2020

PROTOCOLO DE BUENAS PASSWORDS.

DERECHO DE LA RED

Contenido

1. SUMARIO.

Ante el avance de Internet y la tecnología nos encontramos cada vez más y más expuestos a un mundo interconectado, hoy día nuestra rutina se basa fundamentalmente en utilizar la Red para cualquier gestión ya sea trabajar, comprar, acceder a plataformas de ocio, etc.

Por ello cada vez es más frecuente tener que utilizar contraseñas y cuentas de usuario para acceder a los diversos sistemas que utilizamos. Consecuentemente tendemos a utilizar patrones de contraseñas, claves comunes, passwords sencillas para facilitarnos el trasiego de tener que recordarlas todas.

Esta guía pretende aportar consejos sobre el establecimiento de contraseñas seguras, gestores de contraseñas que ayuden al usuario a recordar cada una de ellas y "rompedores" de contraseñas para verificar si la password que estamos utilizando es realmente segura.

Para poder llevar a la práctica, por parte de los usuarios, todo lo que se expone en ella se hará una demostración de cómo utilizar un gestor de contraseñas.

Como apunte debemos tener en cuenta que existen una serie de software y webs capaces de determinar si la contraseña elegida es lo suficientemente segura o no. La proliferación de diversos tipos en el mercado permite que podemos encontrar en Internet bastantes comprobadores de contraseñas, aunque estos podrían guardar tu contraseña en una base de datos así que mejor no utilizarlos.

2. PALABRAS CLAVE.

- ☐ Usuario.
- ☐ Verificación.
- ☐ Gestor
- ☐ Competencias.

3. ALCANCE DE LA GUÍA.

Esta guía identifica las competencias básicas necesarias para el manejo y el establecimiento de contraseñas (passwords) robustas y seguras. Se aplica a dos niveles:

- ☐ Nivel uno: para administrador de sistemas (*sistema de verificación de contraseñas*).
- ☐ Nivel dos: para usuarios

Las diferentes opciones que se proponen no diferencian entre las habilidades de los usuarios, es decir que cualquiera de ellos podría utilizarlas.

La guía que se propone a continuación intenta abordar una de las principales cuestiones de Ciberseguridad. De este modo no garantiza la seguridad del usuario de modo inequívoco, por lo que dependerá de él adoptar prácticas de seguridad complementarias al establecimiento de buenas passwords.

4. SIGNIFICADO Y USO.

Las contraseñas son el medio de acceso a cualquier sistema, se utilizan como mecanismo de autentificación tanto personal como laboral. Por lo que una contraseña insegura podría traducirse como una puerta abierta al compromiso de datos sensibles y personales.

Esta guía proporciona un resumen de las competencias y habilidades necesarias para poder determinar el uso de una contraseña segura.

Las competencias básicas que se requieren para el desarrollo de la misma no son técnicas o elaboradas para los usuarios pero sí requieren de cierto compromiso de los administradores de sistemas (*sistema de verificación de contraseñas*), gestores de contraseñas y “rompedores” de estas.

5. RESUMEN DE LAS COMPETENCIAS BÁSICAS REQUERIDAS.

El primer requerimiento que necesitamos es que sean contraseñas difícilmente vulnerables.

El segundo requerimiento es conocer ciertas cuestiones previas:

- ☐ Contraseñas fáciles de recordar e introducir, aunque a su vez deben ser difíciles de adivinar.
- ☐ La contraseña no debe guardar relación el usuario, por ejemplo: fecha de nacimiento, lugar favorito, etc.
- ☐ Utilización de contraseñas con una cantidad de caracteres aceptables.
- ☐ Los caracteres deben ser una mezcla de diversos tipos: alfanuméricos, mayúsculas-minúsculas, números y símbolos de puntuación.
- ☐ La dificultad de esto es la dificultad en su recordatorio, pero existen gestores de contraseñas para facilitar este proceso.
- ☐ Apuntar las contraseñas en un bloc o en un documento informático no es una buena opción, puesto que si el archivo es robado se podrá tener acceso directo a diferentes cuentas.
- ☐ Utilizar gestores de contraseñas como sustito podría ser una solución fiable.
- ☐ Comprobar mediante passwords cracker la seguridad de la contraseña elegida.

6. COMPETENCIAS PARA EL ADMINISTRADOR DEL SISTEMA (*SISTEMA DE VERIFICACIÓN DE CONTRASEÑAS*).

El sistema de verificación de contraseñas consiste en la autenticación de la contraseña a la hora de escribirla en un sistema o de autentificarla.

A continuación se pretende resumir las características de un buen sistema de verificación de contraseñas.

- ☐ Debe permitir el reconocimiento de contraseñas de cualquier longitud.
- ☐ No debe ofrecer al usuario mecanismos para recordar la contraseña como: el nombre de tu mascota es…., tu comida favorita es…., el lugar de preferencia de tu padre es…

- ☐ El sistema de verificación de contraseñas debe filtrar y rechazar la contraseña elegida en base a una serie de requerimientos.
  - Si está muy o muy poco usada.
  - Si tiene caracteres repetitivos.
  - Si contiene caracteres secuenciales.
  - Si contiene palabras relacionadas con el contexto. Por ejemplo, en este caso, la palabra Guía.
- ☐ Limitar el número de intentos sin éxito a la hora de introducir la contraseña en el sistema.
- ☐ Facilitar la coordinación con gestores de contraseña.
- ☐ Ocultar la contraseña por defecto.
- ☐ El sistema no debería memorizar la contraseña, pero en el caso en el que lo haga (que es la práctica más común) debe hacerlo de forma segura.
- ☐ Anular las contraseñas con demasiada antigüedad.

7. COMPETENCIAS PARA USUARIOS.

En el caso de que el usuario genere la contraseña debe cumplir con una serie de requisitos mínimos:

- Utilización de contraseñas con una cantidad de caracteres mínimos de 8, pero a mayor número de caracteres más seguras serán.
- Utilizar una serie de palabras encadenas entre sí, de este modo la contraseña será más larga y la deducción de esta no será sencilla. Ejemplo: borrador_sartén.Pantallade183**
- Las contraseñas no deben estar compuestas por datos propios, de este modo una persona conocida o con cierto conocimiento del usuario no pueda adivinarla.
- Tampoco deben componerse por canciones, refranes, frases conocidas, chascarrillos, etc. Ya que la adivinación de estas de forma automática puede ser sencilla.
- No se deben repetir contraseñas para diferentes cuentas o servicios.

- No deben apuntarse las contraseñas en ningún medio.
- No deben comunicarse a terceros.
- Cambiar con periodicidad las contraseñas. Lo más recomendable es una vez al mes.

8. PASSWORD CRACKER.

Estos programas se utilizan para descifrar contraseñas en determinadas aplicaciones. Se utilizan con el permiso del usuario en las aplicaciones que él requiera.

De este modo el objetivo es poder pasar el programa de password cracker así si lo pasan la contraseña se puede determinar como segura y sino no debería utilizarse.

- Debe pasarse el programa en un corto plazo de tiempo.
- Debería pasarse el programa una vez al mes, eliminando (con consentimiento del usuario) las contraseñas que no superen la prueba.
- Avisar al usuario que la contraseña no pasa la prueba para que este pueda modificarla o eliminarla.

9. GESTORES DE CONTRASEÑAS.

Los gestores de contraseñas son una serie de software o aplicaciones que te permiten recordar todas tus contraseñas. Estos gestores permiten tanto gestionar como generar la contraseña. Consisten en grabar o generar la contraseña para el programa o sistema determinado, de este modo se evita que el usuario apunte manualmente la contraseña.

De este modo solo necesitamos recordar la contraseña maestra del gestor, es decir, “la llave maestra” que guarda las demás contraseñas.

Estos gestores pueden parecer inseguros pero la realidad es que mantienen las contraseñas cifradas para que el acceso a ellas sea dificultoso. De este modo podemos utilizar contraseñas seguras, buenas y robustas sin preocuparnos de si nos olvidamos de ellas o no.

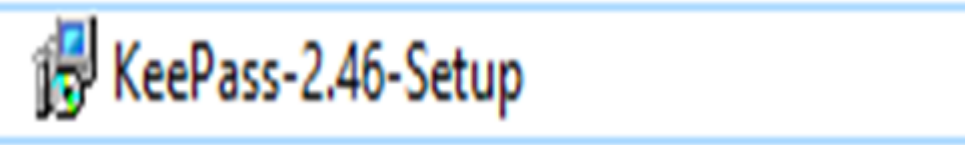
10. GUÍA RÁPIDA DE COMO UTILIZAR KEEPASS.

Keepass es uno de los gestores de contraseñas más importantes del mercado, a continuación se va a mostrar una pequeña guía de cómo crear y gestionar una contraseña segura con este programa paso a paso.

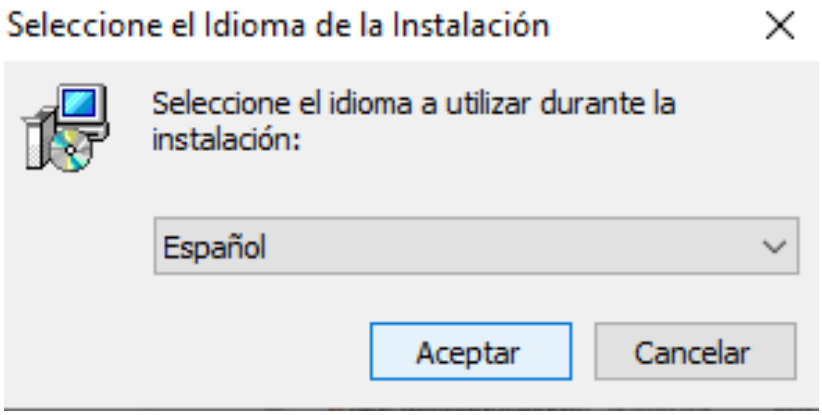
I. DESCARGA E INSTALACIÓN DE KEEPASS.

