**3.21**

**A)**

Deshabilitar la cuenta de invitado en un sistema operativo Windows puede ser una medida de seguridad importante por varias razones:

### **1. Acceso anónimo**

* La cuenta de invitado permite que los usuarios accedan al sistema sin necesidad de autenticación. Esto significa que cualquier persona podría usar la computadora sin proporcionar credenciales, aumentando el riesgo de usos no autorizados.

### **2. Privilegios Limitados, pero no Inofensivos**

* Aunque tiene privilegios limitados, la cuenta de invitado todavía puede acceder a ciertas áreas del sistema y ejecutar algunas acciones que podrían usarse para comprometer la seguridad. Por ejemplo, podría instalar programas maliciosos o explotar vulnerabilidades.

### **3. Dificultad para Rastrear Usuarios**

* Si varias personas usan la cuenta de invitado, no es posible identificar quién realizó qué actividad, lo que complica la auditoría y el seguimiento en caso de problemas.

### **4. Puerta de Entrada para Ataques**

* Los atacantes podrían usar la cuenta de invitado como punto de entrada para ejecutar scripts maliciosos o ataques locales, debido a la ausencia de barreras de autenticación.

### **5. Mejores alternativas**

* Si necesita una cuenta con acceso limitado para ciertos usuarios, es mejor crear cuentas específicas con permisos ajustados a sus necesidades. Esto brinda mayor control y seguridad.

### **B)**

### **1. Reducir ataques de fuerza bruta**

* Los atacantes suelen intentar iniciar sesión en las cuentas predeterminadas como "Administrador", ya que es un nombre conocido y universal en los sistemas Windows.
* Cambiar el nombre obliga al atacante a adivinar tanto el nombre de usuario como la contraseña, aumentando la dificultad

### **2. Mitigar ataques automatizados**

* Muchos programas maliciosos y bots están diseñados para atacar cuentas predeterminadas
* Al cambiar el nombre, se elimina uno de los puntos de entrada predecibles, disminuyendo la efectividad de estos ataques automatizados.

### **3. Confusión para los atacantes internos**

* En entornos corporativos o de red, un atacante interno que busca acceso no autorizado tendrá dificultades si el nombre de la cuenta "Administrador" no es el estándar.
* Esto puede dar tiempo adicional al equipo de seguridad para detectar y prevenir en

### **4. Cumplimiento de políticas de seguridad**

* Muchas normativas y estándares de seguridad (como ISO 27001 o NIST) recomiendan minimizar la exposición de cuentas privilegiadas, lo cual incluye cambiar nombres predeterminados.
* Implementar esta práctica puede contribuir al cumplimiento de dichas normativas.

### **5. Mejor gestión de privilegios**

* Un nombre personalizado para la cuenta de administrador facilita la identificación y diferenciación frente a otras cuentas con permisos elevados.
* Esto puede ser útil en auditorías o análisis de seguridad.

### **6. Mayor control y percepción de seguridad**

* Cambiar el nombre del administrador refleja una política de seguridad proactiva y un enfoque consciente hacia la protección del sistema.

**C)**

### **1. Reducción del riesgo de malware y ataques**

Las cuentas estándar tienen permisos limitados, lo que significa que no pueden realizar cambios críticos en el sistema (como instalar software o modificar configuraciones importantes) sin autorización de una cuenta de administrador. Esto ayuda a:

* Prevenir que programas maliciosos (malware) obtengan control
* Limitar el impacto de un ataque cibernético al restringir las acciones que puede realizar un atacante.

### **2. Prevención de errores críticos del usuario**

* Los usuarios con permisos de administrador pueden realizar cambios que afectan la estabilidad o seguridad del sistema, como borrar archivos esenciales o cambiar configuraciones incorrectamente.
* Una cuenta estándar minimiza el riesgo de errores humanos que puedan dañar el sistema.

### **3. Control y supervisión**

* Es más fácil gestionar el sistema cuando las cuentas estándar necesitan permiso explícito para realizar tareas administrativas. Esto asegura que los cambios importantes sean intencionados y estén supervisados.

3.22

a) **Crear una cuenta estándar de nombre "usuarioDAM" con contraseña:**

1. Abre el **Panel de control**.
2. Ve a **Cuentas de usuario** y selecciona **Administrar otra cuenta**.
3. Haz clic en **Agregar un nuevo usuario en configuración del equipo**.
4. Selecciona **Familia y otras personas** en la ventana **Configuración de cuentas**.
5. Haz clic en **Agregar otra persona a este equipo**.
6. Selecciona **No tengo la información de inicio de sesión de esta persona**.
7. Luego selecciona **Agregar un usuario sin cuenta de Microsoft**.
8. Rellena el nombre de usuario como usuarioDAM y añade una contraseña.

b) **Cambiar el nombre a "manolo":**

1. Vuelve al **Panel de control** y ve a **Cuentas de usuario**.
2. Selecciona **Cambiar el nombre de cuenta**.
3. Selecciona la cuenta usuarioDAM y cambia el nombre a manolo.
4. Inicia sesión con el nombre de cuenta .\manolo y cierra la sesión después.

c) **Cambiar la contraseña para el usuario "manolo":**

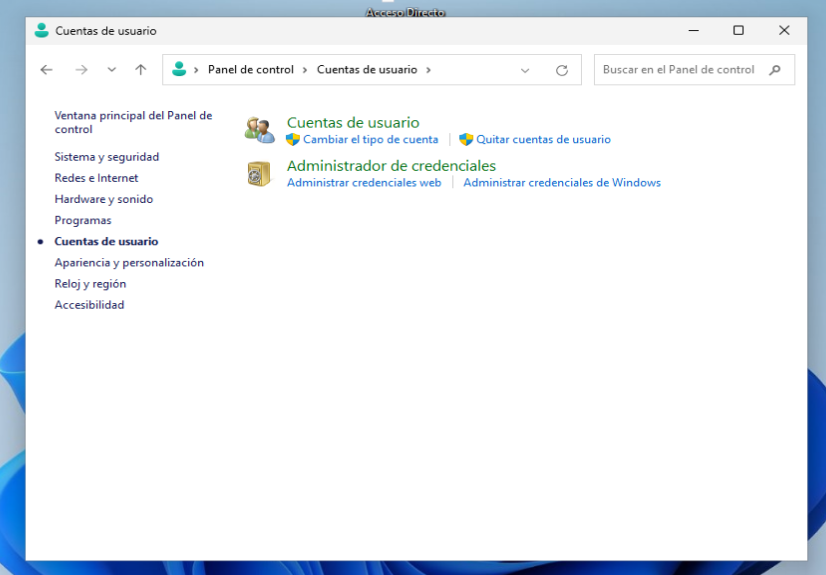
1. Vuelve a **Cuentas de usuario** en el **Panel de control**.
2. Selecciona **Cambiar la contraseña**.
3. Selecciona la cuenta manolo y cambia la contraseña.

