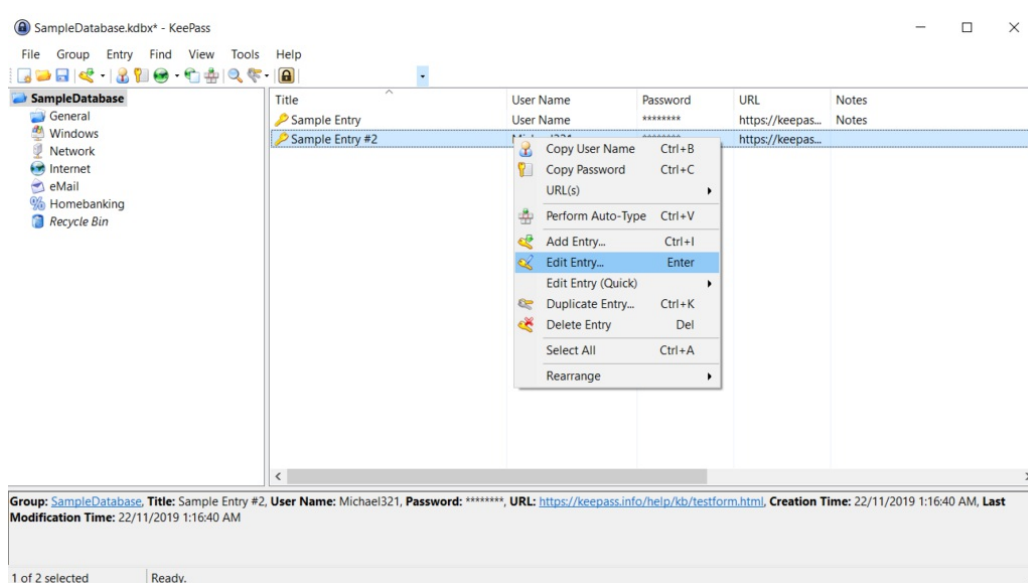


Cómo usar el gestor de contraseñas KeePass

Publicado el [El Informatico](#) - 1 de enero de 2021 -



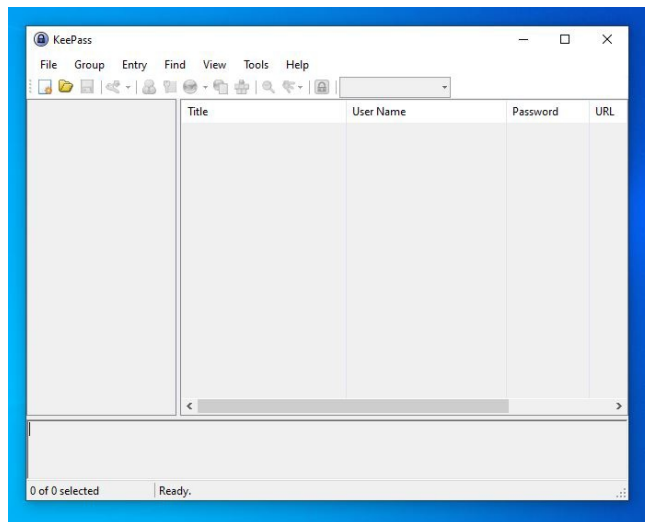
Interfaz del gestor de contraseñas KeePass (Fuente: [Wikipedia](#). Licencia: [GPL](#))

Internet es cada día más complejo y son cada vez más las contraseñas que necesitamos usar. Correos, redes sociales, servicios de almacenamiento en la “nube”, servicios de streaming, juegos... el volumen de contraseñas que podemos llegar a manejar es demasiado grande. Por ese motivo, mucha gente opta por prácticas poco seguras como usar contraseñas débiles muy fáciles de recordar (y también de adivinar) o incluso usar la misma contraseña para todo.

