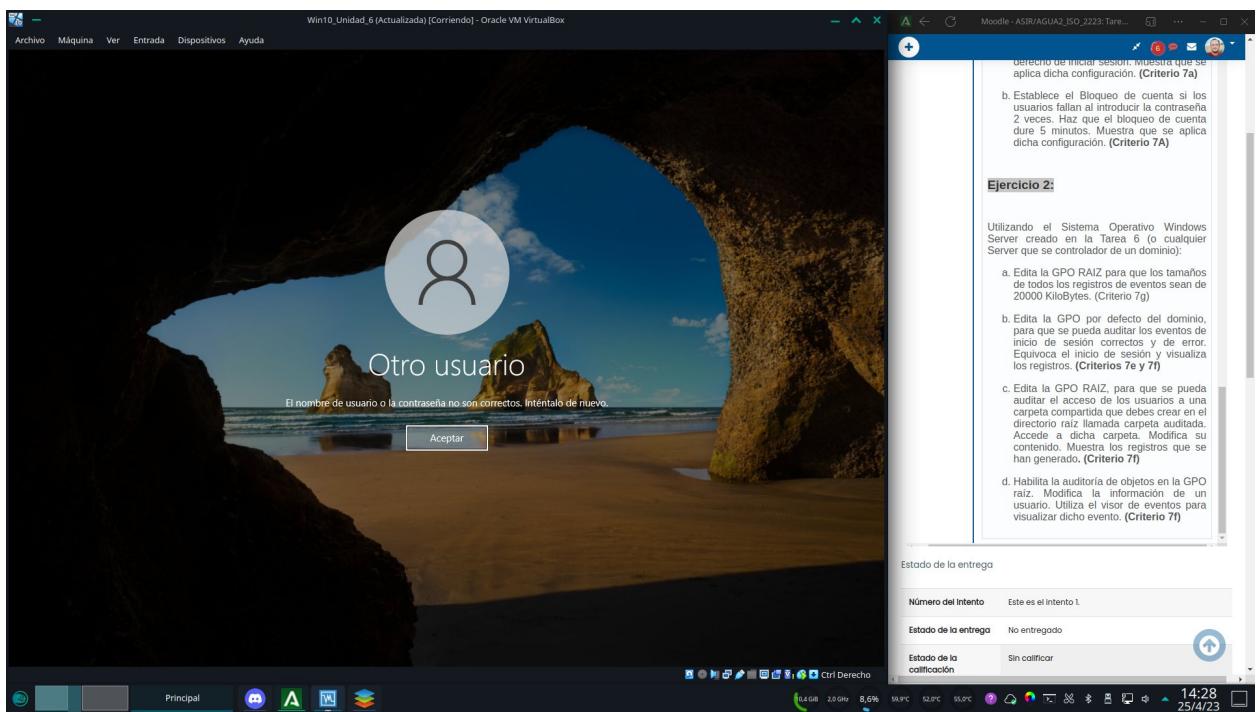


Entramos en el editor de directivas en la directiva raíz y navegamos a configuración de equipo > directivas > configuración de windows > configuración de seguridad > registro de eventos. En dicha sección podemos encontrar las opciones para establecer el tamaño de los registros de eventos en el tamaño deseado, en este caso 20032 (no permite 20000 redondo)

