KeePass nos facilitará enormemente la gestión de usuarios y contraseñas para acceder a sitios privados de Internet.

KeePass

Introduccion

Muchos de los servicios que nos presta Internet, exigen que nos identifiquemos y por eso, cada vez es más normal tener que acceder a sitios web como usuarios autentificados, ejemplo:

- Acceder al correo electrónico (gmail, yahoo mail, hotmail, etc...)
- Acceder a redes sociales (facebook, tuenti, etc...)
- Acceder a foros privados
- Editar webs en gestores de contenidos (MediaWiki, Joomla, Drupal,...)
- Subir videos o fotos (youtube, picasa, flickr, ...)
- Acceder a plataformas web de formación (Mentor, ISFTIC, Universidades, ...)
- Facturas electrónicas: compañías de luz, gas, teléfono, móvil, internet.

Para acceder a cualquiera de estos lugares, es necesario introducir el **nombre de usuario y la contraseña** , lo que nos exige acordarnos de decenas de nombres de usuario y decenas de contraseñas, así como decenas de URLs para acceder a dichos sitos web.

Muchos sitios web requieren autentificación

Muchas personas para simplificar, deciden utilizar el **mismo nombre de usuario y la misma contraseña para todos los sitios** , lo cual es cómodo, pero supone un riesgo de seguridad importante ya que si algún usuario malintencionado consigue averiguar nuestra contraseña, podrá entrar en todos nuestros sitios privados. Esto les ha pasado esto a algunos personajes públicos y les ha causado varios problemas.

Otras veces utilizamos **contraseñas fáciles** como números sencillos, nuestros apellidos, fecha

de nacimiento, teléfono, login del usuario, etc. A menudo, cuando utilizamos contraseñas un poco más raras, solemos **anotarla en un post-it**, lo cual es más inseguro que tener una contraseña sencilla.

Cada vez se hace más necesario tomar conciencia de la importancia de utilizar unas contraseñas seguras parar evitar que nadie **suplante nuestra identidad** ocasionándonos graves problemas.

KeePass es una aplicación que nos facilitará enormemente la gestión de usuarios y contraseñas para acceder a sitios privados de Internet.

Características principales de KeePass

- Almacena URL, nombre de usuario (login), contraseña (password) e información adicional que deseemos.
- Función de Escritura Automática (acceder a los sitios automáticamente).
- Base de datos cifrada de forma segura y protegida con contraseña maestra y/o un archivo llave.
- Generador de complejas contraseñas.
- Traducido a varios idiomas (Español, Catalán, Gallego, etc...).
- Software libre (licencia GPL). Versiones para Windows, Linux y MAC. Código fuente disponible.

La contraseña maestra da acceso al resto de contraseñas

Utilizando KeePass

En sistemas **Windows**, KeePass se puede descargar desde el enlace: KeePass download . Descargaremos en una carpeta temporal (ejemplo en C:/TEMP) la versión **KeePass Portable** . Una vez descargado el archivo zip con la versión portable de KeePass, debemos descomprimirlo utilizando algún descompresor como WinZip o 7zip

y lo mejor es descomprimirlo en nuestra memoria USB para utilizar KeePass en cualquier PC sin necesidad de instalación.

Para instalar KeePass en **Ubuntu** (solo disponible para las últimas versiones de Ubuntu), se pueden utilizar los repositorios de Ubuntu, por lo tanto, la instalación es tan sencilla como ejecutar el siguiente comando desde una consola: sudo apt-get install keepassx

Idioma Español

Para ejecutar KeePass en **Windows**, debemos hacer doble clic en el archivo **KeePass.exe** que se encuentra en la carpeta donde hayamos descomprimido KeePass Portable.

Inicialmente el programa está en Inglés, pero KeePass está traducido a varios idiomas entre los que se encuentran el Español, el Catalán y el Gallego. Para seleccionar el idioma Español, necesitamos descargar el archivo de idioma desde el enlace: KeePass translations . Debemos descomprimir el archivo de idioma Spanish.lng en la carpeta donde se encuentre el programa. Después ejecutaremos KeePass.exe e iremos a
View > Change Language > Spanish
. Para otros idiomas, habrá que repetir el mismo proceso.

Una vez seleccionado el idioma Español, debemos reiniciar keepass. Veremos la pantalla inicial de KeePass:

Pantalla inicial de KeePass

La pantalla de KeePass inicialmente aparece vacía. Lo primero que tendremos que hacer es crear una nueva base de datos en la que almacenar nuestras contraseñas. Para ello, iremos a Archivo > Nuevo.

