**Doble factor de Autenticación en SS.OO**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Ubuntu**](#_g59i8ewd3ed3) **2**

[**2.1 Google Authenticator:**](#_5d38uxjyswtl) **2**

[**3. Windows**](#_64ohcqjdumfm) **8**

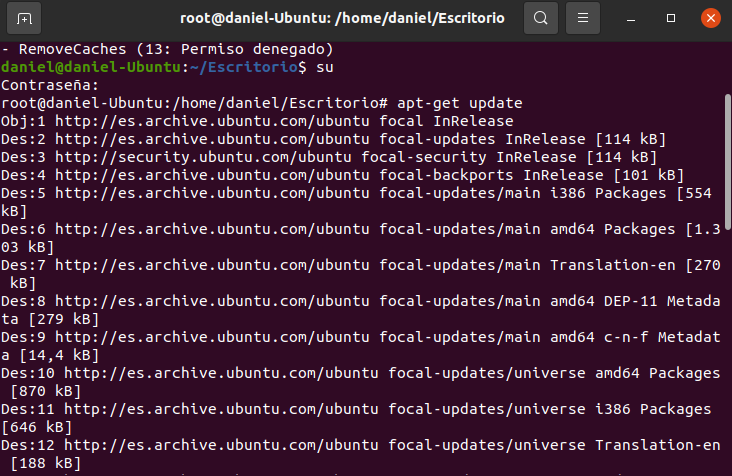
[**3.1 SaasPass:**](#_y5aus6nt3c7z) **8**

# **2. Ubuntu**

### **2.1 Google Authenticator:**

1 Preparar una máquina Ubuntu con recomendaciones de optimización vistas en clase.

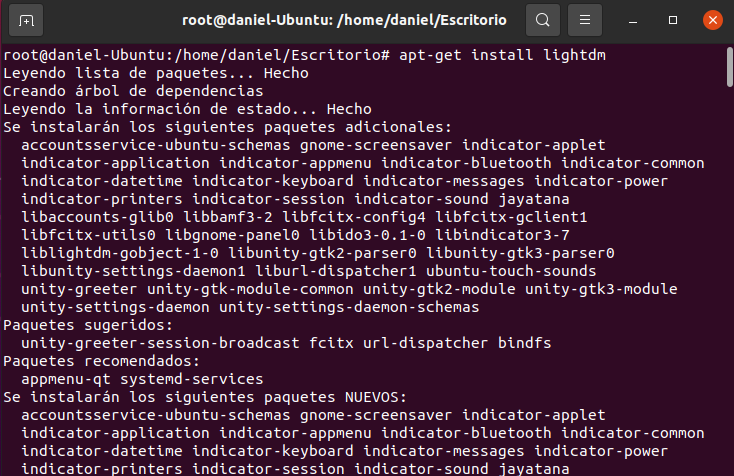
2. Actualizar listado de paquetes en la máquina



3. Instalar paquete correspondiente a Google Authenticator (libpam-google-authenticator)



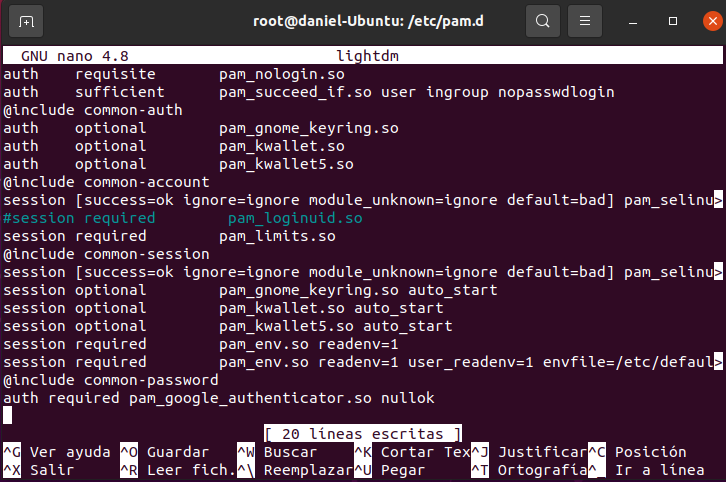
4. Instalar gestor de sesión lightdm



5. Configurar entre los parámetros de lightdm la opción para que puedan seguir iniciando

sesión los usuarios en la máquina que no activen la verificación en dos pasos.