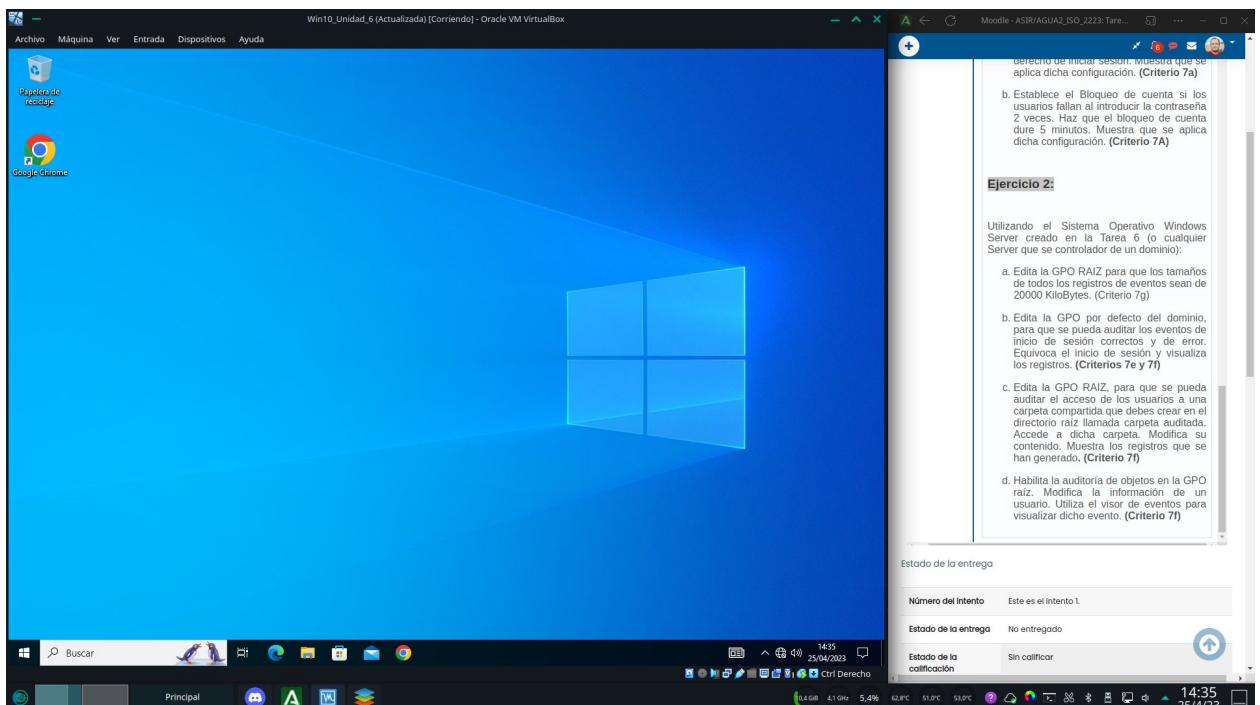


Para el siguiente apartado navegamos desde configuración de seguridad > directivas locales > directiva de auditoria, y en el apartado auditar eventos de inicio de sesión hacemos los cambios oportunos

# Ismael Carrasco Cubero



Equivocamos el login para ver si deja rastro en los eventos



A continuación nos logueamos correctamente

# Ismael Carrasco Cubero

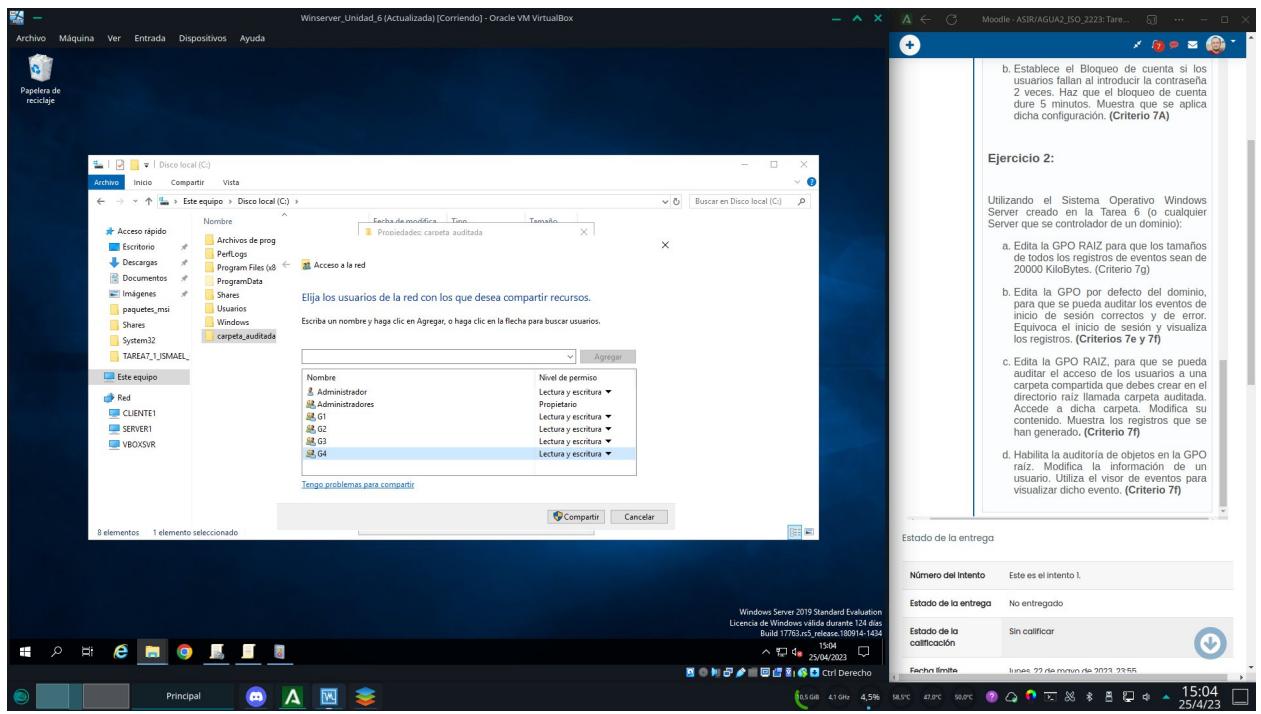
The screenshot shows the Windows Event Viewer interface. On the left, a tree view includes 'Visor de eventos (local)', 'Vistas personalizadas', 'Registros de Windows' (selected), 'Aplicación', 'Seguridad' (selected), 'Sistema', 'Eventos reenviados', and 'Registros de aplicaciones y suscripciones'. The main pane displays a table of events under the 'Seguridad' category. One event is selected, showing details: Subject (Id. de seguridad: SYSTEM, Nombre del cuenta: SERVER15, Dominio de cuenta: TAREAS64, Id. inicio de sesión: 0x4198E), Tipo de inicio de sesión: 3, and Description (Este evento se genera cuando se destruye una sesión de inicio. Puede estar correlacionado de manera positiva con un evento de inicio de sesión mediante el valor id. de inicio de sesión. Los id. de inicio de sesión solo son únicos entre reinicios en el mismo equipo.). The right pane shows the 'Acciones' menu for the selected event, with options like 'Abrir registro guardado...', 'Crear vista personalizada...', 'Importar vista personalizada...', 'Vaciar registro...', 'Filtrar registro actual...', 'Propiedades', 'Buscar...', 'Guardar todos los eventos como...', 'Adjuntar tarea a este registro...', 'Ver', 'Actualizar', and 'Ayuda'. A context menu for the event is also open, listing 'Evento 4634, Microsoft Windows security auditing', 'Propiedades de evento', 'Adjuntar tarea a este evento...', 'Guarder eventos seleccionados...', 'Copiar', 'Actualizar', and 'Ayuda'. The status bar at the bottom shows system information like CPU usage, memory, and date.