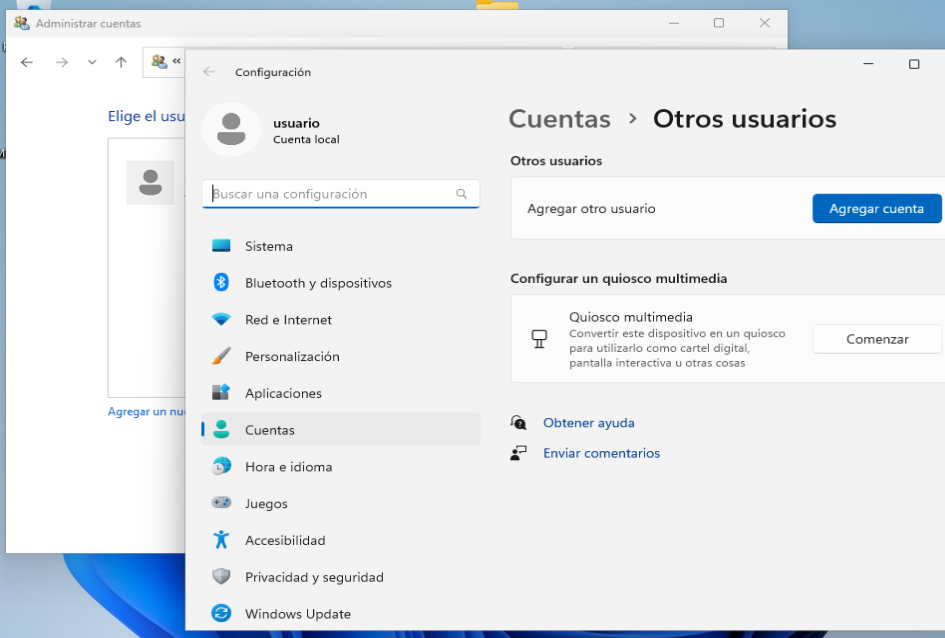
d) **Cambiar la cuenta como administrador**

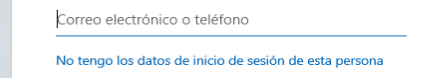
Claro, aquí tienes los pasos para cambiar el tipo de cuenta de "manolo" a administrador:

1. Abre el **Panel de control**.
2. Ve a **Cuentas de usuario** y selecciona **Administrar otra cuenta**.
3. Selecciona la cuenta manolo.
4. Haz clic en **Cambiar el tipo de cuenta**.
5. Selecciona **Administrador** y luego haz clic en **Cambiar el tipo de cuenta**.

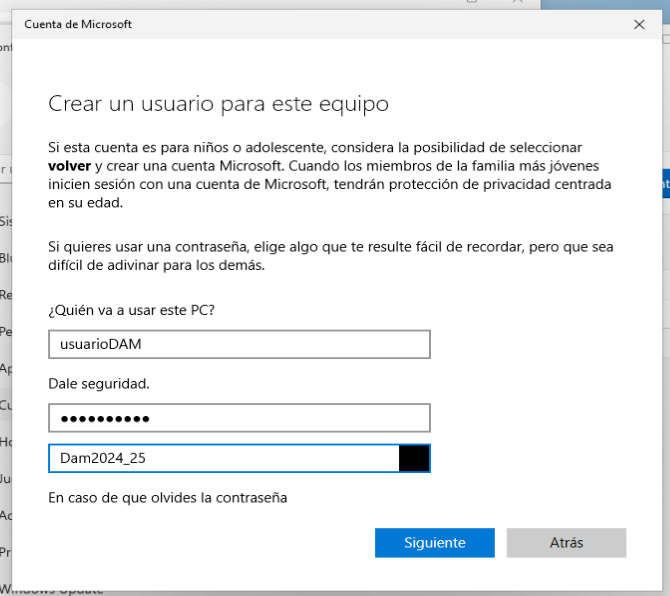
a)







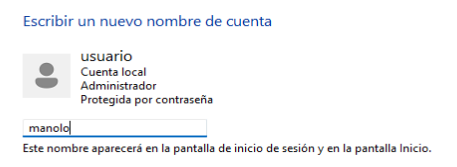




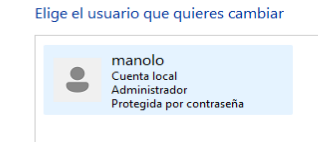
b)

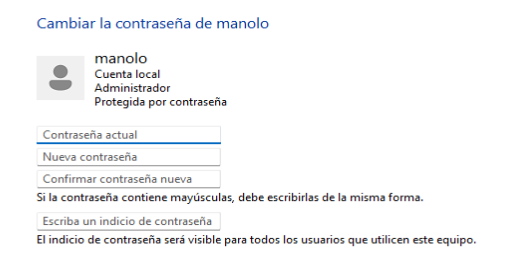
Repetimos los pasos para llegar a la cuenta del usuario en el panel del control





c)

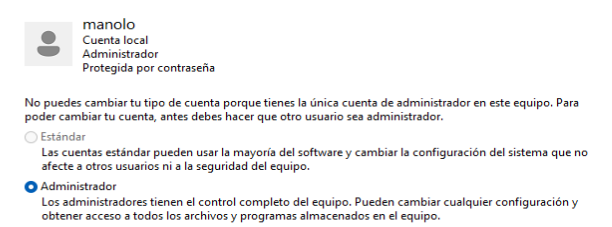




Al cambiar la contraseña para el usuario "manolo", podrías perder acceso a archivos cifrados, contraseñas guardadas en el navegador y otras credenciales almacenadas en el sistema operativo bajo la contraseña anterior. Estas credenciales generalmente no son recuperables a menos que tengas una copia de seguridad anterior.

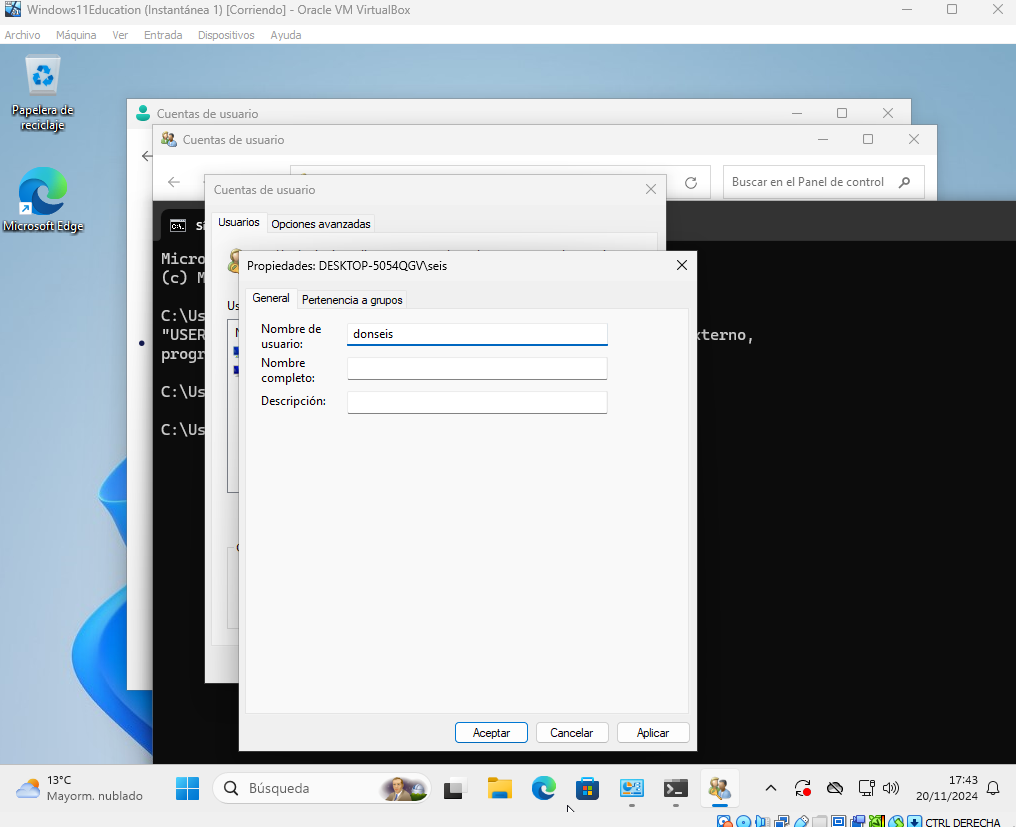
d)