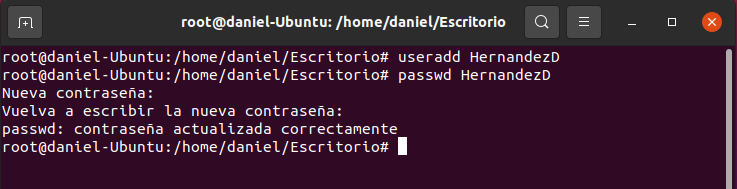
Es necesario añadir esta última línea en el fichero de configuración de lightdm para su correcto funcionamiento.

6. Crear un usuario en la máquina [segundoapellido+primeraletradelnombre]. Iniciar sesión

con éste usuario y activar doble factor de inicio de sesión (2SA). Al configurar Google

Authenticathor nos preguntará sobre varias opciones. Inicialmente activar siempre las

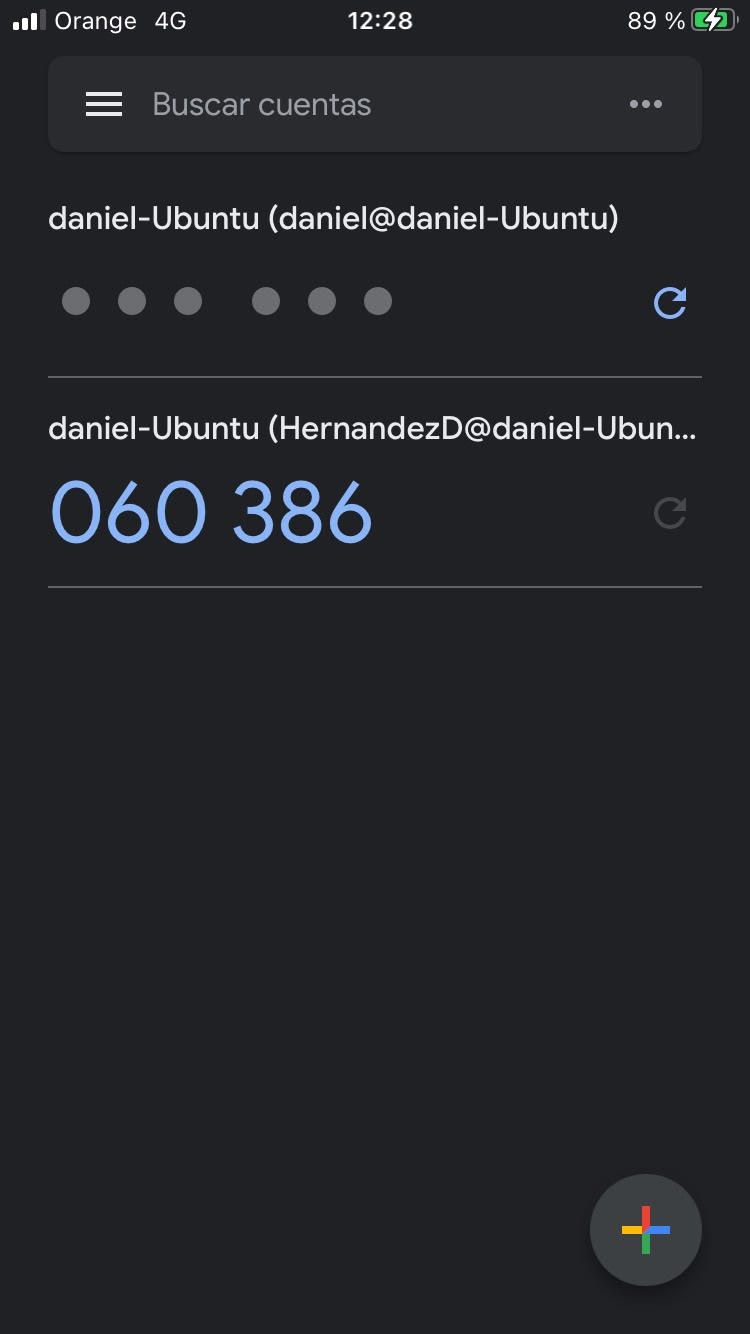
que nos den mayor seguridad.