Se muestran eventos que coinciden con los inicios de sesión tanto fallido como correcto, no obstante la información es demasiado técnica y no soy capaz de interpretarla.

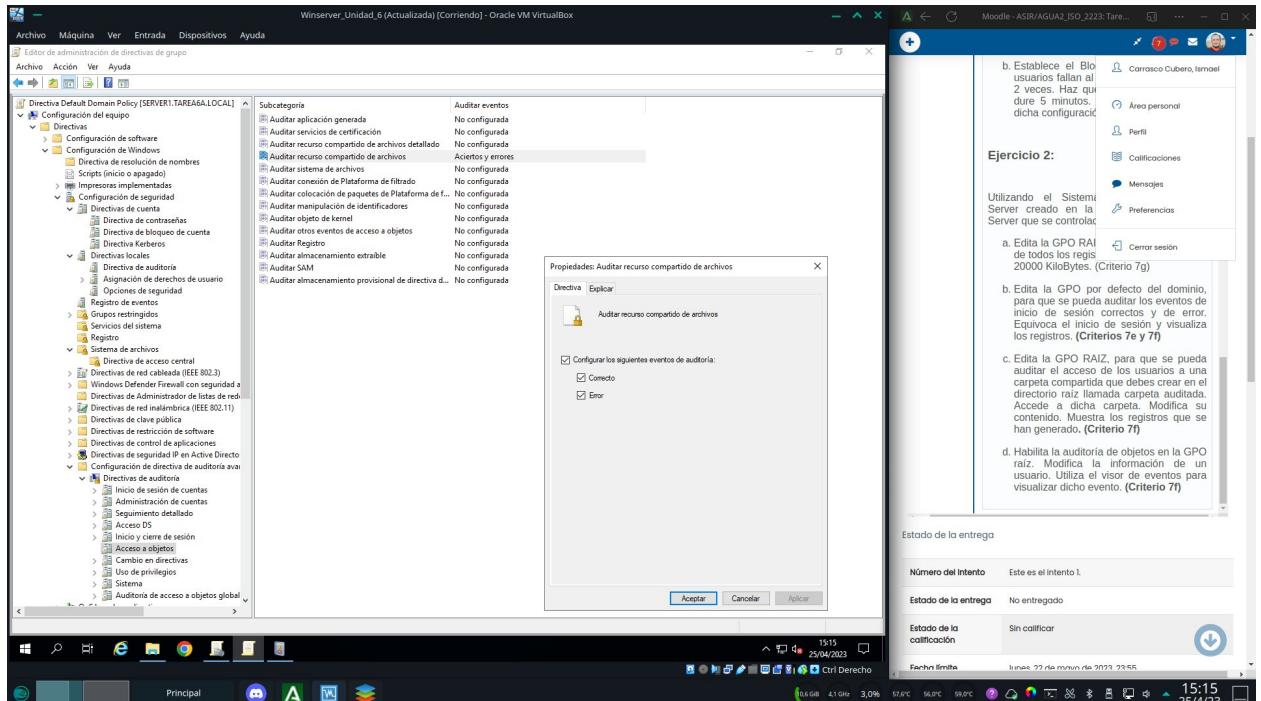
The screenshot shows a Windows File Explorer window. The left sidebar shows 'Este equipo' (Local Computer) with 'Este equipo', 'Red', and 'CLIENTE1', 'SERVER1', 'VBOXSVR'. The main pane shows a folder structure for 'Disco local (C:)': 'Archivos', 'Inicio', 'Compartir', 'Vista'. The 'Vista' tab is selected, showing columns for 'Nombre', 'Fecha de modificación', 'Tipo', and 'Tamaño'. A folder named 'carpeta\_audited' is visible. The status bar at the bottom shows system information like CPU usage, memory, and date.