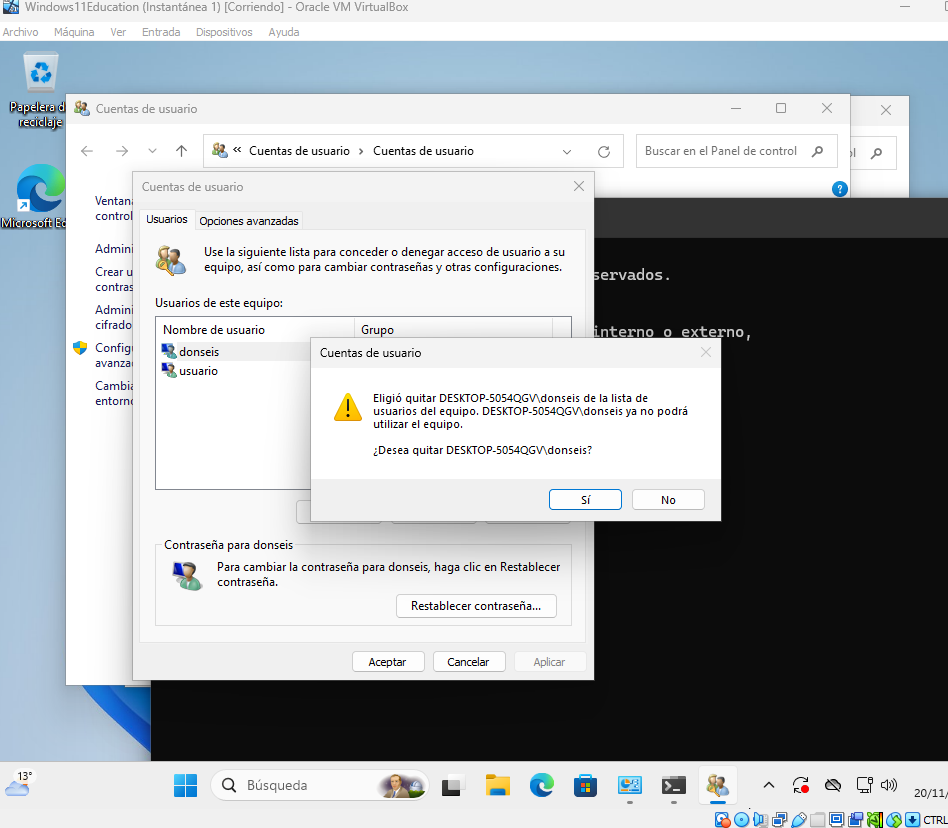
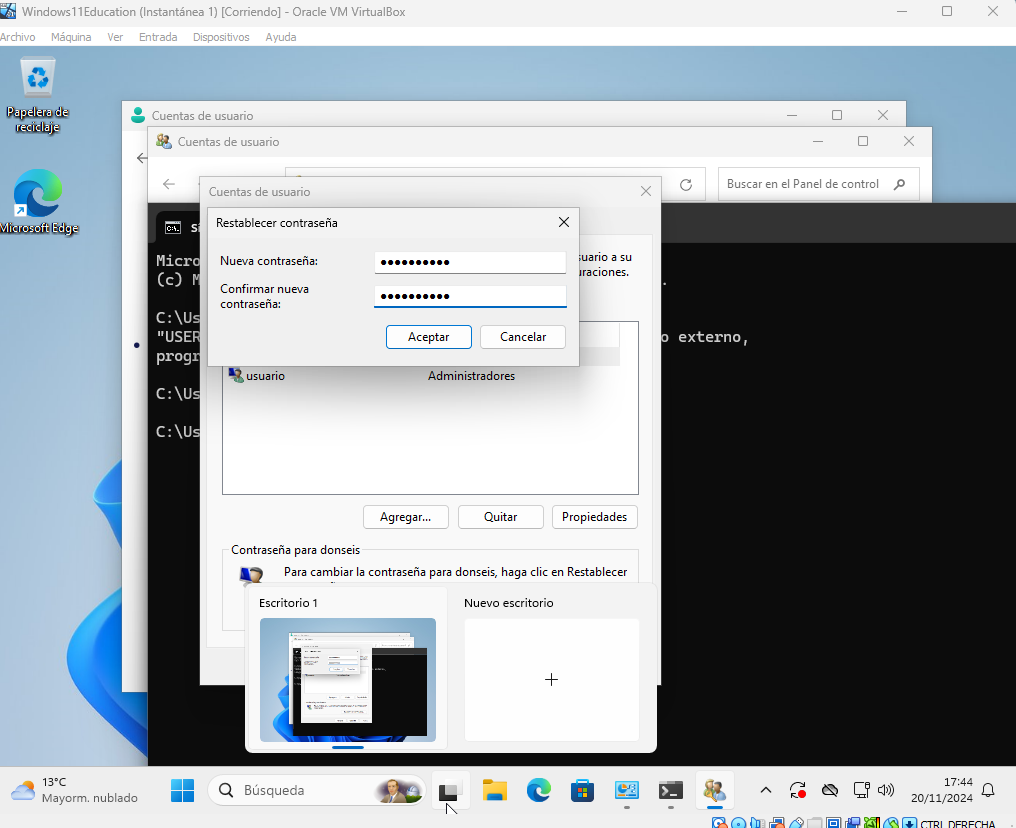
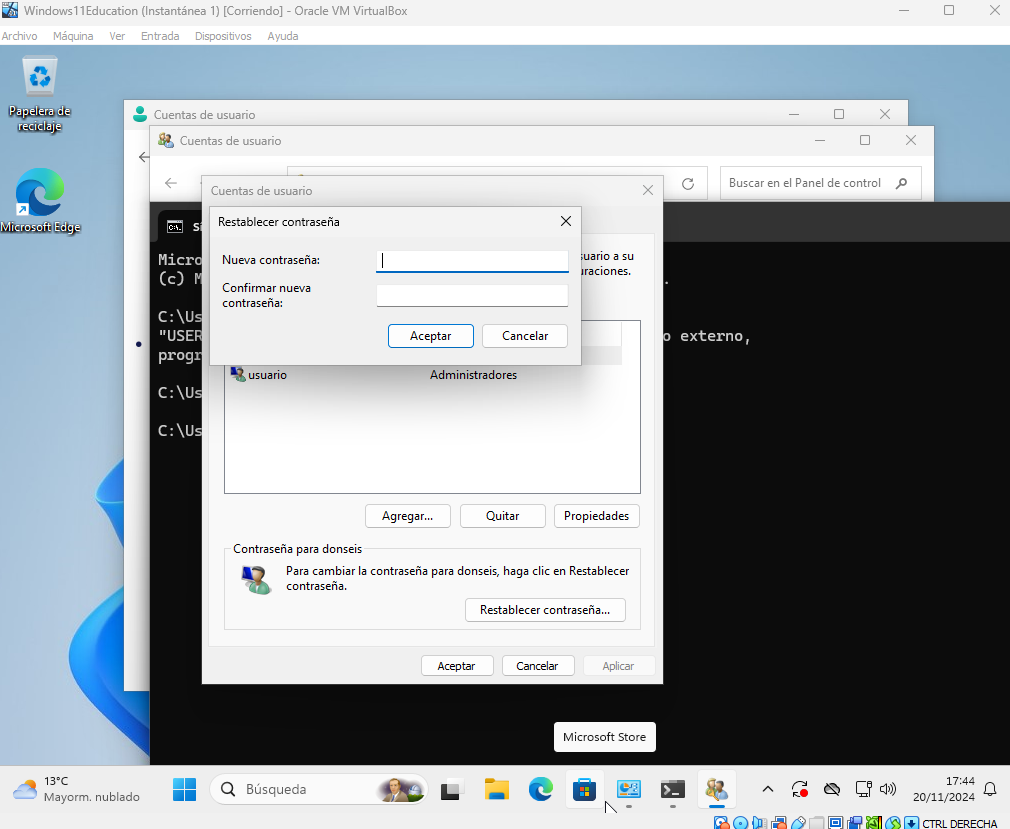




