



**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

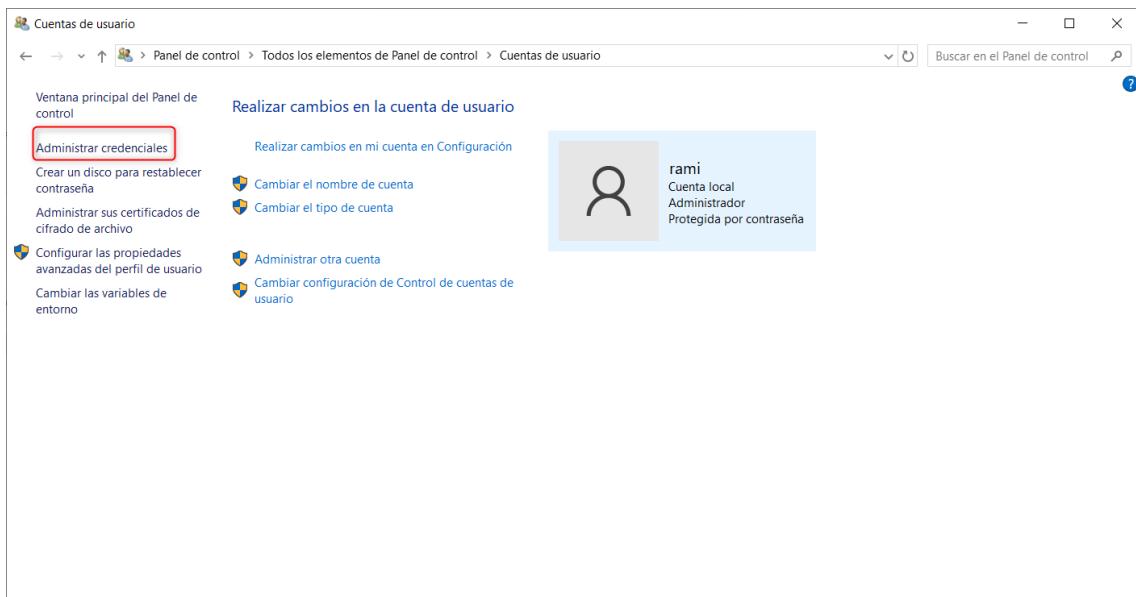
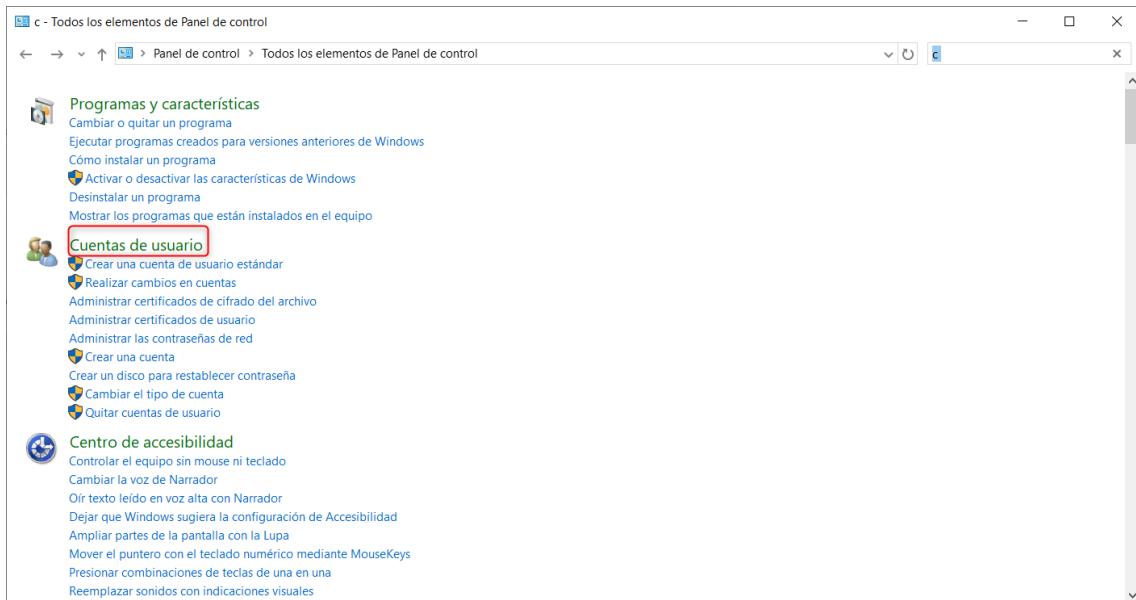
Contenido

1- Gestión de credenciales en Windows	3
1.1. Acceso al almacén	3
2- Crear una credencial	5
2.1 Ver y documentar	6
3.Eliminar credencial.....	7
4.Realizar copia de seguridad	8
5.Reflexión	10
1.Gestión de credenciales en Linux	11
1.1Instalación de PasswordSafe	11
2.Crear archivo .psafe3	12
3.Crear entradas.....	14
4.Localizar archivos	18
5.Verificar cifrado.....	19
1. Generación y verificación de certificados X.509	20
1.Generar clave privada.....	20
2.Crear CSR	20
3.Emitir certificado	21
4.Ver contenido del certificado	21
5. ver la huella del hash	23

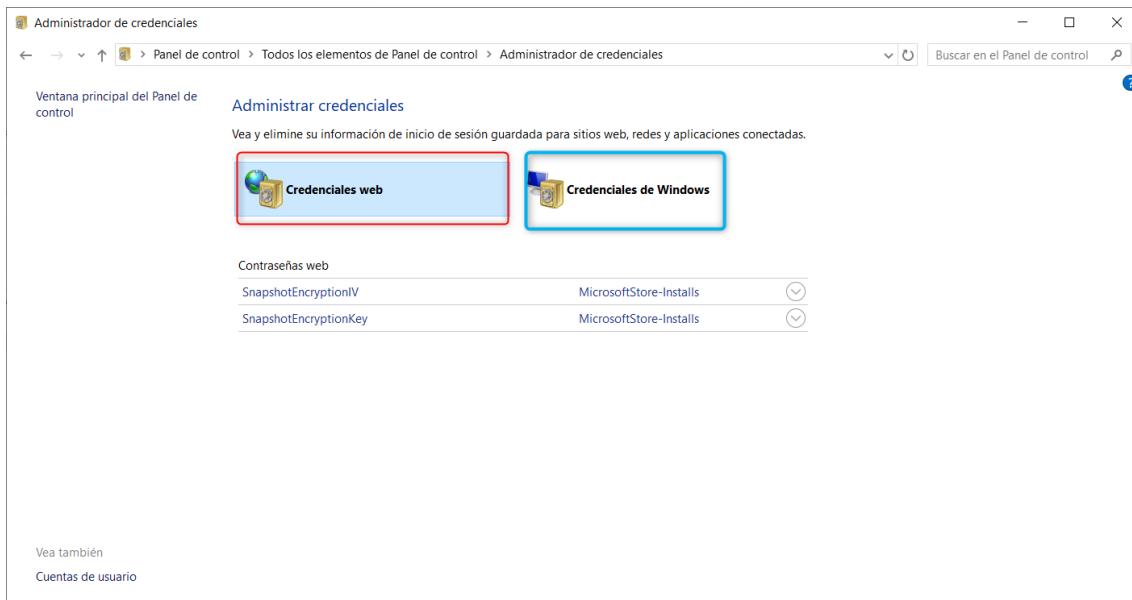
1-Gestión de credenciales en Windows

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.

