Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

CONFIGURA SISTEMAS DE CONTROL DE ACCESO Y AUTENTICACIÓN DE PERSONAS PRESERVANDO LA CONFIDENCIALIDAD Y PRIVACIDAD DE LOS DATOS

Héctor Ramírez López

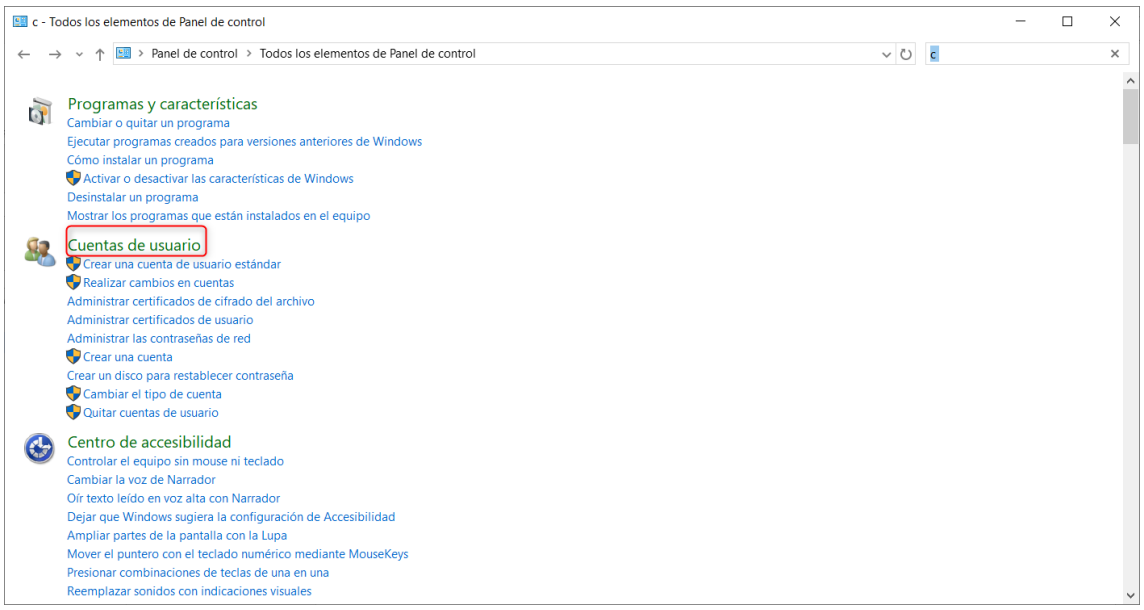
Índice

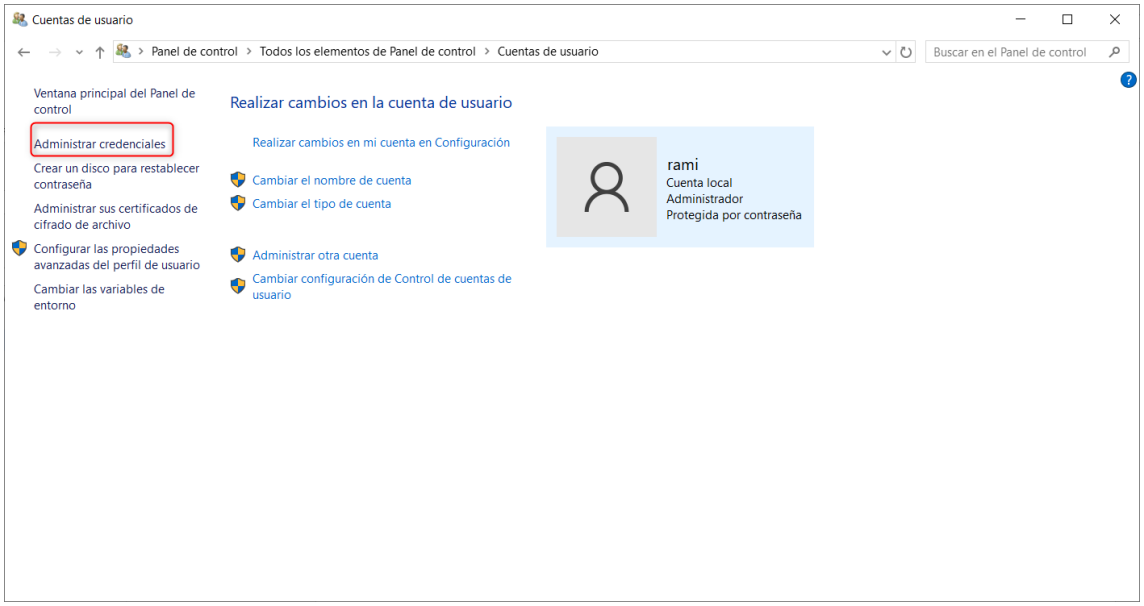
Contenido

1-Gestión de credenciales en Windows

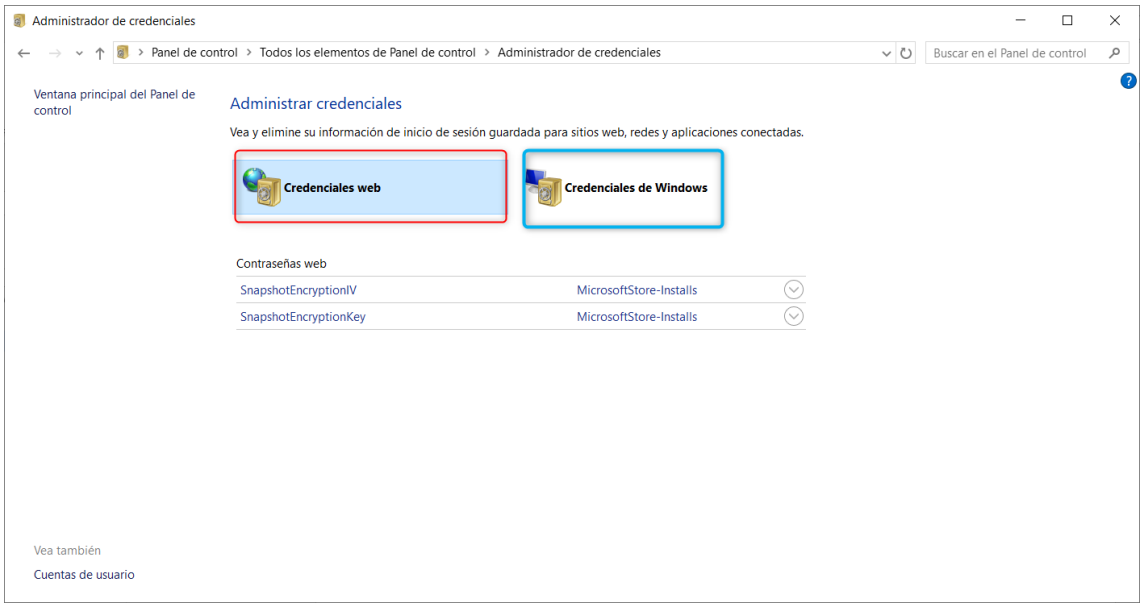
1.1. Acceso al almacén

Abriremos el panel de control nos iremos a buscar el apartado de cuentas y ahí dentro nos vamos a administrar credenciales.