1. Link de descarga: https://keepass.info/download.html
2. Proceso de instalación.

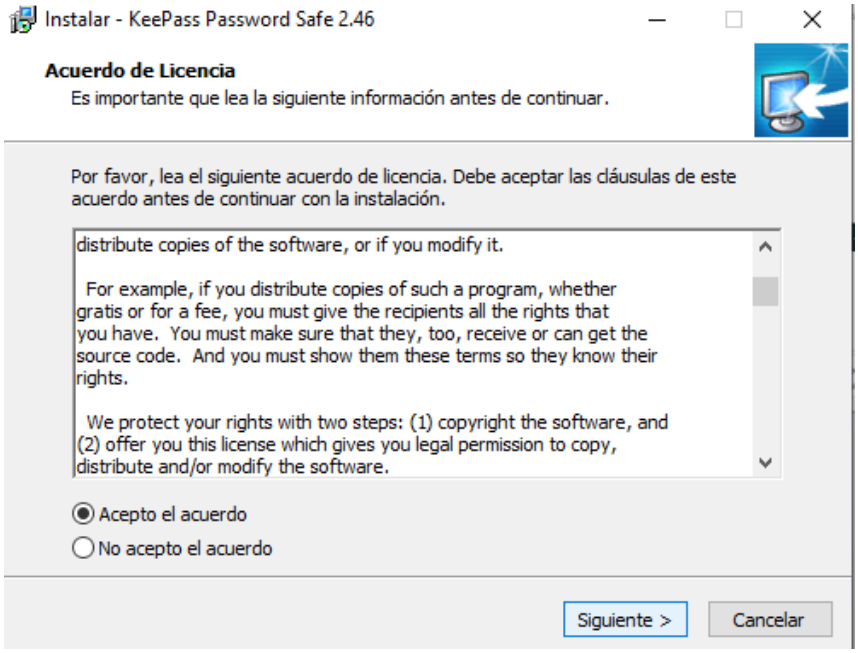
   1º Una vez descargado clicamos sobre el instalador.



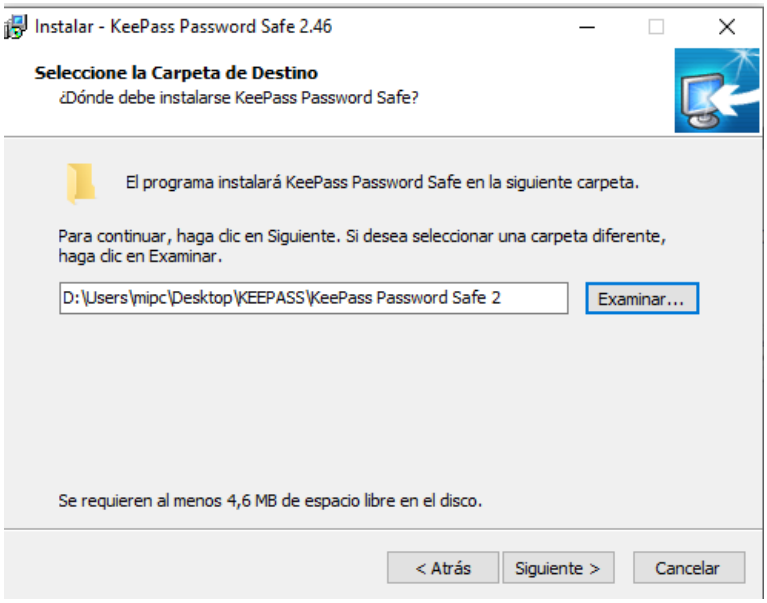
   2º La primera pantalla que podemos encontrar es un elector de idiomas, por lo que elegimos idioma en el que queremos configurar el programa. En este caso en Español. Aceptamos.



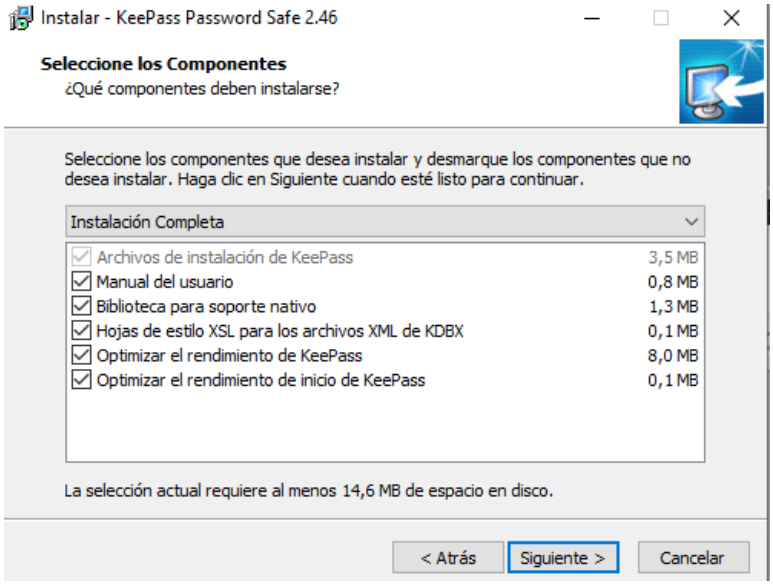
   3º La tercera pantalla que nos muestra el programa es el acuerdo de licencia, una vez que lo leemos lo aceptamos y clicamos en siguiente.



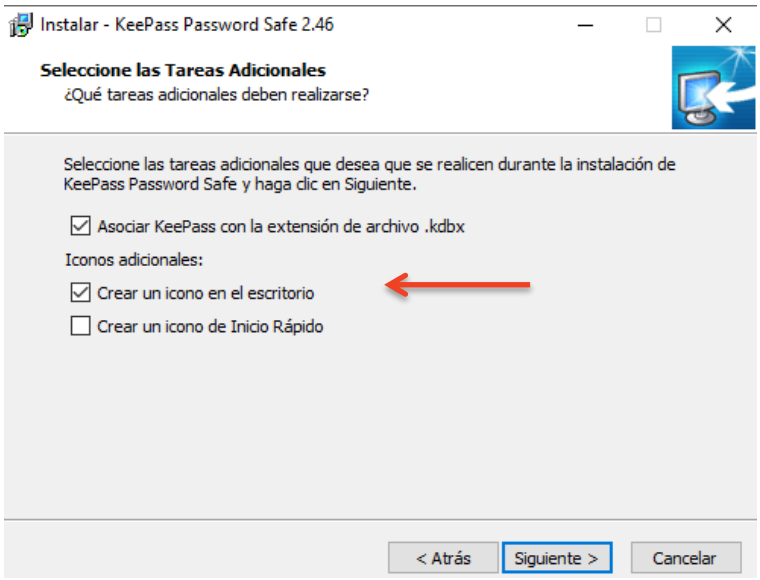
4º Una vez aceptado el acuerdo, debemos elegir la carpeta de instalación. Para ello clicamos sobre examinar y elegimos la carpeta de destino que deseemos. A continuación clicamos sobre siguiente.



5º Aceptamos las opciones de instalación y clicamos en siguiente.



6º A continuación se nos muestra una pantalla para seleccionar tareas sobre la instalación. Por comodidad vamos a crear un icono en el escritorio. De este modo es más sencillo encontrar el archivo a simple vista. Por lo tanto clicamos sobre la opción y a continuación en siguiente.

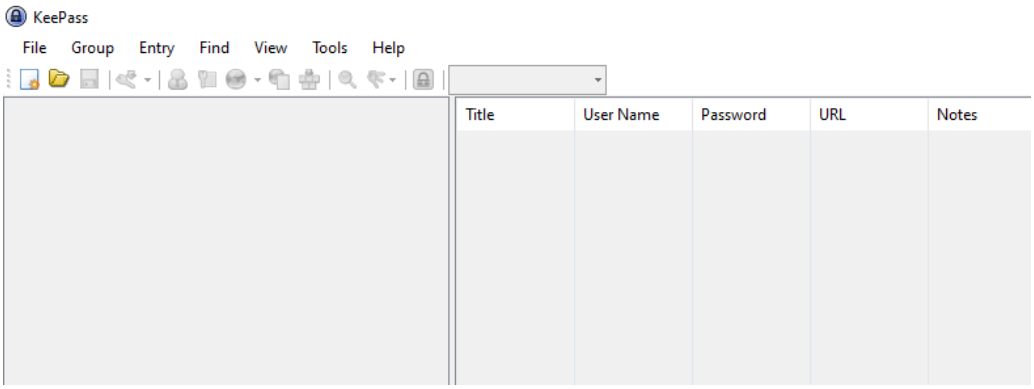


7º El siguiente desplegable que se nos muestra es un resumen de las opciones que hemos marcado, por lo que revisamos los datos y si están correctos clicamos en instalar.

8º Una vez finalizado el proceso, clicamos en finalizar y ya estaría instalado KeePass.

II. CREACIACIÓN DE LA BASE DE DATOS Y LA MASTER PASSWORD

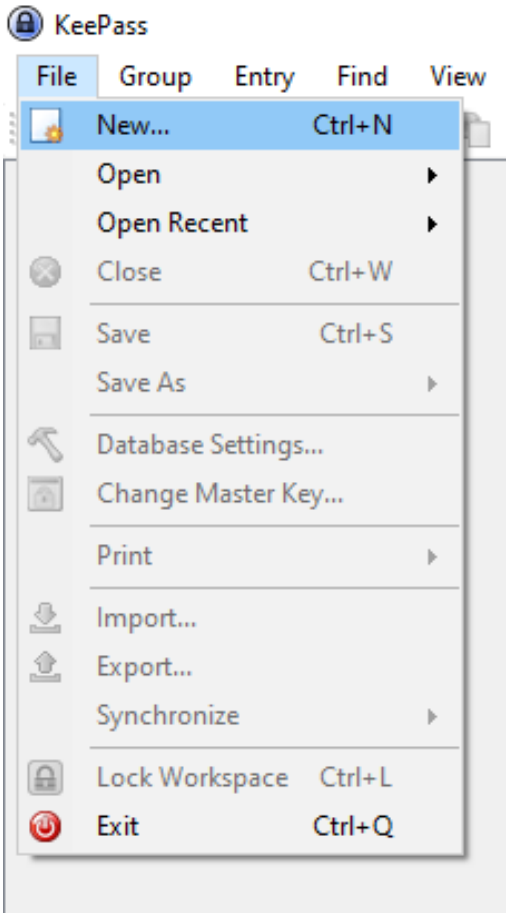
1- Una vez descardo e instalado en el PC abrir el programa con doble click. La primera imagen que nos vamos a encontrar es la siguiente.