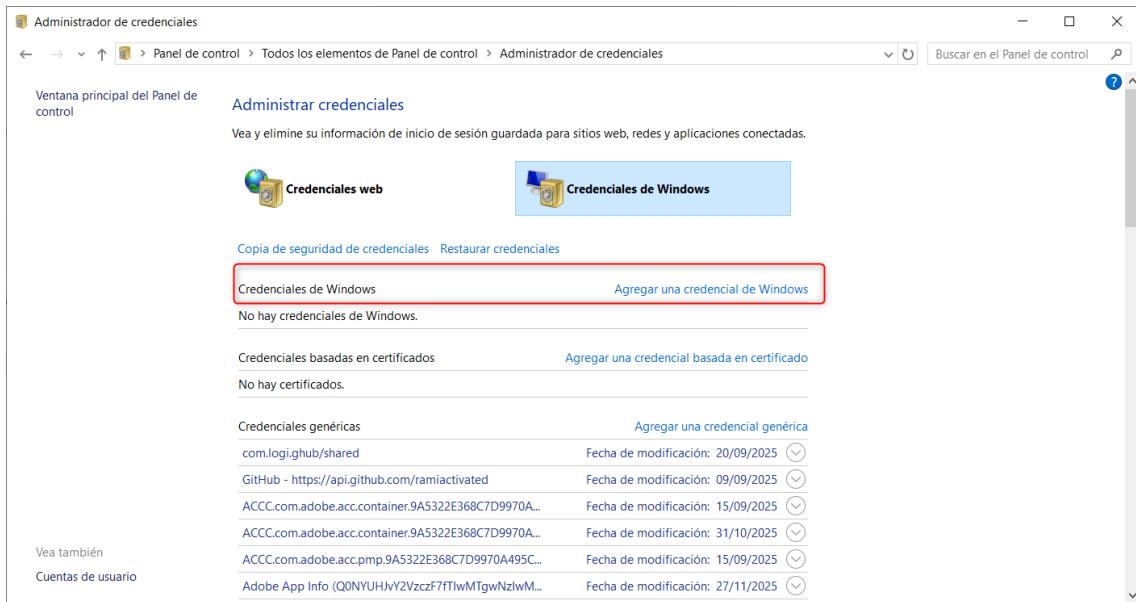


Aquí dentro encontraremos las credenciales web y las de Windows, las credenciales web son claves que Windows almacena para iniciar sesión automáticamente en sitios web o servicios en línea por ejemplo páginas web de Edge o servicios de Microsoft como OneDrive, las de Windows se utilizan para autenticarse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

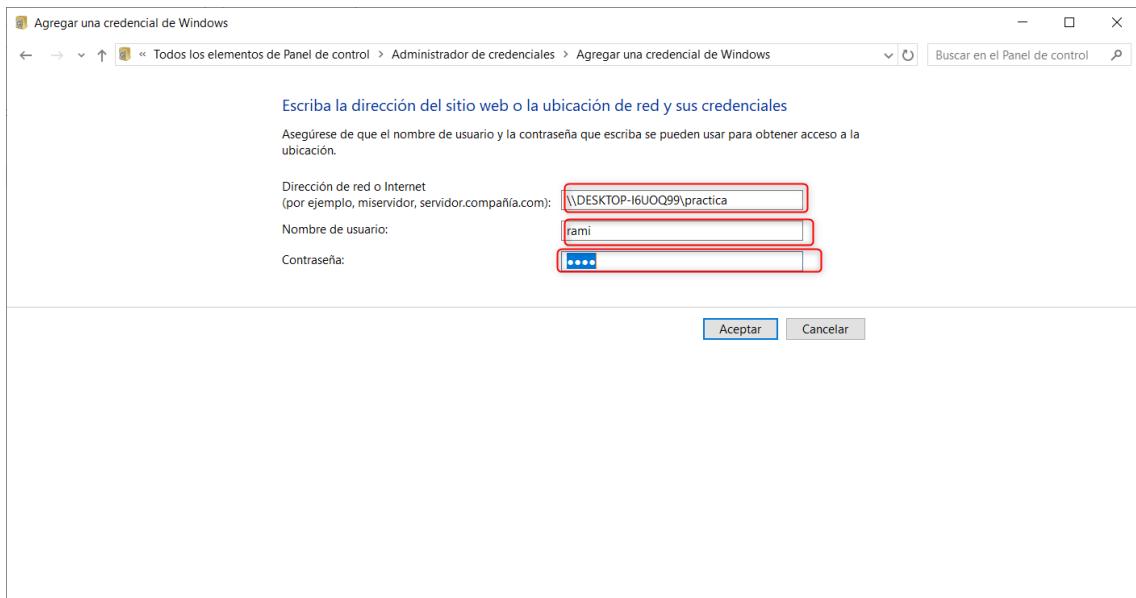


2-Crear una credencial

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

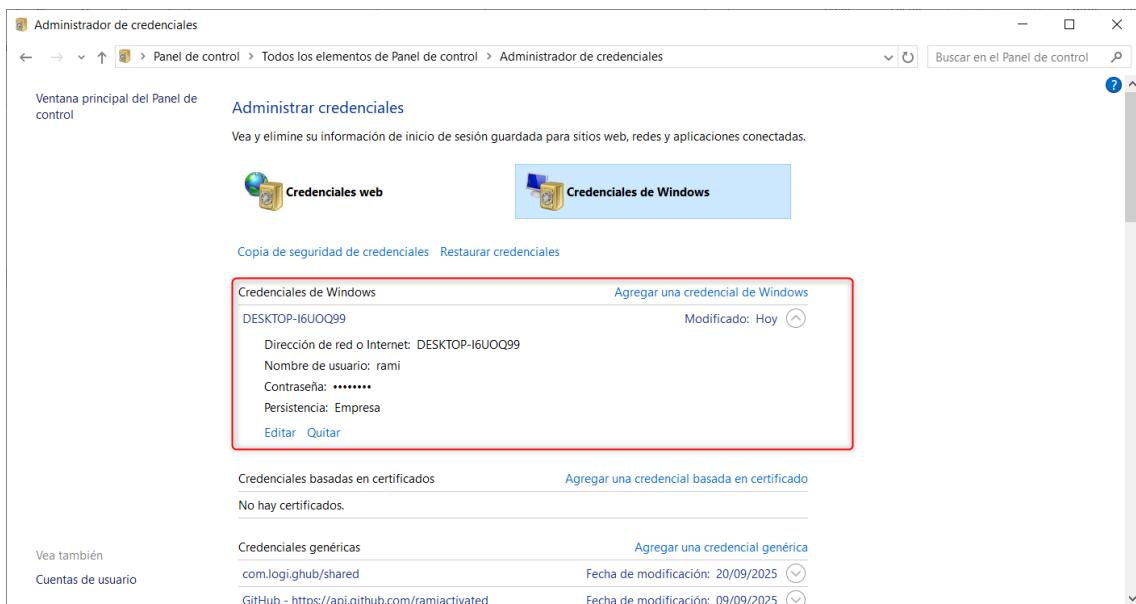
Después de crear la credencial en credenciales de windows, aparece la credencial con los siguientes datos:

Direccion de red: DESKTOP-I6UOQ99

Nombre de usuario: rami

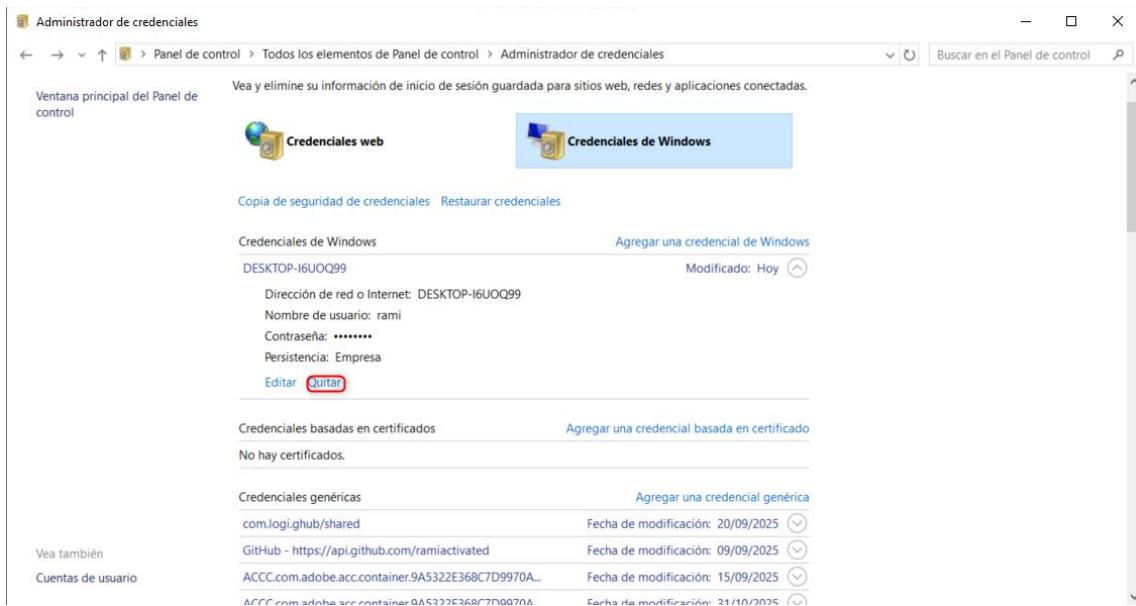
Modificado: hoy

Tipo: Credencial de Windows



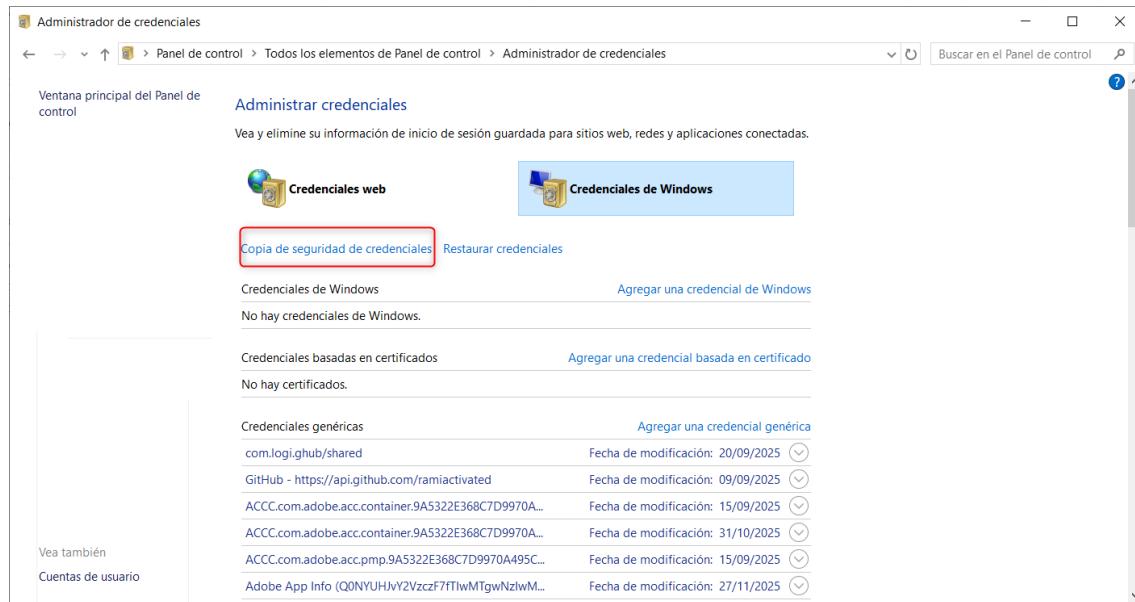
3. Eliminar credencial

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.