3.24





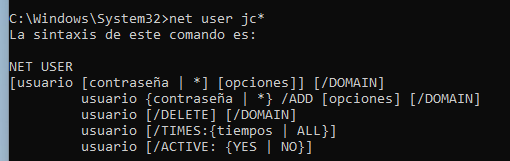
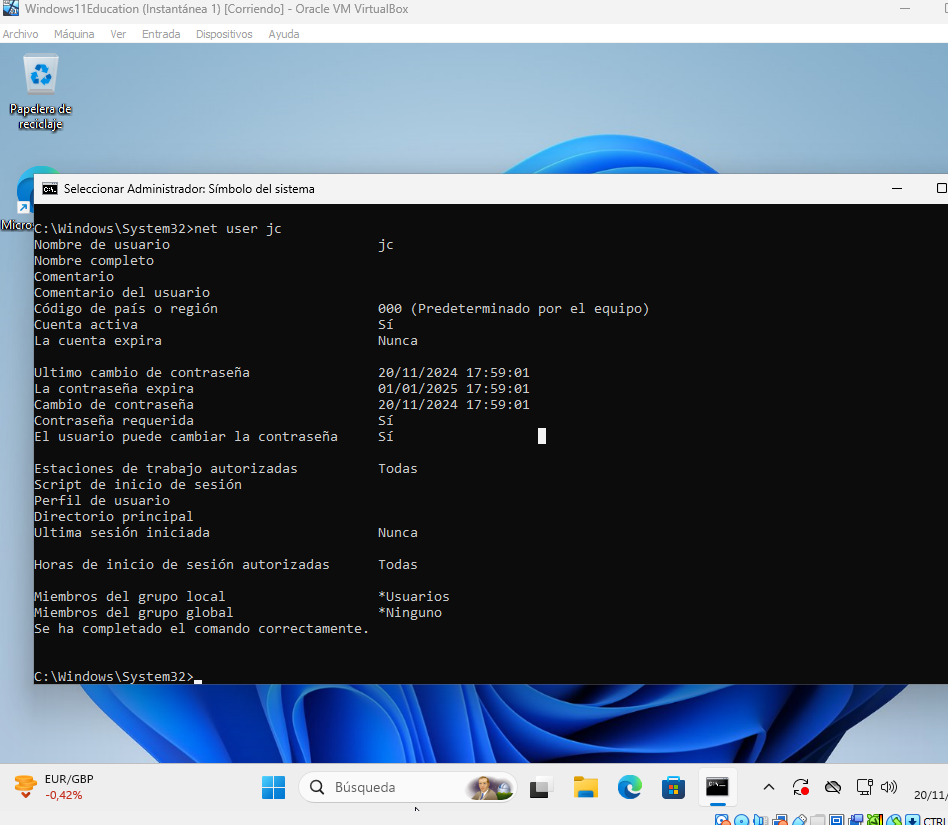


