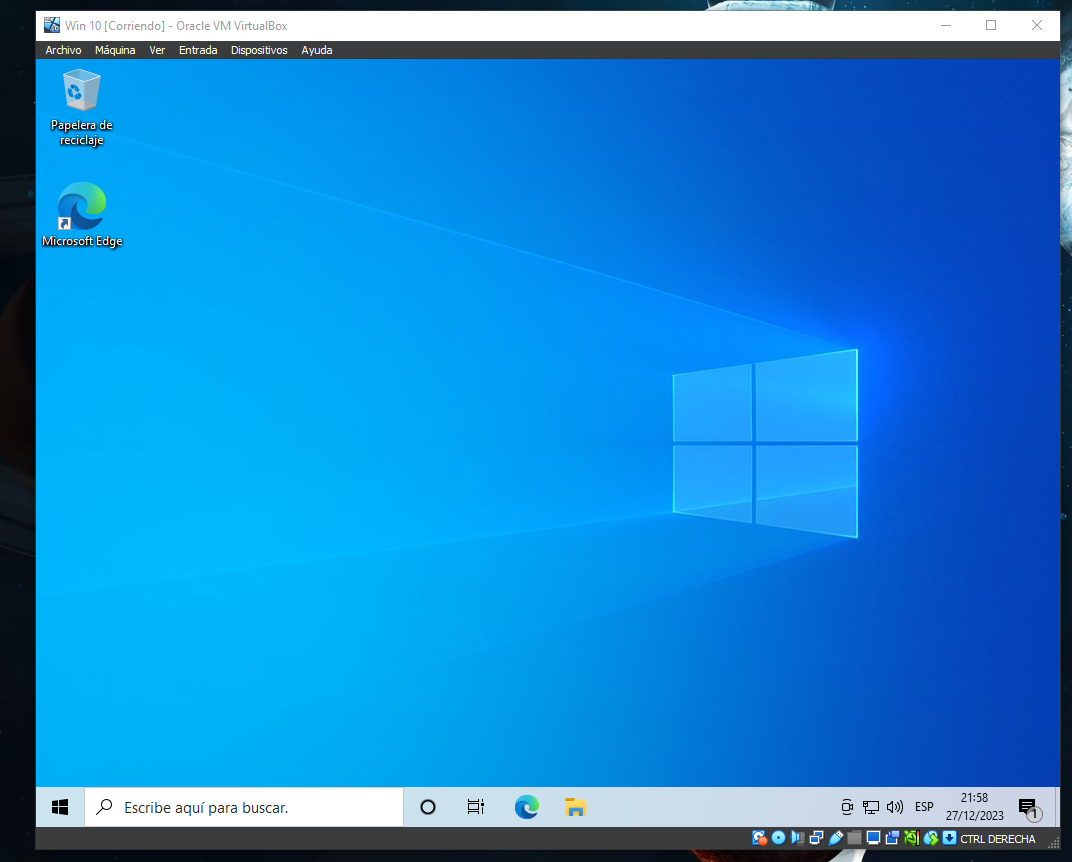
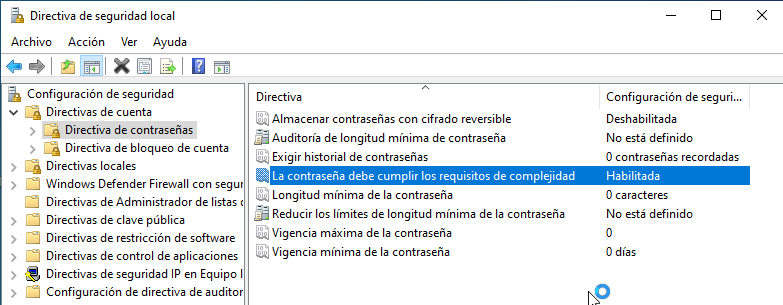
# Trabajo Práctico N 12

**Ejercicio 1:**

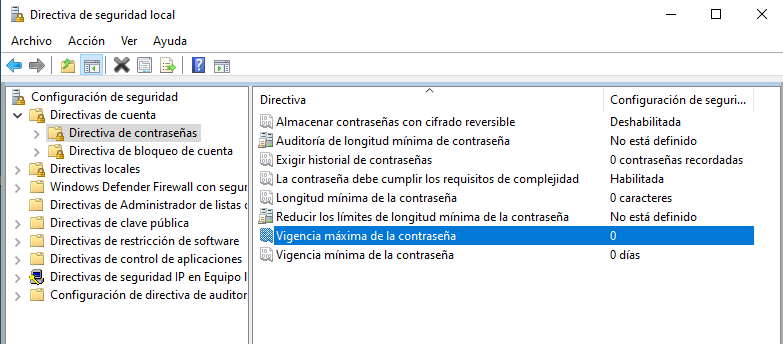
1. Ingresar a un equipo con Windows (nuestra VM).



