

EDGAR ALVARADO  
DEVOPS BOOTCAMP  
DESAFIO 16

## OBJETIVO

Conocer las herramientas y buenas prácticas en seguridad informática.

Aplicar estrategias para proteger información personal y profesional.

Configurar contraseñas seguras y utilizar directivas de grupo o local, para un control más exhaustivo.

Familiarizarse con antivirus, y sistemas de detección de intrusos.

## WINDOWS

### USER ACCOUNT CONTROL

1. Configurar User Account Control para que solicite confirmación siempre.

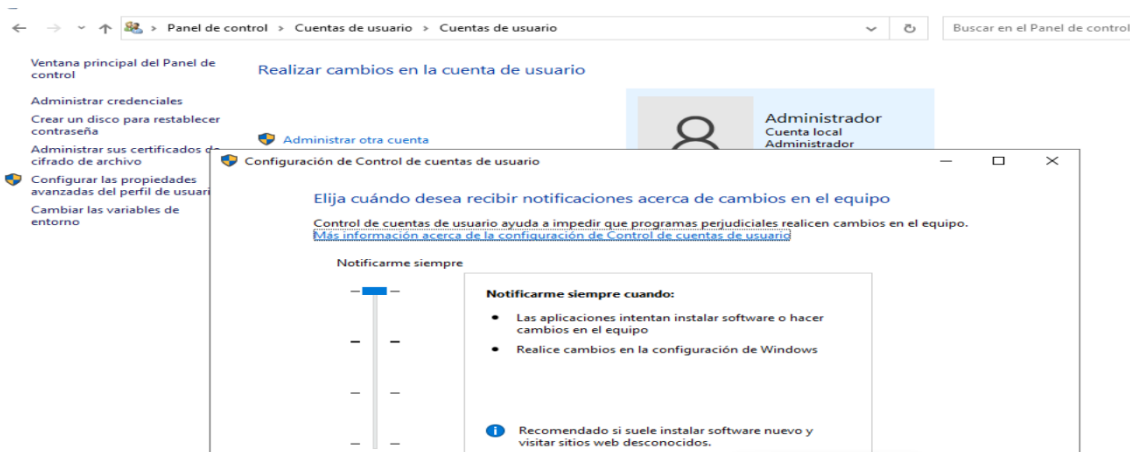
Abrir el Panel de Control.

Ir a Cuentas de usuario.

Hacer clic en Cambiar configuración de Control de Cuentas de Usuario.

Mover el control deslizante hasta Siempre notificar.

Hacer clic en Aceptar.

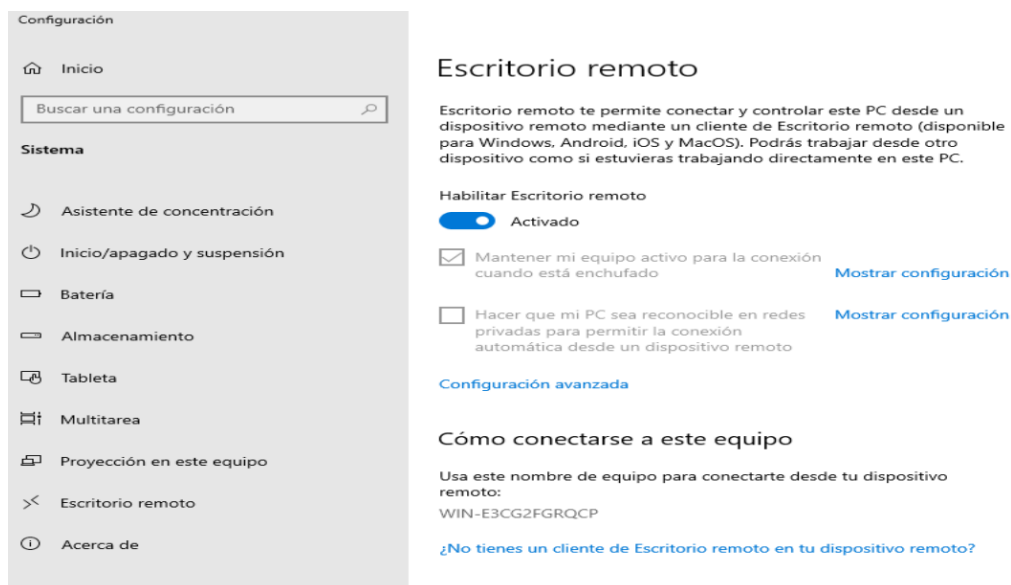


## REMOTE DESKTOP

2. Habilitar el acceso por Remote Desktop.

Ir a Sistema > Configuración remota

Marca la opción "Permitir conexiones remotas a este equipo"