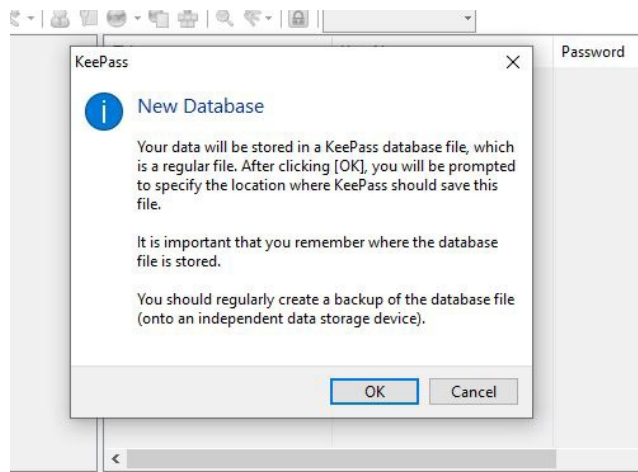
Aunque hay gente que anota éstas contraseñas en un cuaderno, al final el volumen de contraseñas es tal, que puede llegar a resultar poco práctico. Para éstos casos, podemos usar **un gestor de contraseñas** como, por ejemplo, **KeePass**.

KeePass es un gestor de contraseñas Open Source y gratuito que nos permite gestionar nuestras contraseñas mediante categorías. Para ello, utiliza una base de datos cifrada con un algoritmo basado en AES, y cuya contraseña deberemos recordar (mejor una que mil). KeePass se puede descargar para Windows y Linux desde la página web oficial: keepass.info. Las nuevas versiones 2.xx están basadas en .NET, y por tanto se pueden ejecutar en Linux usando [Mono](#). Existe una versión específica para dispositivos Android llamada [KeePassDroid](#), compatible con las

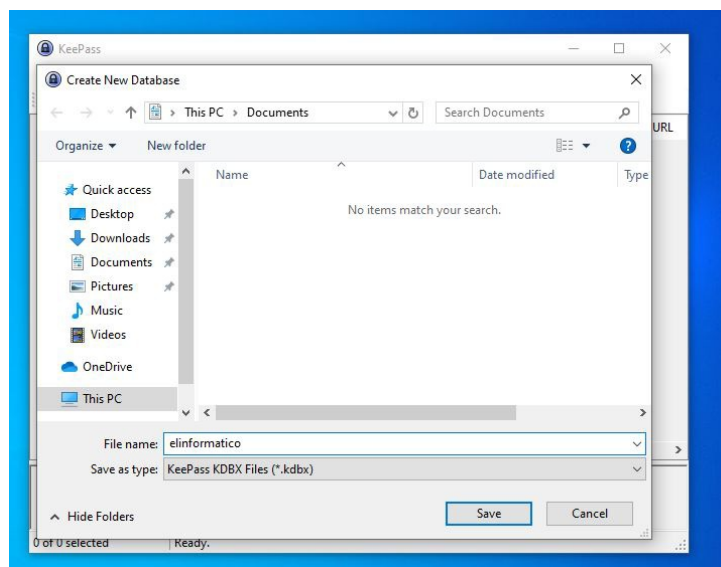
bases de datos de la versión de PC.



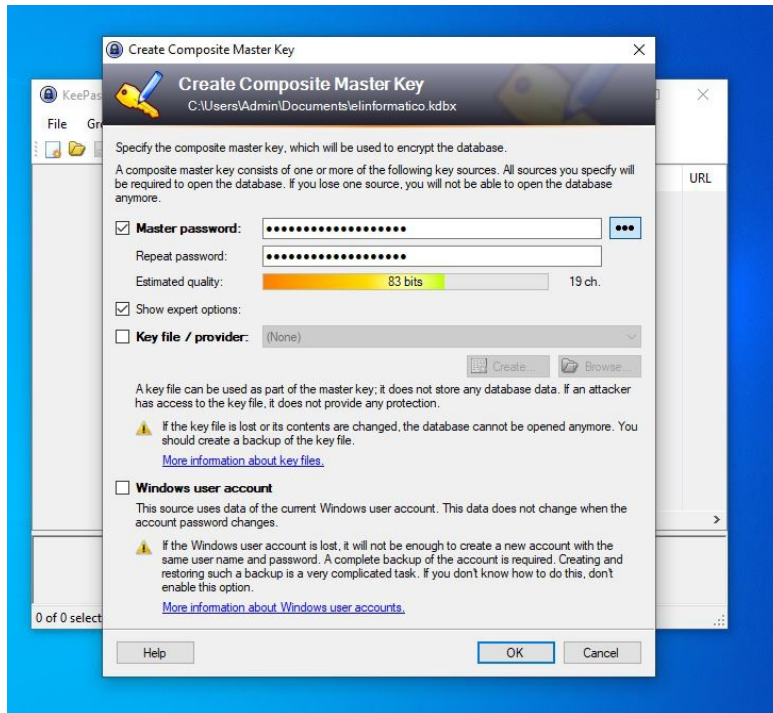
Al iniciar la aplicación por primera vez, se nos presentará la interfaz vacía. Para poder almacenar contraseñas, es necesario crear primero la base de datos. Para ello, pulsa sobre el botón **New** de la barra de herramientas, o pulsa **Ctrl+N** en tu teclado.



