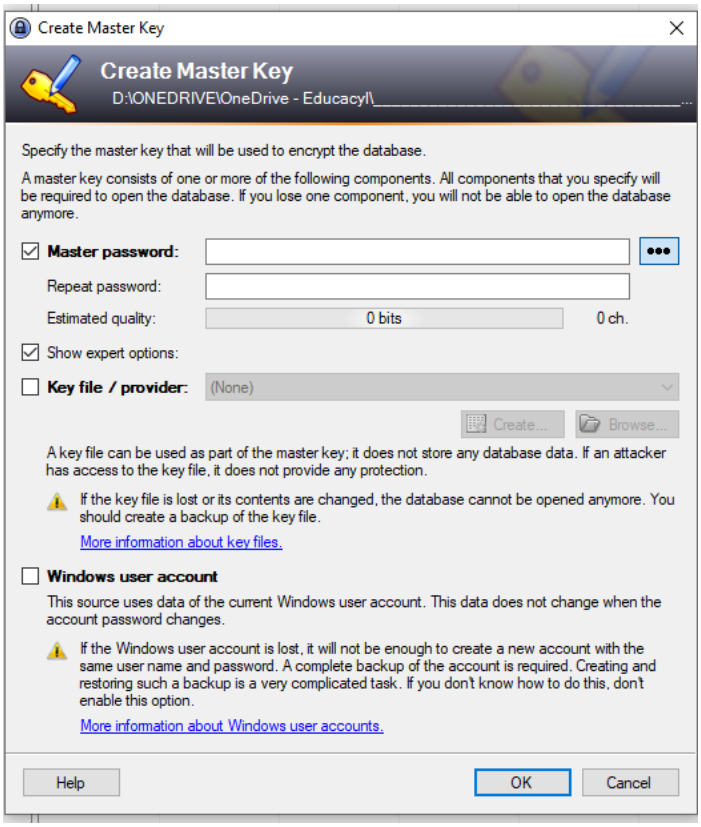
SEMINARIO TIC

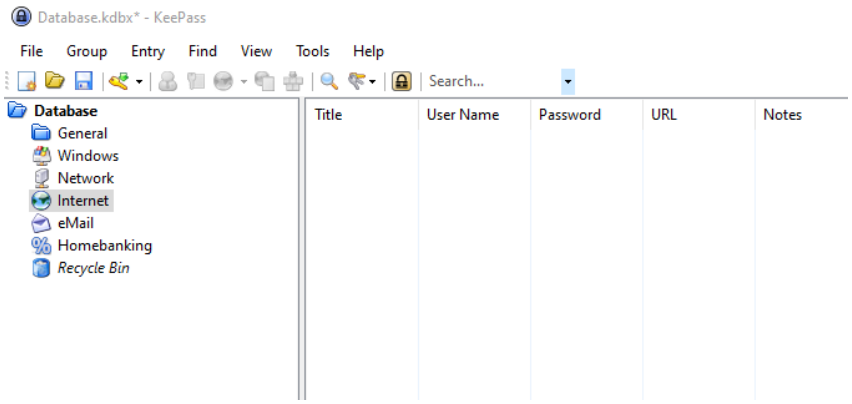
ANEXO SESION 4: GESTORES DE CONTRASEÑAS GRATUITOS

GESTORES DE CONTRASEÑAS PARA PC (WINDOWS)

KeePass: Es un programa gratuito para PC que nos permite guardar en un archivo encriptado todas nuestras contraseñas. Una vez instalado el programa tendremos que decirle dónde queremos guardar ese archivo de contraseñas: **Database.kdbx**



Puesto que es un archivo encriptado, podemos guardarlo en nuestra nube de OneDrive para poder importarlo después desde las aplicaciones móviles y sincronizar los contenidos.