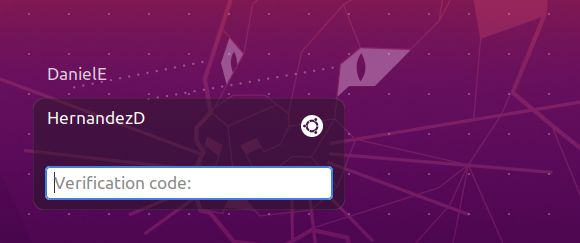




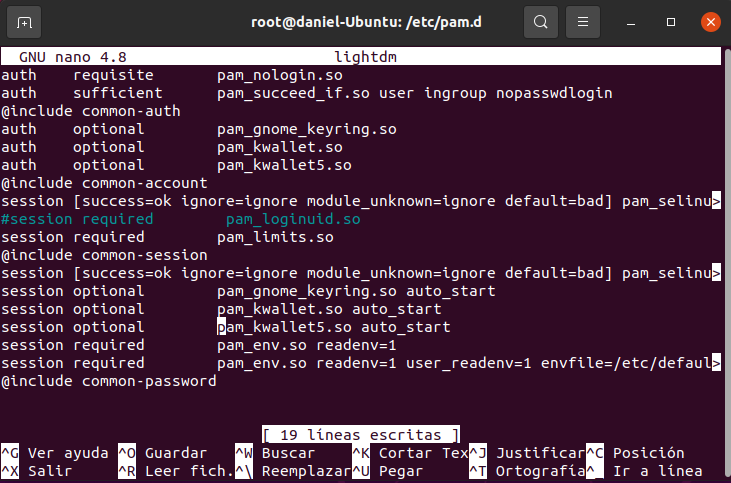
7. Instalar Google Authenticator en el dispositivo móvil y vincular el inicio de sesión de

Linux con el código QR que fue generado.





8. Explica de qué forma se puede deshabilitar el inicio con doble factor.



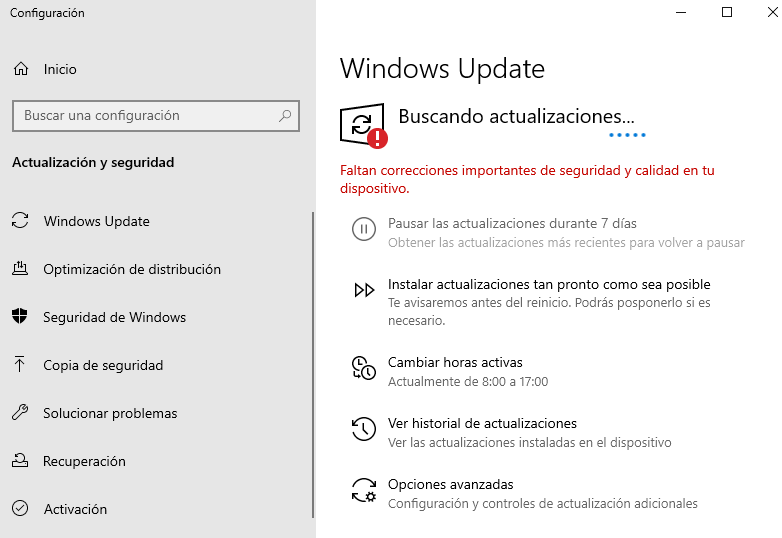
Lo único necesario sería eliminar la línea añadida en el fichero de configuración de lightdm o en su defecto comentar dicha línea.