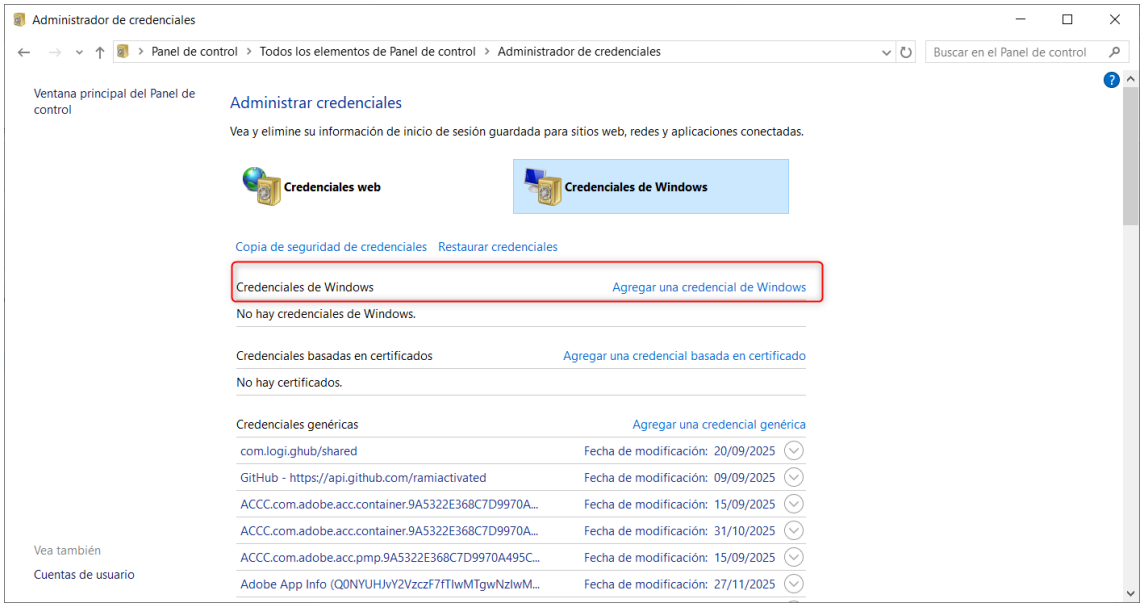


Aquí dentro encontraremos las credenciales web y las de Windows, las credenciales web son claves que Windows almacena para iniciar sesión automáticamente en sitios web o servicios en línea por ejemplo páginas web de Edge o servicios de Microsoft como OneDrive, las de Windows se utilizan para autenticarse en recursos del sistema y la red por ejemplo en unidades de red compartidas, escritorios remotos o en active directory.

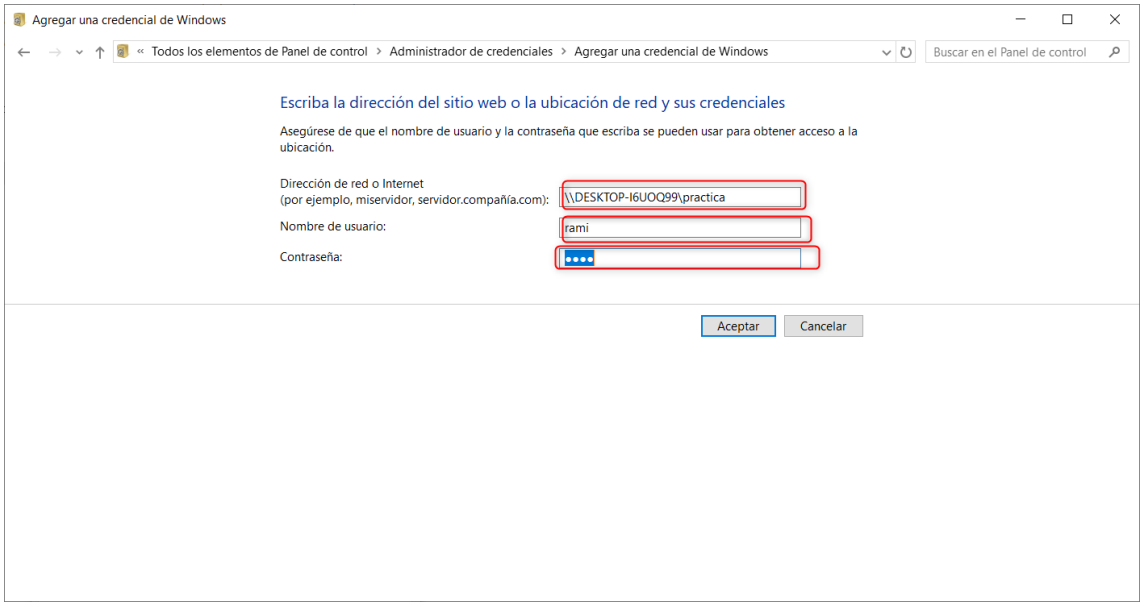


2-Crear una credencial

Ahora crearemos una credencial para ello en el apartado de credenciales de windows le daremos en agregar una credencial de Windows.



Se nos abrirá la siguiente ventana allí introducimos la dirección de nuestro recurso compartido, el nombre de usuario en este caso el usuario local y su contraseña.



2.1 Ver y documentar

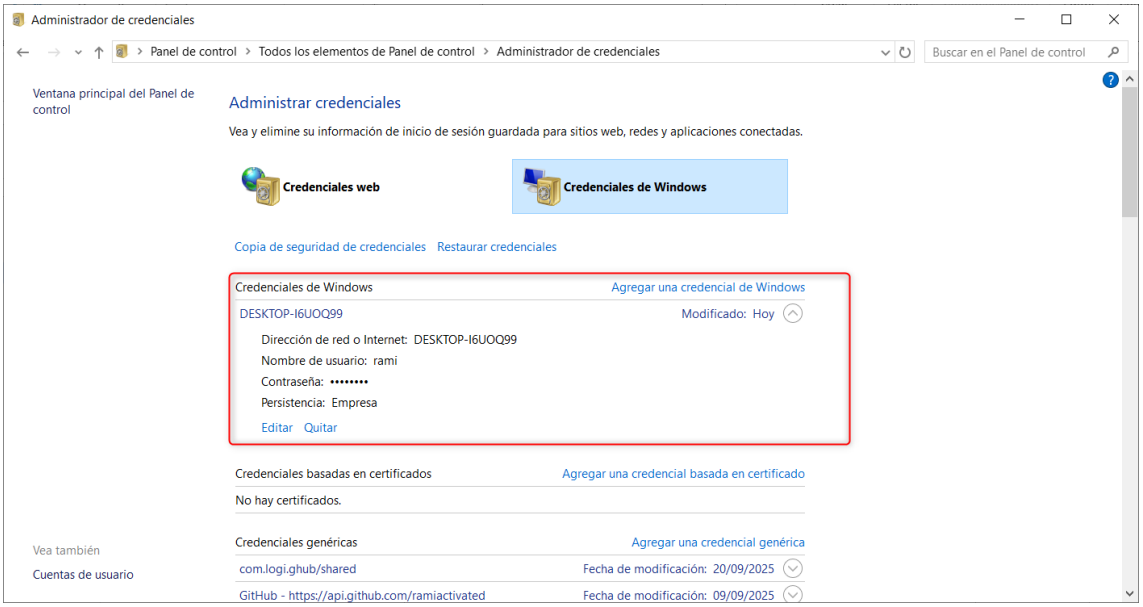
Después de crear la credencial en credenciales de windows, aparece la credencial con los siguientes datos:

Direccion de red: DESKTOP-I6UOQ99

Nombre de usuario: rami

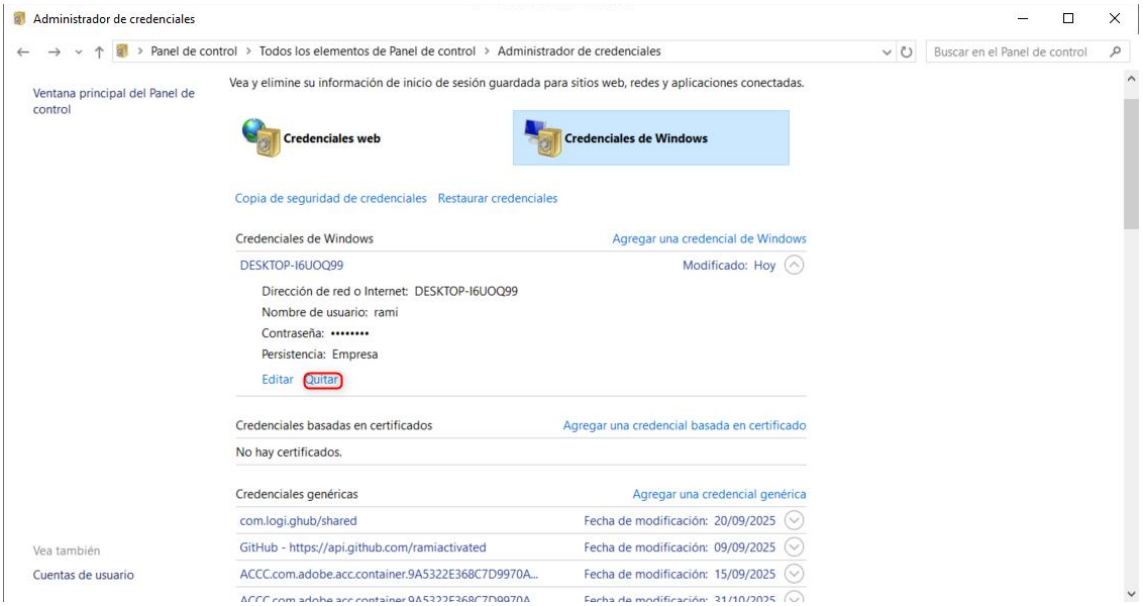
Modificado: hoy

Tipo: Credencial de Windows



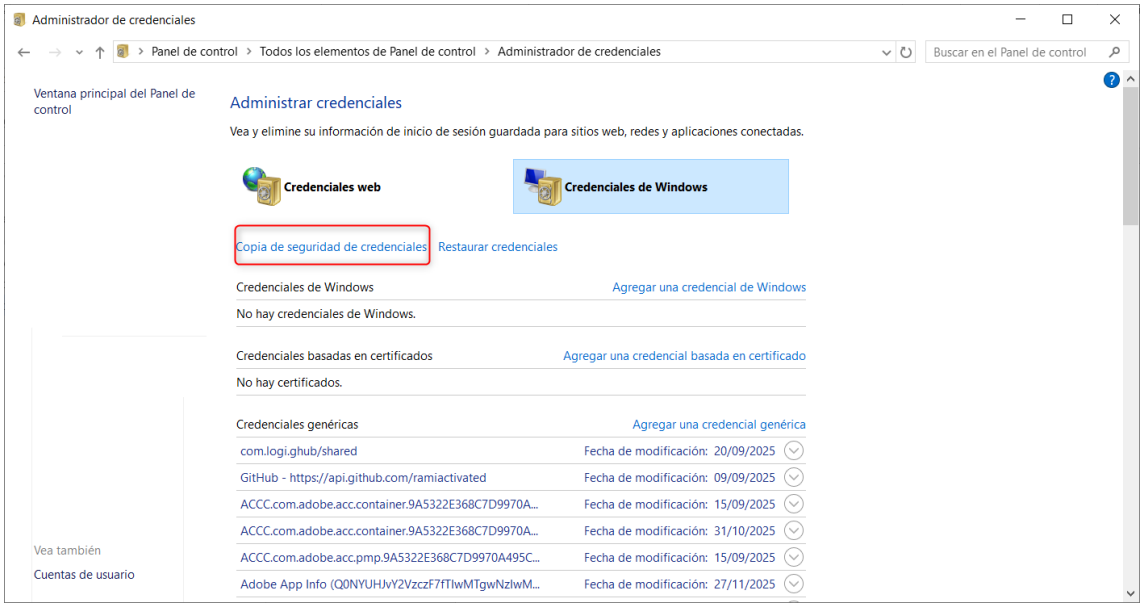
3.Eliminar credencial

Para eliminar la credencial entramos de nuevo al administrador de credenciales y a credenciales de Windows buscamos la credencial que creamos, la desplegamos y seleccionamos la opción quitar.

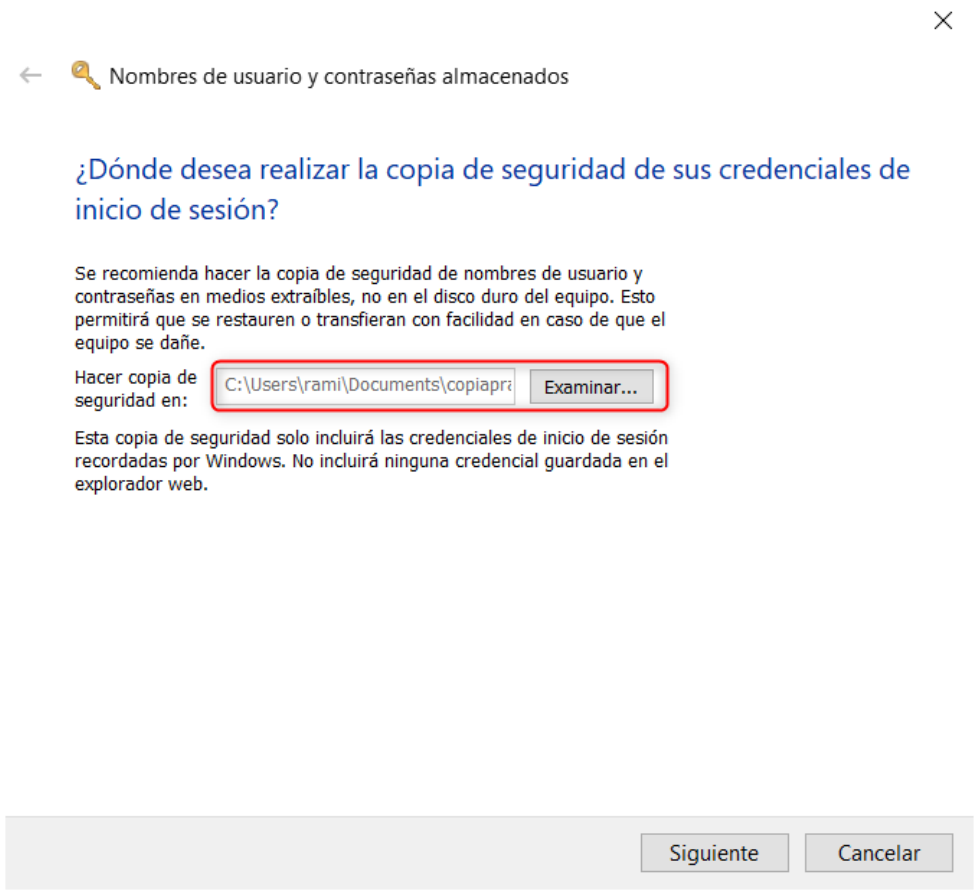


4.Realizar copia de seguridad

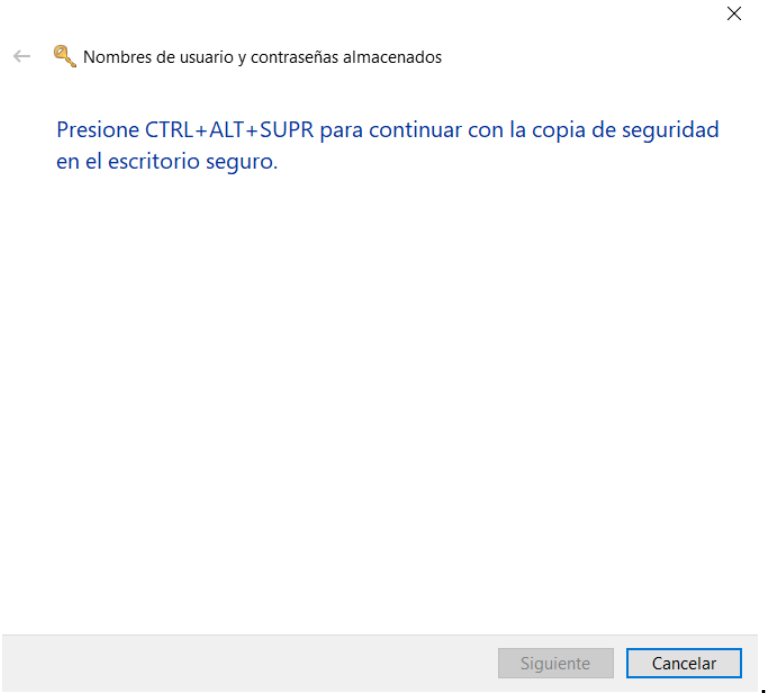
Para este paso seleccionaremos la opción de copia de seguridad de credenciales.