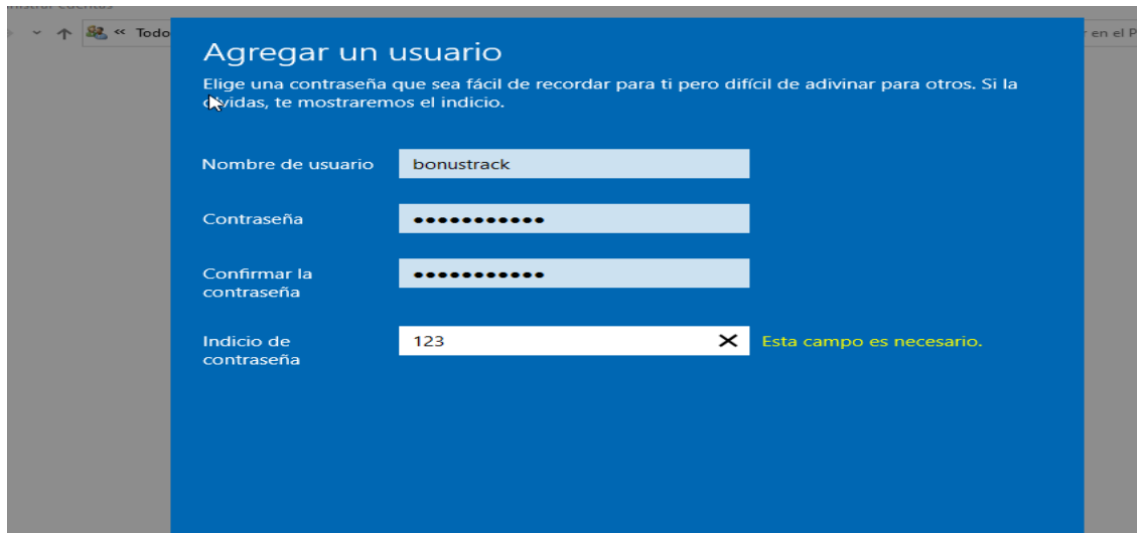
3. Crear una cuenta de usuario llamada bonustrack.

Abrir el Panel de Control.

Ir a Cuentas de usuario > Administrar otra cuenta > Agregar una nueva cuenta en Configuración del PC.

Selecciona Agregar un usuario sin cuenta de Microsoft.

Introducir bonustrack como nombre de usuario.



4. Asignar permisos básicos (users) al usuario creado anteriormente.

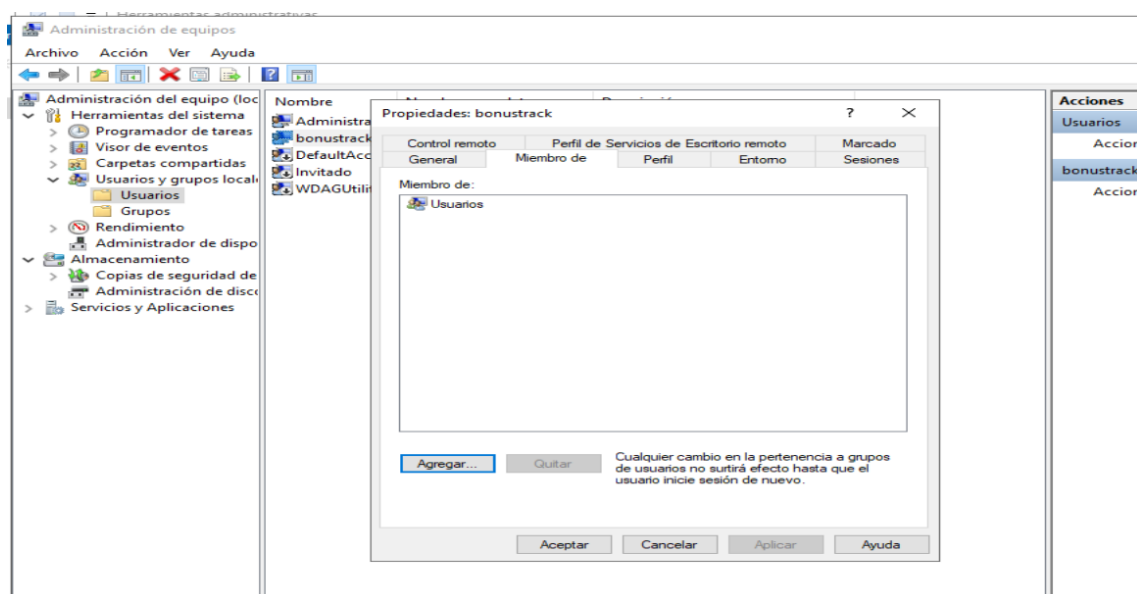
Ir a Panel de Control > Sistema y seguridad > Herramientas administrativas > Administración de equipos.

En el panel izquierdo, expandir Usuarios y grupos locales.

Hacer clic en Usuarios y localizar bonustrack.

Hacer clic derecho en bonustrack y seleccionar Propiedades.

Ir a la pestaña Miembro de y ver de que Usuarios esté listado.