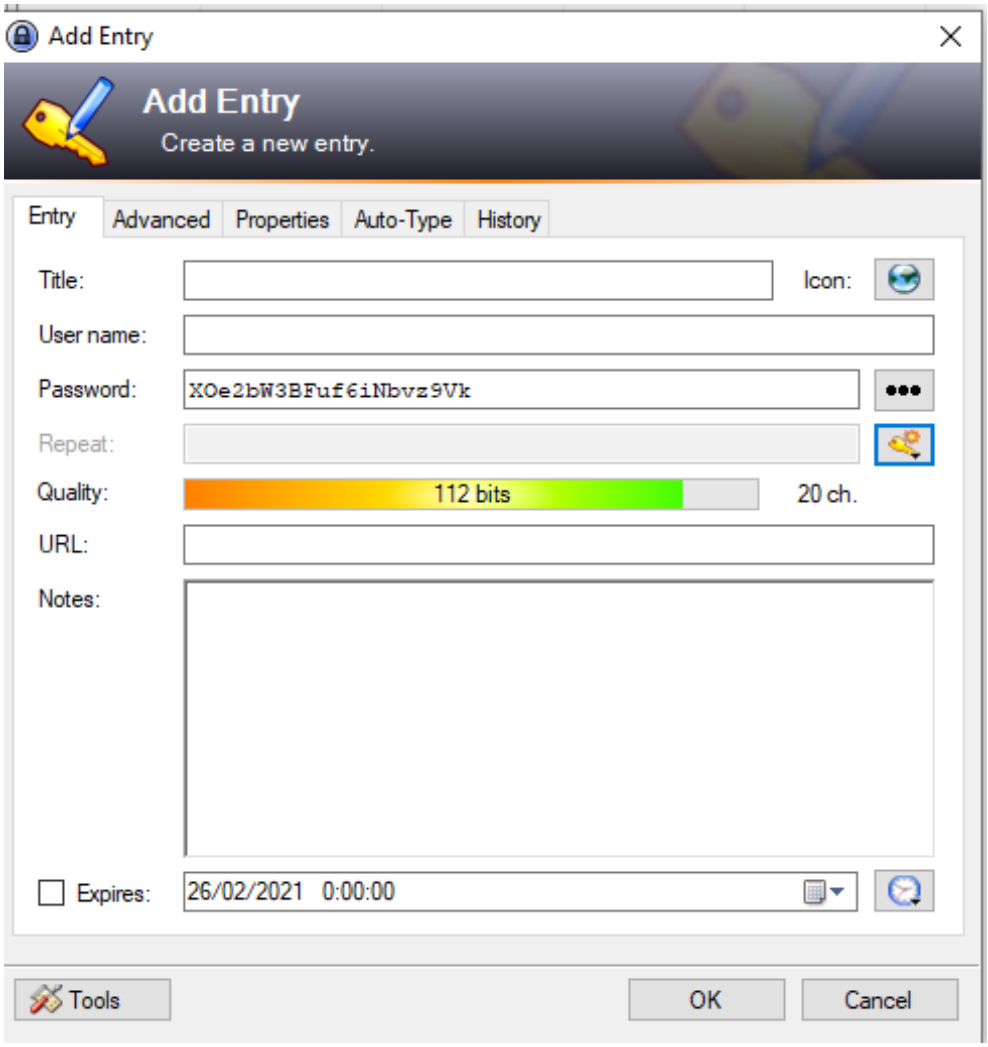
Completaremos los datos referentes al nombre de la base de datos y finalizaremos su configuración. Una vez en la pantalla principal, seleccionaremos la categoría donde queremos añadir la contraseña y pulsaremos en 

Nos aparecerá la siguiente ventana donde introduciremos todos los datos de la clave en cuestión. Por ejemplo:

TITLE: Correo Mercurio

USER NAME: profesor@fpmercurio.org

PASSWORD: Ranadero5%enelMundo!