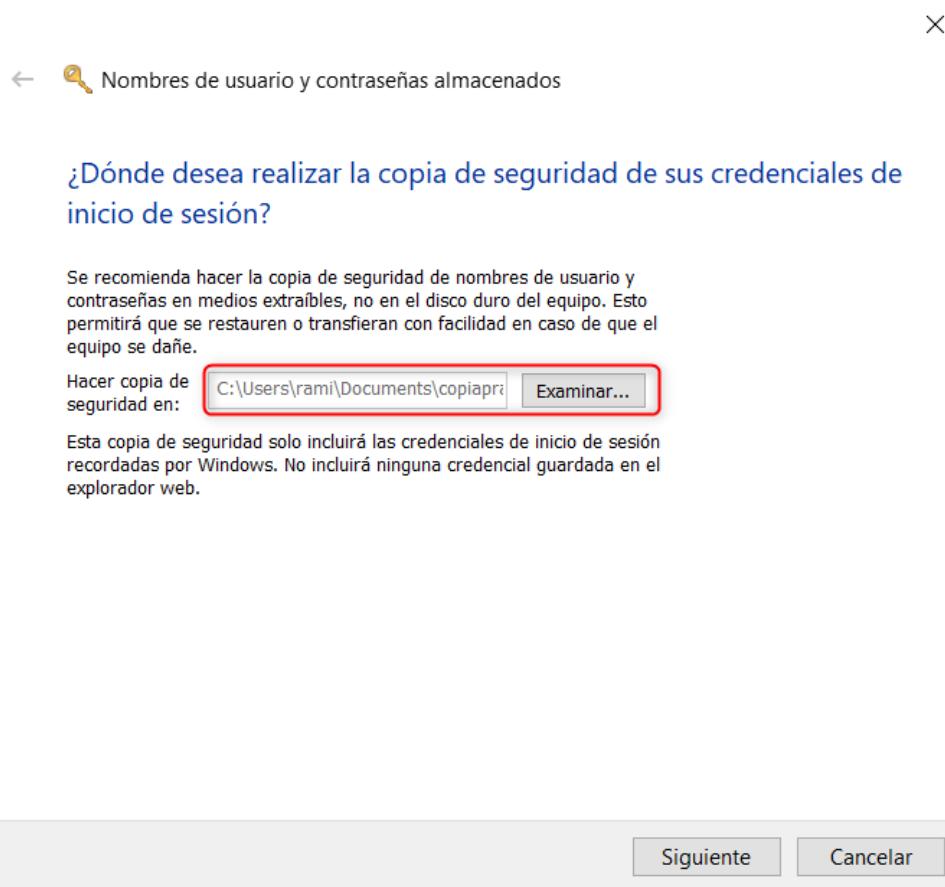


4. Realizar copia de seguridad

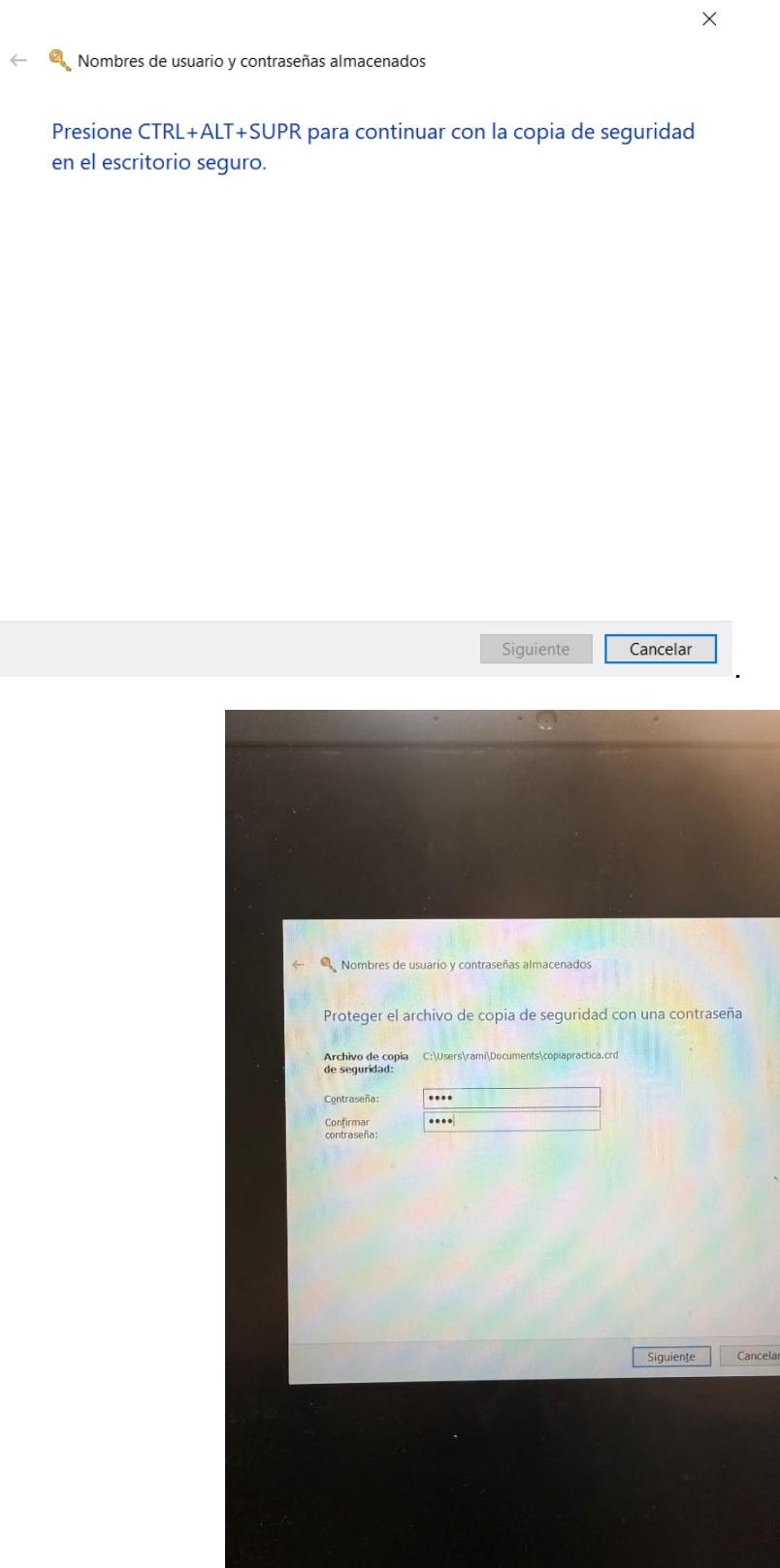
Para este paso seleccionaremos la opción de copia de seguridad de credenciales.



Se nos abrirá el asistente de copias de seguridad y seleccionaremos la ruta 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 ransomware con permiso de admin lo que cifraría toda la información.

1. Gestión de credenciales en Linux

1.1 Instalación de PasswordSafe

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

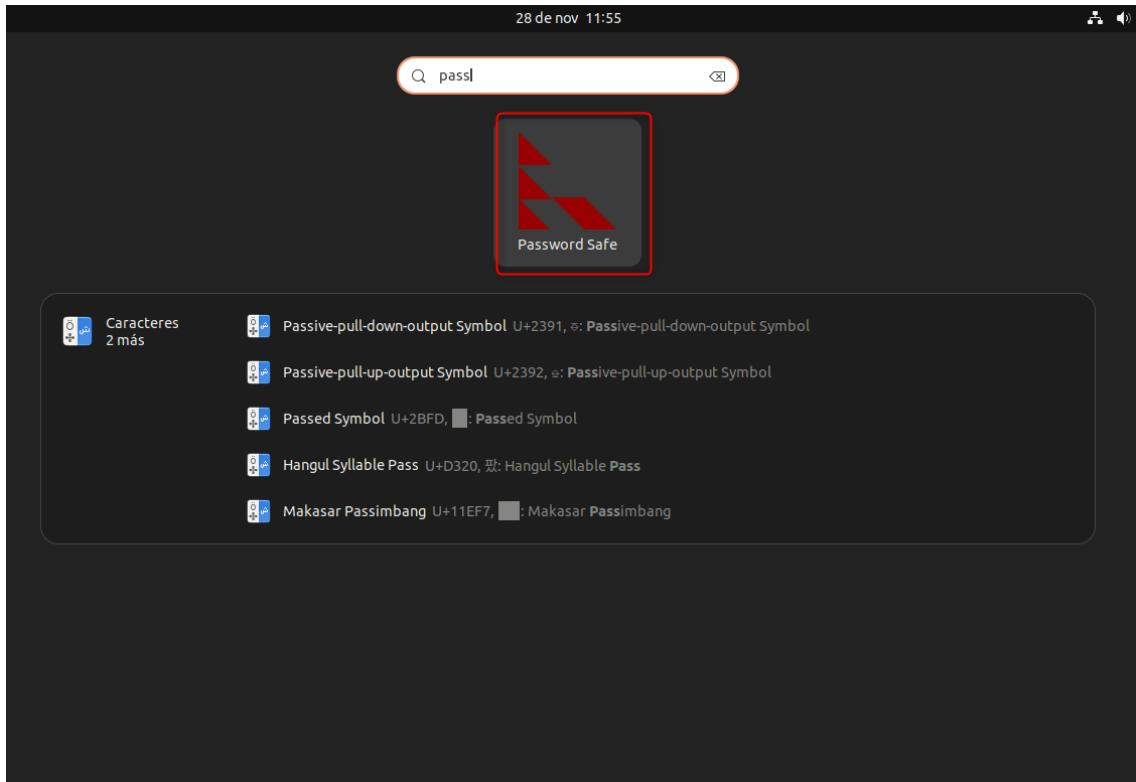
```
rami@rami-VirtualBox:~$ sudo apt update
[sudo] contraseña para rami:
Obj:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Obj:2 http://es.archive.ubuntu.com/ubuntu jammy InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu jammy-updates InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu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

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

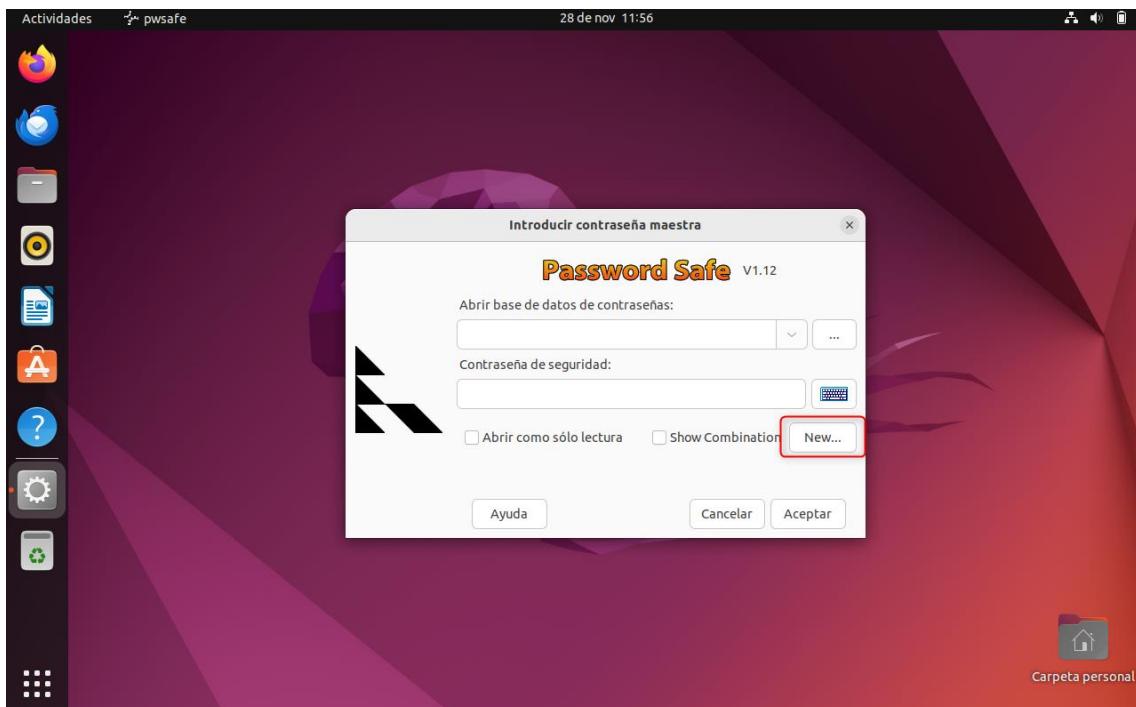
```
rami@rami-VirtualBox:~$ sudo apt install passwordsafe
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libqrencode4 libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5 libxerces-c3.2
  libykpers-1-1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