The right side of the screen shows a Moodle task page titled 'Tarea 9 ISO Directivas de seguridad y auditorías'. It includes sections for 'Descripción de la tarea', 'Información de interés', 'Evaluación de la tarea', 'Anexo', 'Licencia de recursos', and 'Estado de la entrega'. The 'Estado de la entrega' section shows 'Número del intento: Este es el intento 1.', 'Estado de la entrega: No entregado', 'Estado de la calificación: Sin calificar', and a download icon. The status bar at the bottom shows system information like CPU usage, memory, and date.

Para el siguiente punto comenzamos creando la carpeta

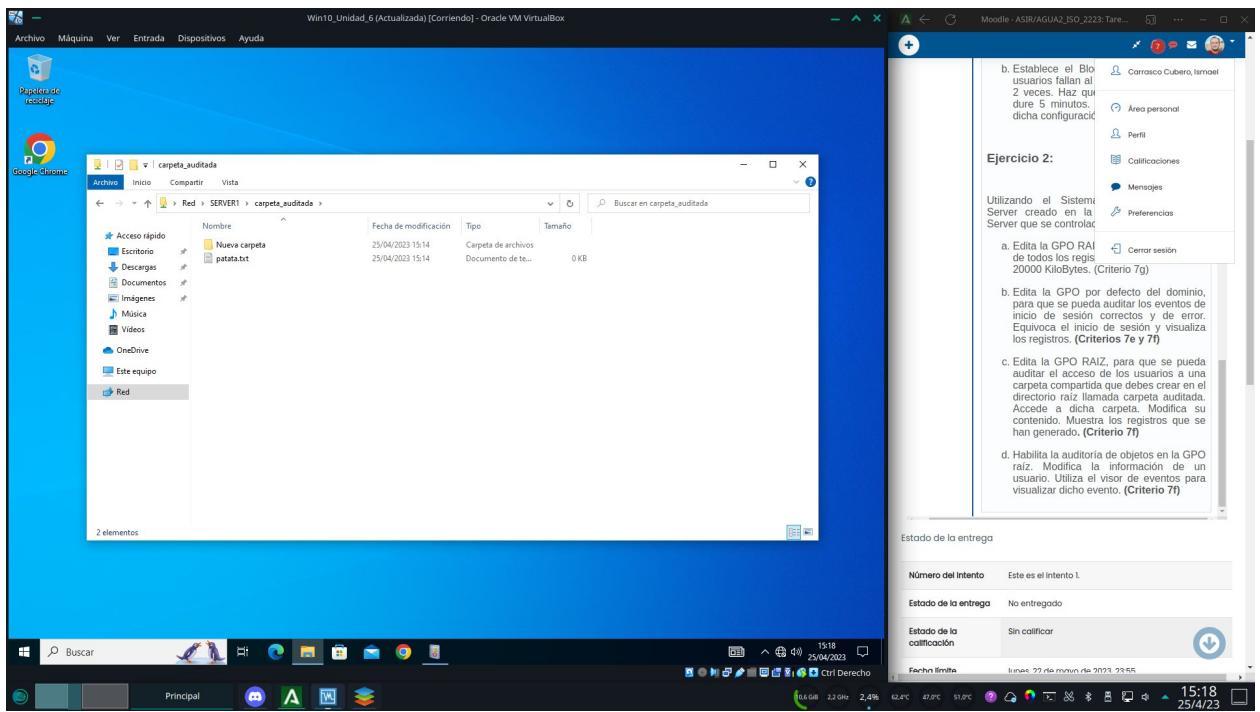


La compartimos con los grupos que contienen los usuarios y asignamos permisos (recordemos que estamos usando un dominio con usuarios y grupos ya creados)