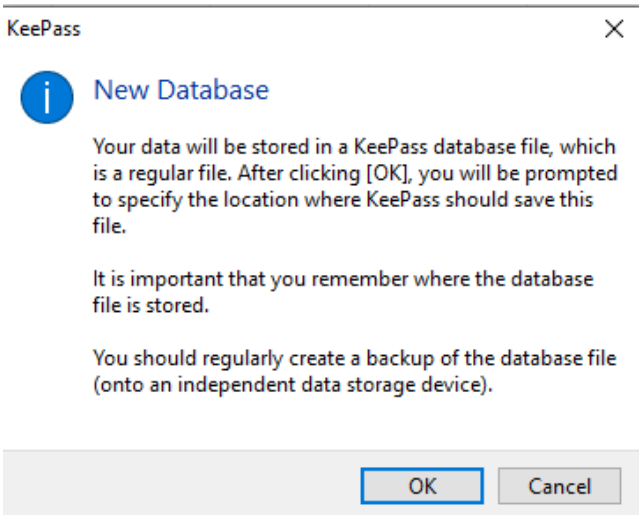
En ella observamos un pag en blanco. El primer paso que debemos hacer es introducir una Master Password, es decir, una contraseña maestra bajo la cual se guardarán todas las contraseñas que queramos escribir. Por lo tanto, esta será la única contraseña que debemos recordar.

Para crear esta Master Password debemos:

1º Clicar sobre File y new



2º A continuación se nos desplegará un comentario de explicación sobre la nueva base de datos que vamos a crear. Una vez que lo leemos clicamos sobre Ok. Se adjunta una traducción del mensaje.

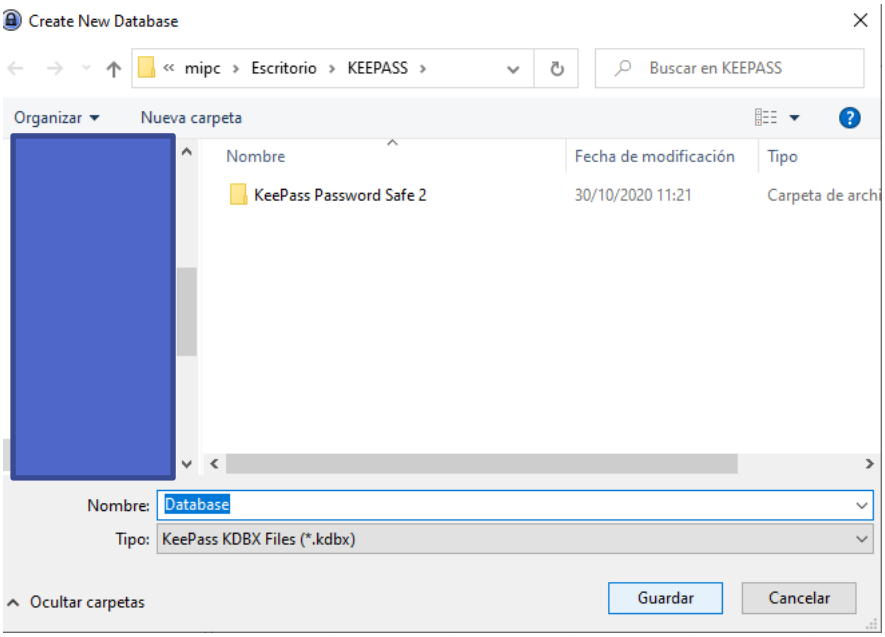


Sus datos se almacenarán en un archivo de la base de datos KeePass, que es un archivo normal. Después de hacer clic en ok, se le pedirá que especifique la ubicación donde KeePass debe guardar este archivo.

Es importante que recuerde dónde se almacena el archivo de la base de datos.

Debería crear regularmente una copia de seguridad del archivo de la base de datos (en un dispositivo de almacenamiento de datos independiente)

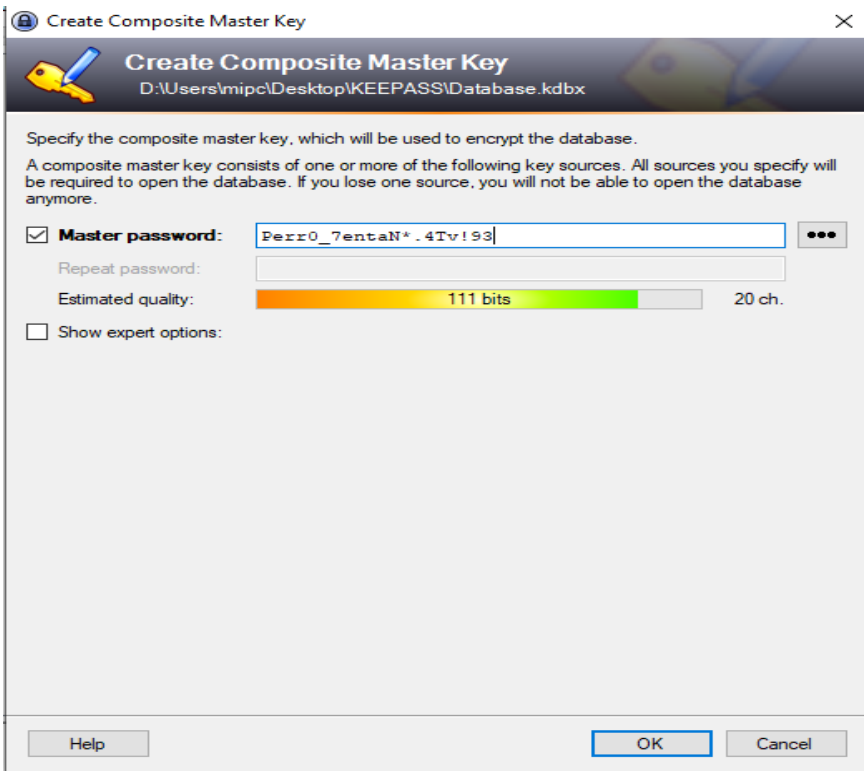
3º A continuación, tal y como nos indica el mensaje debemos guardar el archivo de la base de datos en una dirección. En este caso seguiremos utilizando la carpeta de demostración, pero cuanto menos visible esté la carpeta de destino mejor. Una vez guardada clicamos sobre guardar.



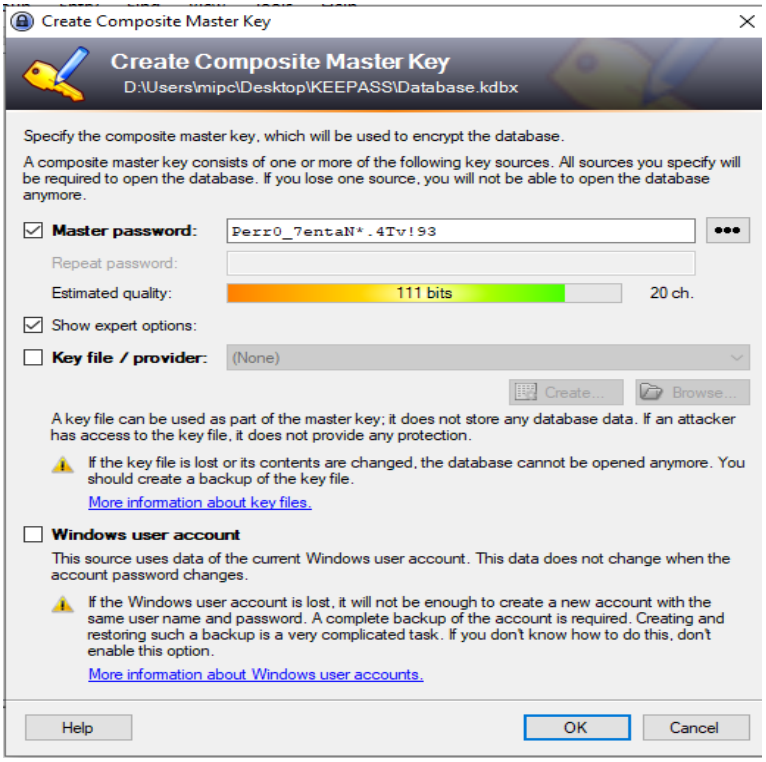
4º La siguiente pantalla que nos muestra es la creación de la llave maestra, es decir la contraseña que nos daría acceso al programa y por tanto a la base de datos con las demás contraseñas creadas. Se aconseja seguir los pasos de contraseña robusta que se explicaron previamente. A continuación se mostrará una contraseña robusta a modo de ejemplo.

Una de las características más importantes que tenemos en la creación de esta llave maestra es que nos muestra en forma de bits el grado de seguridad que tiene, para ello utiliza un gradiente de colores.

En el caso de la contraseña que nosotros hemos elegido contiene 20 caracteres de diferentes formatos, esto el programa lo ha traducido en 111 bits, siendo una contraseña muy robusta. Aunque como vemos podemos seguir escribiendo caracteres para fortificarla más aún.



5º Si clicamos sobre la opcion de mostrar opiones expertas podemos observar la siguiente información:

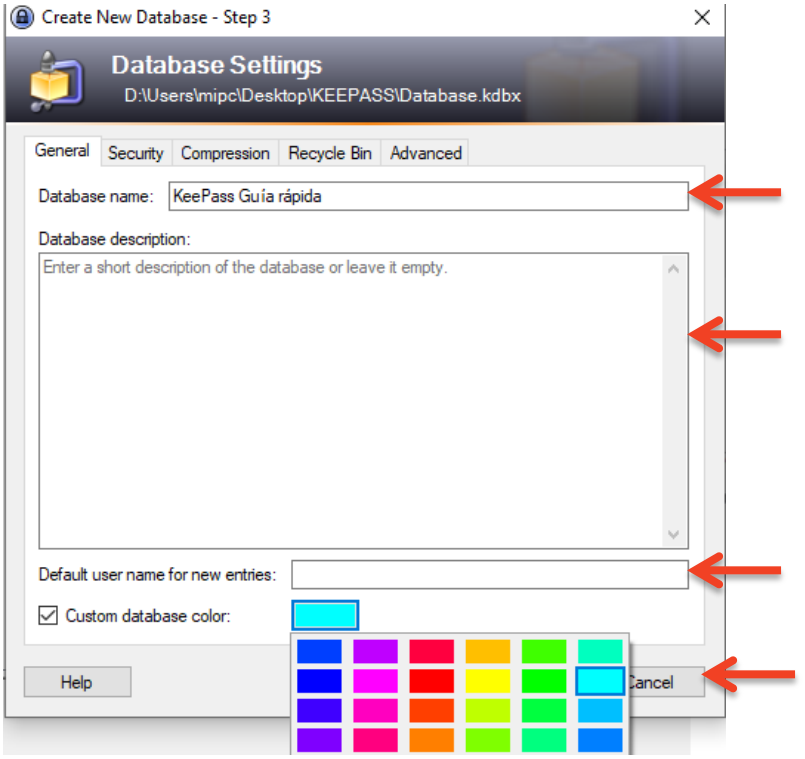


La primera opción que nos muestra es Key file/provide. Consiste en utilizar un archivo de claves como parte de la llave maestra. Puede ser peligroso ya que si el archivo es atacado la base dedatos que guarda nuestras contraseñas se vería comprometida. Al igual que si el archivo es eliminado o modificado. Por lo tanto nosotros no vamos a clicarla, aunque eso queda a opción del usuario.