2.Crear archivo .psafe3

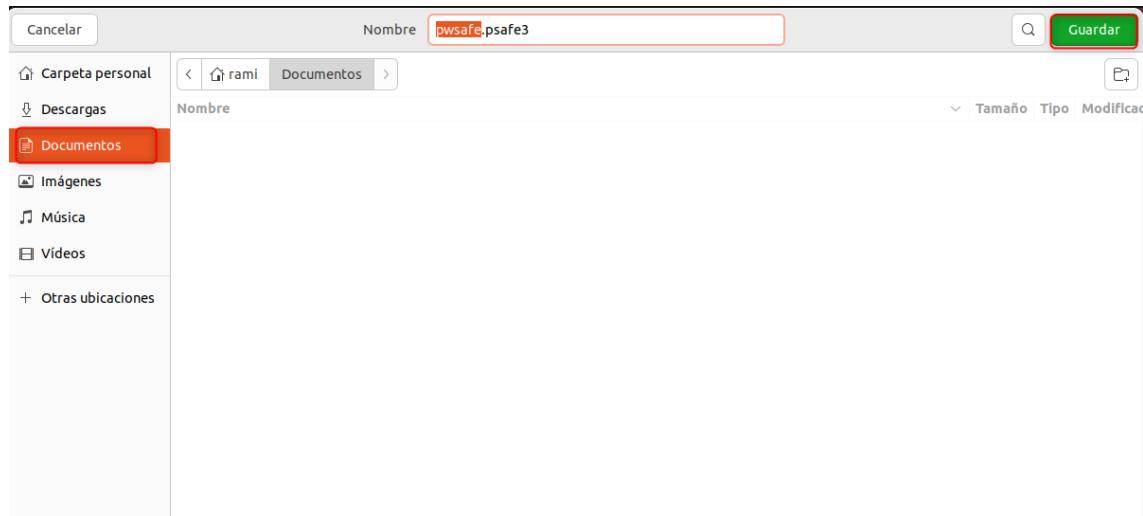
Abrimos passwordsafe



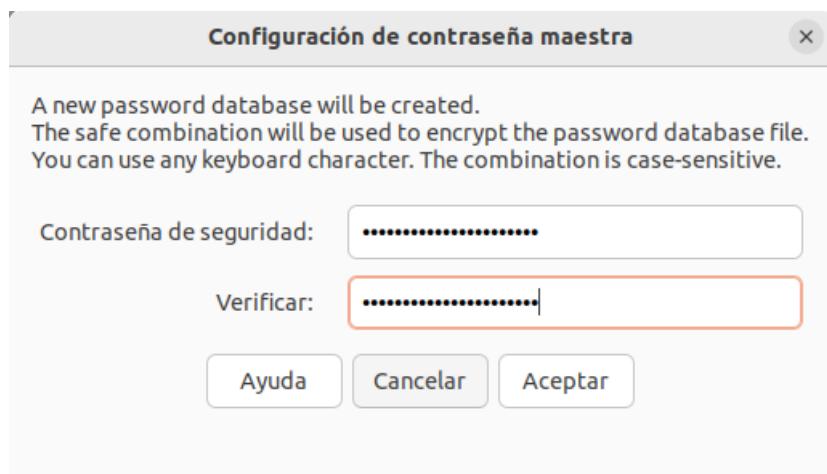
Ahora le daremos a la opción de new para crear el archivo.



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

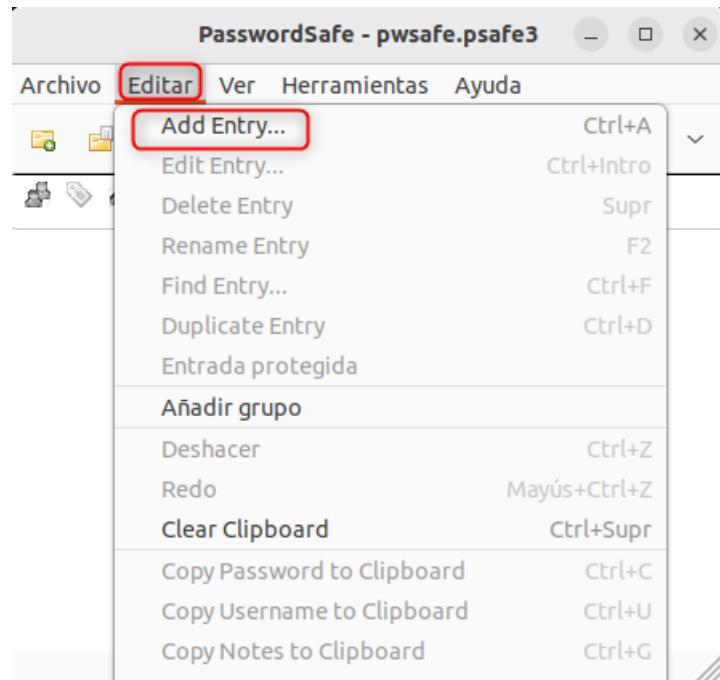


Ahora nos pedirá configurar una contraseña para el archivo, la introducimos y le damos a aceptar. La herramienta no me indica debilidad de contraseña.

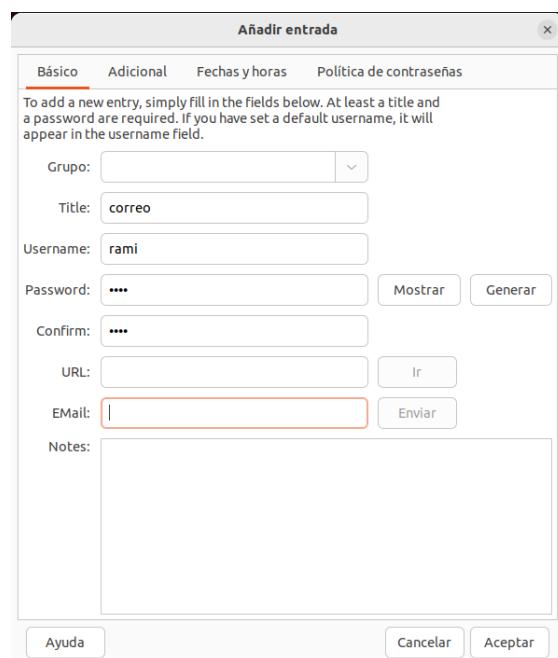


3.Crear entradas

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

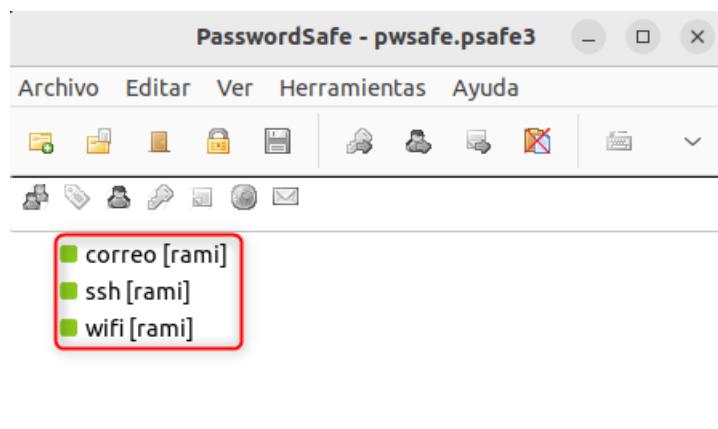


Se nos abrirá la pestaña para crear la entrada, creamos 3 entradas distintas.