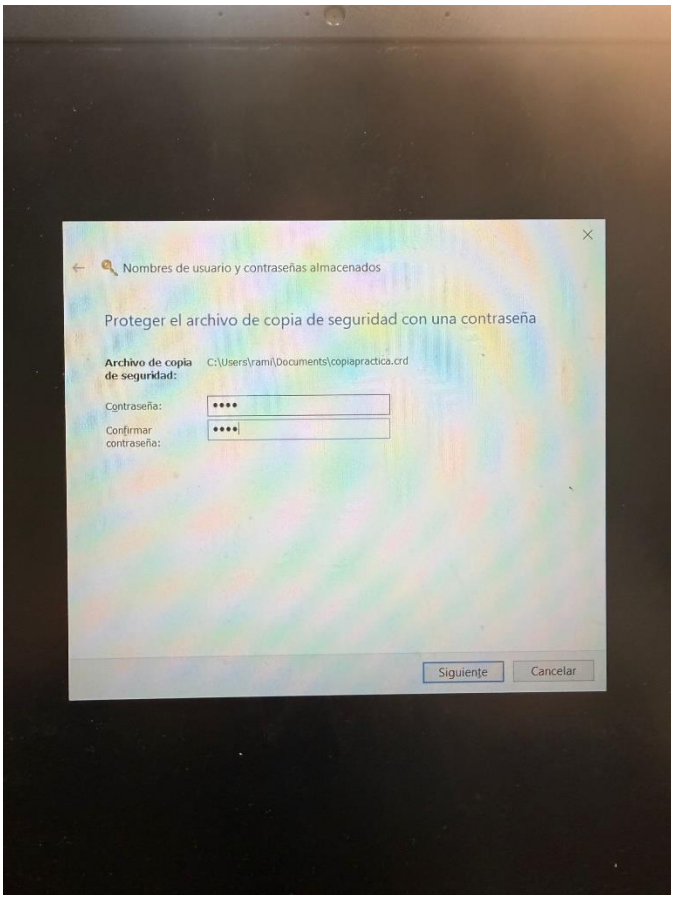


Se nos abrirá el asistente de copias de seguridad y seleccionaremos la ruto donde queremos que se nos guarde la copia.



Al darle a siguiente nos pedirá apretar una secuencia de teclas y después una contraseña para guardar la copia





5.Reflexión

Si un malware eleva privilegios podría conseguir el control total del sistema por ejemplo podría desinstalar e instalar aplicaciones o modificar políticas de seguridad también podría acceder a las contraseñas almacenadas, a las credenciales de windows, archivos privados etc y desactivar antivirus o firewalls por ultimo lo que considero más importante podría ejecutar un ramsomware con permiso de admin lo que cifraría toda la información.

1.Gestión de credenciales en Linux

1.1Instalación de PasswordSafe

Lo primero ejecutamos el comando sudo apt update para actualizar el sistema.

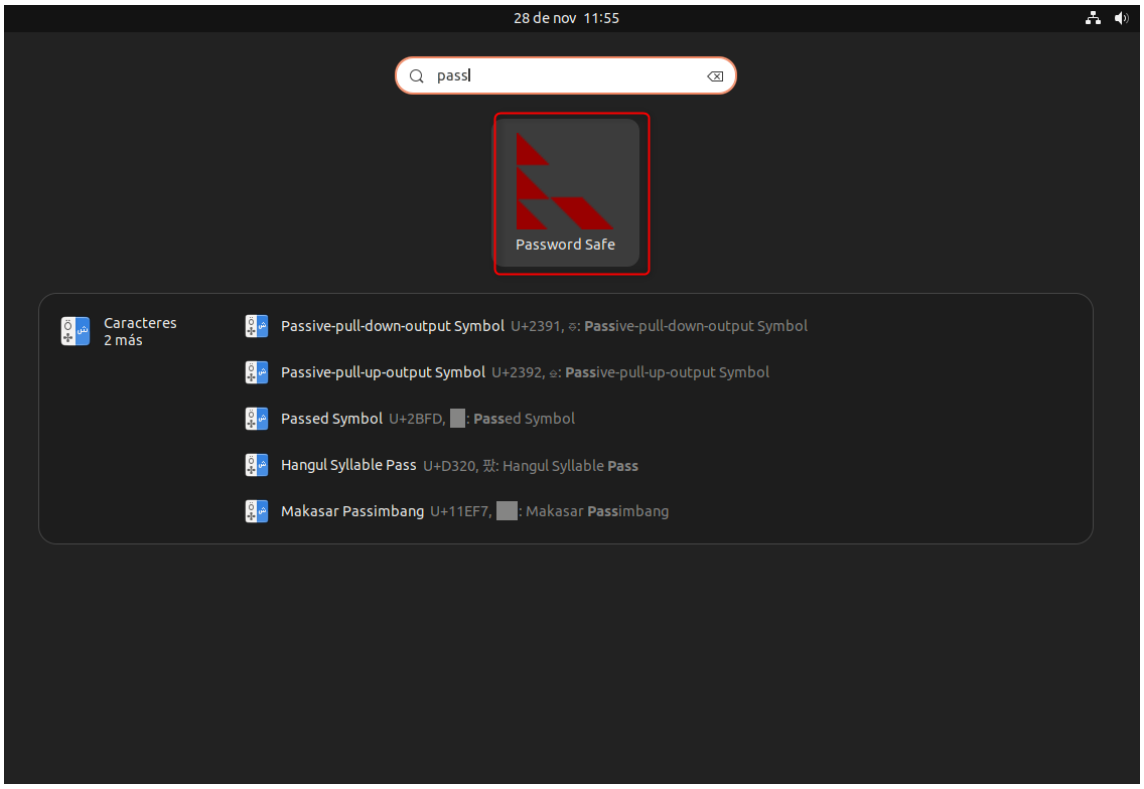
```
rami@rami-VirtualBox:~$ sudo apt update
[sudo] contraseña para rami:
Obj:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu jammy-backports InRelease
```

Ahora ejecutamos el comando sudo apt install passwordsafe para instalar la herramienta.

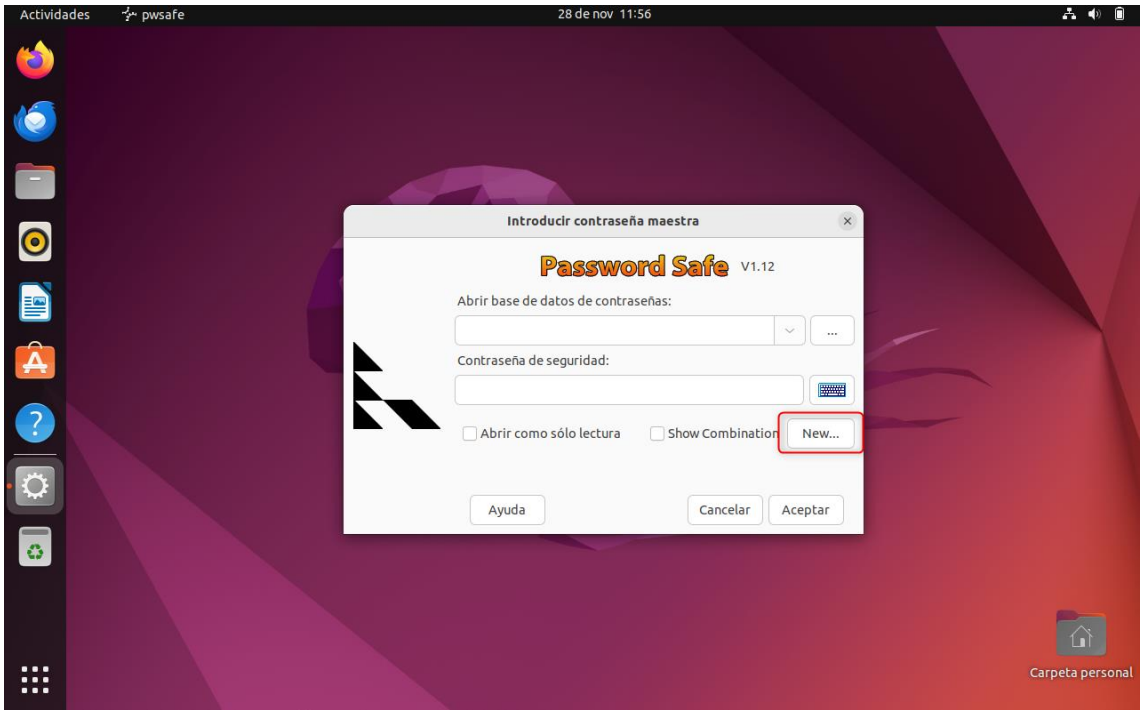
```
rami@rami-VirtualBox:~$ sudo apt install passwordsafe
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libqrencode4 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5 libxerces-c3.2
  libykpers-1-1 libyubikey-udev libyubikey0 passwordsafe-common xvkbd
Se instalarán los siguientes paquetes NUEVOS:
  libqrencode4 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5 libxerces-c3.2
  libykpers-1-1 libyubikey-udev libyubikey0 passwordsafe passwordsafe-common
  xvkbd
```