# **3. Windows**

### **3.1 SaasPass:**

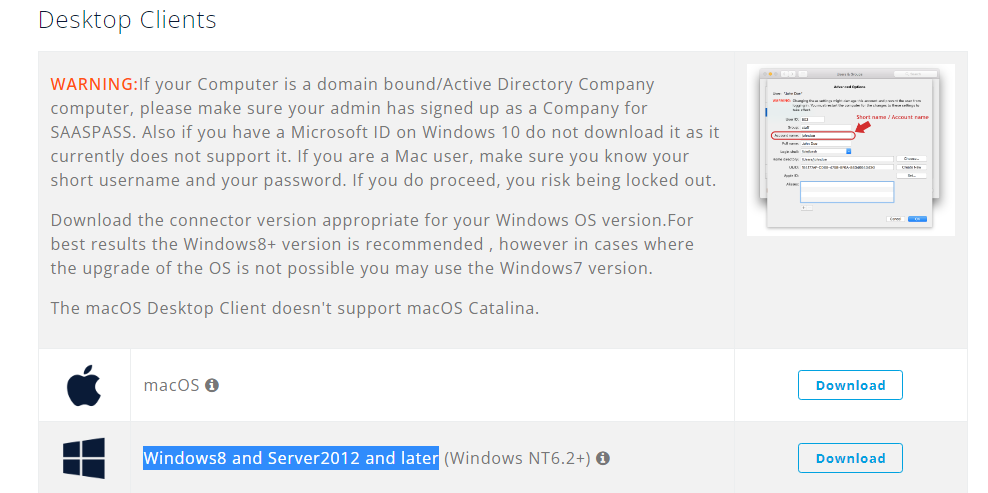
1. Preparar una máquina con Windows 10 siguiendo las recomendaciones de optimización vistas

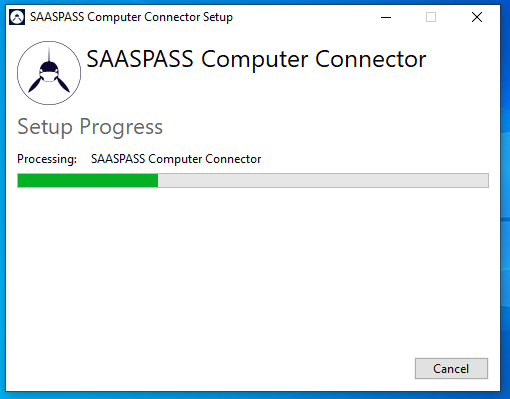
2. Actualizar el S.O. con los últimos parches y actualizaciones