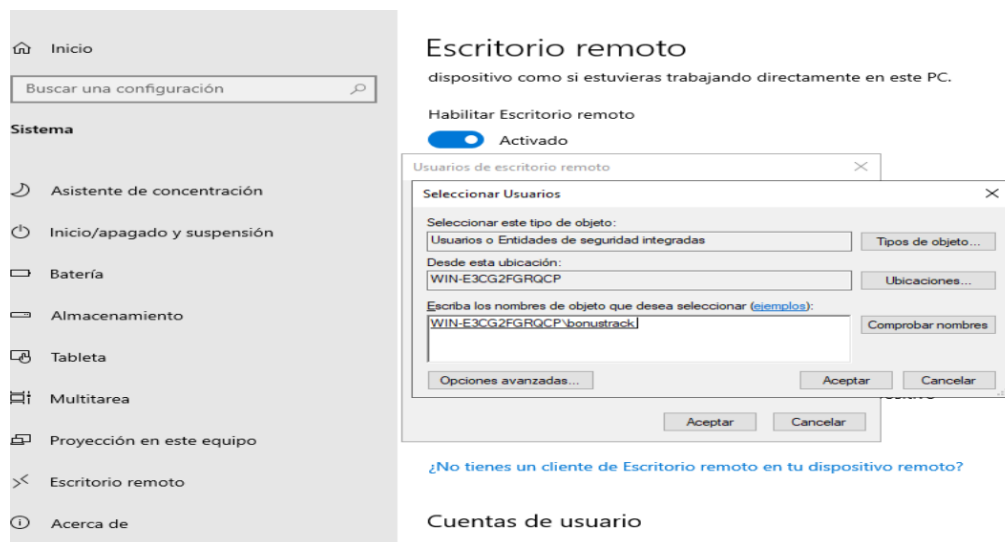
5. Conceder privilegios al usuario bonustrack para tener la posibilidad de iniciar sesión a través de Remote Desktop.

Abrir Propiedades del sistema desde Panel de Control > Sistema y seguridad > Sistema.

Hacer clic en Configuración de acceso remoto.

En la pestaña Remoto, hacer clic en Seleccionar usuarios.

Agregar bonustrack y haz clic en Aceptar.



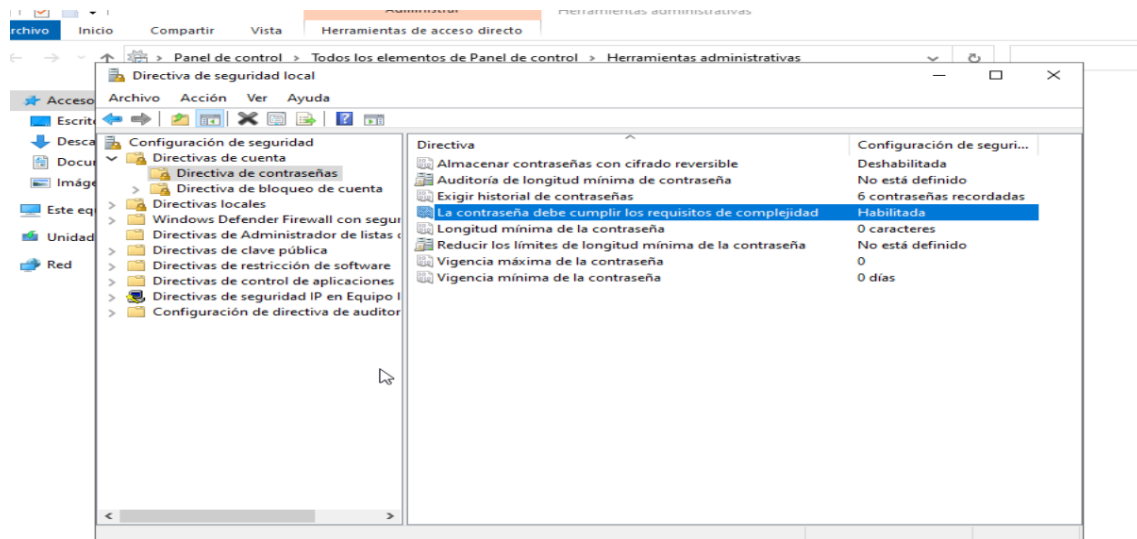
## DIRECTIVAS DE SEGURIDAD

6. Habilitar la complejidad de contraseñas.

Abrir Herramientas administrativas > Directiva de seguridad local.

Ve a Directiva de cuenta > Directiva de contraseñas.

Activa La contraseña debe cumplir los requisitos de complejidad.

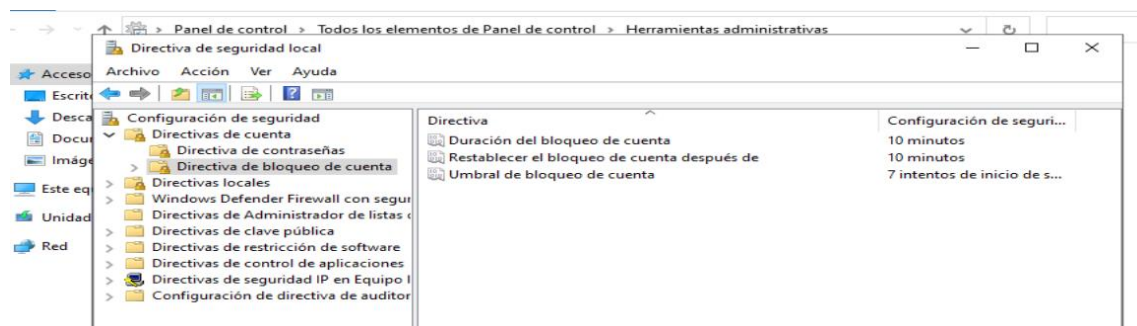


## 7. Configurar:

- No expiren las contraseñas.
- Contraseñas con 10 caracteres de longitud.
- Evitar la reutilización de las últimas 10 contraseñas.



- Bloqueo de cuentas luego de 7 intentos fallidos.
- Desbloqueo automático después de 10 minutos.