2.Crear archivo .psafe3

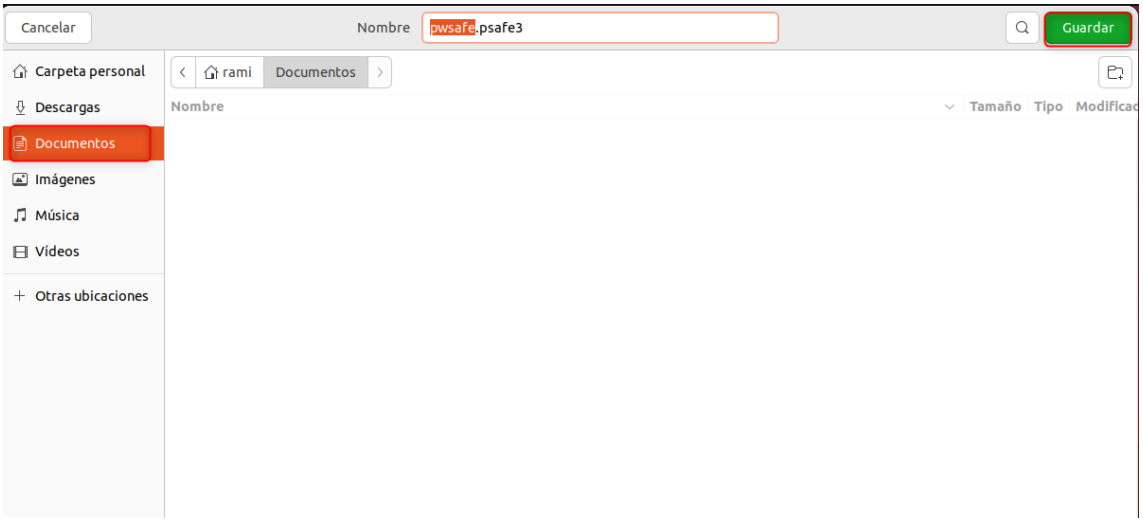
Abrimos passwordsafe



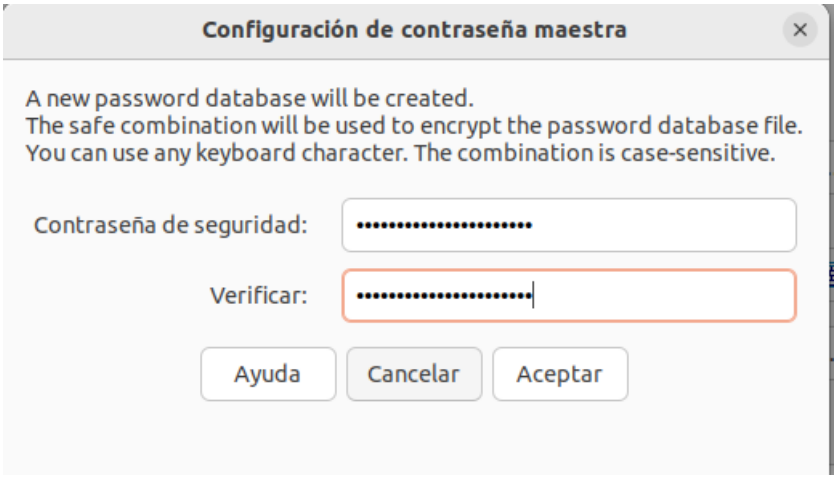
Ahora le daremos a la opción de new para crear el archivo.



Elegiremos donde guardar el archivo en este caso lo guardare en documentos y le damos a guardar.

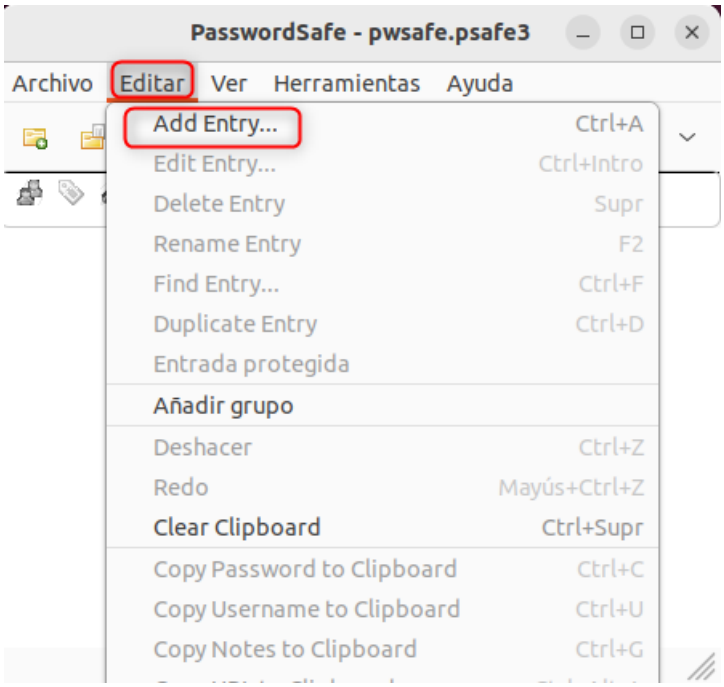


Ahora nos pedirá configura una contraseña para el archivo, la introducimos y le damos a aceptar. La herramienta no me indica debilidad de contraseña.

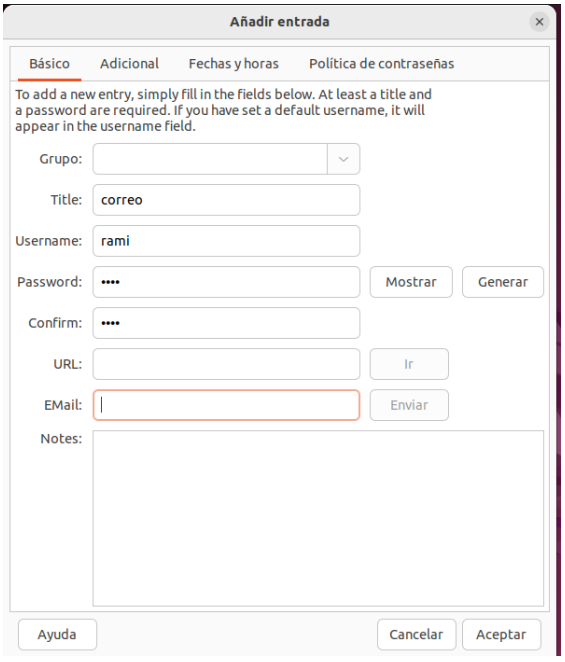


3.Crear entradas

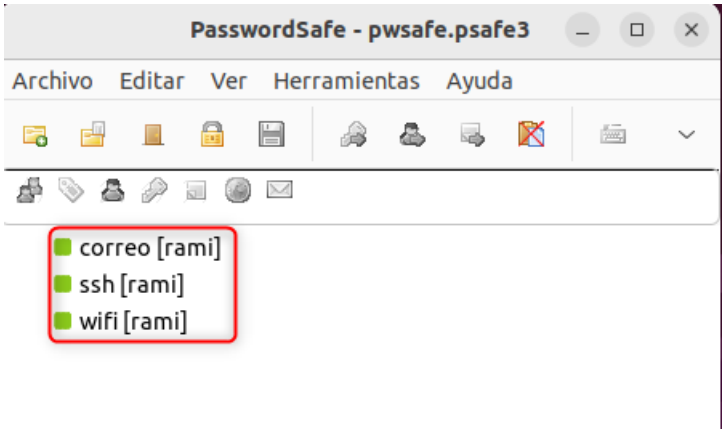
Cuando abramos el archivo nos vamos a la pestaña editar y le damos a add entry.