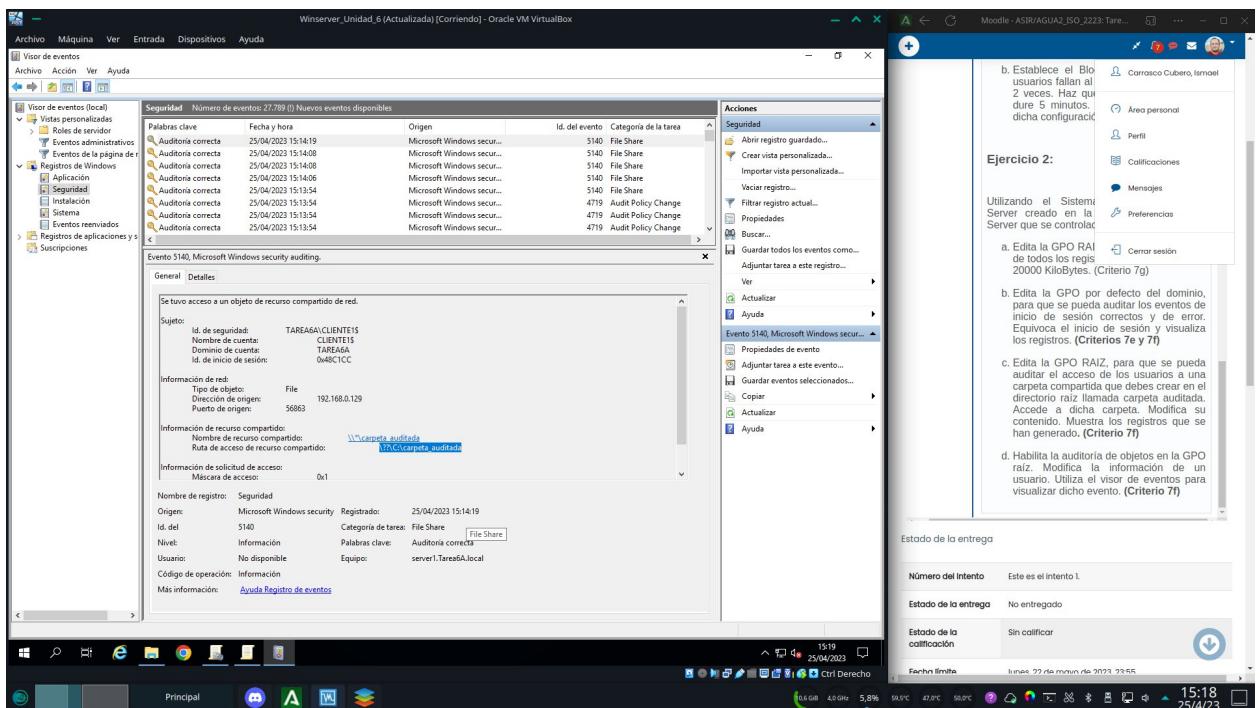


Volvemos al editor de la directiva raíz y navegamos hasta configuración del equipo > directivas > configuración de windows > configuración de seguridad > configuración de directiva de auditoria avanzada > directivas de auditoria > acceso a objetos, y en dicha sección escogemos la opción auditar acceso compartido a archivos y lo habilitamos.