f) no

**3.25**

**a) si**



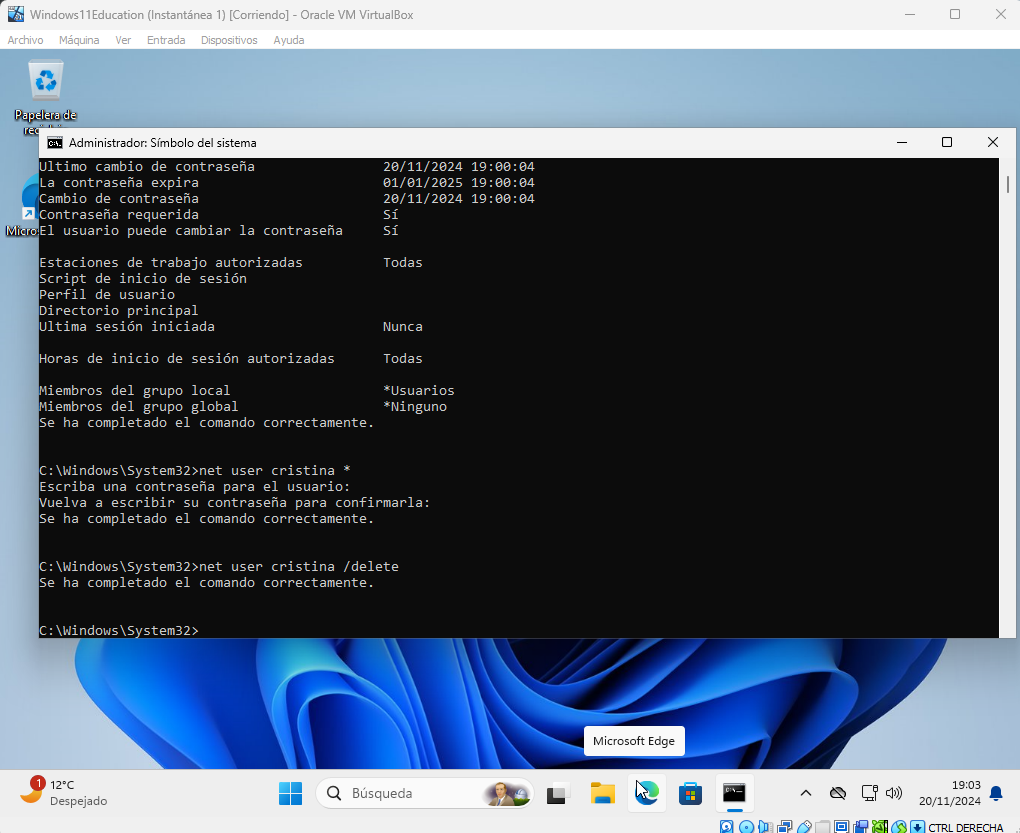
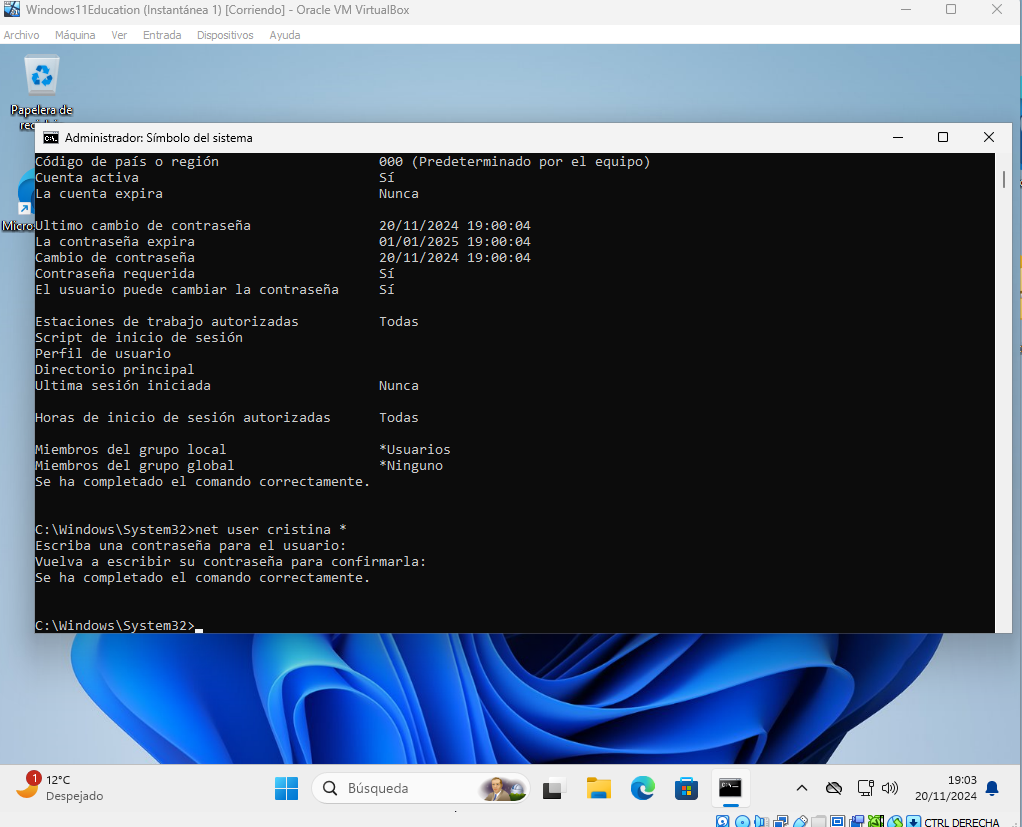
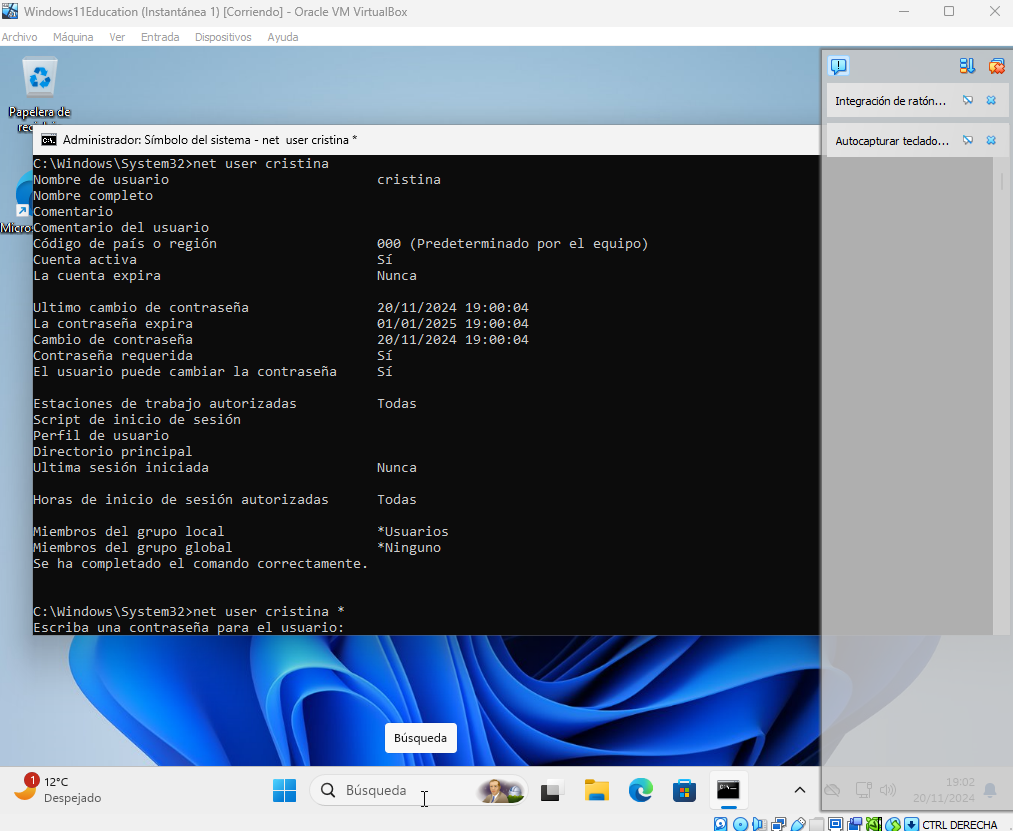
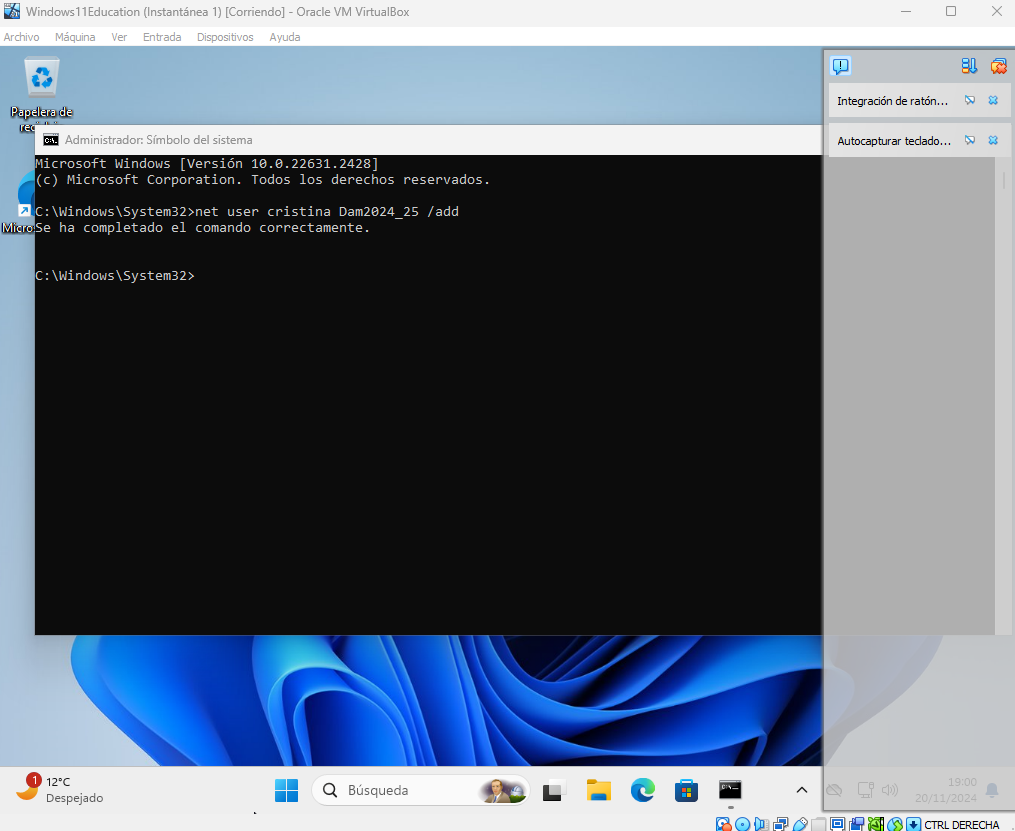