Al iniciar el asistente para la creación de la base de datos, KeePass te informa de que debes recordar la ubicación de la base de datos, así como hacer copias de seguridad periódicas de la misma. Haz click sobre **OK**.



Selecciona la ubicación donde quieras guardar la base de datos y pulsa sobre **Save**. La carpeta personal de documentos, o en Linux tu carpeta de usuario, son buenos lugares para almacenar la base de datos. También puedes crear una carpeta compartida con otros usuarios si quieres compartir esa base de datos con otros usuarios, o incluso en una unidad de red si quieres que esté disponible en otros equipos de la red. Ojo, eso sí, de quien puede acceder a ese archivo. Aunque la base de datos estará encriptada, es peligroso que otra persona ajena se haga con ella.



Una vez selecciones el lugar donde se almacena la base de datos, el programa te pedirá una **contraseña de encriptación**. Como alternativa (o complemento) a la contraseña, KeePass te ofrece las opciones de **usar un archivo llave (Key file)**, o incluso **iniciar sesión con tu cuenta actual de Windows (Windows user account)**.

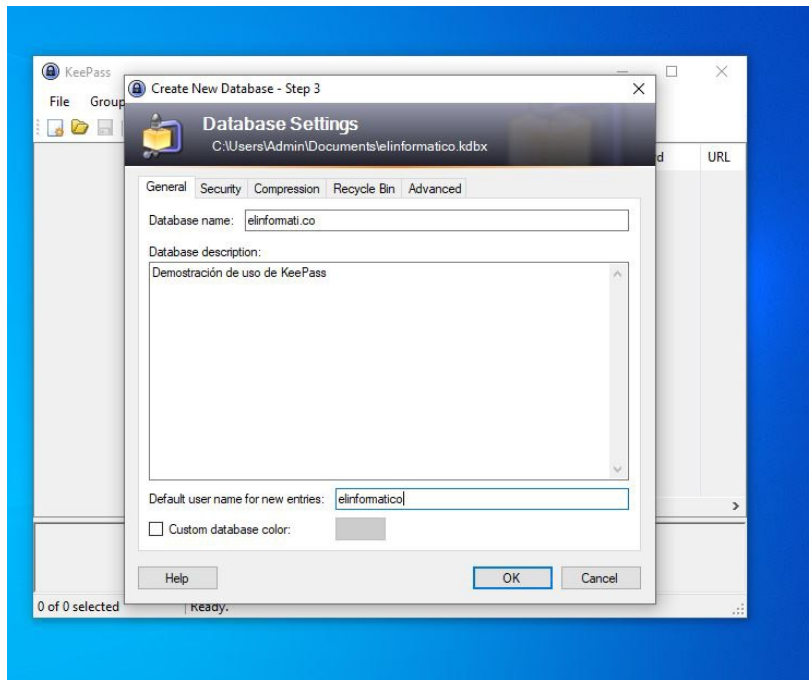
Recomiendo usar **sólo una contraseña**. Si usas un archivo de llave, cualquiera que tenga acceso a ese archivo podrá desbloquear la base de datos. Y si usas una cuenta de usuario, cualquiera que inicie sesión con tu usuario puede acceder a tu base de datos. Además, ten en cuenta que si la ligas a tu cuenta de usuario, la base de datos tomará en cuenta tu **ID de usuario**. Esto quiere decir que, si pierdes la cuenta, perderás el acceso a tu base de datos aunque crees otra cuenta con el mismo nombre.