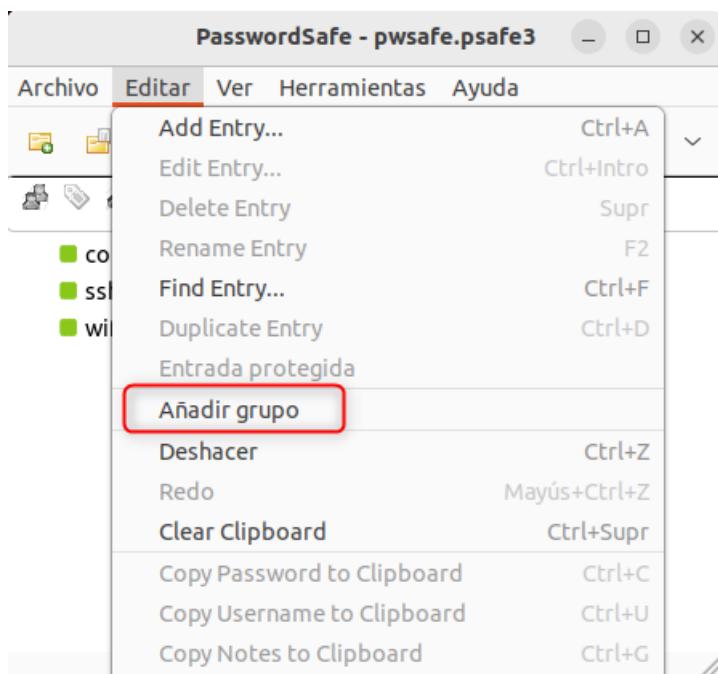


Básico	Adicional	Fechas y horas	Política de contraseñas
To add a new entry, simply fill in the fields below. At least a title and a password are required. If you have set a default username, it will appear in the username field.			
Grupo:			
Title:	correo		
Username:	rami		
Password:	****	Mostrar	Generar
Confirm:	****		
URL:		Ir	
EMail:			Enviar
Notes:			
<input type="button" value="Ayuda"/> <input type="button" value="Cancelar"/> <input type="button" value="Aceptar"/>			

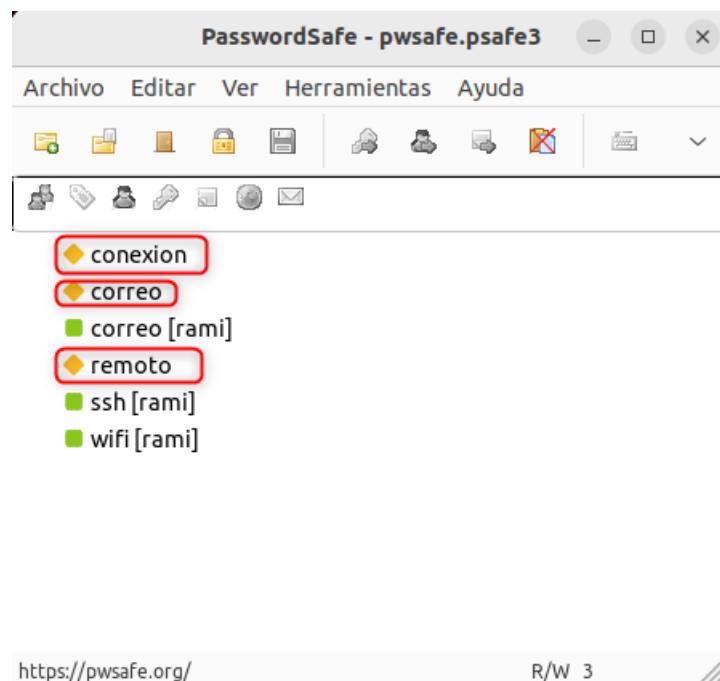
Cuando las hayamos creado no quedara así.



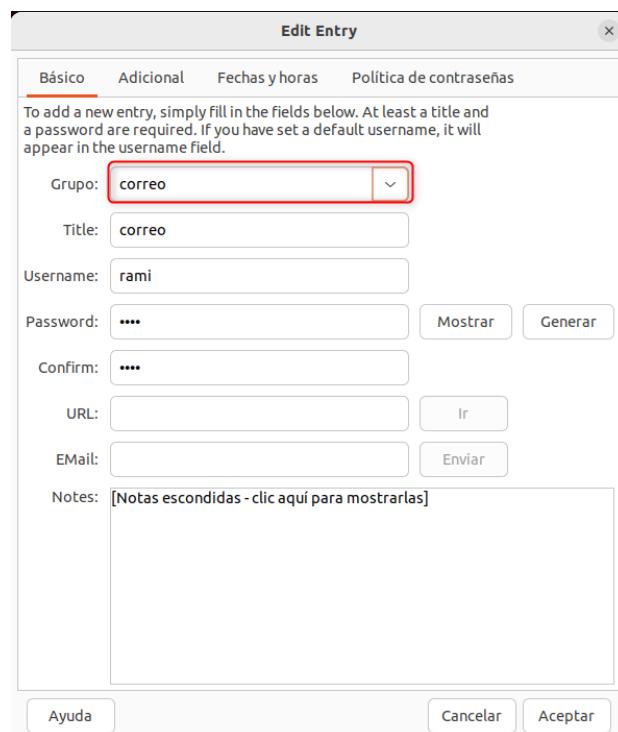
Ahora vamos a clasificarlas por grupo para ello nos vamos a la opción editar y añadir grupo.



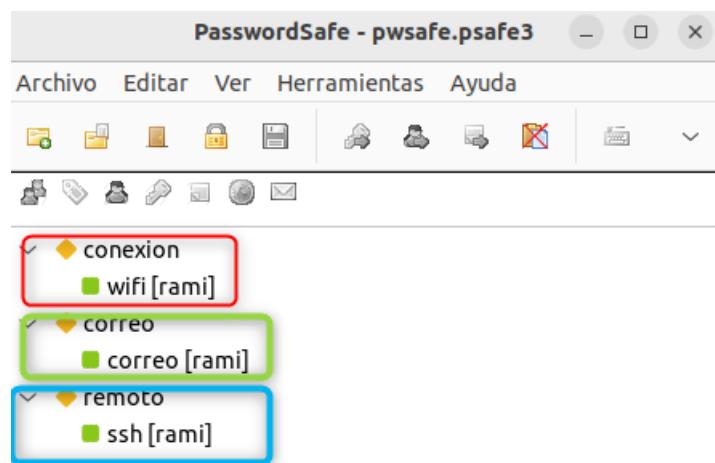
Vamos a crear 3 grupos una vez creados nos quedara así.



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.