**3.26**

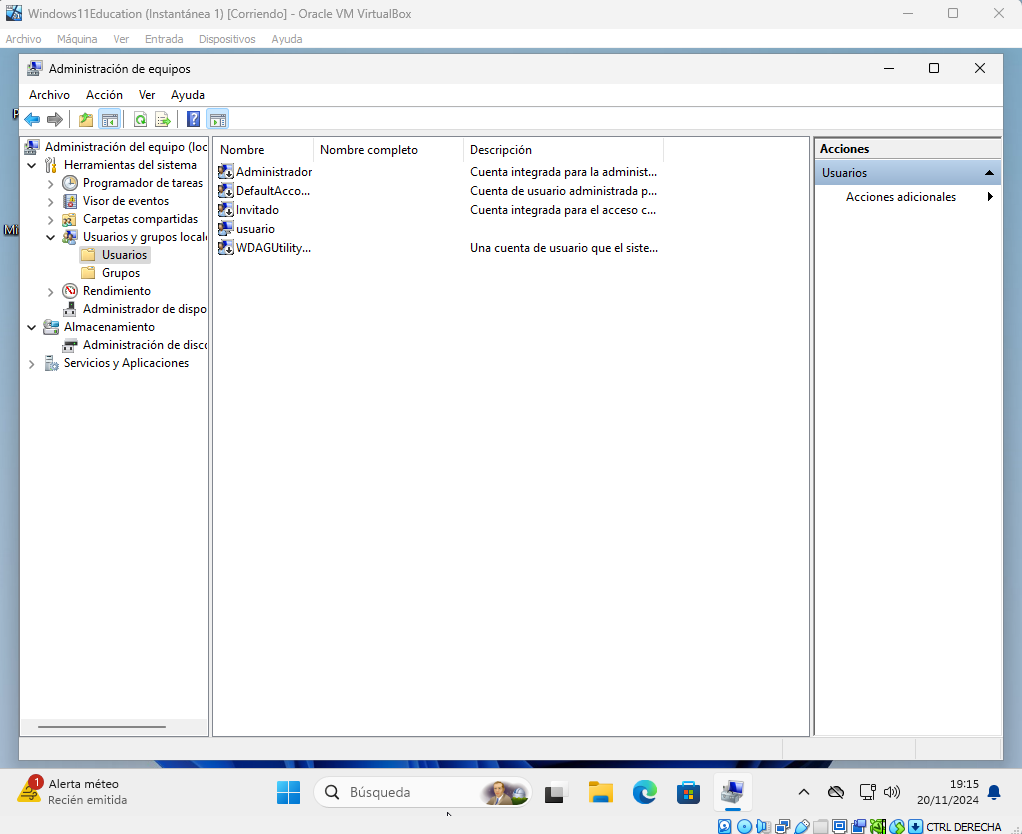
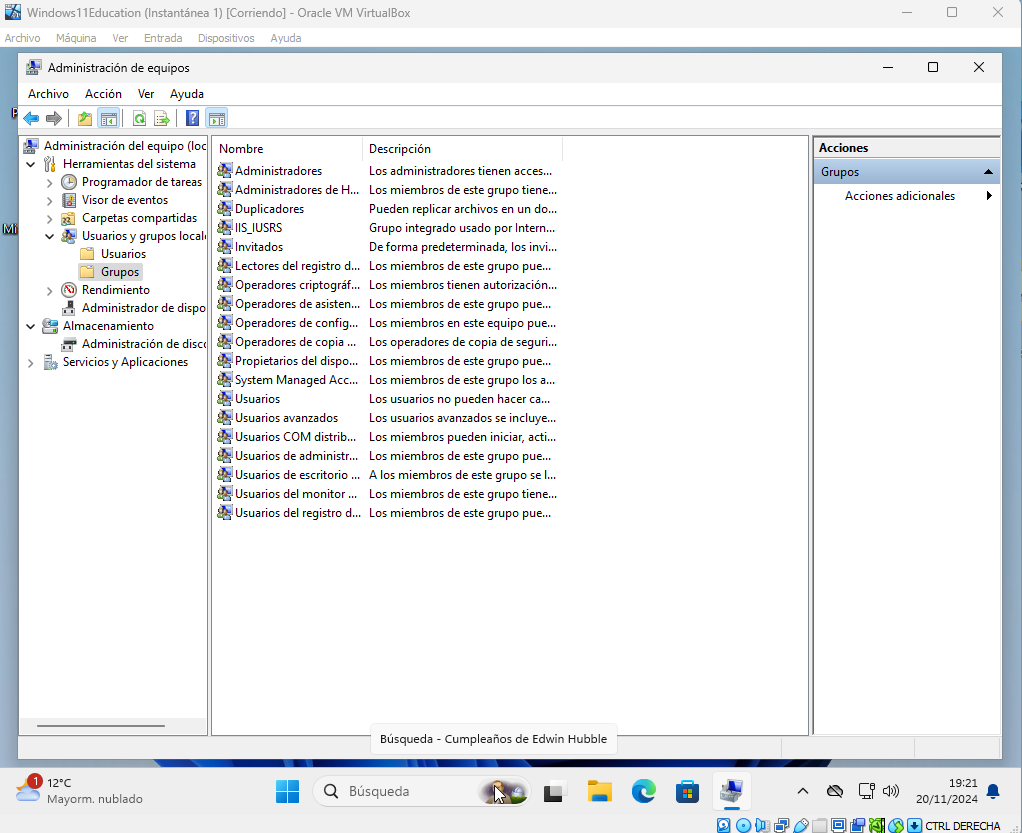
a) **1. Mejora la seguridad en el inicio de sesión**

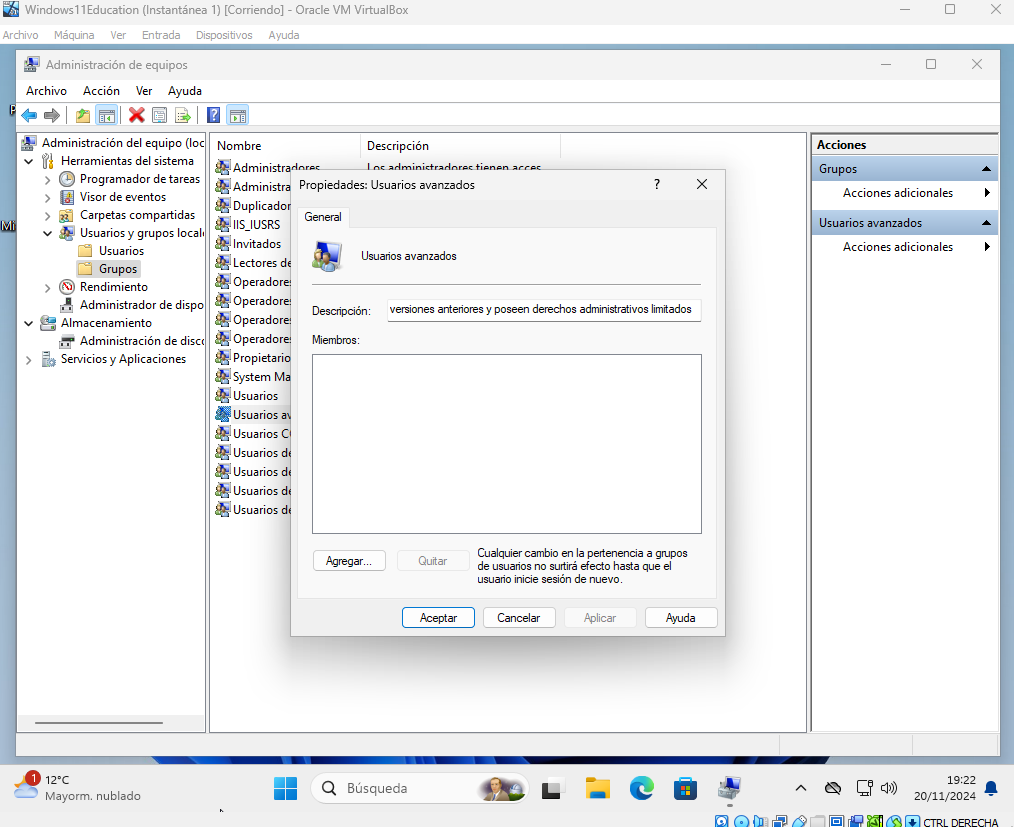
### **2. Proporciona una capa adicional de autenticación**

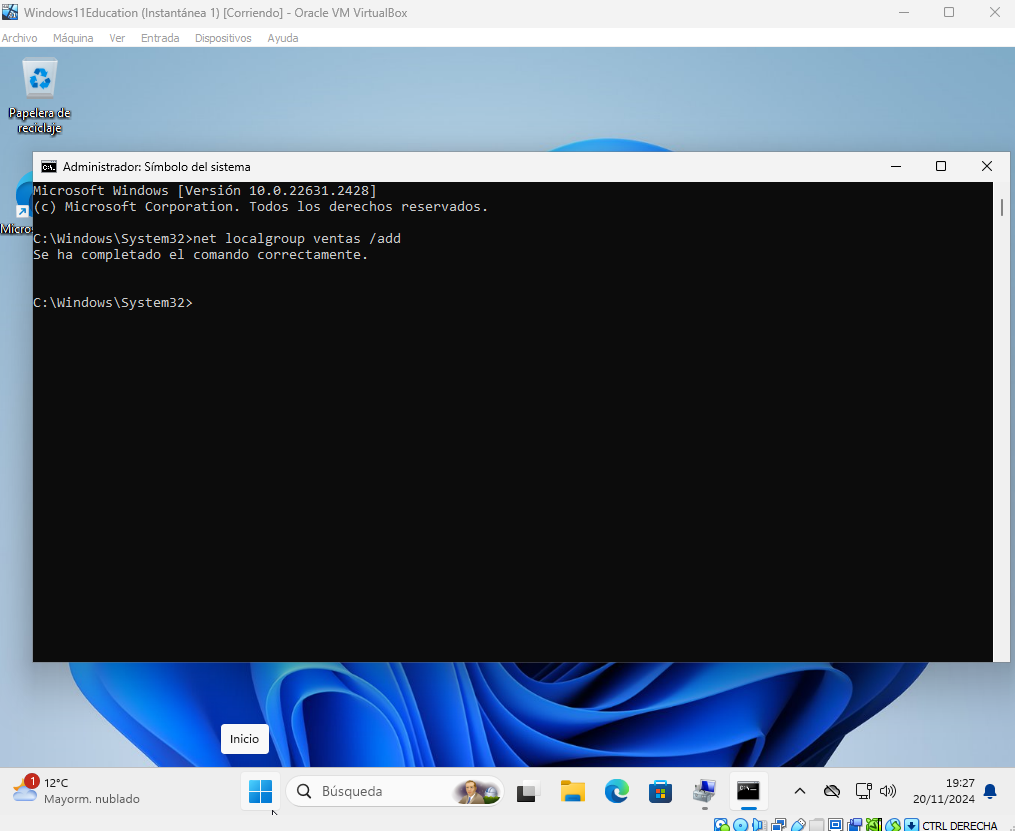
### **3. Añade un paso más al inicio de sesión**