La segunda opción hace referencia a la cuenta de usuario de windows. Consiste en utilizar los datos de la cuenta del usuario de windows. Estos datos no cambian cuando la contraseña de la cuenta cambia. También puede generar un peligro importante para el usuario por lo que tampoco vamos a clicarla como opción.

Por lo tanto una vez introducida nuestra contraseña clicamos en Ok.

6º A continuación vamos a crear la base de datos. La primera imagen que nos sale consite en darle forma e imagen a la base de datos.



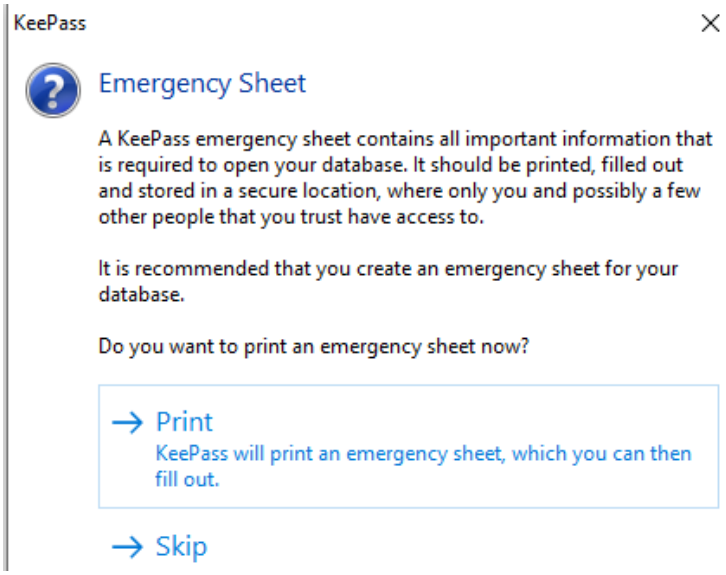
En la primera pantalla (general) podemos ponerle nombre a nuestra base de datos.

Escribir una descripción de esta.

Dejar el nombre por defecto para nuevas entradas.

Elegir un color para esta.

Una vez creada al gusto del usuario clicamos en ok, y nos muestra la siguiente pantalla de advertencia.

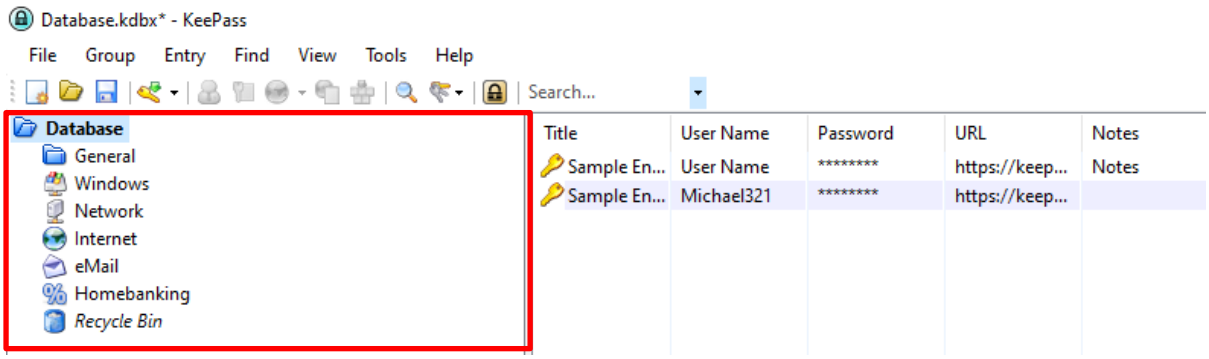


En esta nos muestra un mensaje sobre una imprimir y rellenar una hoja para abrir la base de datos. Recomienda imprimirla por defecto, en nuestro caso le

damos a saltar (skip). Pero el usuario que desee imprimirla únicamente debe clicar sobre Print.

III. ESTUDIO DE LAS DIFERENTES OPCIONES DE KEEPASS

Una vez elegida la opción que queramos la siguiente pantalla que vamos a ver es la pantalla inicial de la base de datos. En ella vamos a observar varios ejemplos por defecto.

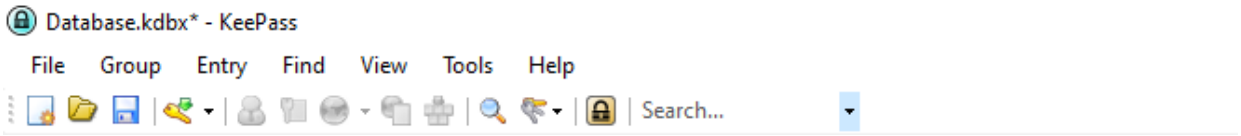


Vamos a echar un vistazo sobre la pantalla de incio del sistema, como ya hemos dicho tenemos dos ejemplos de contraseñas en la pantalla de inicio.

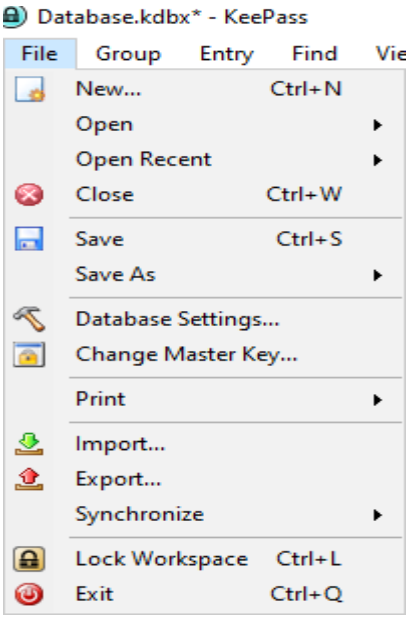
En el panel de la izquierda de tenemos la base de datos generada con varias opciones, basicamente consiste en un organizador de múltiples opciones.

- **General**: en esa opción podemos ubicar las contraseñas que no corresponda a un destino concreto.
- **Windows**: podemos guardar las contraseñas referidas a los sistemas o relacionadas con estos.
- **Network**: consiste en otro organizador para redes de trabajo.
- **Internet**: Aquí podemos ubicar las passwords referidas a webs o registros de internet.
- **E-mail:** Es la ventana que nos guardaría las password referidas a correos electrónicos.
- **Homebankig**: podemos ubicar en esta sección las contraseñas de acceso a nuestro perfil del banco.
- **Recycle bin**: Es decir la papelera, donde se ubican las contraseñas eliminadas.

En la parte superior de la pantalla podemos ver unas opciones bastante intuitivas sobre el progrma que estamos utilizando.

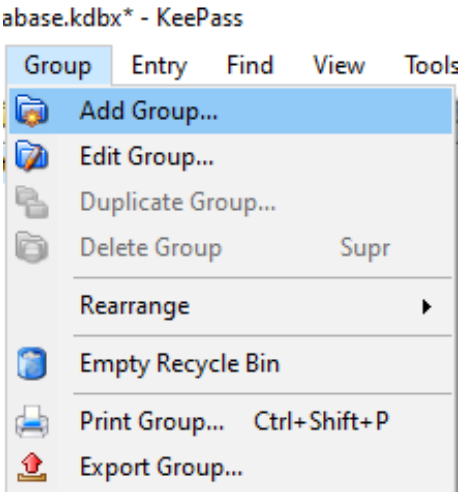


Las opciones que nos muestra File son:



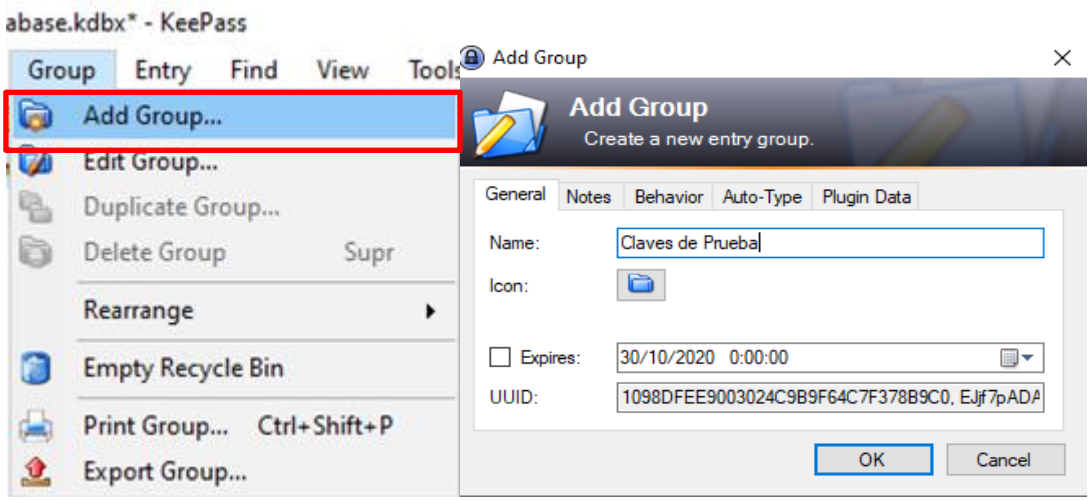
Básicamente nos muestra las diferentes opciones que podemos encontrar con la gestión de archivos; abrir uno nuevo, abrir recientes, guardarlos, importarlos, configurarlos, etc.

Las opciones que propone group son:



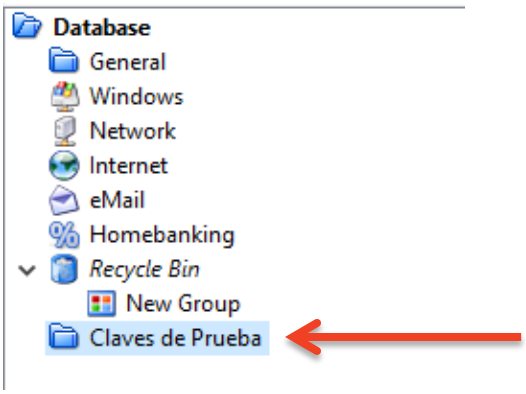
Las opciones se resumen básicamente en crear o editar nuevos grupos. Así como exportar, configurar, reciclar o imprimir los grupos creados.

Crear un nuevo grupo consiste básiscamente en crear una sección más en nuestro panel. Por ejemplo.