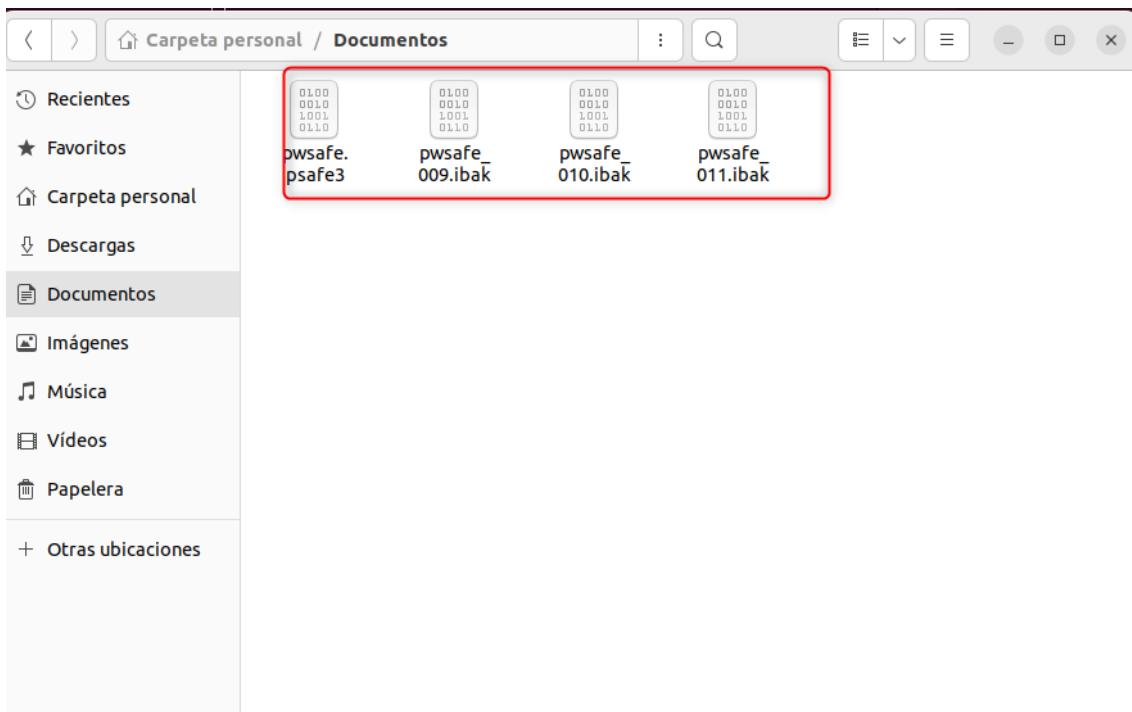


Una vez movidas todas las entradas nos quedara así, wifi dentro del grupo conexión, correo dentro del grupo correo y ssh dentro del grupo remoto.



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

```
rami@rami-VirtualBox: ~/Documentos
```

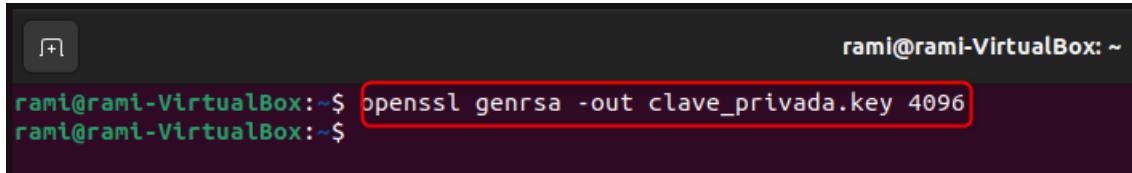
Al ejecutar el comando el archivo no nos saldrá en texto plano.

```
|%ud$++M++5{++W++++^+++++bX++s|3g+V]++*++{++++A+z}H;++B++++^v+n++p#++}++[  
++==+cAu+>q+S +Z+t++)<>@yN+0+^++2A++b++V>+++j+W+)++g+X!++&E++  
>sL+x?(+_)+Z+"++  
>Q++>++++hY+P++_+P^+Tq+++++++=++C+++$+ll(4+b?++K++b+J+0RL\+We+=+++++( ;+0+=+,+y+  
+C++++~%7++&++Eh+ B++A++l++^U'++To"+&+B)]m++++%++t?++C+++++ +Hl+1+G:+:b=+  
++q+ "+#/++d+a+N+EQ++++l+++++u+@+z+E++<+u$+n+K++X+n+S/l++++8+$++y+\++T+++.+E0調 9VQ  
>vd++$+{u+++'k+v+j9+`)}++@Ff+qhy++++4++-+/+獮K+^Vo+++/+5/X  
>+d++f++&+|lV+-h;+p++++(++E++<i+o+u+M+E*X  
+)+|++,+  
+R+ | +p#++++++f [ +w+^@+3++찰 , +P+P  
+M+9]+8+V+^3++g+D+f+U+1+2++6\+L(OA+)/x+  
+!+Z+_.+S+u+?+;3SDr++LG+n++VF+y+`3+J+j++{+@++  
+PWS3-E0FPWS3-E0F+6++7++  
'\c++Y~z++H++a++:++H>+rami@rami-VirtualBox:~/Documentos$
```

1. Generación y verificación de certificados X.509

1. Generar clave privada

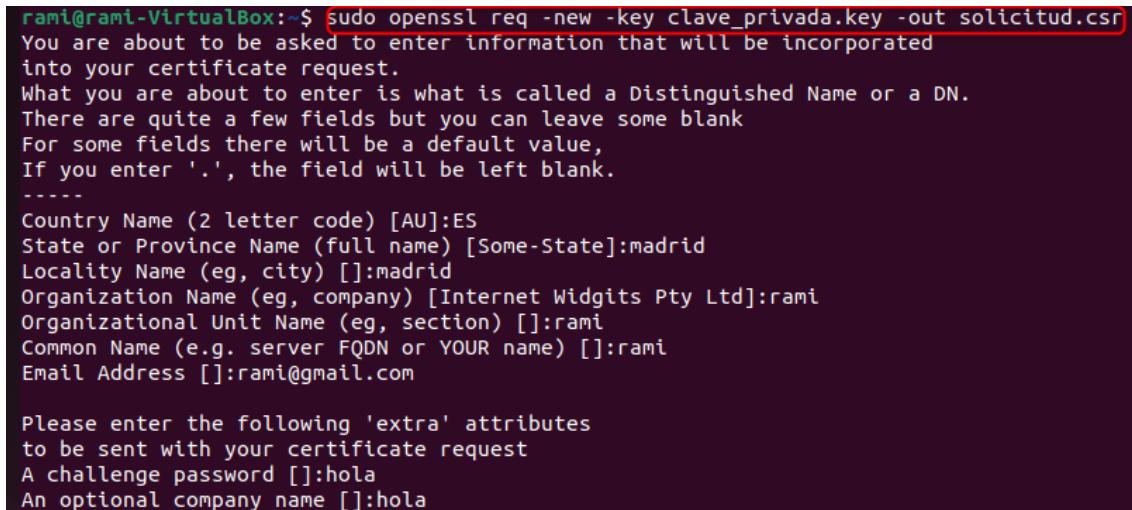
Primero habrá que generar la clave privada con el comando openssl genrsa -out clave_privada.key 4096.



```
rami@rami-VirtualBox:~$ openssl genrsa -out clave_privada.key 4096
rami@rami-VirtualBox:~$
```

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.



```
rami@rami-VirtualBox:~$ sudo openssl req -new -key clave_privada.key -out solicitud csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:madrid
Locality Name (eg, city) []:rami
Organization Name (eg, company) [Internet Widgits Pty Ltd]:rami
Organizational Unit Name (eg, section) []:rami
Common Name (e.g. server FQDN or YOUR name) []:rami
Email Address []:rami@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:hola
An optional company name []:hola
```

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.

```
rami@rami-VirtualBox:~$ openssl x509 -req -days 365 -in solicitud.csr -signkey clave_privada.key -out certificado.crt
Certificate request self-signature ok
subject=C = ES, ST = madrid, L = madrid, O = rami, OU = rami, CN = rami, emailAddress = rami@gmail.com
```

4.Ver contenido del certificado

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

- Número de serie

```
Serial Number:
42:23:fc:bd:5e:4a:76:df:96:bd:51:83:4e:3f:29:64:ca:2b:06:0a
```

- Emisor

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

```
Issuer: C = ES, ST = madrid, L = madrid, O = rami, OU = rami, CN = rami, emailAddress = rami@gmail.com
Validity
```

- Validez (notBefore/notAfter)

Esto indica la validez del certificado.

```
Validity
Not Before: Nov 28 11:59:02 2025 GMT
Not After : Nov 28 11:59:02 2026 GMT
```