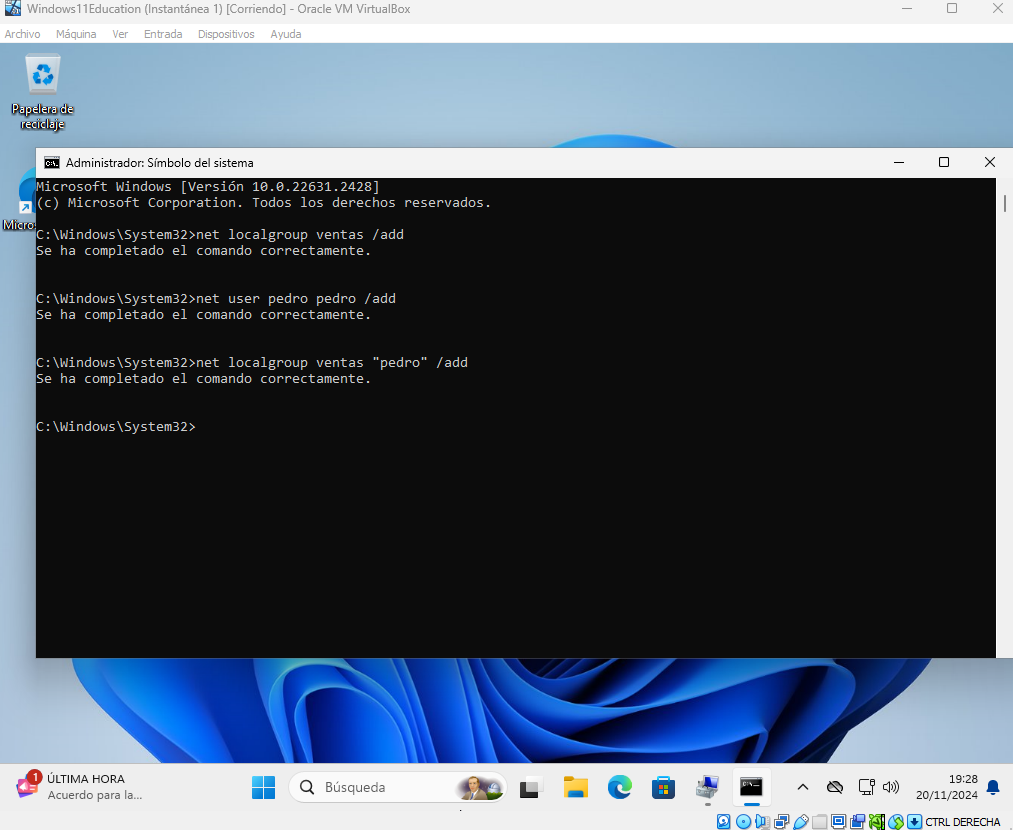
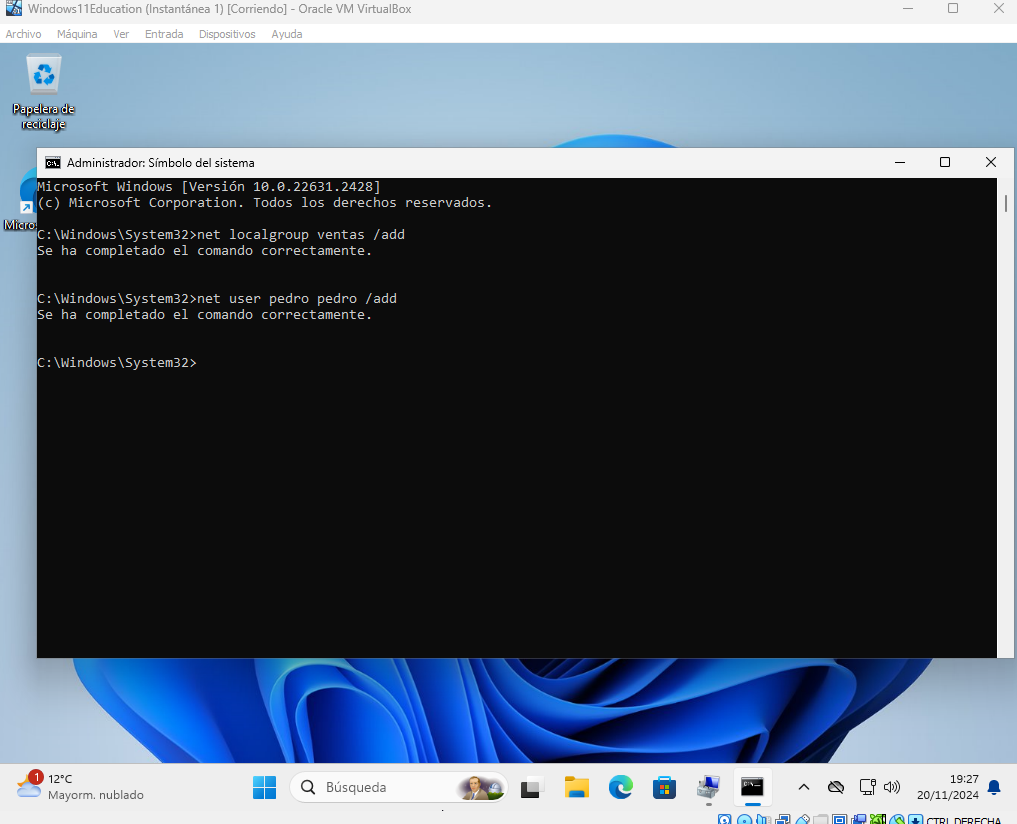
b) 

**3.27**





“Los usuarios avanzados se incluyen para la compatibilidad con versiones anteriores y poseen derechos administrativos limitados”



**3.29**

a) si, si

b) no, no, si, si

**3.30**

### **a) Abrir Directiva de seguridad local**

1. **Presiona** Win + R para abrir la ventana "Ejecutar".
2. **Escribe** secpol.msc y presiona **Enter**.