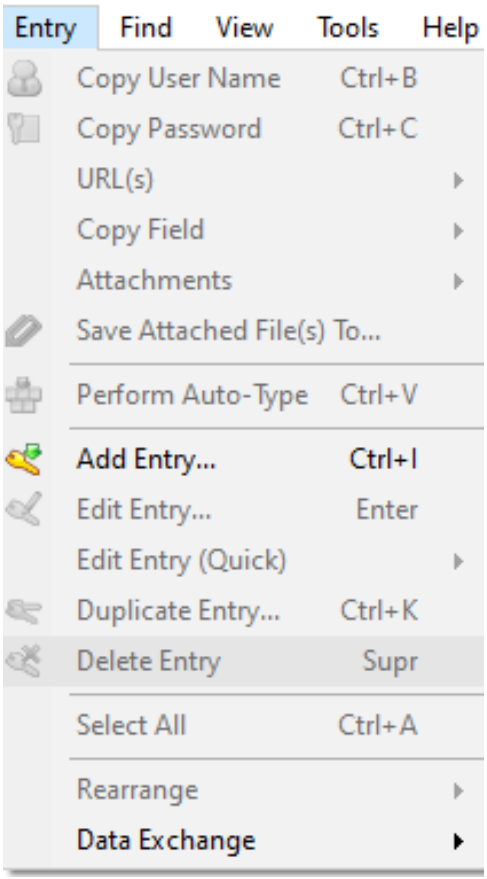


Para crear un nuevo grupo podemos observar una lista de opciones, en la pantalla general nos da la opción de nombrarlo, en este caso hemos elegido Clasves de Prueba. También podemos seleccionar el icono que queremos que nos muestre en el panel de entrada, así como la fecha de creación, si queremos que expire y la referencia que da el programa.

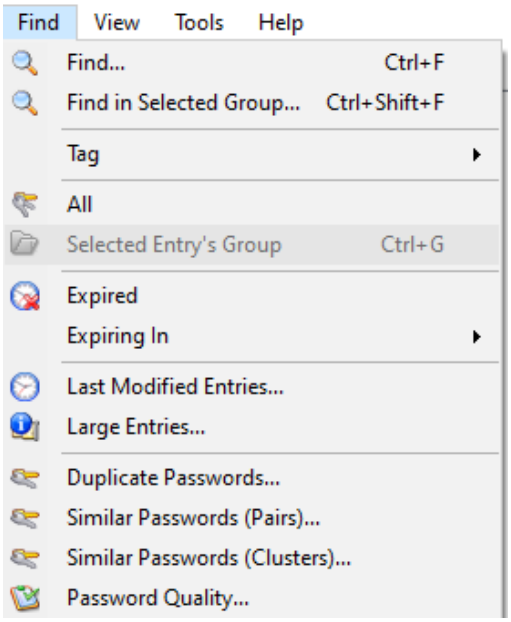
En las siguientes pestañas podemos configurar las diversas opciones. Si clicamos en Ok, se nos generará el grupo en el panel de control.



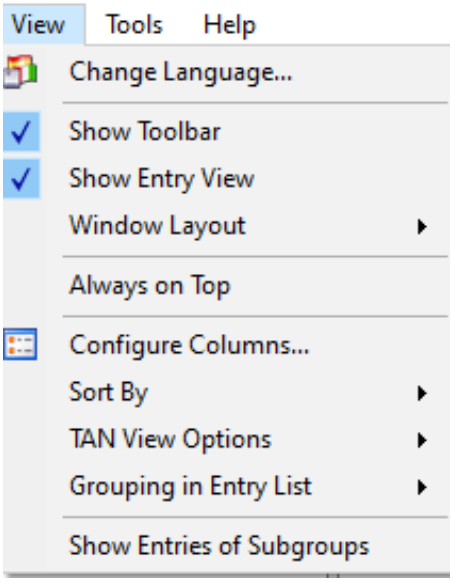
La siguiente pestaña, en la barra superior del programa, que encontramos tiene diferentes opciones. En entry las opciones que tenemos están hasta el momento bloquedas, pero encontramos desbloqueda la opción que nos permite crear una llave de modo directo. (Lo veremos en la siguientes imágenes).



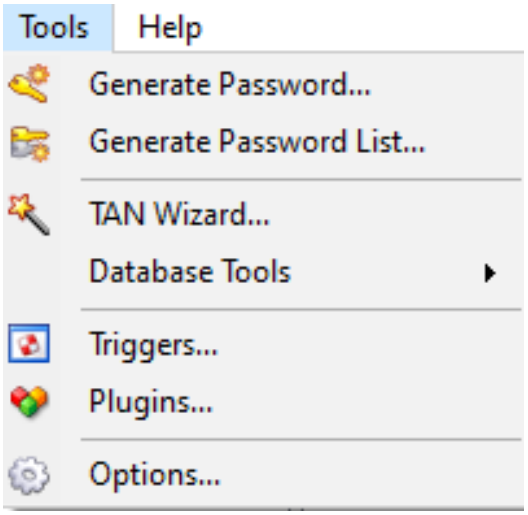
En la pestaña de File podemos observar una interfaz intuitiva sobre búsquedas y gestiones simples de contraseñas como duplicados, etiquetas, tiempo de expirar contraseñas, etc.



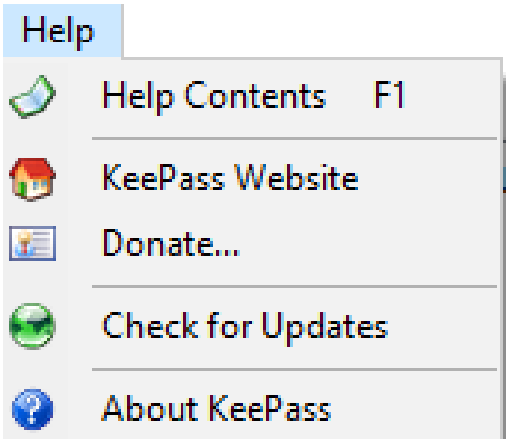
En la pestaña de View encontramos múltiples opciones de configuración, como elegir el lenguaje (habría que descargarse una compilación), mostrar barras de herramientas, etc.



Por su parte en la pestaña de tools, encontramos diferentes opciones de pluggins, herramientas para la base de datos, generadores de contraseñas y listas de contraseñas. Estas opciones se explicarán más adelante.



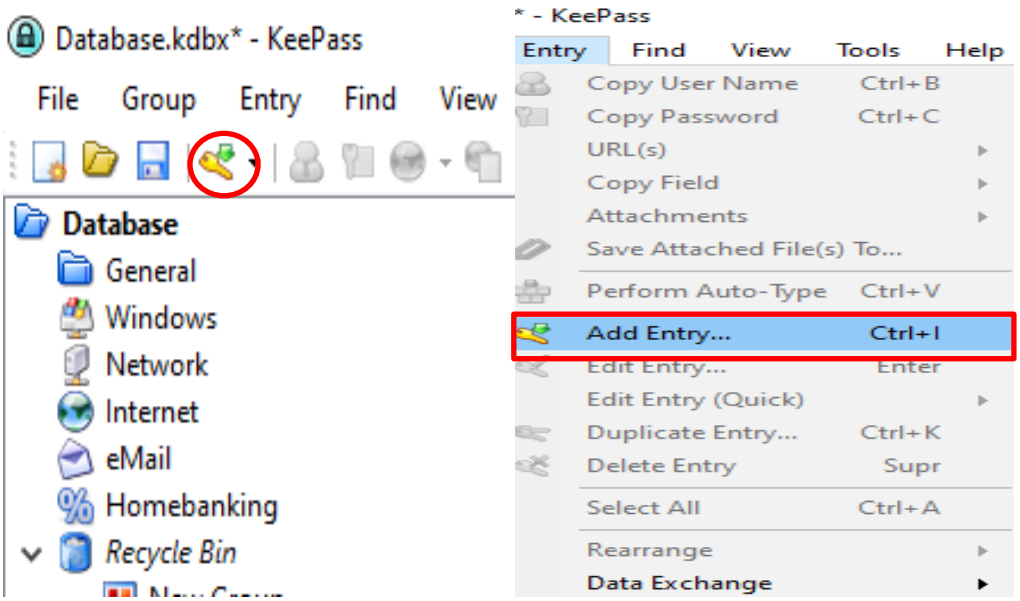
En cuanto a la pestaña de help, encontramos diferentes opciones para ayudar al usuario a utilizar de un modo más eficientes el programa, redirigiéndolo a links de ayuda, entre otras cuestiones.



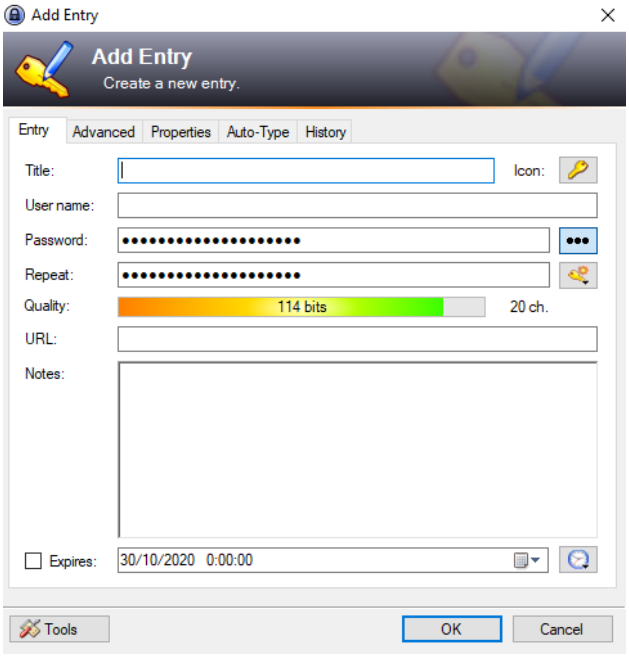
La segunda barra de herramientas que nos muestra el programa nos da acceso directo a diferentes opciones como guardado automático, crear nuevos archivos, buscadores, etc.