- Clave pública

```
Subject Public Key Info:  
    Public Key Algorithm: rsaEncryption  
        Public-Key: (4096 bit)  
            Modulus:  
                00:e7:55:4a:54:46:a9:e5:0b:7c:91:f0:09:d9:36:  
                75:76:34:1a:68:e4:8b:dc:ca:5c:03:3d:18:26:1e:  
                bc:4d:24:22:5d:7b:c8:77:ed:8a:0a:72:ed:39:ea:  
                06:ff:63:89:6f:b0:0c:07:b6:1b:63:10:d9:a7:20:  
                cd:34:3a:cc:f3:db:36:c3:18:66:87:a1:bc:ed:ef:  
                3a:a6:a7:a5:01:9d:24:7b:6a:0e:0b:fc:67:c3:01:  
                d8:5f:a7:73:a2:d9:d2:87:09:1e:ae:81:88:09:2e:  
                94:a8:fc:8e:bd:4c:02:32:be:5d:90:e6:14:98:65:  
                b2:cb:b3:2a:07:b6:69:71:ea:8c:aa:1f:4a:bf:a3:  
                2f:70:dd:2b:6d:d0:74:21:5b:dd:b4:45:c6:8c:84:  
                1d:60:ab:ff:57:8b:07:20:6b:82:91:aa:7e:bd:3e:  
                32:1b:65:f0:06:8e:04:ad:5f:2b:b3:ce:3c:a6:78:  
                8c:7d:cc:e3:c4:b5:2c:f9:26:e9:41:62:98:45:3c:  
                5f:5a:4c:68:fc:e5:a2:45:11:35:e8:76:0d:cb:57:  
                0c:78:9f:b7:f0:d6:57:3f:f9:c3:c7:1e:01:58:20:  
                04:e2:39:4b:6b:63:49:1a:67:6b:d4:f4:25:67:4c:  
                03:17:a1:40:f3:16:82:93:15:e8:a3:74:5f:2c:95:  
                35:34:f4:6a:a5:ec:ef:e7:2e:ea:57:9e:28:ca:c3:  
                68:c3:2f:80:0e:97:66:de:43:4b:db:dc:d5:18:c5:  
                68:e2:f3:b4:de:40:a4:ae:92:62:d2:87:1f:dd:ce:  
                b5:c8:22:ea:ad:c0:66:eb:08:55:67:87:a4:ec:8b:  
                b5:97:83:46:72:4a:55:ab:dc:ec:6c:d7:79:57:f0:  
                df:a2:0c:45:08:1e:92:42:30:cd:80:1d:fc:21:63:  
                ef:38:7a:4d:aa:73:43:e3:25:fa:44:93:ba:b1:ba:  
                d0:47:26:48:8b:2c:95:b2:e8:67:37:c4:90:97:bf:  
                2e:10:7b:46:b7:5c:a2:19:64:07:51:b6:50:ab:74:  
                90:9f:30:87:59:d4:8c:7f:9a:2c:d6:44:2f:df:5b:  
                27:7a:38:46:4d:74:72:94:ae:77:76:ec:e5:04:e4:  
                37:0f:47:02:89:ac:7f:19:63:1c:1d:a1:b4:b4:2e:  
                a8:c8:fa:c9:b6:e9:66:32:88:d0:85:75:e5:26:fa:  
                ba:28:2c:04:98:70:64:a8:b6:16:14:15:2f:f2:ca:  
                70:1f:31:e9:ad:ff:05:fb:cf:b9:d1:89:07:5f:94:  
                91:03:86:7c:81:f4:02:04:17:20:dd:37:f0:4e:c0:  
                c1:a1:91:17:70:e0:b1:fa:a0:e1:7f:8c:a6:ae:02:  
                90:21:e5
```

- 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.

```
ades  [-] Terminal 28 de nov 13:20
[+] rami@rami-VirtualBox: ~
[+] rami@rami-VirtualBox:~$ openssl x509 -fingerprinting -sha256 -in certificado.crt
-----BEGIN CERTIFICATE-----
MIIFFTCCA2UCFEIj/L1eSnbflr1Rg04/KWTKKwYKMA0GCSqGSIB3DQEBCwUAMHsxCzAJBgNVBAYTAKVTMQ8wDQYDVQQIDAZtYWRYaWQxDzANBgNVBAcMBm1hZHJpZDENMAsgA1UECgwEcMftaTENMAsgA1UECwwEcMftaTENMAsgA1UEAwEcMftaTEdMBsGCSqGSIB3DQEJARYOcmftaUBnbWFpbC5jb20wHhcNMjUxMTI4MTE10TAyWhcNMjYXMTI4MTE10TAyWjB7MQswCQYDVQQGEwJFUzEPMA0GA1UECAwGbWFkcmIkMQ8wDQYDVQQHDAZtYWRYaWQxDTALBgNVBAoMBHJhbWkxDTALBgNVBAwvMBHJhbWkxDTALBgNVBAMMBHJhbWkxHTAbBqkqhkiG9w0BCQEWnJhbWlAZ21haWwuY29tMIICIjANBgkqhkiG9w0BAQEFAAOAg8AMIICgKCAGEA51VKVEap5Qt8kfAJ2TZ1djQaaOSL3MpcAz0Yjh68TSQiXXvId+2KCnLt0eoG/20jb7AMB7ybYxDzpyDNNDrM89s2wxhmh6G87e86pqelAZ0ke2oOC/xnwwHYX6dzotnShwker0GICS6UqPy0vUwCMr5dk0YUmGwy7Mqb7ZpcceqMqh9Kv6MvcN0rbdB0IVvdtEXGjIQdYKv/V4sHIGuCkap+vT4yG2XwBo4ErV8rs848pnimfczjxLus+SbpQWKYRTxfWkxo/OWiRRE16HYNy1cMeJ+38NZXP/nDxx4BWCAE4jllLa2NjGmdr1PqlZ0wDF6FA8xaCkxXoo3RfLJU1NPRqpezv5y7qV54oysNowy+ADpdm3kNL29zVGMVo4v003kCkrpJi0ocf3c61yCLqrcBm6whVZ4ek7Iu1l4NGckpVq9zsbd5V/DfogxFcb6sqjDNgb38IWpvoHPnqnND4yX6Rj06sbrQRyZIiyyVsuhnN8Sql78uEhtGt1yiGWQHubZQq3SqnzCHWdSMf5os1kQv31snejhgTXRylK53duzlB0Q3D0cCiay/GWMcHaG0tC6oyPrJtulmMojqhXXlJvq6KCwEmHBkqLYWFBuv8spwHzHprf8F+8+50YkHX5SRA4Z8gfQCBBcg3TfwTsDBoZEcxOCx+qDhf4ymrgKQIEUCAwEAATANBgkqhkiG9w0BAQsFAAOAgEAhB0JsRxblezEcDvmj4rsolXMc8cWZM1I59K7LwWv2+jdZlhuzuhHnr1UAeKZqf3GbRa796zL8Pjy8Zj6SXsm3CAF6NnM0Amz4WPgxzRxq+shaExVz+aUmwP3PGavuzCxW692USD8D8DwPAwxUWg9npF3DhME6csbAj+0VTzvg4NziTzyBePWDRCuUpwddp1LTyhRlTAxC6iu+mfGYHtetlZpEiBKsvoDf43US7v5NwySN//I02q44oXeny0IN/sIIWhWtL9ZkPKWfdEFrcGGsJZdWPcgE1UrflXpfkKP/UqjL9dbtCn2PfVFWtH9yfPHgjhW9RaFewPg3YeeTBrsqc0HTcNuMXKCfrWwbCRJ51JvNr8vU6g+SXNXZwt7zbvwEafXRH/WekqGNR7/mzBPCn8CRpNC6V0VLpCj1JXj8X6KQaM8p402BVR96DB0WkHqeF8WuWvMcobUa7vPKj7xXPYWHd0p7DFkYbMpLg0hoRrWz0omn0J7V5IpE20u0yjDPnz46rymtnw3TNT8oYhSjc+Cu9HFm+CnNIAXZyMbn2MutxDLje4lMGh5g954FcarmVnmU7Y0fyuWUfIiusbXJlp/Y8QpnXyNGOIid2NTCBMCfCsUNvK5RacMHFhNqD4Lmb9yDJ7XVF/6Zmg0nYjsA69+k7Md5jw2XAqvMR8=
-----END CERTIFICATE-----
[+] rami@rami-VirtualBox:~$
```



Universidad
Francisco de
Vitoria
*Centro de
Documentación
Europea*
UFV Madrid