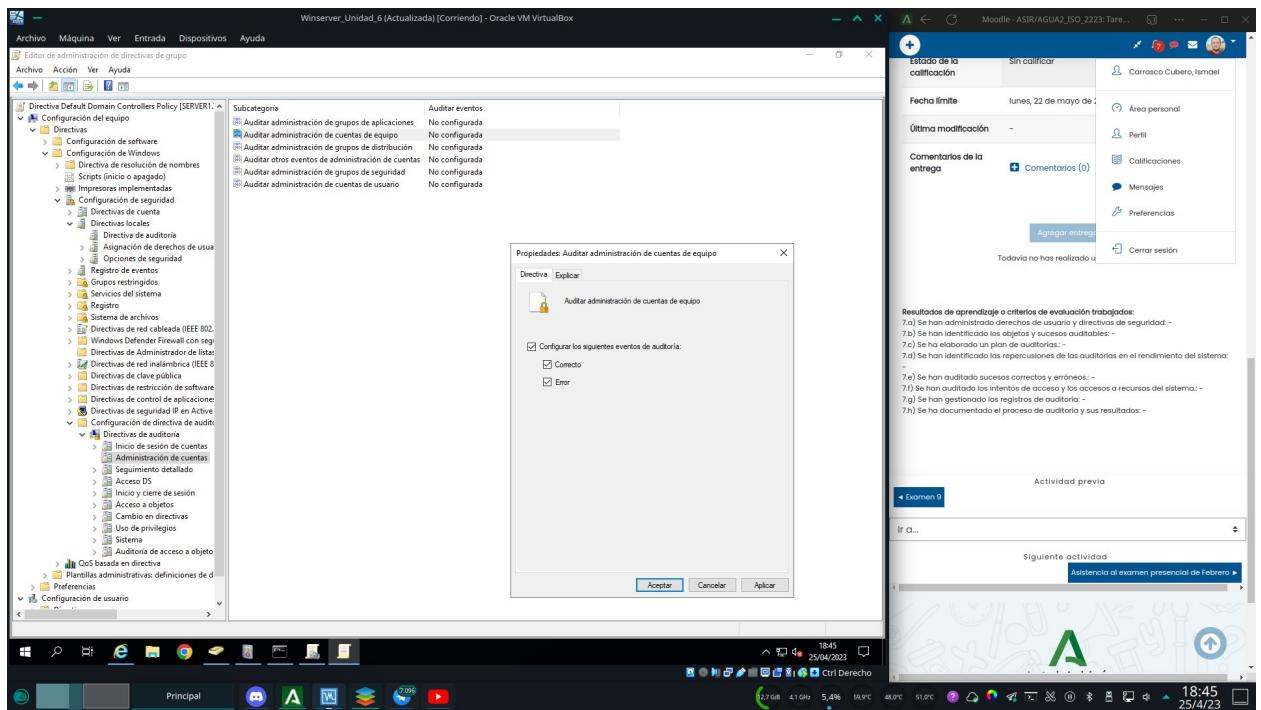
# Ismael Carrasco Cubero



Si ahora en el cliente añadimos cosas en la carpeta compartida...

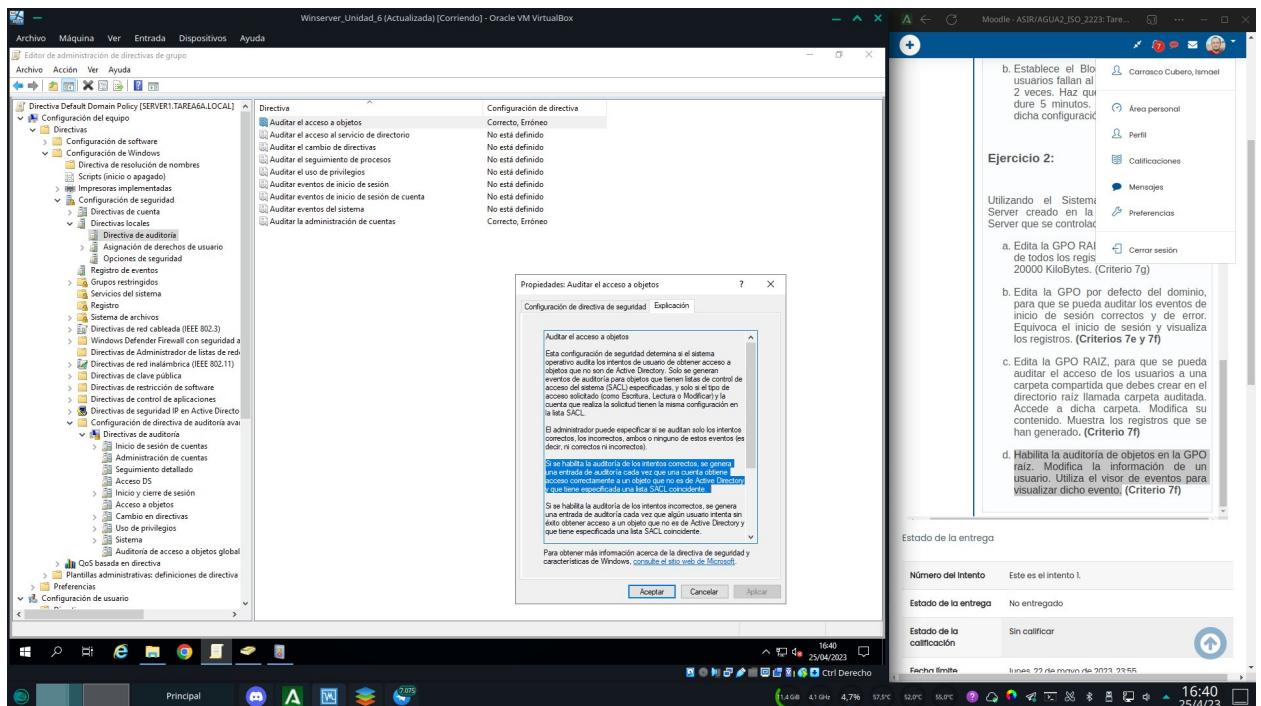


Vemos que se generan los correspondientes eventos.