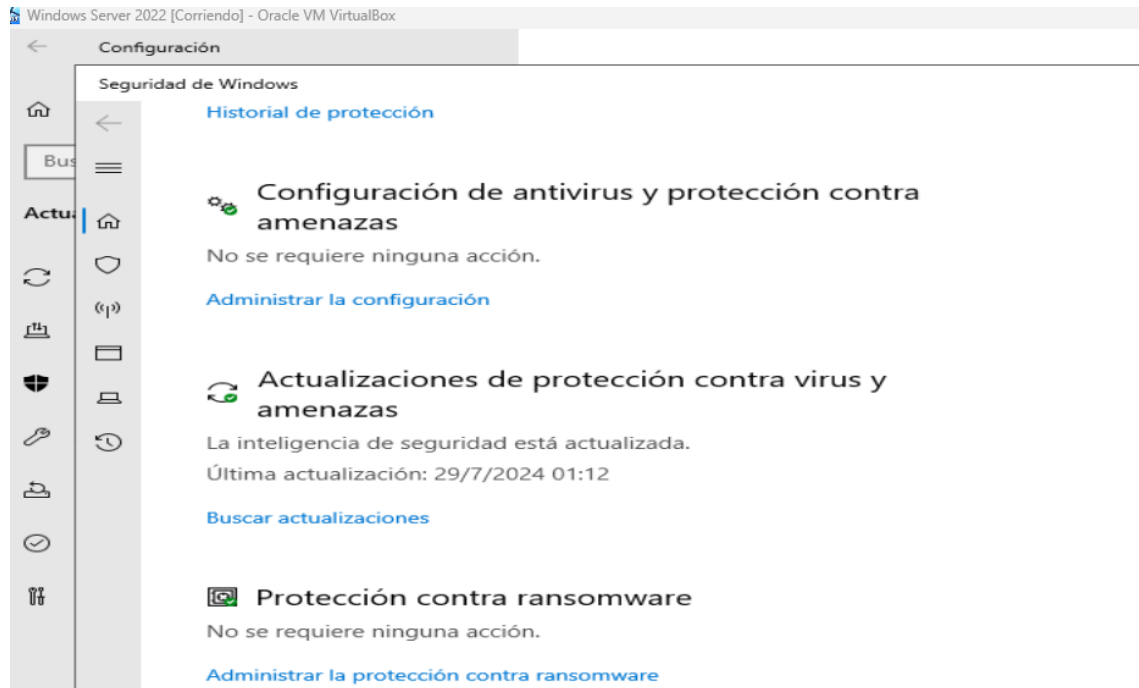
## WINDOWS DEFENDER

8. Habilitar Windows Defender (en el caso de que no se encuentre presente).

Abrir Configuración > Actualización y seguridad > Seguridad de Windows.

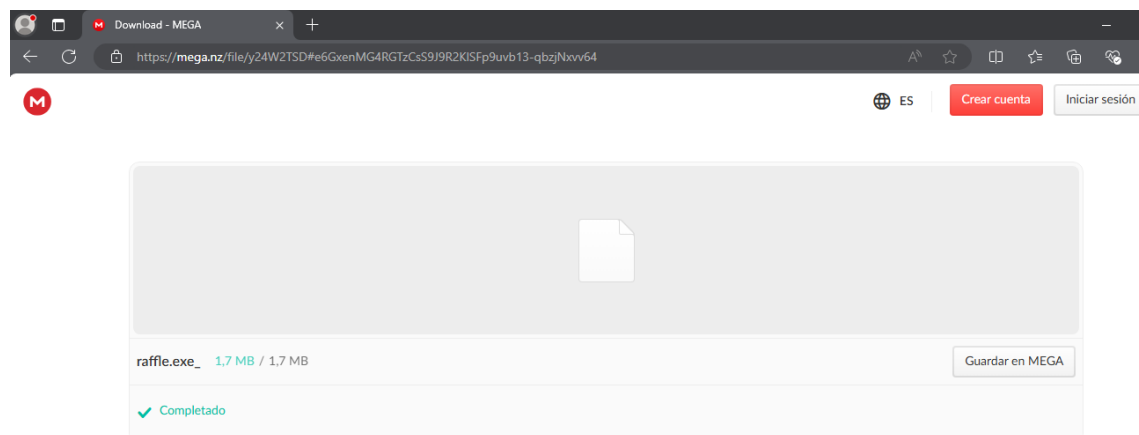
Ir a Protección contra virus y amenazas.

Si no está habilitado, activar Protección en tiempo real.



9. Descargar raffle.exe desde:

<https://mega.nz/file/y24W2TSD#e6GxenMG4RGtZCsS9J9R2KISFp9uvb13qbzjNxvv64>.



10. Verificar que Windows Defender lo haya detectado.

## Protección antivirus y contra amenazas

Protección contra amenazas para tu dispositivo.

### Amenazas actuales

Se han detectado amenazas. Inicia las acciones recomendadas.