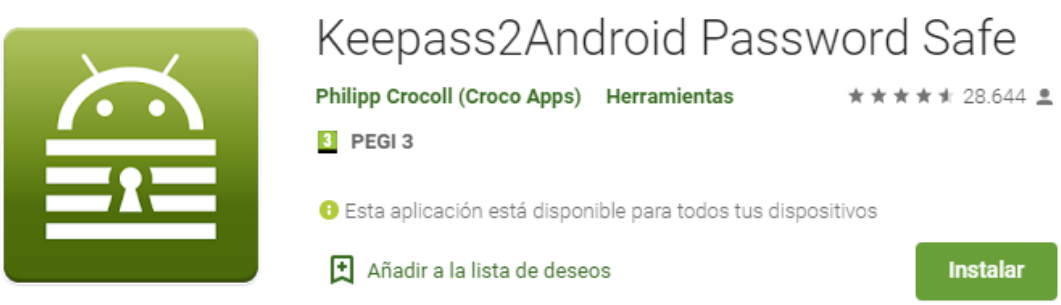


Pulsando en el botón que hay a la derecha de “Repeat” podremos generar contraseñas aleatorias para ese sitio web o aplicación.

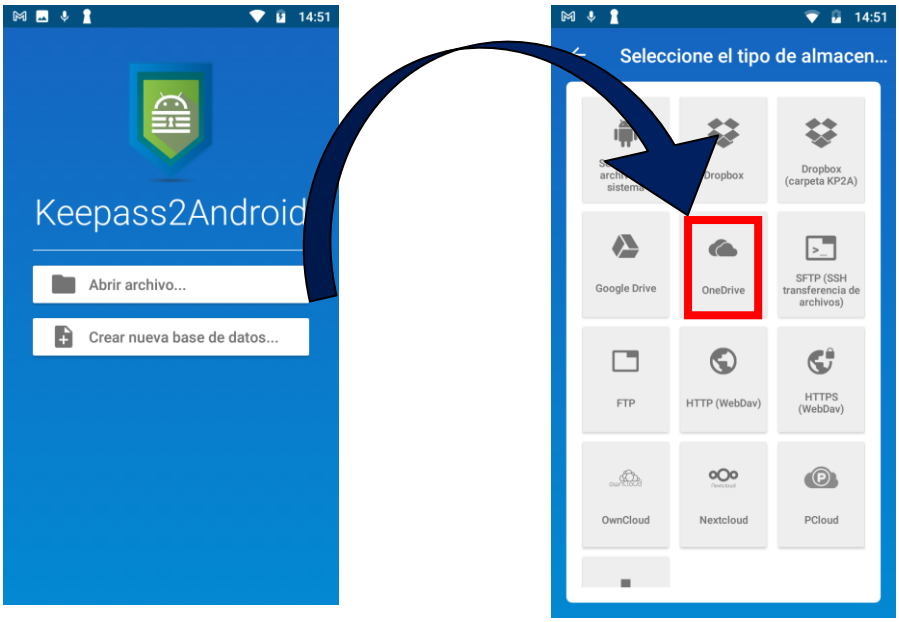
GESTORES DE CONTRASEÑAS PARA MÓVIL (ANDROID)

Para favorecer la sincronización de la base de datos de la aplicación de PC, tenemos disponibles varias aplicaciones para Android. Aquí os proponemos: **Keepass2Android Password Safe**.

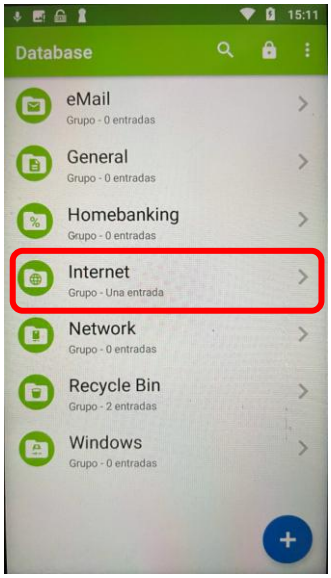
Keepass2Android Password Safe:



Una vez instalada en nuestro dispositivo móvil, lo primero que nos aparece al abrir la aplicación es una pantalla donde nos permite abrir un archivo encriptado (por ejemplo el previamente guardado en OneDrive). Nos pedirá la clave maestra del archivo que previamente pusimos en KeePass para desbloquear la base de datos y sincronizarlos con esta aplicación.