El programa nos pedirá que proporcionemos una contraseña maestra (Master Password) para

proteger la nueva base de datos. Esa contraseña es la **única contraseña que debemos recordar** . Con la contraseña maestra tendremos acceso a todas las URLs, usuarios y contraseñas almacenadas en nuestra base de datos. Si perdemos nuestra contraseña maestra, perderemos el acceso a la base de datos de KeePass ya que no se puede recuperar.

Establecemos la contraseña maestra

El programa nos pedirá que introduzcamos de nuevo la contraseña maestra, para evitar errores al teclear y una vez comprobado que las dos contraseñas introducidas coinciden, aparecerá la ventana con la base de datos cargada.

En la siguiente captura vemos la pantalla que aparece nada más crear una base de datos.

Base de datos recién creada

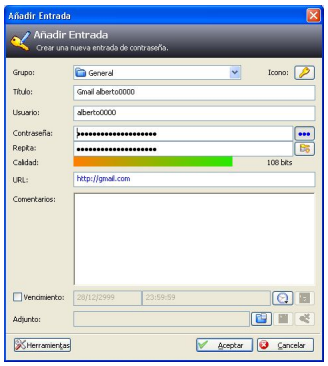
Observamos que aparece una carpeta llamada **General** desde la que cuelgan cinco carpetas que nos servirán para clasificar nuestras contraseñas. Estas carpetas podemos eliminarlas,

cambiarlas de nombre o crear nuevas carpetas, así como personalizar los iconos.

Añadir entradas

Vamos a crear una entrada. Supongamos que queremos almacenar el usuario y la contraseña de nuestra cuenta de correo de Gmail. Los datos básicos que vamos a almacenar son la URL, el nombre de usuario y la contraseña. Supongamos que los datos son los siguientes: **URL**: ht tp://gmail.com
nombre de usuario
: alberto0000
contraseña
: manzana

Para añadir la nueva entrada debemos ir a Editar > Añadir Entrada.



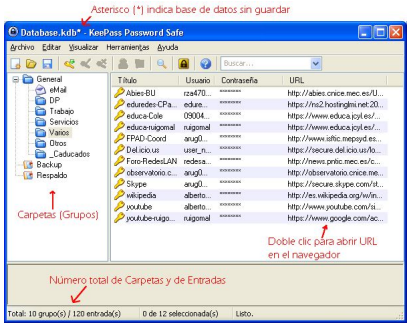
Añadir entrada

A continuación explicaremos brevemente los campos más significativos de la ventana anterior:

- **Grupo:** Carpeta en la que se almacenará la entrada
- **Título:** Título de la entrada. Se recomienda coincida con el título de la página
- **Usuario:** El login de usuario
- **Contraseña:** La contraseña del usuario. La barra -Calidad- (representa la seguridad de la misma)
- **URL:** La URL del sitio web
- **Comentarios:** Apartado para introducir información adicional, observaciones, etc...
- **Vencimiento:** Si nuestro sitio web, por seguridad nos obliga a cambiar la contraseña cada ciento tiempo, podemos establecer esta alarma que nos indica cuánto falta para que nuestra contraseña caduque.

Si hacemos clic en -Aceptar-, nuestra entrada quedará creada y la base de datos ya no estará vacía, sino que **dispondrá de una entrada**. Al haber modificado la base de datos, en la barra del título de la ventana de KeePass aparece el nombre de la base de datos seguido de un **asterisco**
que significa que nuestra base de datos ha sido modificada pero no ha sido guardada. Al cerrar la aplicación nos preguntará si deseamos guardar la base de datos. También podemos guardar en cualquier momento la base de datos haciendo clic en el icono del disquete de la barra de herramientas.

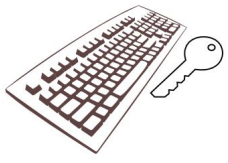
Podemos crear tantas entradas como queramos. En la siguiente captura de pantalla vemos una base de datos con varias entradas creadas:



Podemos crear todas las entradas que necesitemos

Escritura Automática

La función de Escritura Automática (también conocida como función Auto-Tipeo o Auto-Type) es la característica **más importante de KeePass** ya que permite abrir la URL y autocompletar el nombre de usuario y la contraseña, de forma automática.