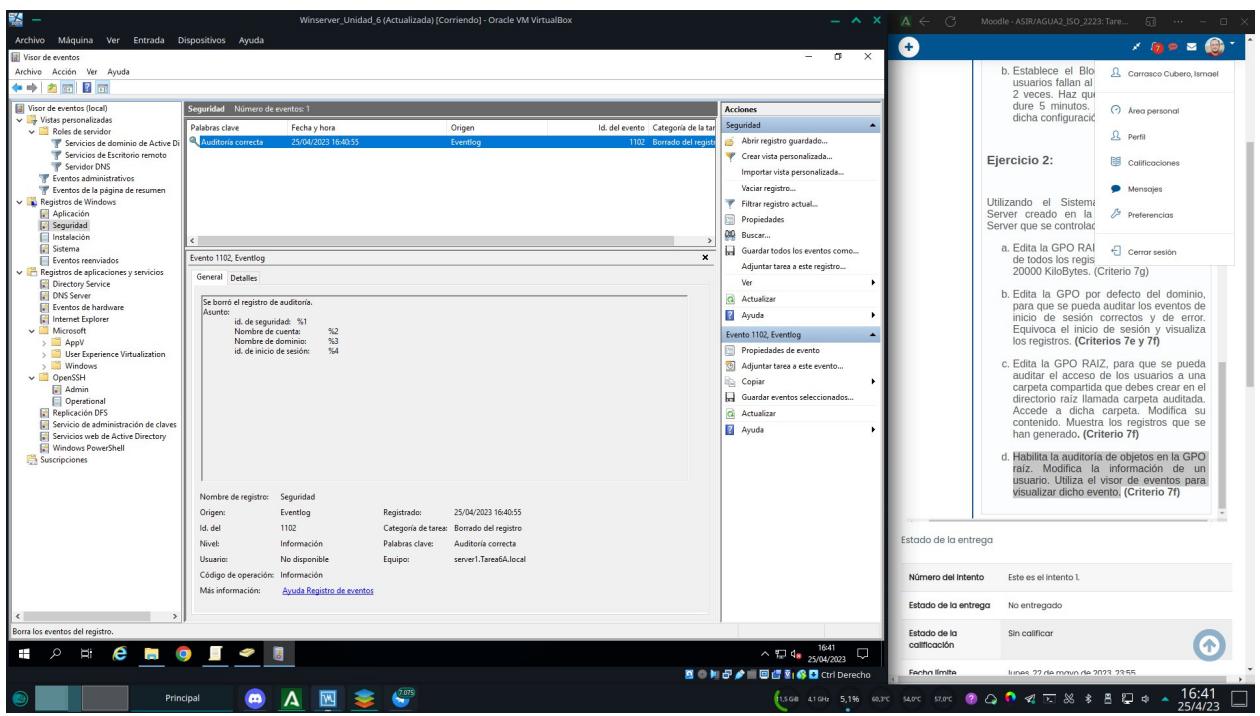


Navegamos hasta directivas de auditoria en configuración de seguridad > configuración de directiva de auditoria avanzada > directiva de auditorias > administración de cuentas, y seleccionamos auditoria de administración de cuentas de usuario y la activamos

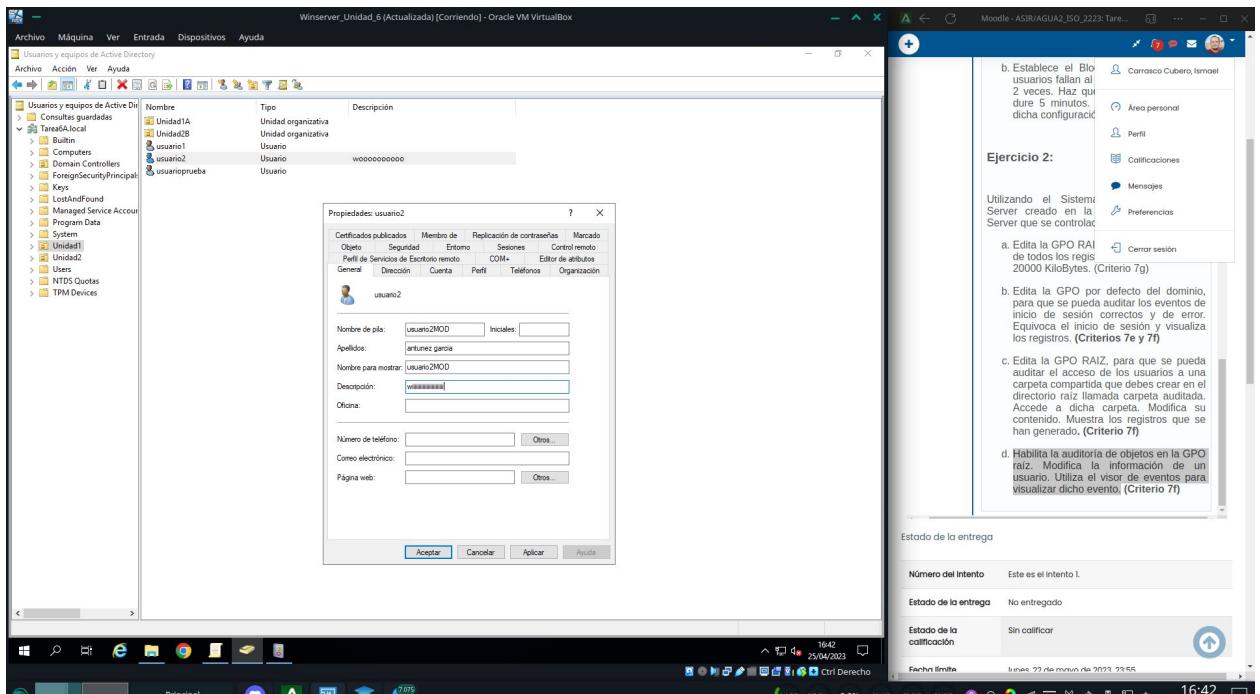
**NOTA:** En teoría el enunciado así como los apuntes, dicen que se modifique la opción de acceso a objetos, pero según su propia descripción en windows dicha opción no audita nada referente a la modificación de dichos objetos, solo cuando algo accede a ellos. De hecho, tras múltiples intentos con dicha opción de la GPO activada, el visor de eventos no muestra ningún evento tras modificar a uno de los usuarios. Sin embargo la de administración de cuentas si que genera los eventos que se piden. Adjunto a continuación una captura de la explicación de la auditoria de acceso a objetos