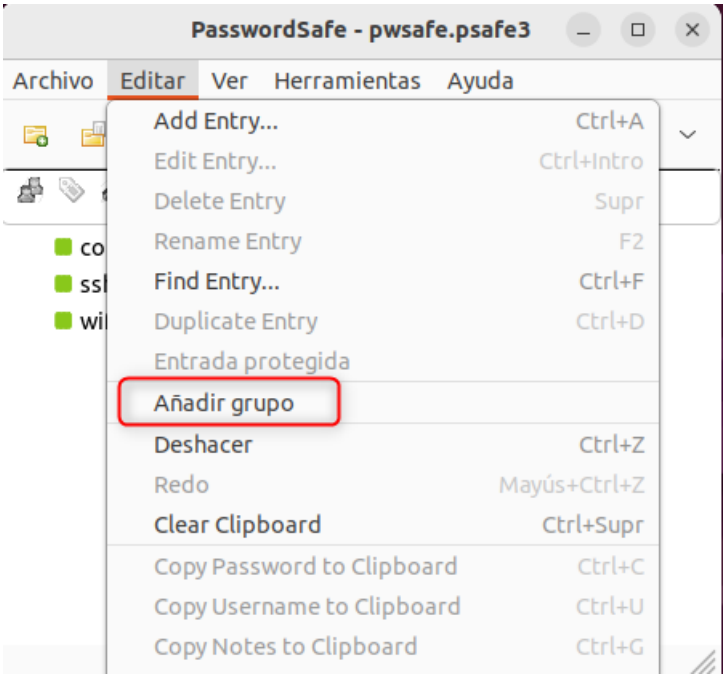
Se nos abrirá la pestaña para crear la entrada, creamos 3 entradas distintas.



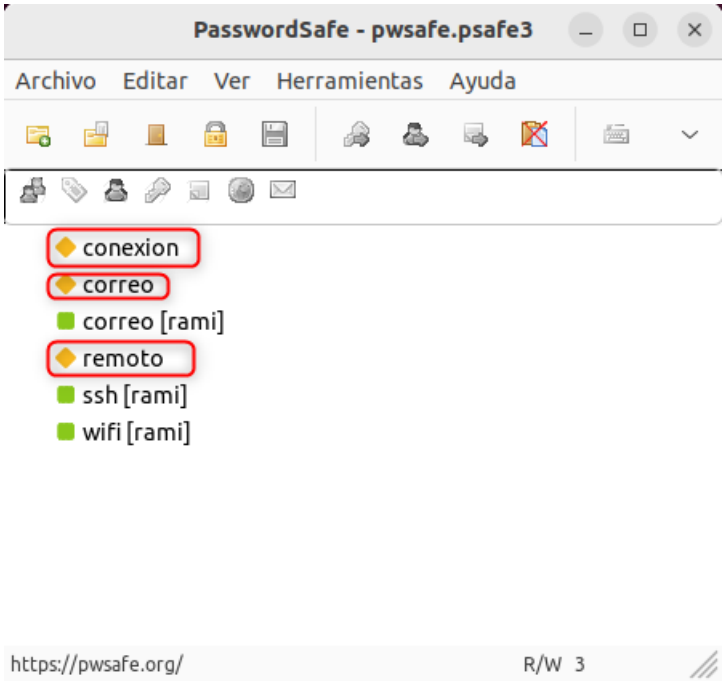
Cuando las hayamos creado no quedara así.



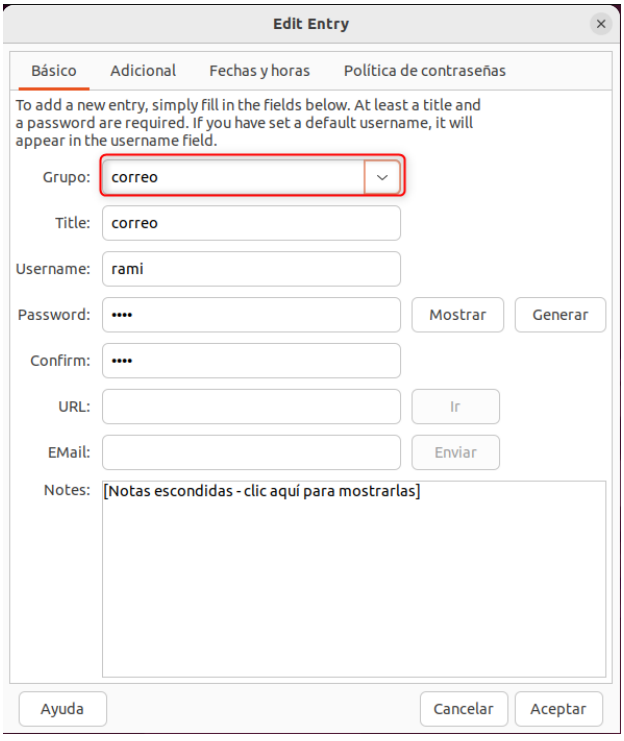
Ahora vamos a clasificarlas por grupo para ello nos vamos a la opción editar y añadir grupo.



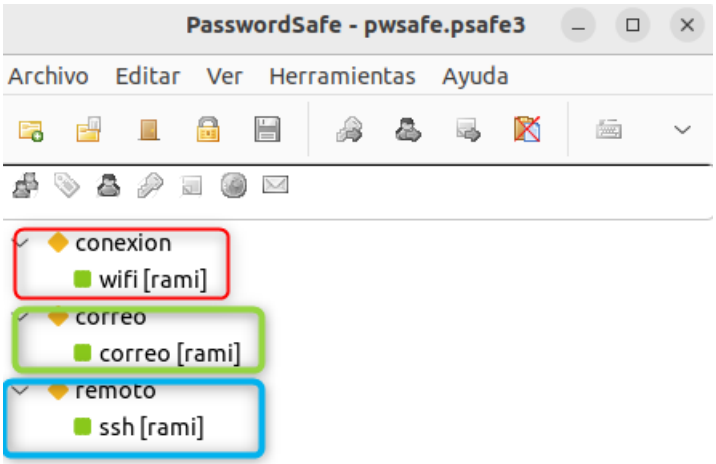
Vamos a crear 3 grupos una vez creados nos quedara así.



Ahora moveremos cada entrada que hemos creado a un grupo, esto lo haremos haciendo click derecho sobre la entrada y seleccionamos la opción edit entry y seleccionamos el grupo donde lo queramos mover, en este caso la entrada correo al grupo correo despues de esta tendremos que mover las demás a su grupo.