Para la contraseña (Para KeePass y para cualquier cosa que necesites una contraseña), utiliza una contraseña bien larga. Que tenga un mínimo de 12 caracteres (cuantos más, mejor), que utilice todo tipo de caracteres mezclados (letras mayúsculas, minúsculas, números, y algunos símbolos como \$, @, etc.), que sea relativamente fácil de

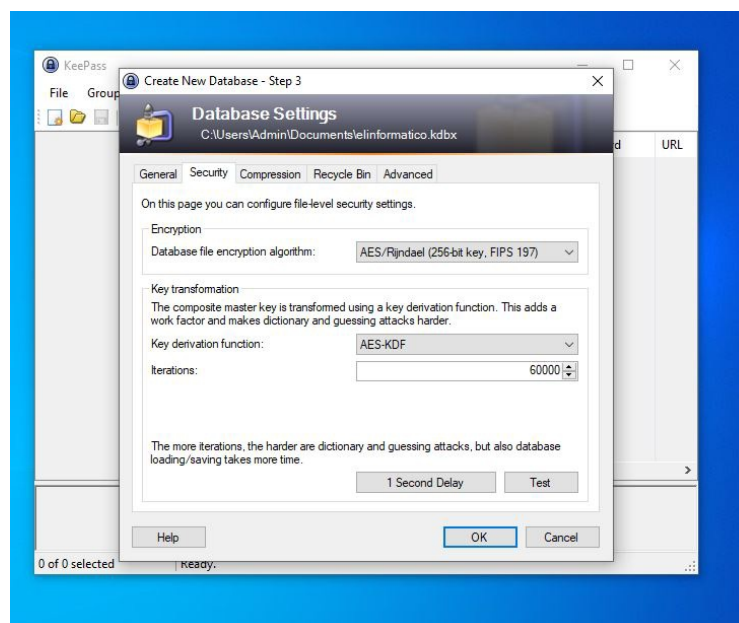
memorizar para ti, pero que sea muy complicado de adivinar para los demás, y que no contenga palabras con significado. Asegúrate además de que sólo usas esa contraseña con KeePass, de modo que sea única.

Recuerda que, una vez empieces a utilizar KeePass, sólo tendrás que recordar ésta contraseña. Ya que las demás se encuentran dentro de la base de datos.

Introduce la contraseña dos veces en Master Password y Repeat Password, y pulsa OK para ir al siguiente paso.



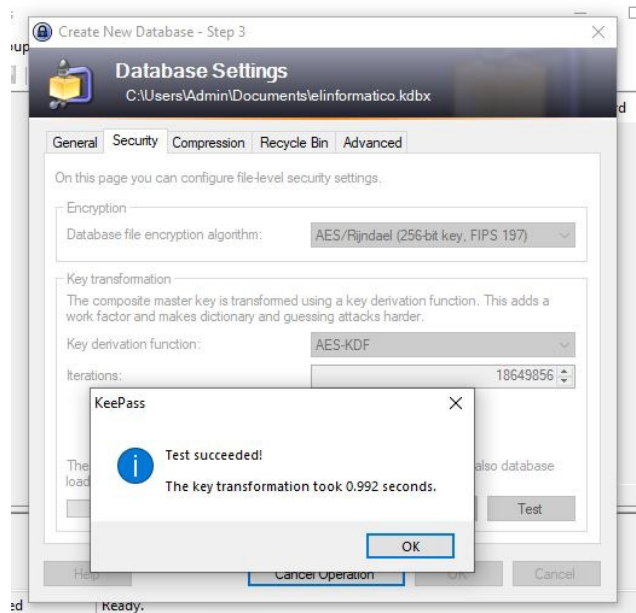
En el siguiente paso, puedes darle un nombre a tu base de datos y redactar una descripción. Esto es importante si vas a administrar varias bases de datos.



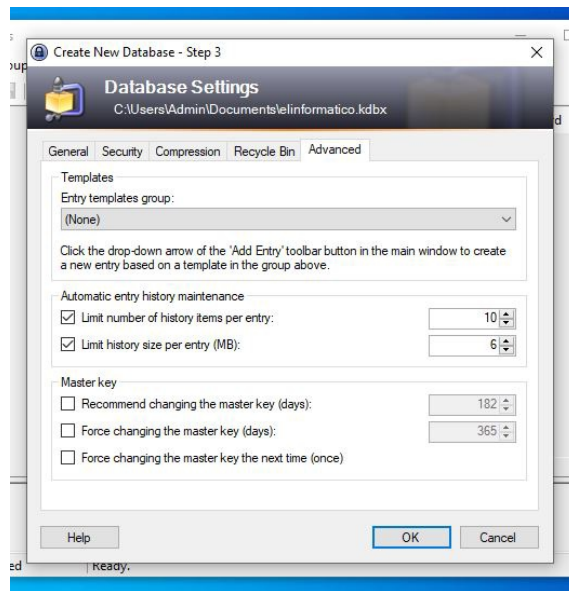
En la pestaña de seguridad (Security), podrás especificar los parámetros de la

encriptación de tu base de datos. **Esto es muy importante**, ya que en caso de que alguien sustraiga tu base de datos pero no tenga acceso a la clave, los parámetros especificados aquí, así como la longitud y complejidad de la contraseña, determinarán la dificultad para poder desencriptar la base de datos mediante ataques de fuerza bruta.