Trojan:Win32/Startpage!MSR  
30/7/2024 00:30 (Activo)

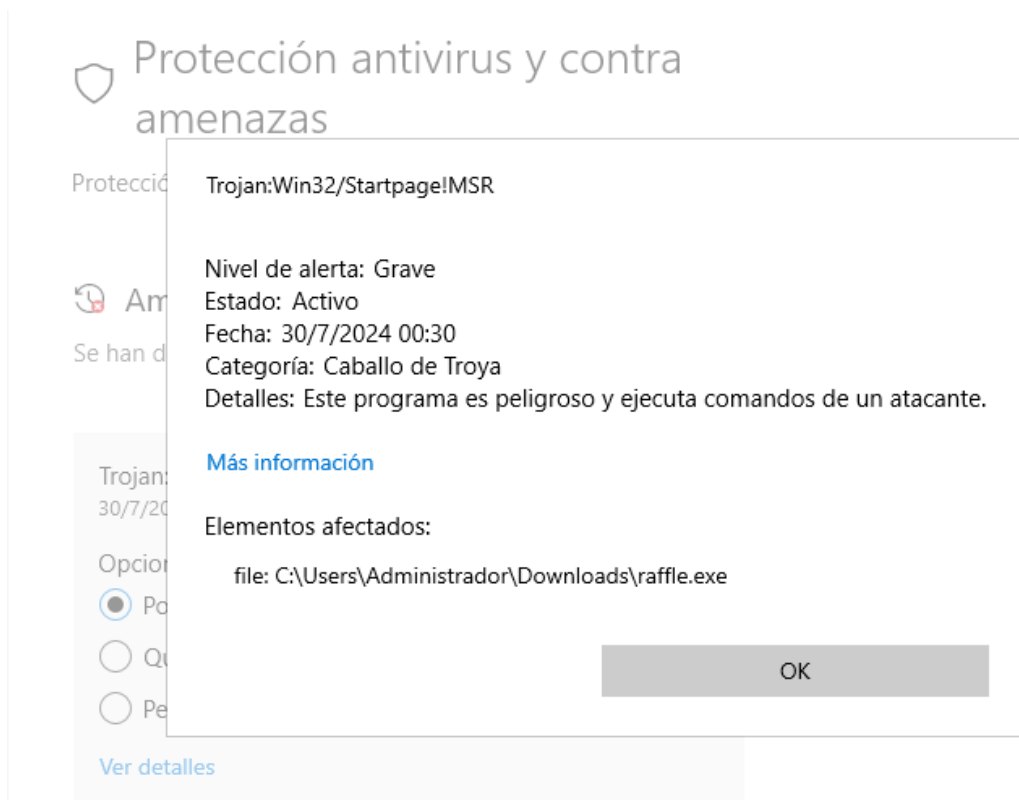
Grave

Iniciar acciones

[Opciones de examen](#)

[Amenazas permitidas](#)

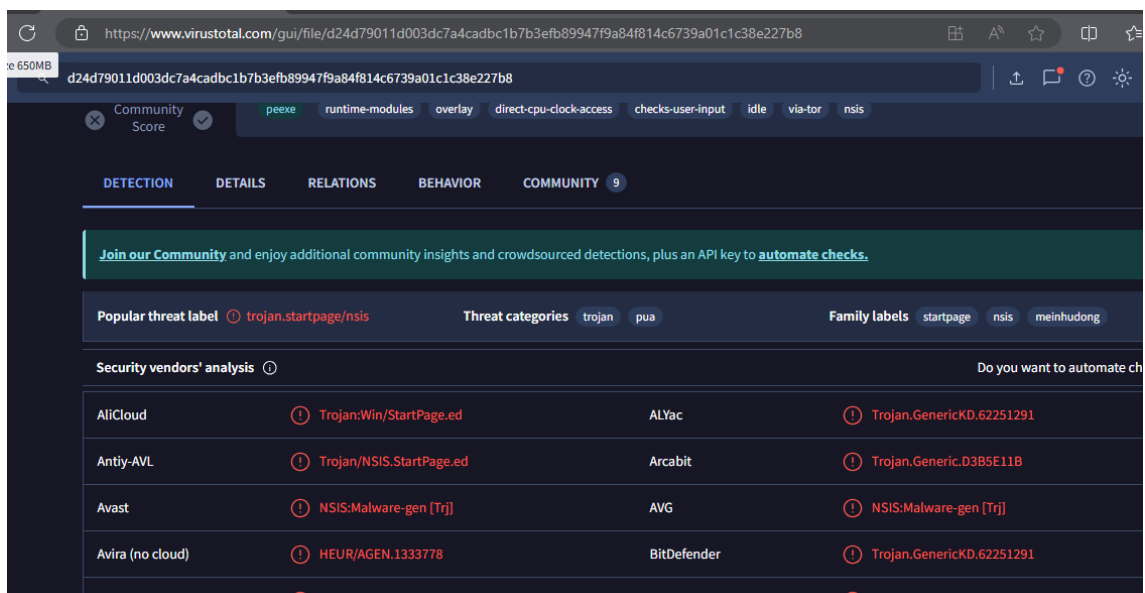
[Historial de protección](#)



11. Subir el archivo descargado al sitio VirusTotal.

<https://www.virustotal.com/gui/home/upload>

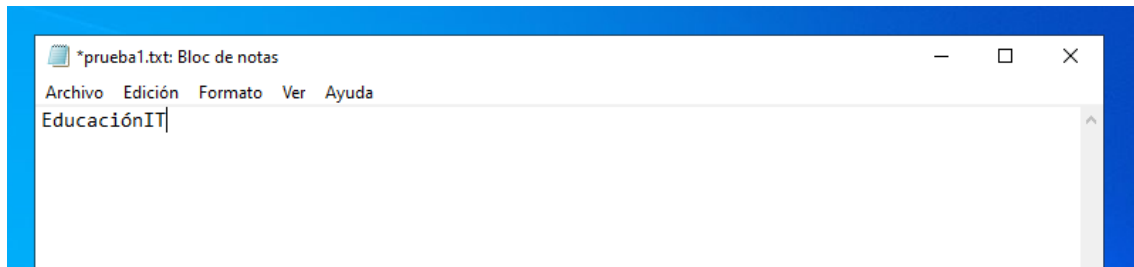
12. Analizar y mostrar el resultado.