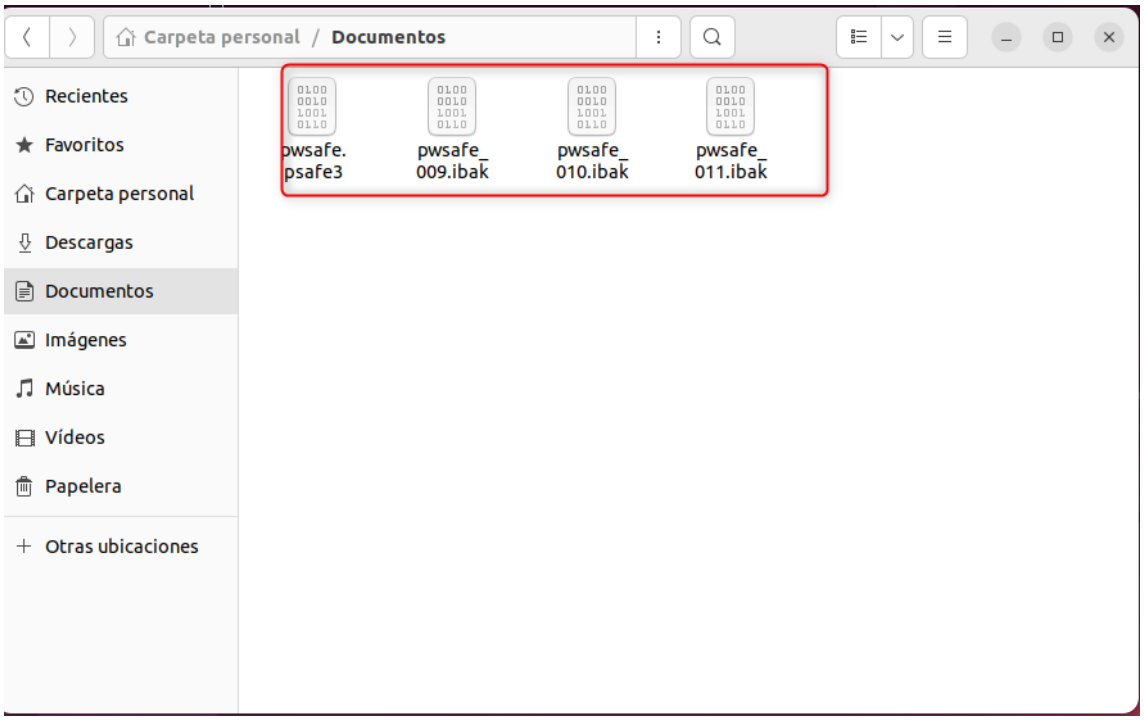


Una vez movidas todas las entradas nos quedara así, wifi dentro del grupo conexión, correo dentro del grupo correo y ssh dentro del grupo remoto.



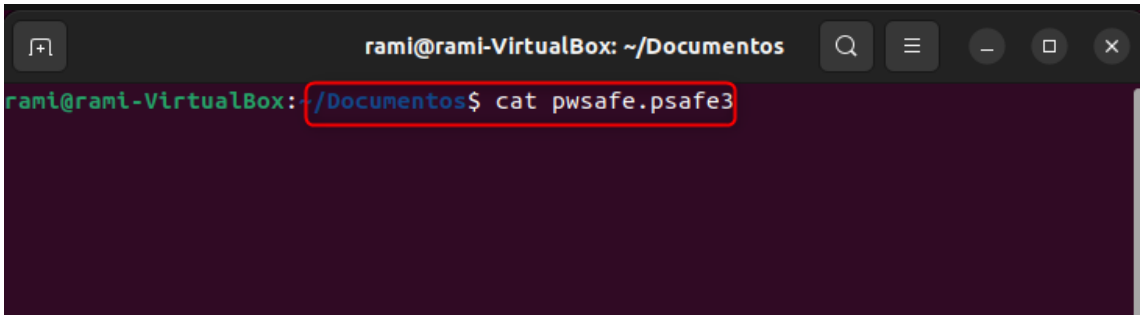
4.Localizar archivos

Los archivos se localizan en la carpeta de documentos



5.Verificar cifrado

En este paso vamos a confirmar que están cifrados y que el archivo es ilegible, para comprobarlo nos movemos a la carpeta de documento que es donde esta el archivo y hacemos un cat pwsafe.psafe3

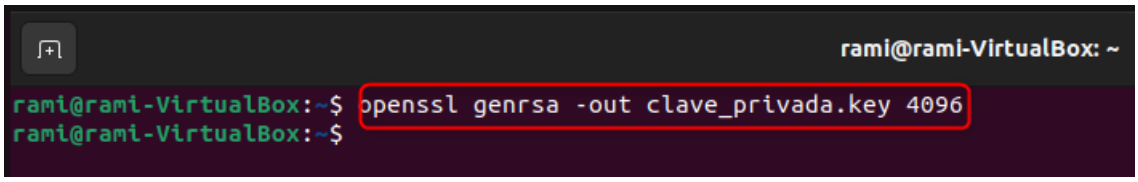


Al ejecutar el comando el archivo no nos saldrá en texto plano.

1. Generación y verificación de certificados X.509

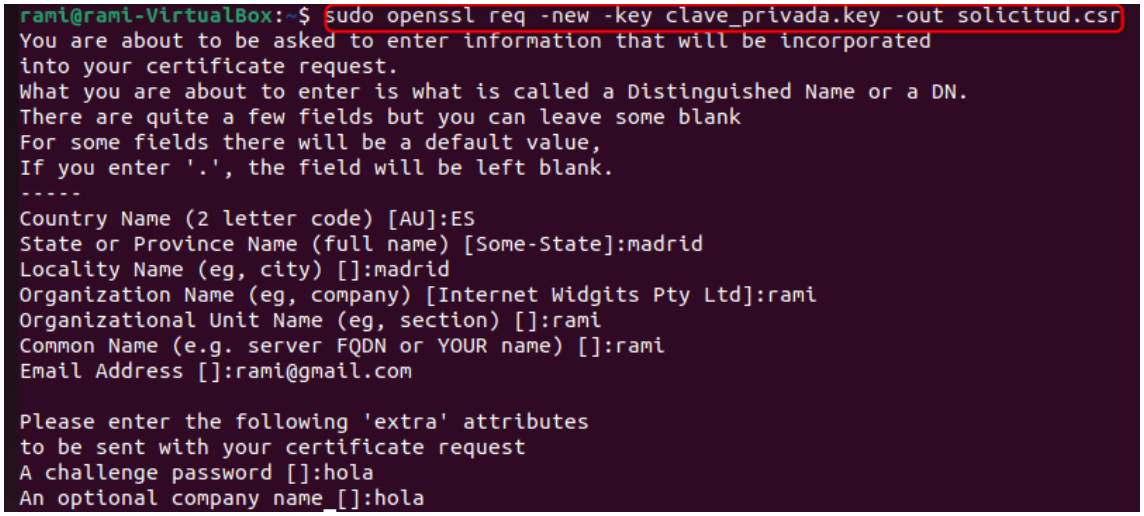
1.Generar clave privada

Primero habrá que generar la clave privada con el comando openssl genrsa -out clave_privada.key 4096.



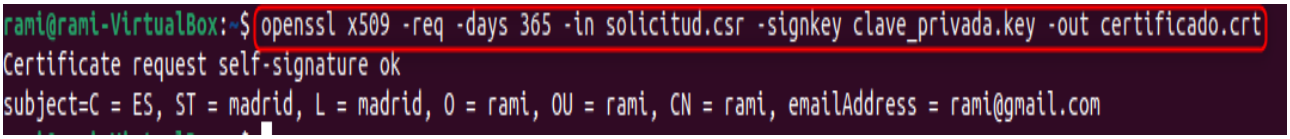
2.Crear CSR

Ahora introduciremos en la clave privada los campos identificativos con el comando openssl req -new -key clave_privada.key -out solicitud.csr.



3.Emitir certificado

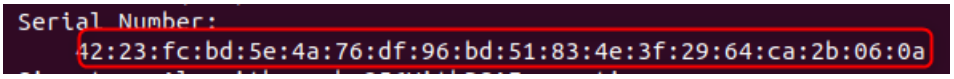
El próximo paso será emitir el certificado esto se hace con el comando openssl x509 -req -days 365 -in solicitud.csr -signkey clave_privada.key -out certificado.crt.



4.Ver contenido del certificado

Ahora veremos el contenido de certificado con el comando openssl x509 -in certificado.crt -text -noout.