### **b) Habilitar una directiva que impida contraseñas fáciles de adivinar**

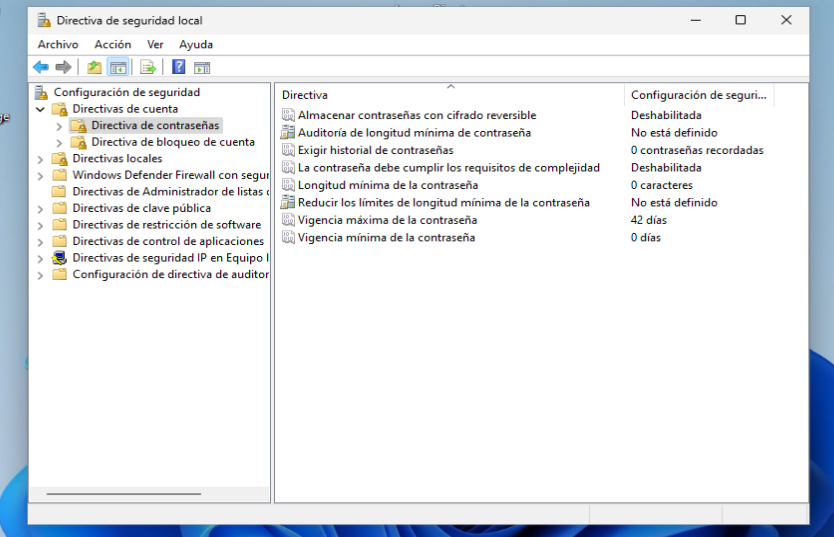
1. En la ventana de Directiva de seguridad local, **ve a** Configuración de seguridad > Directivas de cuenta > Directivas de contraseñas.
2. **Haz doble clic** en Requerir que las contraseñas cumplan con los requisitos de complejidad.
3. **Activa** esta opción y **configura** los requisitos de complejidad, como incluir mayúsculas, minúsculas, números y caracteres especiales.

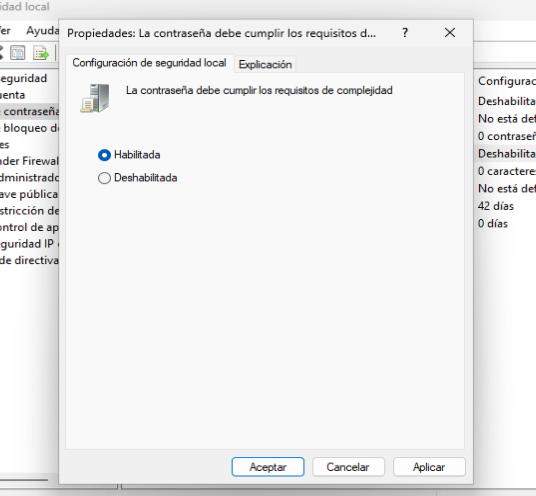
### **c) Obligar a que la contraseña tenga una longitud mínima de 10 caracteres**

1. En la misma ventana de Directivas de contraseñas, **haz doble clic** en Longitud mínima de la contraseña.
2. **Establece** la longitud mínima en **10 caracteres** y **guarda los cambios**.

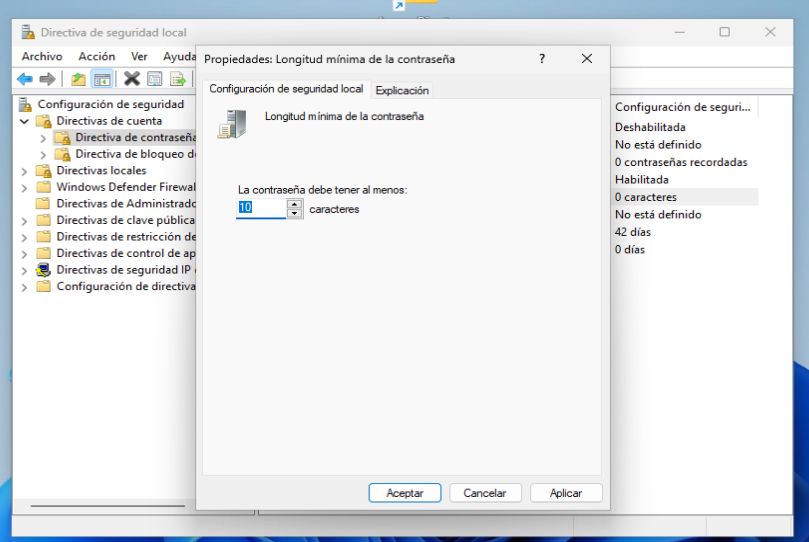
**b)**







c)



3.31

### **a) Configuración de la directiva de bloqueo de cuenta**

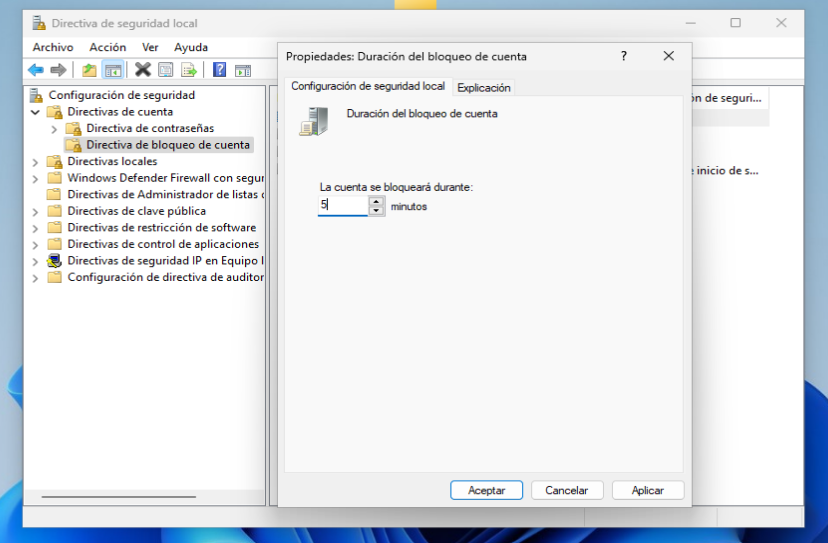
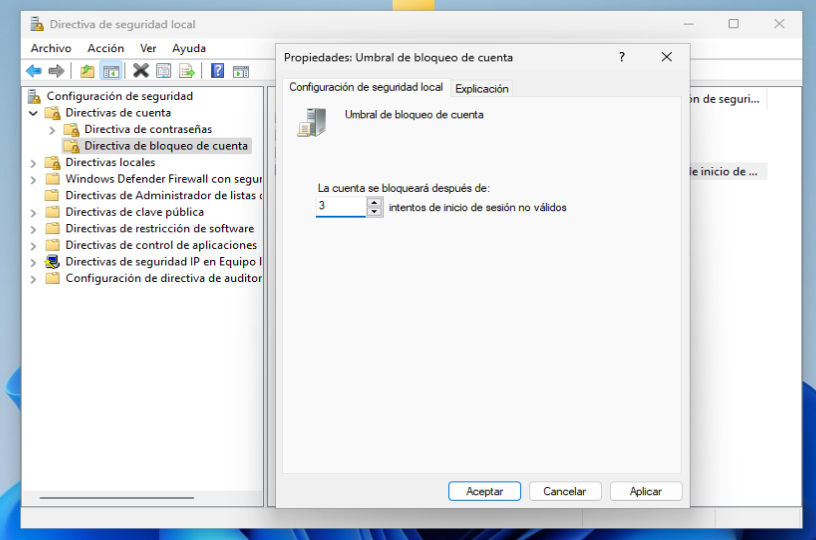
1. **Abre** la **Directiva de seguridad local** presionando Win + R, escribiendo secpol.msc y pulsando **Enter**.
2. **Navega** a Configuración de seguridad > Directivas de cuenta > Directiva de bloqueo de cuenta.
3. **Haz doble clic** en Umbral de bloqueo de cuenta.
4. **Establece** el número de intentos fallidos en 3. Haz clic en **Aplicar** y luego en **Aceptar**.
5. **Haz doble clic** en Duración del bloqueo de cuenta y **establece** el valor a 5 minutos. Haz clic en **Aplicar** y luego en **Aceptar**.
6. **Haz doble clic** en Restablecer contador de bloqueo de cuenta después de y **establece** el valor a 5 minutos. Haz clic en **Aplicar** y luego en **Aceptar**.

### **b) Prueba de la directiva de bloqueo**

1. Cierra la sesión actual.
2. Con la cuenta del usuario creada durante la instalación de Windows 11, **introduce la contraseña incorrecta 3 veces**.

Después de los 3 intentos fallidos, la cuenta se bloqueará automáticamente. Tendrás que esperar 5 minutos antes de poder intentarlo de nuevo

a)

b)