HASHES

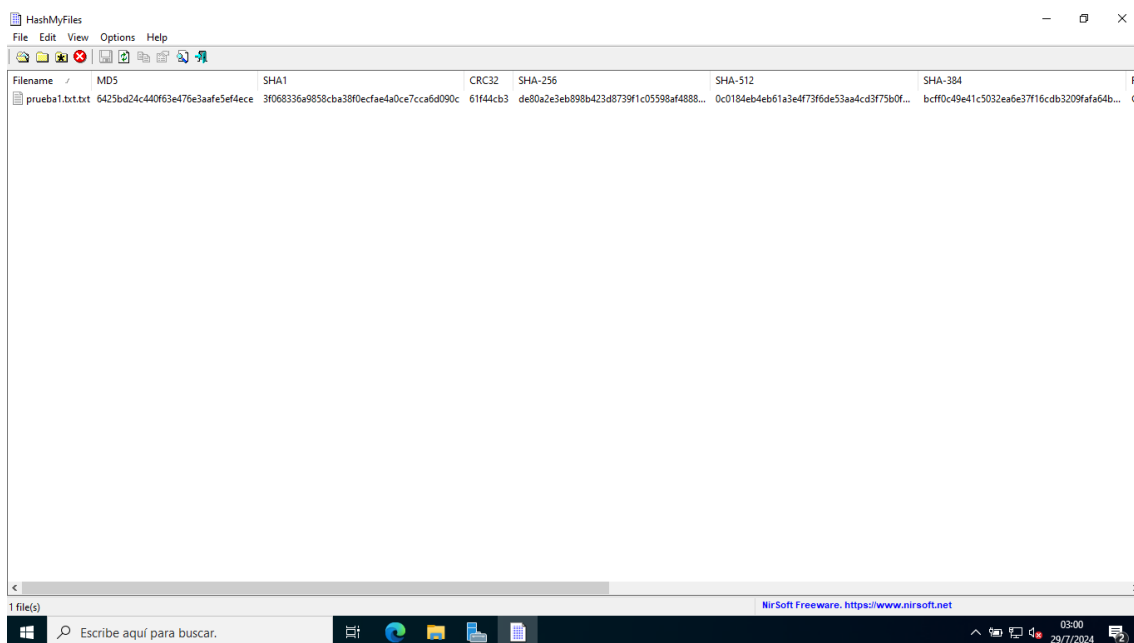
13. Crear un archivo de texto plano con el nombre prueba1.txt en donde el contenido del archivo sea únicamente EducaciónIT.



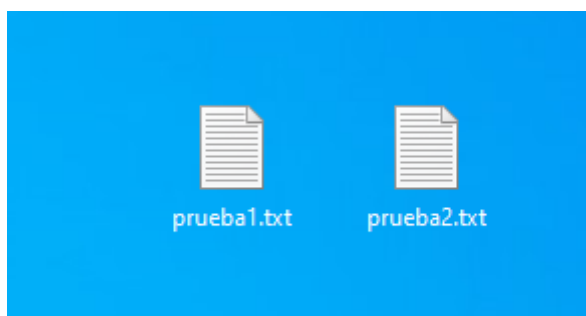


14. Calcular los valores hash del archivo con diferentes algoritmos, utilizando la herramienta HashMyFiles.

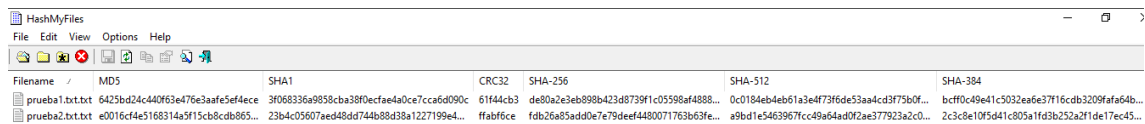
[https://www.nirsoft.net/utls/hash\\_my\\_files.html](https://www.nirsoft.net/utls/hash_my_files.html)



15. Crear un segundo archivo, agregar el siguiente contenido EducacionIT1, agregando un 1 (uno) al final, y guardar con el nombre prueba2.txt.



16. Volver a calcular los hashes y verificar si los mismos han cambiado con respecto a los anteriores.



Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-384
prueba1.txt	6425bd24c440f63e476e3afe5ef4e	3f068336a9858cba38f0ecfae4a0ce7cca6d090c	61f44cb3	de80a2e3eb898b423d8739f1c05598af4888...	0c0184eb4eb61a3e4f73f6de53aa4cd3f75b0f...	bcff0c49e41c5032eae6e37f16cdb3209fa64b...
prueba2.txt	e0016cf4e5168314a5f15cb8cdb865...	23b4c05607aed48dd744b88d38a1227199e4...	ffabf6ce	fdb26a85add0e7e79deef4480071763b63fe...	a9bd1e5463967f7cc49a64ad0f2ae377923a2c0...	2c3c8e10f5d41c805a1fd3b252a2f1de17ec45...