IV. CÓMO CREAR Y GESTIONAR UNA CONTRASEÑA PARA UN ARCHIVO.

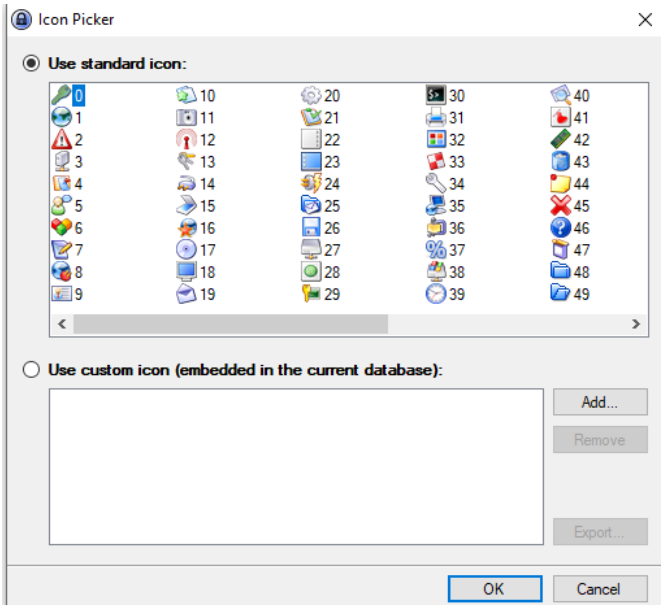
1º Para crear una entrada con la contraseña tenemos que clicar sobre la opción de la llave en la segunda barra de herramientas que encontramos. Al igual que encontramos la opción en el desplegable de Entry en la barra superior de herramientas.



2º Una vez dentro se nos genera una pestaña para configurar la entrada con la contraseña, ya generada por defecto.



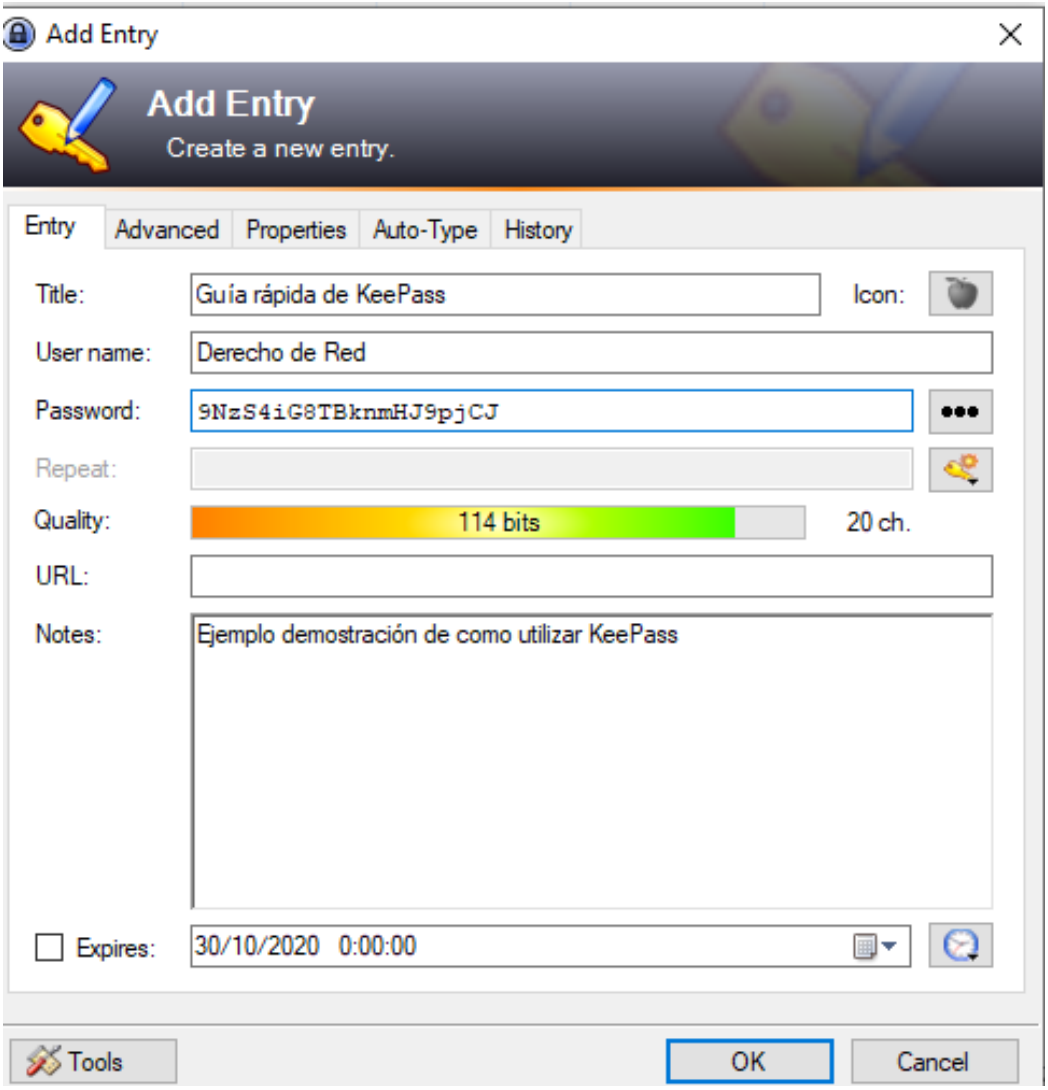
Analizando un poco la entrada podemos configurar el título de la entrada, agregarle un nombre de usuario, cambiar el icono con el que queremos que se nos muestre. Podemos elegir el icono que queramos e incluso añadir alguno propio.



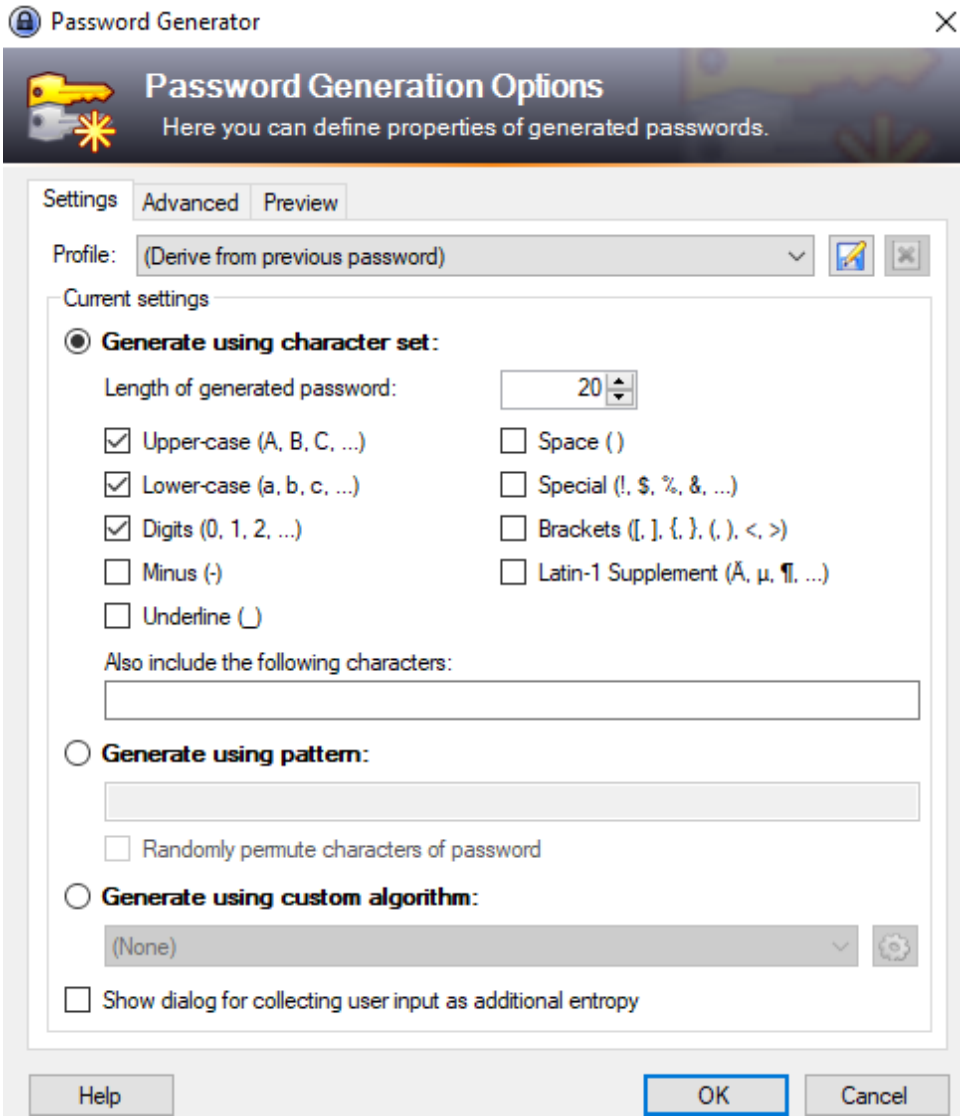
En cuanto a la contraseña encontramos una por defecto que podemos ver si clicamos en los puntitos que encontramos al lado de la barra de password, como podemos observar en la imagen a continuación se puede considerar una contraseña segura. Esta contraseña se puede modificar.

A continuación tenemos la opción de ponerle una URL, así como de escribir algunas notas o de hacer que expire en una fecha concreta (si no marcamos esa opción la contraseña no expira).

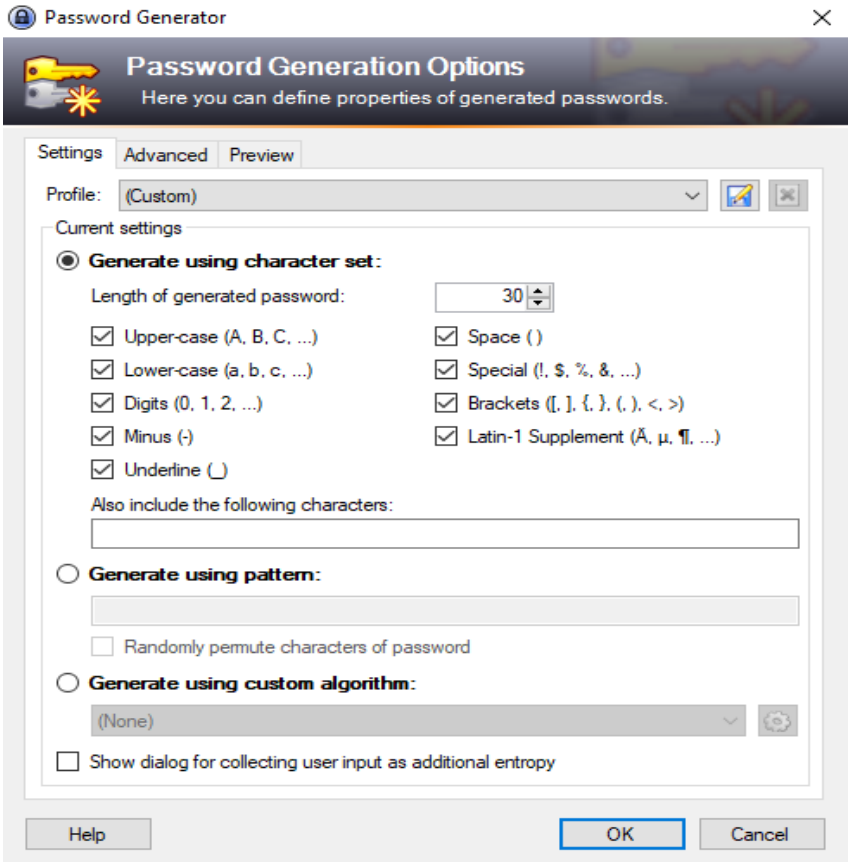
A continuación vamos a mostrar un ejemplo de cómo sería la contraseña creada.