El parámetro más importante a cambiar en éste caso, es el de **Iterations**. Este parámetro determina cuantas repeticiones se usan a la hora de generar la clave de encriptación. A mayor número de iteraciones, mayor será el tiempo que tarda en generarse la clave, y por tanto el tiempo que se tarda en probar una clave durante un ataque de fuerza bruta. Pero también aumentará el tiempo que se tarda en cargar o guardar la base de datos. Si haces click en **1 Second Delay**, el programa probará cuál es el número de iteraciones necesarias para que el proceso tarde un segundo. Puedes comprobar el tiempo pulsando sobre **Test**.

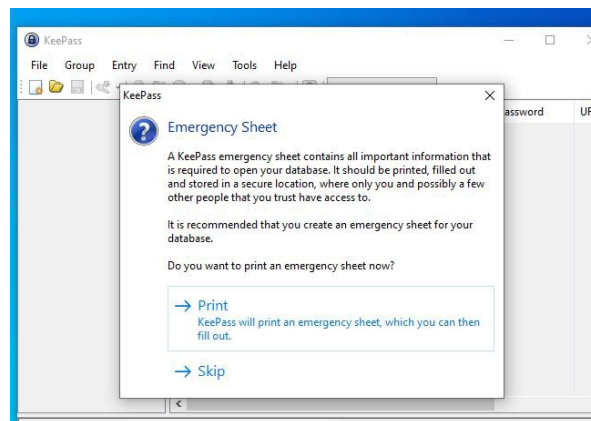


Recuerda que, dependiendo de las prestaciones del equipo que utilices, el tiempo que tarda en computarse una clave puede ser **mayor o menor**. Esto quiere decir que lo que para ti tarda 1 segundo, para un atacante con una red extensa dedicada a la criptografía podría tardar milésimas por clave. Un segundo debería de ser relativamente seguro.



Por último, en la pestaña de **Avanzado (Advanced)**, puedes establecer algunos parámetros como, por ejemplo, forzar el cambio de clave pasados unos días.

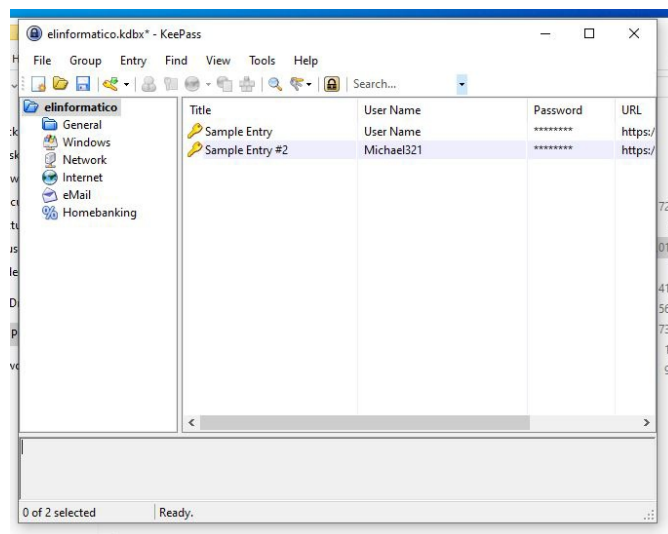
Al finalizar el asistente, pulsa sobre OK.



KeePass te ofrecerá la posibilidad de imprimir una hoja con algunos de los parámetros de la base de datos, donde además podrás anotar tu contraseña. No es necesario, ya que puedes anotarlo tú a mano si quieres. Pulsa “Print” si quieres hacerlo, o “Skip” si no.

Asegúrate de tener la contraseña bajo resguardo. Ya que si se te

olvida, o si la pierdes, no podrás recuperar tus datos, lo cuál sería un desastre. ¡MUCHO OJO!