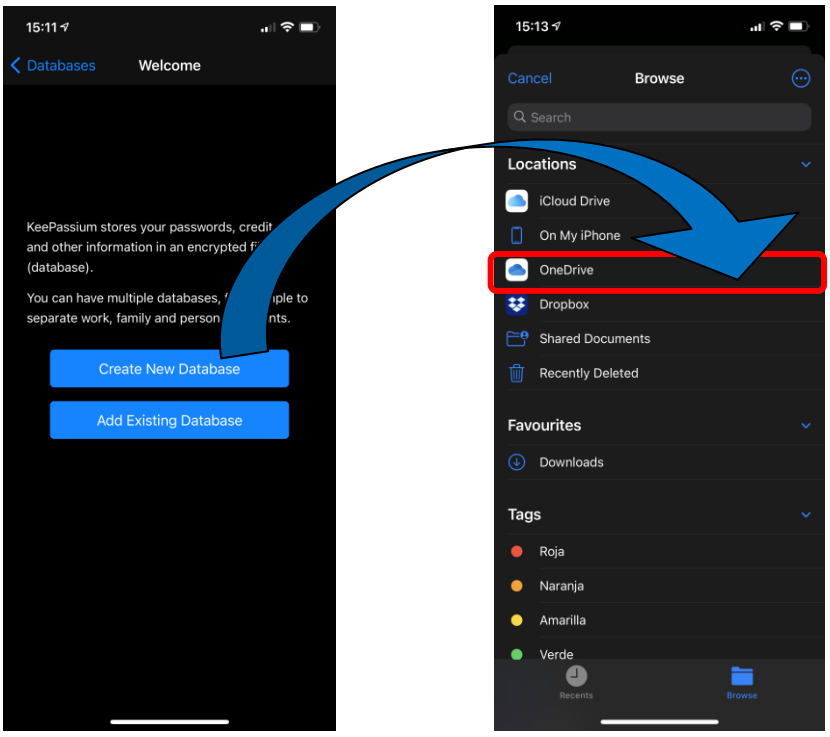
Introducimos los datos de la cuenta de educa.jcyl para acceder a ella (si en el móvil no la tenemos instalada). Una vez localizado el archivo de la base de datos, recordamos que se llama: **Database.kdbx** nos aparecerán sincronizadas todas las contraseñas que tenemos en nuestro PC.



GESTORES DE CONTRASEÑAS PARA MÓVILES APPLE (iOS - iphone)

Para favorecer la sincronización de la base de datos de la aplicación de PC, tenemos disponibles varias aplicaciones para móviles con sistema operativo iOS (iPhone). Aquí os proponemos: **KeePassium**

KeePassium: Una vez descargada la aplicación del AppStore nos aparece una ventana similar al caso anterior, donde nos permite crear una base de datos o añadir una base de datos ya existente. Seleccionamos esta última opción y pulsamos en "Browse" para buscar dentro de nuestro iPhone la aplicación OneDrive y seleccionar la carpeta donde se encuentre la base de datos.



De esta forma nos sincronizará todos los datos que tengamos en el PC, en la app.

GESTORES DE CONTRASEÑAS PARA MAC OS (Ordenadores Apple)

Strongbox: Para sistemas operativos Mac OS disponemos de la aplicación Strongbox. Podemos descargarla desde el Mac App Store y también desde el App Store (ya que dispone de versión móvil para iphone). Como en todas las versiones gratuitas, siempre disponen de menos características que la versión de pago, pero en estos casos y para nuestro uso a nivel personal, es más que suficiente.

Download on the App Store

Download on the Mac App Store

De igual modo que en las aplicaciones anteriores, podemos acceder a la base de datos encriptada que tenemos disponible en OneDrive y al seleccionarla nos sincronizará todas las claves que en ella aparezcan.

CONCLUSIONES:

Con respecto a la diferencia entre estas aplicaciones y la vista en la hoja de actividades del seminario, es que **Keeper** guarda esa base de datos en su nube de forma encriptada pero su versión para PC (ordenador) fuerza a la versión de pago para poder utilizarla.

Por ello aunque su versión de móvil funciona muy bien, desde el **departamento de informática recomendamos cualquiera de las opciones vistas en este anexo** teniendo en cuenta que generamos un archivo encriptado a nivel local que deberemos guardar en OneDrive para sincronizarlo con todos los dispositivos.