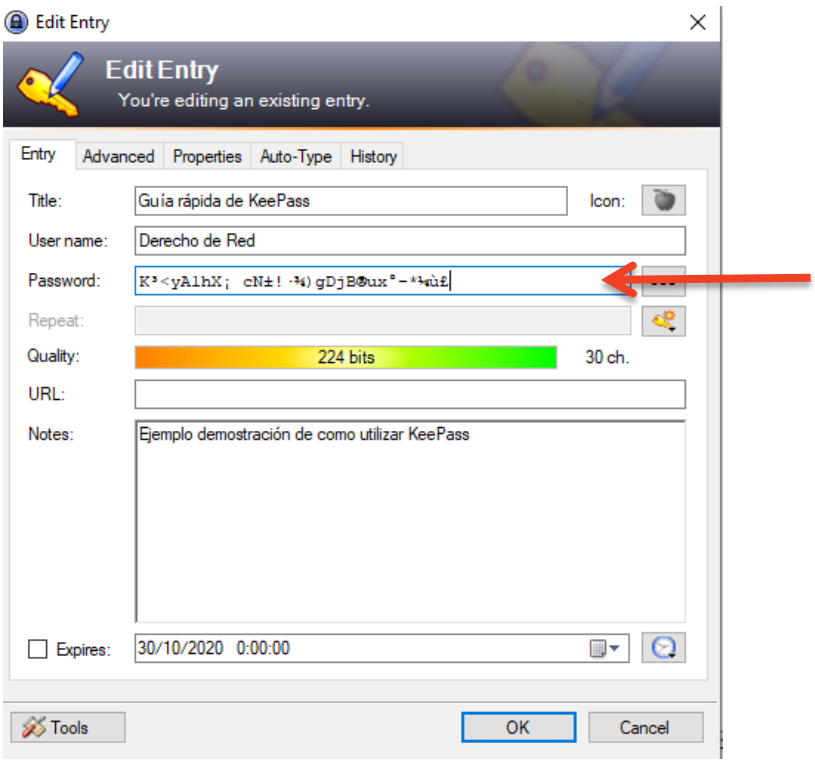
Un dato a destacar de esta pestaña es que si clicamos en el icono de al lado de la barra de repeat se nos muestra un generador de contraseña automático que podemos configurar, tanto en número de caracteres como el tipo, etc. En nuestro caso demostrativo lo vamos a dejar por defecto.



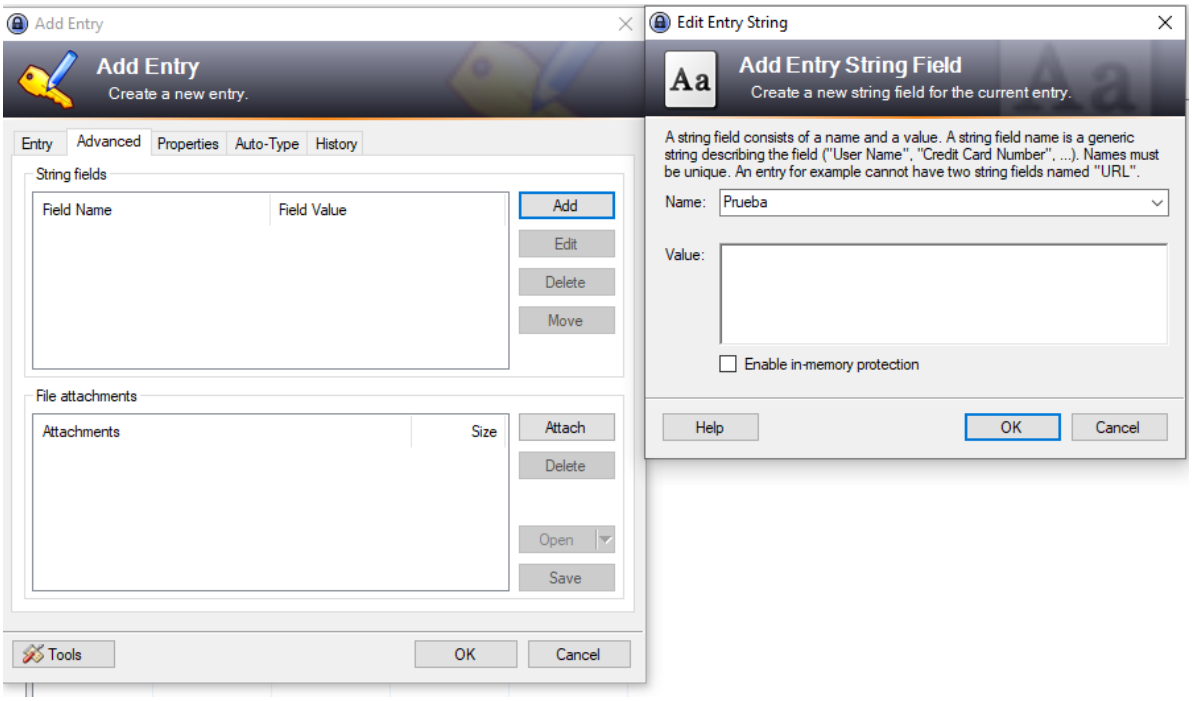
A continuación se muestra un ejemplo de como utilizar el generador. Como hemos dicho el generador de contraseñas se puede configurar, aunque a mayor cantidad y tipo de caracteres mayor seguridad podemos encontrar, por ello vamos a marcalos todos y a subir el número de caracteres a 30.

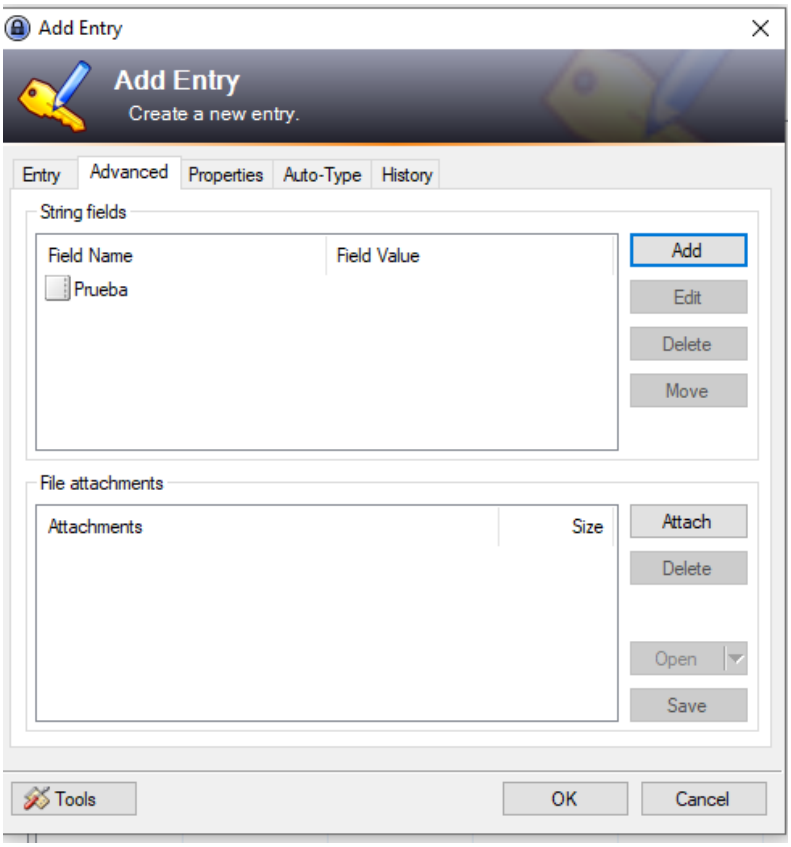


Si clicamos en ok se nos genera una contraseña con todo lo puesto.

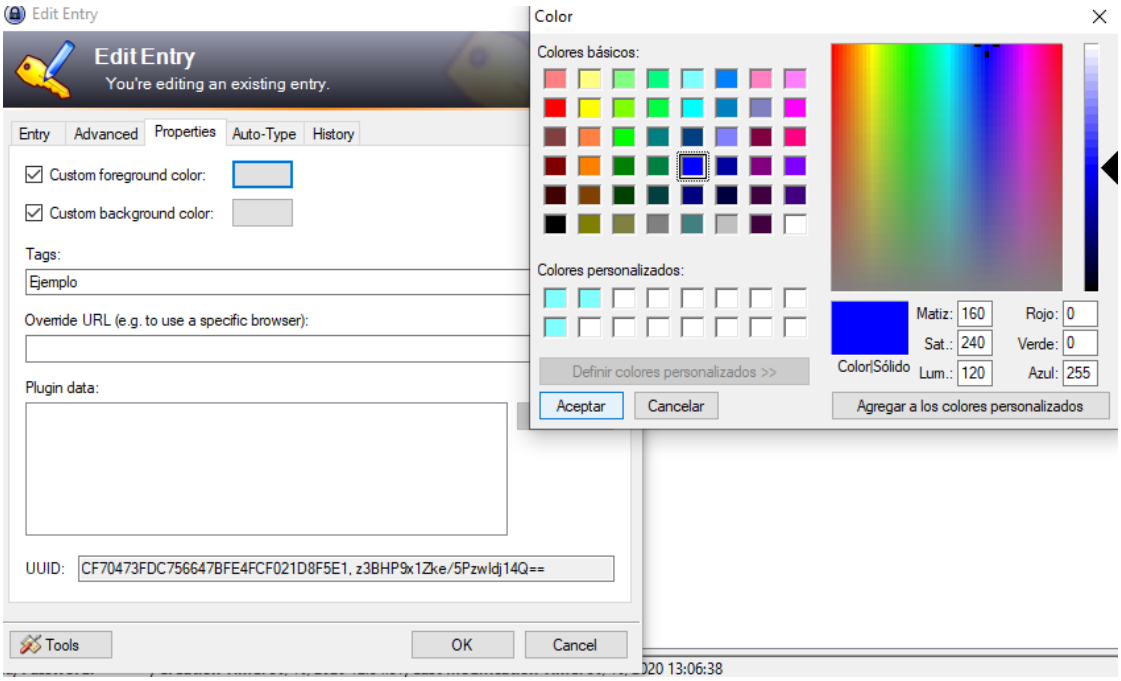


En la siguiente pantalla de “advanced” podemos configurar la contraseña para un archivo concreto por ejemplo vamos a llamarlo prueba.