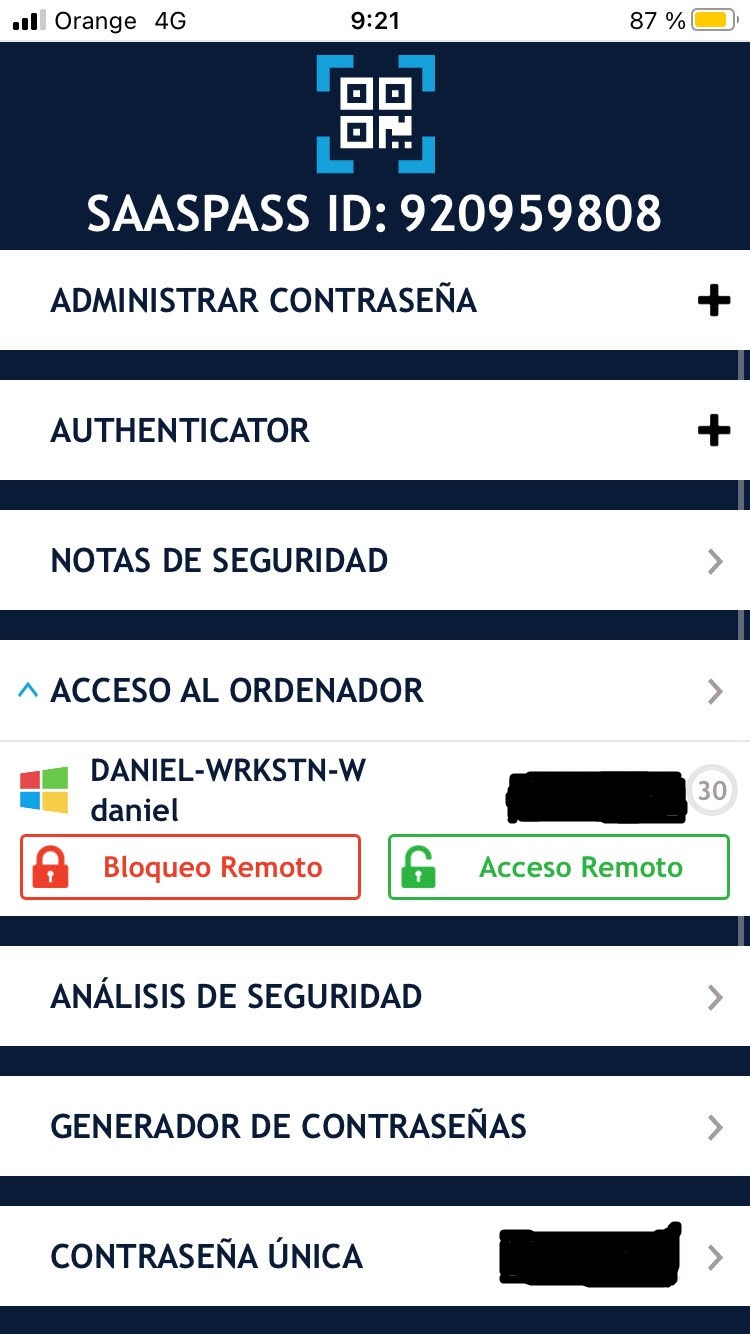
3. Iniciar sesión con el usuario que hemos creado en el punto 1

4. Instalar SaasPass en la máquina virtual. Para descargarlo desde su página oficial nos vamos al apartado Desktop Clients.



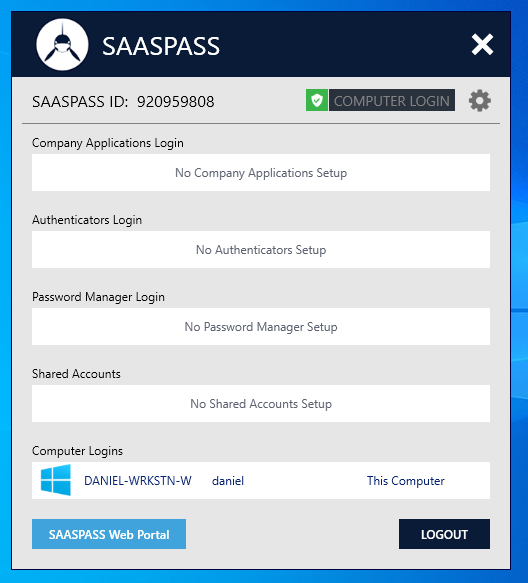
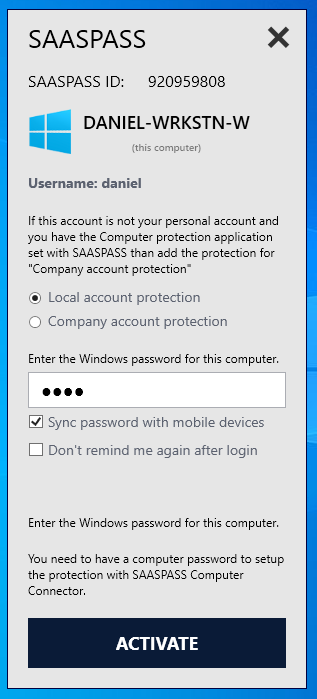