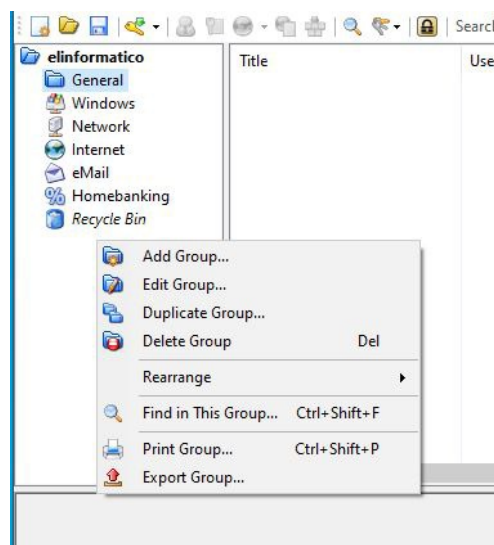


Una vez finalizado el asistente, la interfaz de KeePass cambia y nos muestra el contenido de la base de datos, que de momento sólo tiene dos claves de demostración que podemos borrar seleccionándolas y pulsando la tecla **Suprimir**.

Gestión de contraseñas

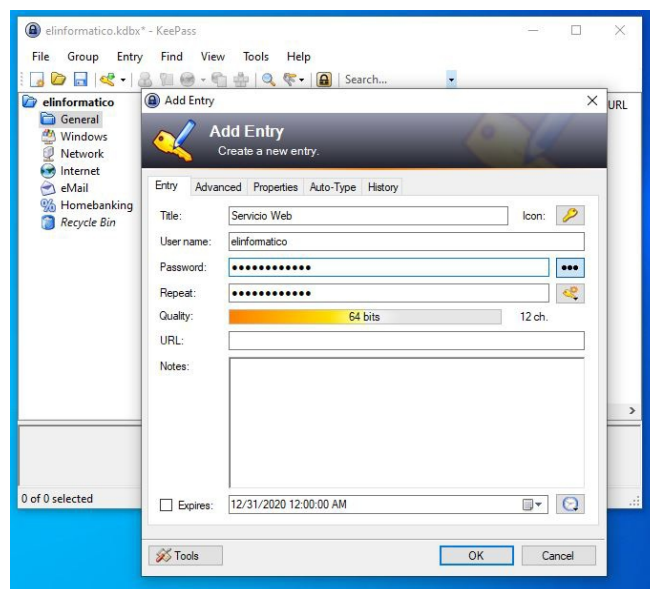
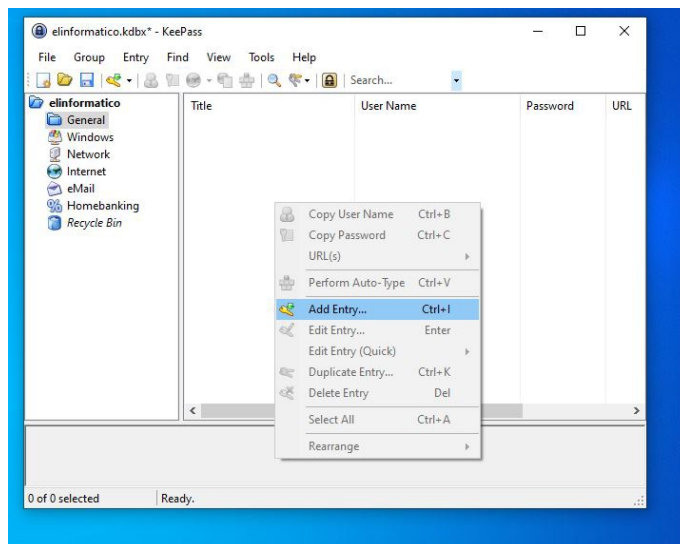
La interfaz de KeePass se divide en dos paneles. En el panel de la izquierda, tenemos los **grupos de contraseñas**. Estos grupos funcionan como categorías dentro de las cuales se pueden almacenar contraseñas.


Si haces click derecho sobre éste panel, podrás editar los diferentes grupos, añadir nuevos grupos, o borrarlos.