## VOLÚMENES DE DISCOS CIFRADOS

17. Usar VeraCrypt para crear un volumen de disco cifrado de 10 MB que utilice el algoritmo de Hash SHA 512 y el algoritmo de cifrado AES.

<https://www.veracrypt.fr/en/Downloads.html>

Descarga e instala VeraCrypt desde su sitio oficial.

Abrir VeraCrypt y selecciona Crear volumen.

Seleccionar Crear un archivo contenedor cifrado.

Definir el tamaño del volumen como 10 MB.

Eligeir SHA-512 para el hash y AES para el cifrado.

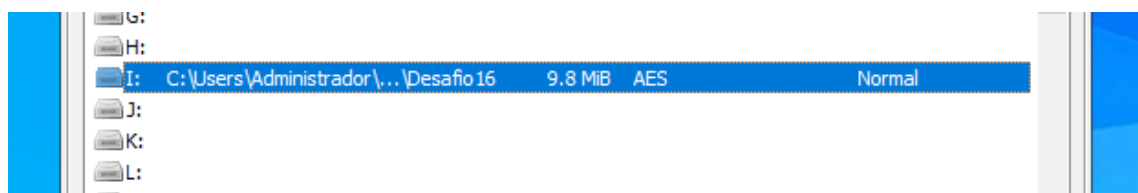
Completar el proceso de creación.

18. Montar el volumen cifrado.

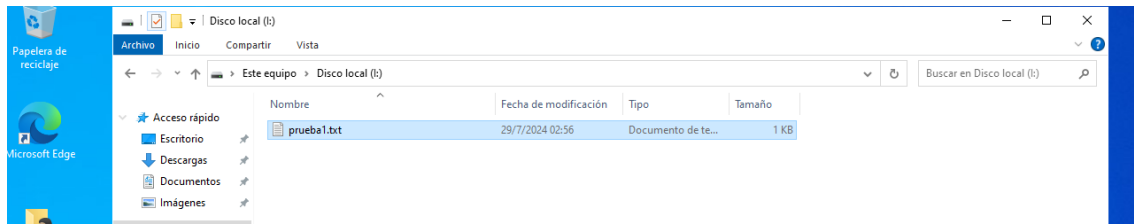
Seleccionar una letra de unidad.

Hacer clic en Seleccionar archivo y elegir el volumen creado.

Hacer clic en Montar e ingresar la contraseña.



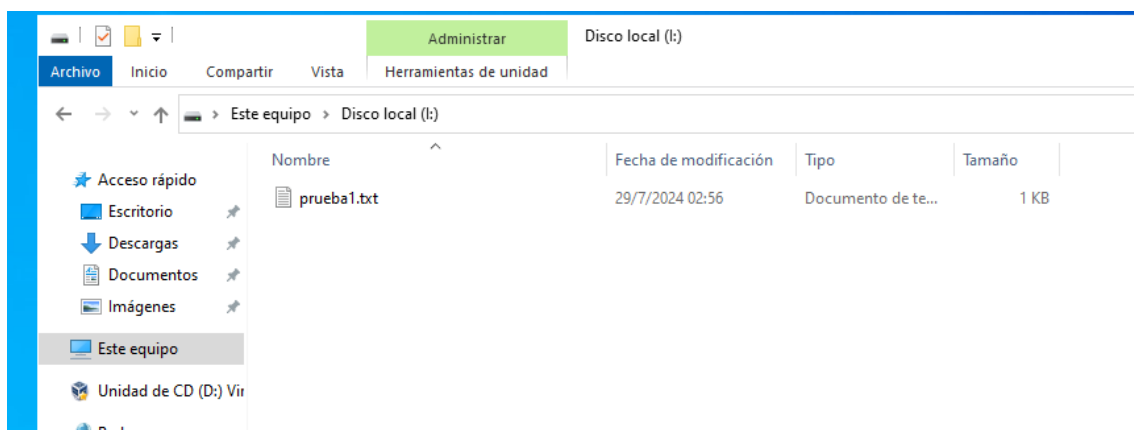
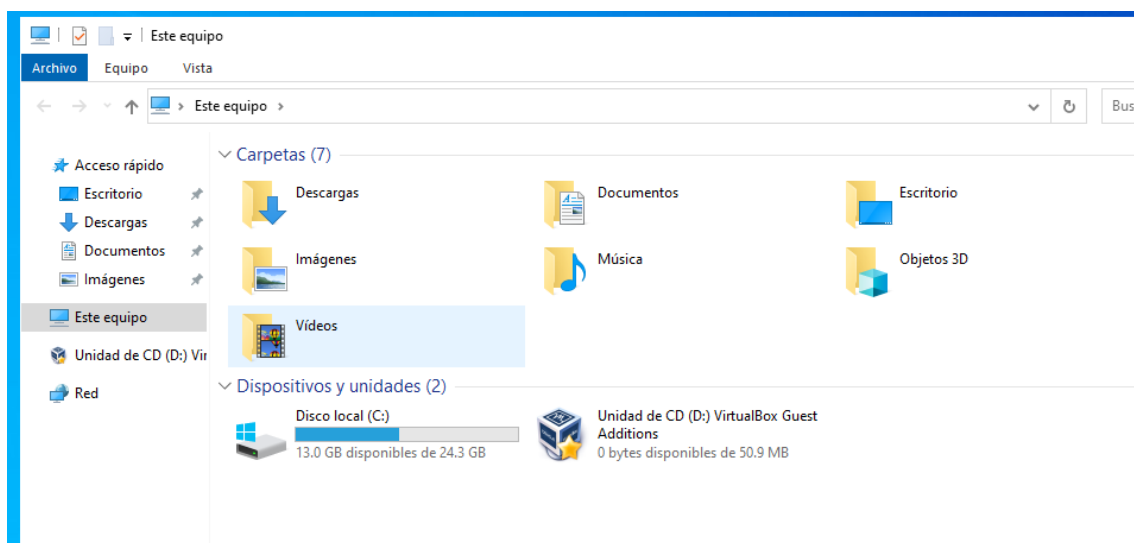
19. Almacenar el archivo prueba1.txt del ejercicio 13 dentro del volumen.