5. Instalar SaasPass en nuestro dispositivo móvil.

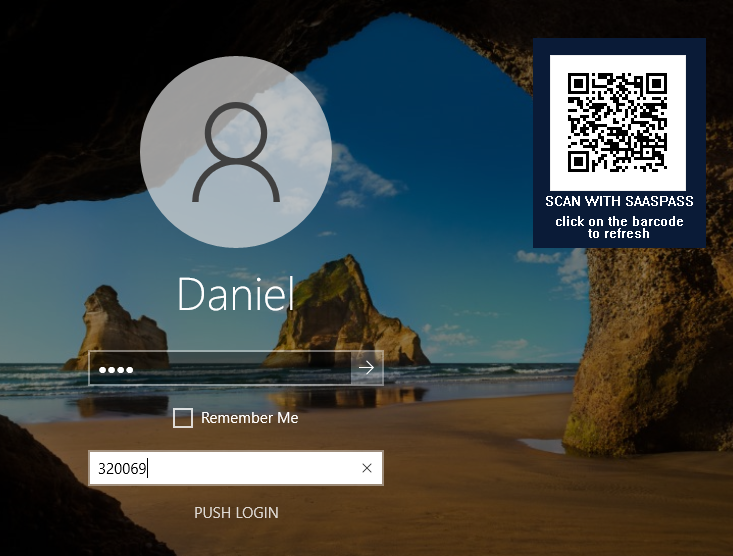


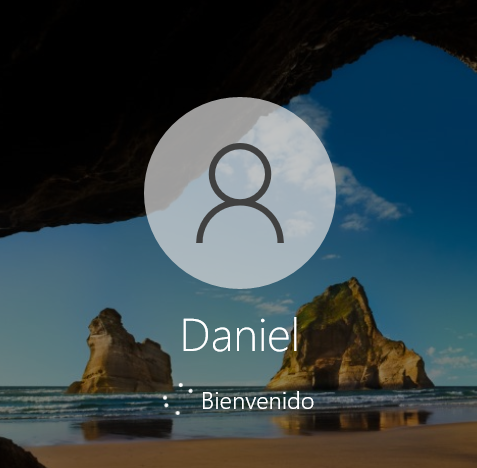
6. Realizar la vinculación entre el inicio de sesión en la cuenta de Windows y la aplicación

SaasPass como segundo factor. En los pasos de configuración nos pedirá introducir el teléfono móvil como herramienta de recuperación.

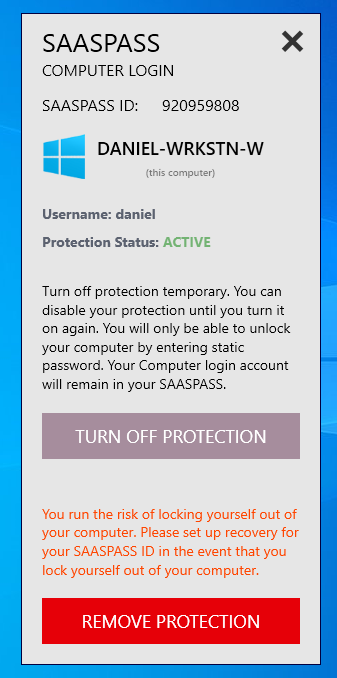


7. Cerrar sesión y volver a logearse con el usuario para verificar que funciona.





8. Explica cómo deshabilitar el inicio de sesión que hemos configurado.



Con la ayuda de interfaz gráfica llegamos a este menú que nos permite quitar temporalmente las protecciones de doble factor de autenticación o directamente desactivarla.