Las nuevas contraseñas que almacenes se almacenarán en el grupo seleccionado. Estas contraseñas se gestionan en el panel de la derecha. Para añadir una nueva contraseña, haz click derecho sobre dicho panel, y pulsa sobre **"Add Entry"**, o pulsa

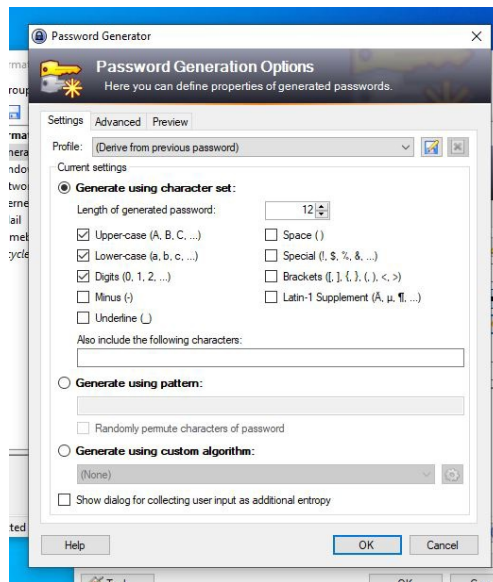
la combinación de teclas **Ctrl+I**.



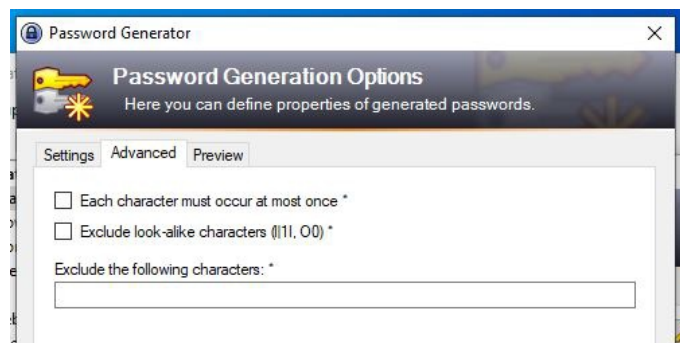
En la ventana de la contraseña, podrás especificar un título para la contraseña, un nombre de usuario, y la contraseña asociada. Si no quieres repetirla dos veces y estás seguro de que nadie está mirando tu pantalla, puedes hacer click sobre el botón de los **tres puntos**  para mostrar la contraseña.

Si no tienes claro qué contraseña poner, el botón de la llave con la chispa  te permitirá abrir un asistente para generar una contraseña. Para ello, en el menú que se abre, haz click sobre **Open Password Generator**.



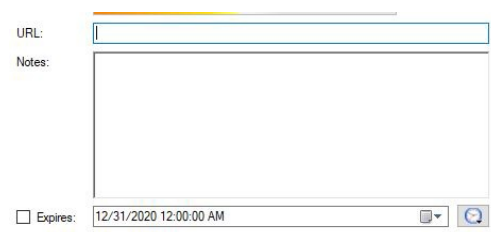


En esta ventana puedes seleccionar todos los parámetros que quieras para tu contraseña. Recomiendo activar Upper Case, Lower Case, Digits, Underline, y Special.

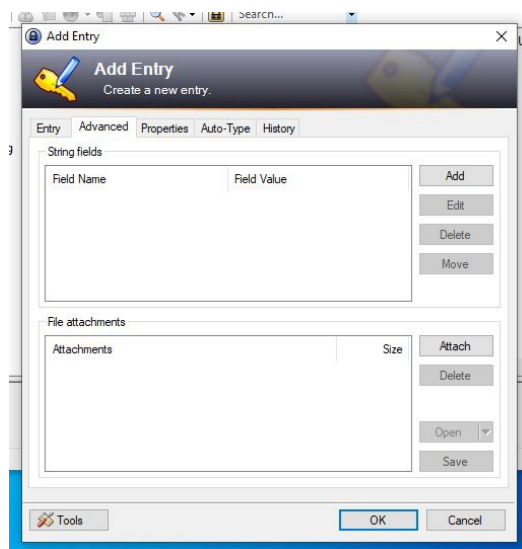


En la pestaña de Advanced del generador de contraseñas puedes también especificar si quieres que cada carácter sea único, y si quieres excluir caracteres que tengan una apariencia similar a otros caracteres.

Al finalizar, pulsa sobre OK para volver a la pantalla de creación de contraseña con la contraseña generada.