• Número de serie

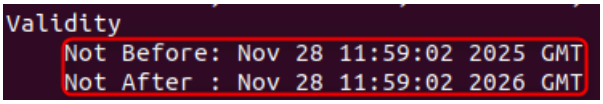


• Emisor

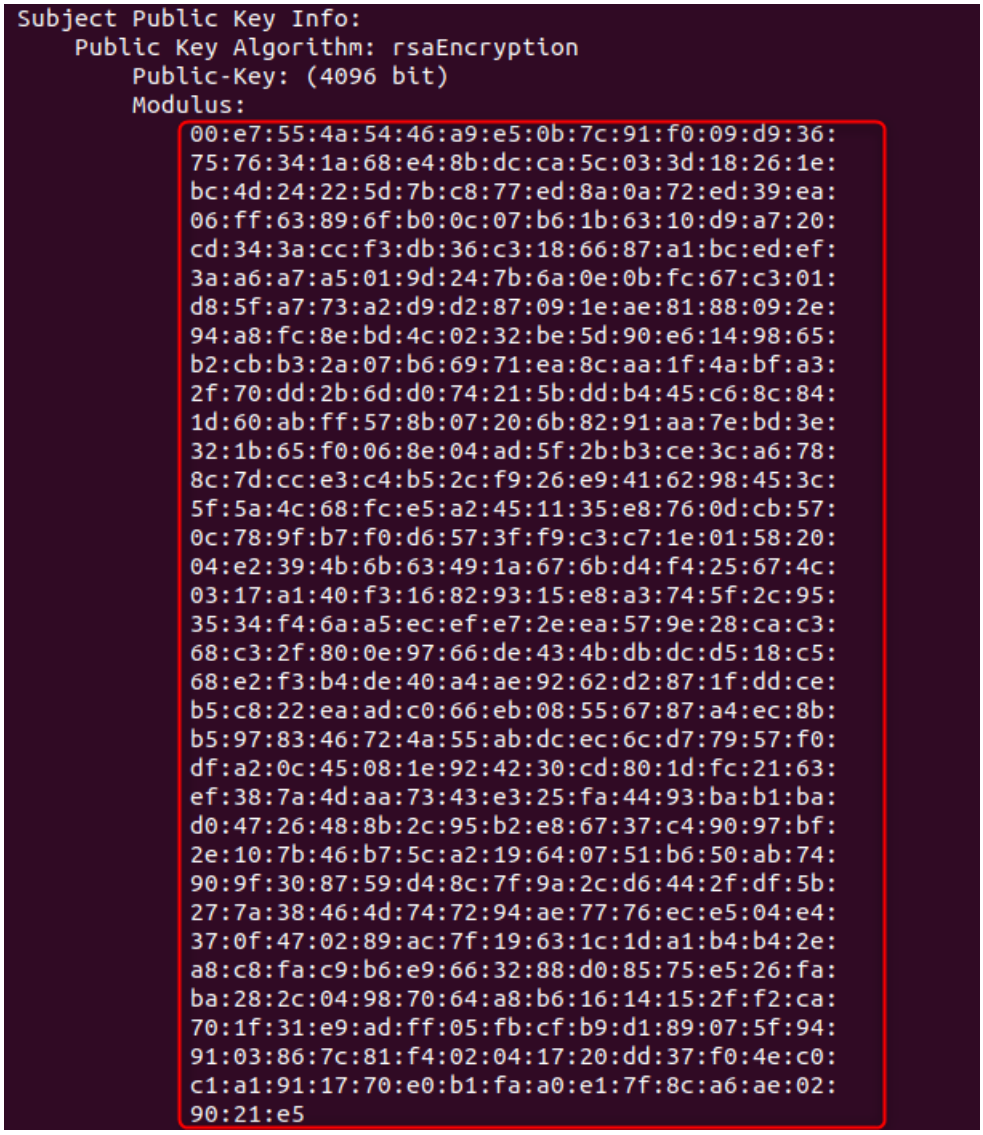
Indica por quien fue emitido el certificado también podemos ver el sujeto

• Validez (notBefore/notAfter)

Esto indica la validez del certificado.



• Clave pública

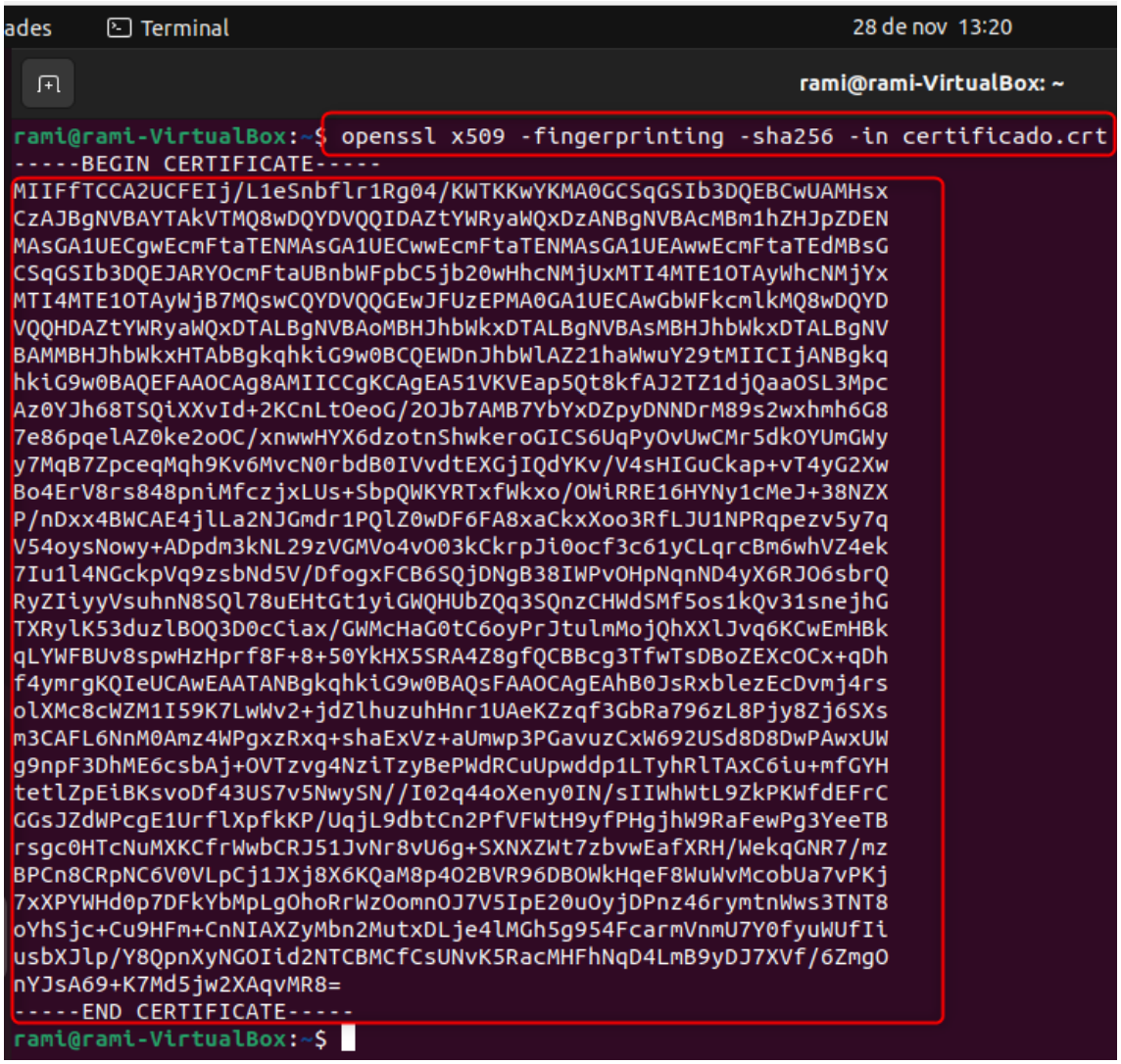


• Extensiones (EKU, SAN)

Las extensiones EKU y SAN son componentes de los certificados digitales X.509 que añaden información específica sobre cómo puede usarse el certificado y a qué entidades está asociado

5. ver la huella del hash

Por último, vamos a ver el hash del certificado para verificar su integridad esto lo hacemos con el comando openssl x509 -fingerprint -sha256 -in certificado.crt.



Universidad Francisco de Vitoria
Centro de Documentación Europea
UFV Madrid

RAMIREZ LOPEZ HECTOR - 53858461M

Firmado digitalmente por RAMIREZ LOPEZ HECTOR - 53858461M
Fecha: 2025.11.28 13:25:39 +01'00'