20. Desmontar el volumen, volver a montarlo y verificar si los archivos se encuentren intactos.

Seleccionar el volumen y hacer click en Desmontar.

Volver a montar el volumen y verificar que prueba1.txt esté presente.



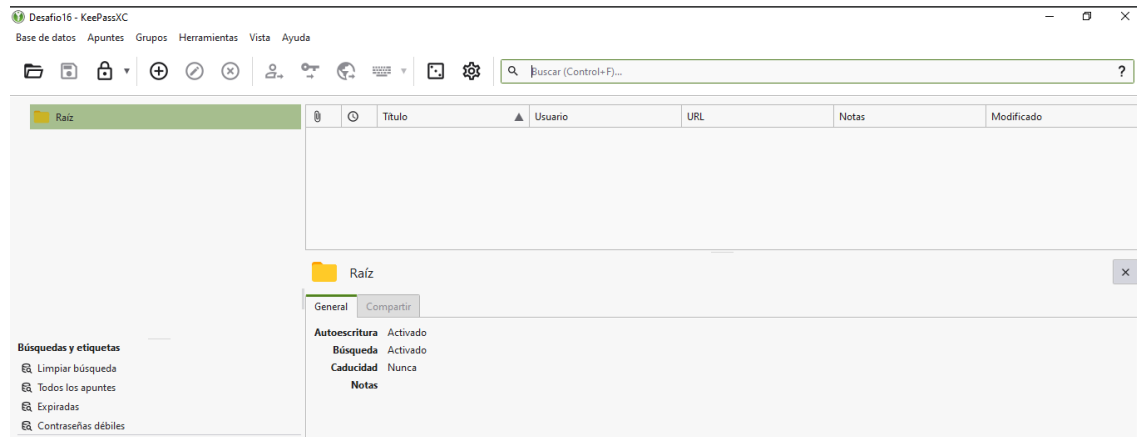
## ALMACENAMIENTO DE CONTRASEÑAS

21. Usar KeePassXC para crear una base de datos de contraseñas.

<https://keepassxc.org/download/#windows>

Descargar e instalar KeePassXC

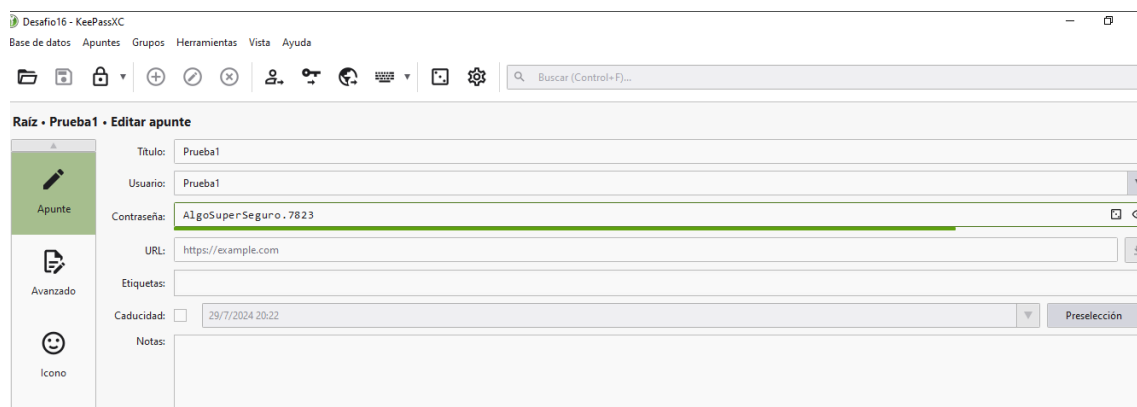
Abrir KeePassXC y selecciona Nuevo para crear una base de datos de contraseñas.



22. Almacenar credenciales con los siguientes datos:

a. Usuario: Prueba1.

b. Contraseña: "AlgoSuperSeguro.7823"



23. Cerrar KeePassXC y volver a abrir.

24. Verificar si la contraseña que se ha almacenado esté presente en la base.



Raíz / Prueba1


General

Avanzado

Autoescritura

Usuario Prueba1

URL

Contraseña  AlgoSuperSeguro.7823

Caducidad Nunca

Etiquetas

Notas