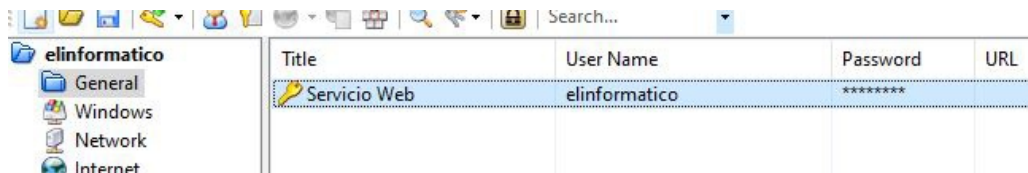
Si quieres además recordar la URL del servicio al que pertenece tu contraseña, puedes anotarlo en el campo URL. En Notes puedes hacer algunas anotaciones al respecto, y por último puedes activar el campo Expires si quieres que la contraseña caduque tras un tiempo para avisarte de que debes cambiarla.






Si necesitas hacer algunas anotaciones más avanzadas, puedes hacerlo desde la pestaña **Advanced**. Si por ejemplo necesitas anotar el valor de otros campos asociados a tu contraseña, puedes añadirlos en el apartado **String fields**.

Si también necesitas algún archivo junto a la contraseña, puedes adjuntar los archivos en el apartado **File attachments**. Puede servir, por ejemplo, para almacenar archivos con claves **PGP**.

Pulsa OK cuando finalizes.

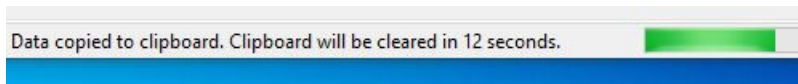


Aunque la contraseña está creada, no estará almacenada en la base de datos. Para guardar los cambios que has realizado en la base de datos, pulsa sobre el botón de **Guardar** . **Asegúrate siempre de guardar todos los cambios que realices en la base de datos.**

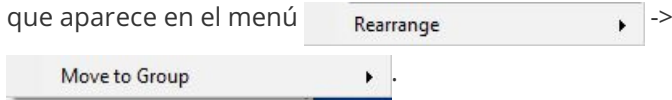
Las contraseñas que guardes aparecen en una lista dentro de la categoría seleccionada. Puedes hacer doble click sobre una contraseña para acceder a los valores de la misma (y modificarlos si lo necesitas), o si por ejemplo quieres iniciar sesión, puedes hacer click derecho sobre la contraseña y seleccionar **Copy User Name**  para copiar el nombre de usuario en el portapapeles, y **Copy Password**  para copiar la contraseña.

Podrás pegar estos valores en el formulario de inicio de sesión que utilices pulsando la combinación de teclas Ctrl+V. Por tu seguridad, los datos copiados sólo estarán disponibles durante 12 segundos, tras los cuales **KeePass borrará tu**


portapapeles.



Si quieres mover una clave a otro grupo distinto, puedes mover cualquier clave haciendo click derecho sobre la misma, y seleccionando un grupo dentro de la lista que aparece en el menú



Puedes usar ésta función para categorizar tus claves o incluso para recuperar claves de la papelera de reciclaje si te has equivocado al borrarlas.

Por último, cuando quieras mantener KeePass abierto en segundo plano sin cerrarlo por un tiempo, asegúrate de utilizar la función **Lock Workspace** .

Cuando vuelvas a la ventana de KeePass, te solicitará la clave de la base de **datos**. Esto es importante, sobre todo si estás en una oficina o un entorno donde hay más gente.



ANTERIOR

Por un feliz 2021

SIGUIENTE

Aprende a identificar el malware al navegar en internet

Buscar ...



Entradas Recientes

- [Encriptación LUKS con CRYPTSETUP](#)
- [Se acabaron las bromas. A partir de ahora vas a estar constantemente vigilado en todas partes.](#)
- [Microsoft anuncia su nueva versión de su sistema operativo: Windows 11](#)
- [La historia de Internet en España](#)
- [Terminología moderna usada en tecnología digital](#)

- [Desactiva la ejecución de JavaScript de los archivos PDF, en Firefox y TOR browser.](#)

Categorías

[Actualidad](#)[Android](#)[Básicos](#)[Ciberseguridad](#)[Criptografía](#)[Emulación / Virtualización](#)[FOSS](#)[Hacking](#)[Informática](#)[Internet](#)[Juegos](#)[Opinion](#)[Otros](#)[Personal](#)[Privacidad](#)[Programación](#)[Tecnología](#)[Time Machine](#)[Tutoriales](#)

RSS

[Subscribirse al feed RSS](#)[Inicio](#)[Catálogo](#)[Tutoriales](#)[Política de privacidad](#)[Política de Cookies](#)[Acerca de mi](#)[Acerca de ElInformati.co](#)