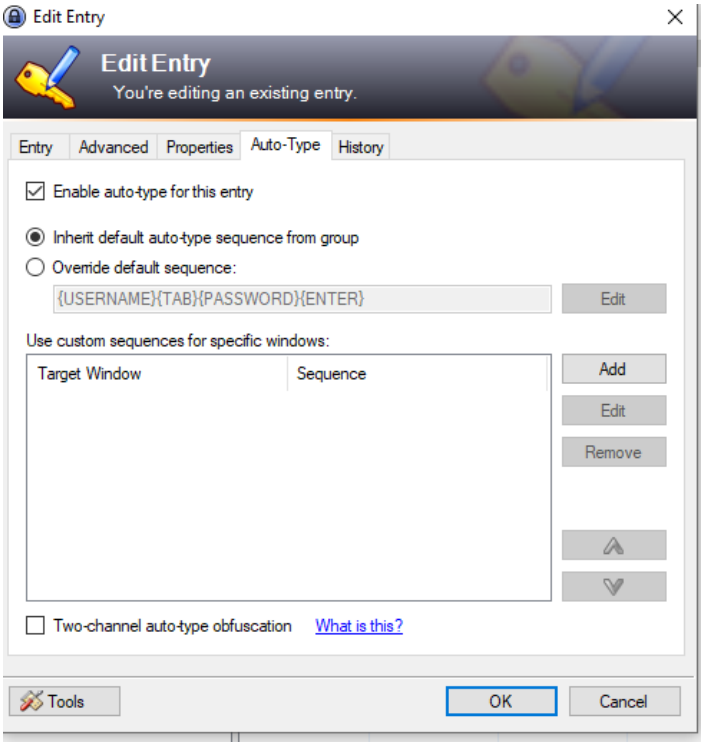




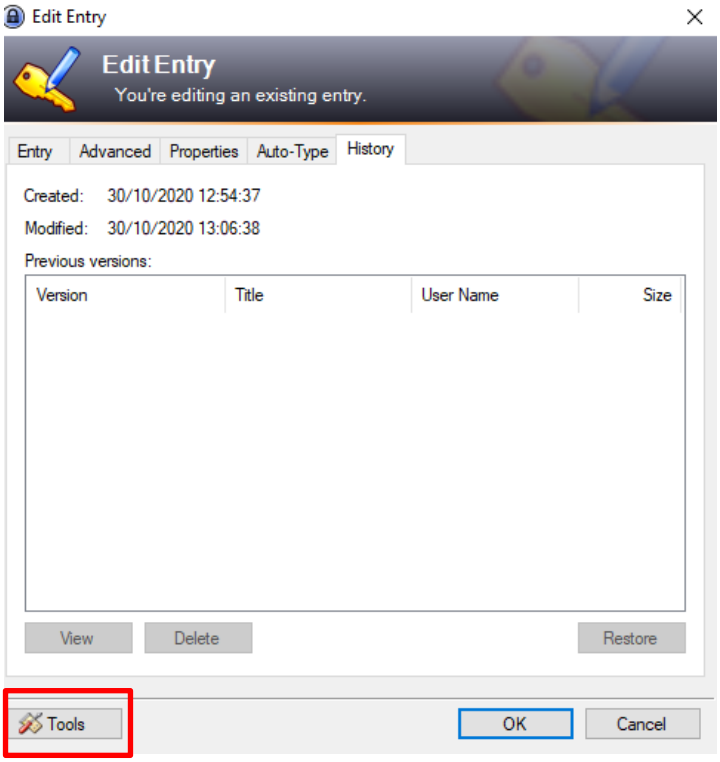
Una vez creada clicamos en ok. En la siguiente pestaña de propiedades podemos configurar el color, poner etiquetas y escribir una URL.



En la siguiente pestaña “auto type” podemos configurar la entrada o dejarla poder defecto, en este caso la vamos a dejar por defecto.



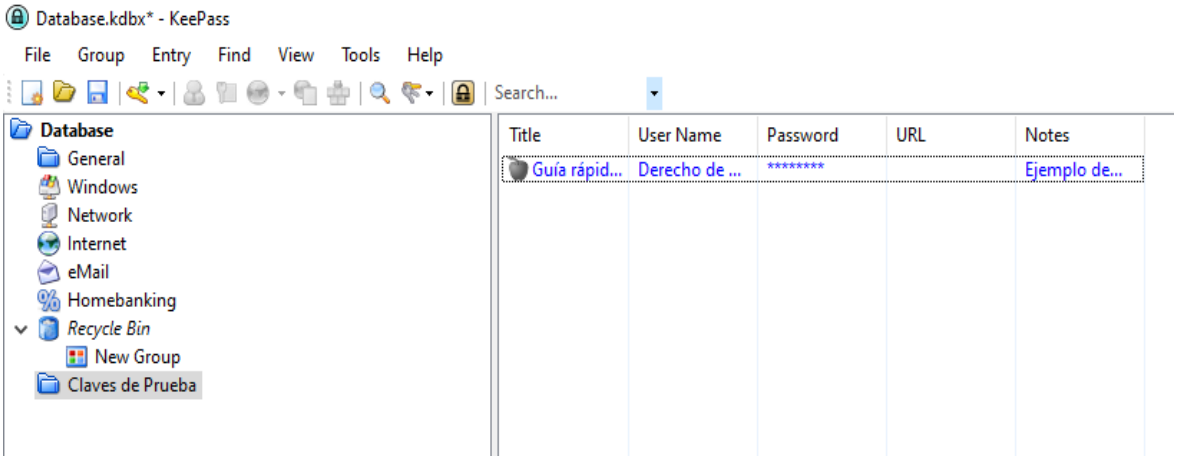
La última pestaña que se nos muestra es el historial de cambios de la contraseña, en este caso está limpio porque está recien creada.



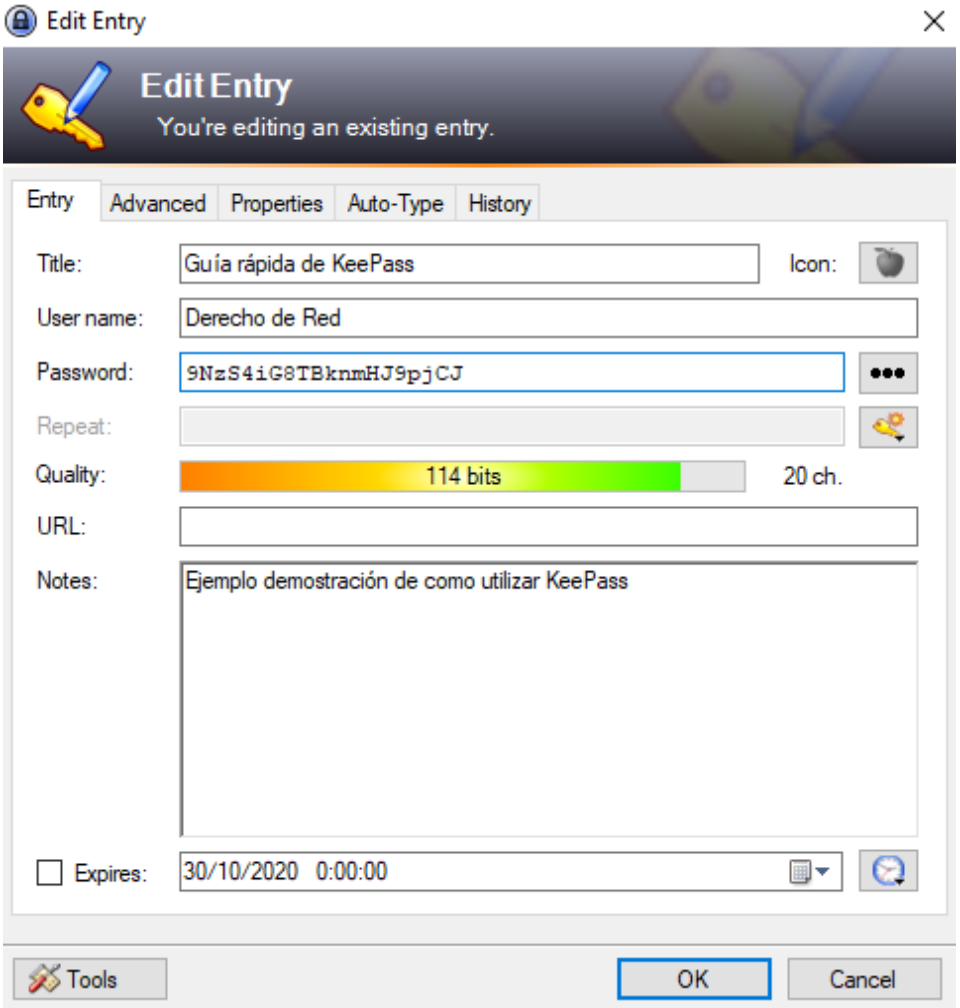
Clicamos en Ok y así se ha terminado de configurar la entrada.

Por último añadir que el botón de herramientas (Tools) encontramos varias opciones de ayuda para configurar las entradas.

7º Para finalizar el proceso podemos observar que la entrada que hemos creado está en nuestro panel de control.



Como podemos ver la contraseña la hemos ubicado en la carpeta que hemos creado previamente. Si clicamos dos veces sobre la contraseña encontramos la información que hemos configurado. Por lo tanto de este modo tenemos guardada la contraseña.



10. DOCUMENTOS DE REFERENCIA.

- ☐ ASTM E3046-15, Standard Guide for Core Competencies for Mobile Phone Forensics, ASTM International, West Conshohocken, PA, 2015, www.astm.org.

- ☐ Normas de creación y uso de contraseñas NP40. Guía de Seguridad de las TIC CCN-STIC 821. Febrero 2018.

- ☐ Documentación propia sobre gestores de contraseñas.

- ☐ Programa Keepass

- ☐ Password crackers ECUDRED