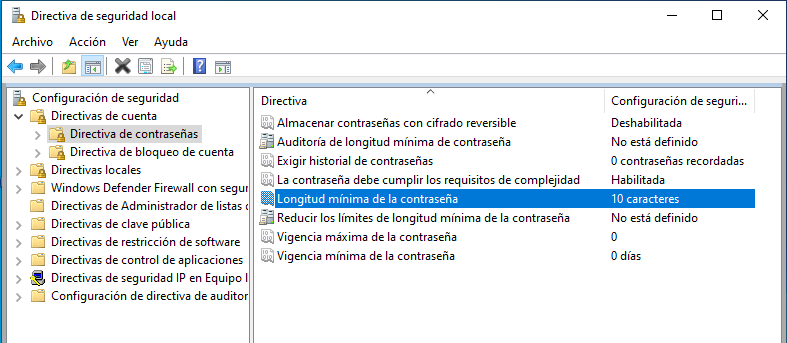
1. Habilitar la complejidad de contraseñas.



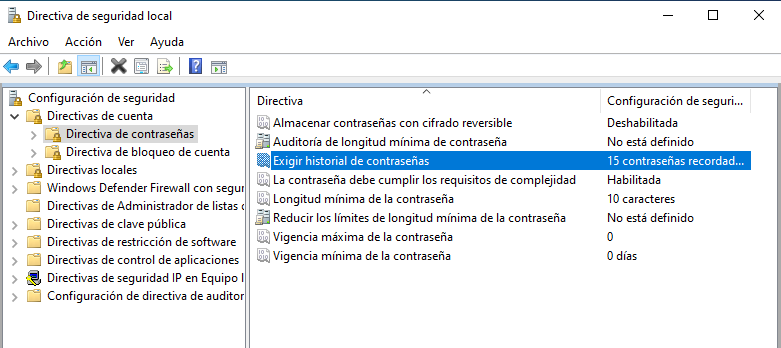
1. Configurar que las contraseñas no expiren.



1. Requerir que las contraseñas tengan, al menos, 10 caracteres de longitud.

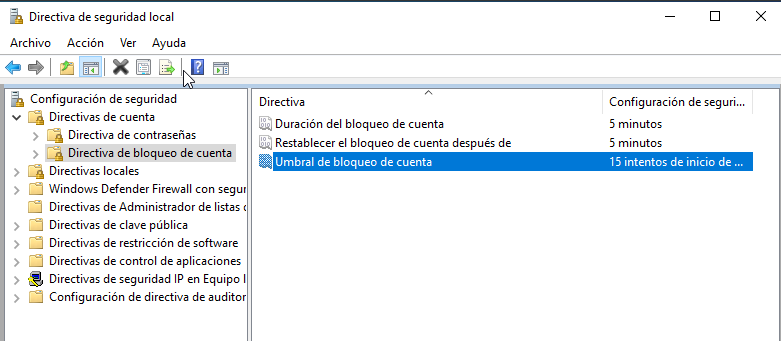


1. Configurar el historial para evitar la reutilización de las últimas 15 contraseñas.

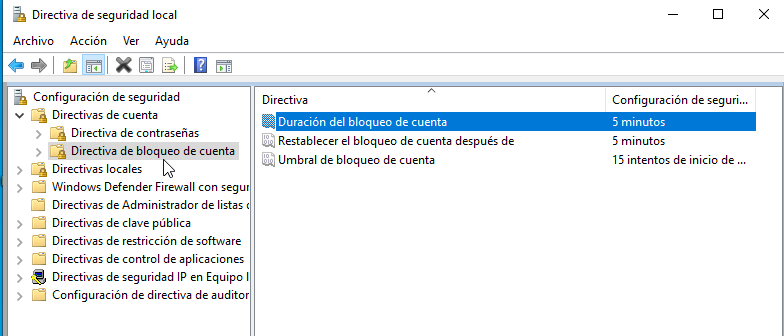


**Ejercicio 2:**

1. Configurar el bloqueo de cuentas luego de 5 intentos fallidos.



1. Configurar el desbloqueo automático después de 5 minutos.



**Conclusión:**

Una buena opción de ataque podría ser el de fuerza bruta (aunque se haya configurado el bloqueo después de 5 intentos).

Otra puede ser la complejidad de la contraseña, en donde si se pone una contraseña fácil esta también es fácil de detectar.