# Ismael Carrasco Cubero

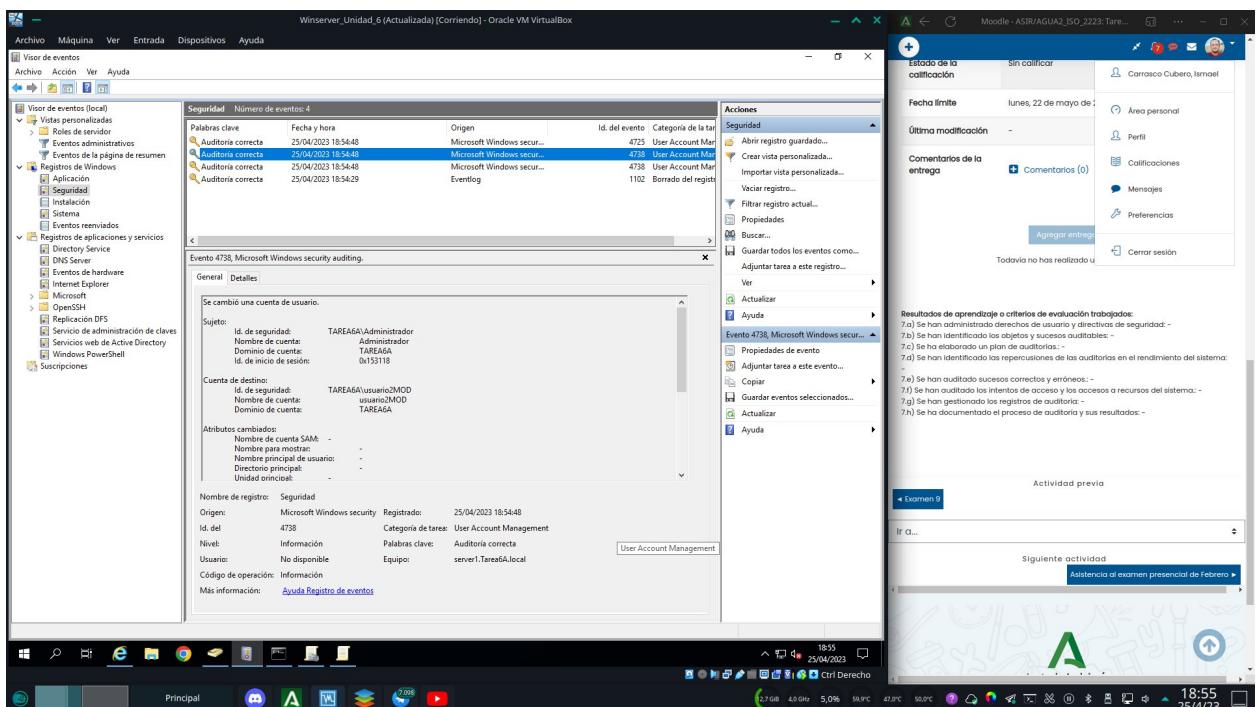


Una vez configurada la GPO vació el visor de eventos, ya que estaba demasiado lleno y era un caos seguir la temporalidad de los mismos.



Editamos un usuario del dominio, le añadiremos una descripción y deshabilitaremos la cuenta

# Ismael Carrasco Cubero



Podemos comprobar en el visor de eventos que se crean los log correspondientes.