KeePass tecleará por nosotros

La escritura automática se realiza en dos pasos:

- **1.- Abrir la URL:** Haciendo doble clic sobre la URL de la entrada almacenada en KeePass, **se abrirá el navegador de Internet y accederá a la URL**
- **2.- Realizar la escritura automática del nombre de usuario y la contraseña:** Desde la ventana del navegador debemos **teclear Ctrl + Alt + A** que es la combinación de teclas de KeePass para **disparar la Escritura Automática**. Se recomienda que el título de la entrada coincida, al menos en parte, con el título de la página de entrada de los sitios web (página de login) para que KeePass pueda distinguir qué usuario y qué contraseña debe escribir.

Normalmente, la página de login, dispone de un **formulario con dos cajas de texto**, una para introducir el **nombre de usuario** y otra para introducir la **contraseña**. KeePass suele detectar correctamente el formulario de entrada y no tiene problemas para introducir el nombre de usuario y la contraseña automáticamente.

En algunos sitios web, la página de login no coincide con la página principal del sitio, en tal caso, la URL que hay que almacenar en KeePass es la **URL de la página de login**.

En otros casos, la página de login es muy compleja con varias cajas de texto que pueden confundir a KeePass y es necesario **personalizar la secuencia de Escritura Automática**, para ello, hay que editar la Entrada haciendo Clic derecho sobre ella > Editar/Visualizar Entrada > Herramientas > Escritura Automática Personalizar Secuencia. En la ventana comentarios aparecerá la **secuencia por defecto** de Auto-Type: {USERNAME}{TAB}{PASSWORD}{ENTER} que significa que KeePass escribirá el nombre de usuario, tecleará un tabulador, escribirá la contraseña y tecleará Intro de forma automática. Si la página de login tiene otro diseño y fuera necesario teclear tres veces el tabulador para escribir la contraseña, **crearíamos la siguiente secuencia**: {USERNAME}{TAB}{TAB}{TAB}{PASSWORD}{ENTER}. Si la página de login pide un código

de verificación (como por ejemplo el correo web del ISFTIC), tendríamos que teclearlo manualmente. En tal caso debemos modificar la secuencia para que nos rellene el usuario y la contraseña, teclee un tabulador para posicionar el cursor en la casilla para introducir el código de verificación, y quitar {ENTER} para que no envíe el formulario:
{USERNAME}{TAB}{PASSWORD}{TAB}

Las funcionalidades de KeePass se pueden incrementar instalando plugins. Uno de los plugins más interesantes es el plugin KeeForm que incrementa las funcionalidades de la escritura automática.

Seguridad en Escritura Automática

KeePass utiliza una **doble técnica** de envío de **pulsaciones** de teclas junto con la utilización del **portapapeles**, de forma que al realizar Escritura Automática, es capaz de despistar a casi todas las aplicaciones espias que suelen utilizar los hackers para capturar contraseñas. La gran mayoría de los troyanos que espían el teclado (KeyLoggers) y espían el portapapeles, son inútiles cuando utilizamos KeePass para identificarnos en los sitios web, por eso, se convierte en una herramienta recomendable principalmente cuando utilizamos un PC que es utilizado por otras personas (PCs del centro educativo, cibercafés, etc...).

Demo en Flash sobre la utilización de KeePass

Generador de contraseñas

KeePass dispone de un Generador aleatorio de contraseñas que puede servirnos para elegir nuestras contraseñas cuando nos registremos en los sitios web. Para utilizarlo debemos ir a **Herramientas > Generador de contraseñas**
, y veremos la siguiente pantalla:

Generador de contraseñas aleatorias

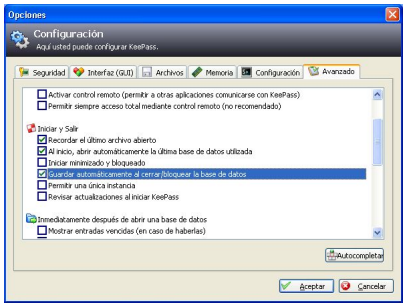
Podemos elegir los caracteres de los que queremos se componga nuestra contraseña (mayúsculas, minúsculas, números y otros símbolos. Debemos asegurarnos que la contraseña que generemos funcione en el sitio web donde la queremos establecer porque a veces no aceptan ciertos símbolos en la contraseña (espacios, comillas, barras, etc...)

Como ahora disponemos de KeePass, en lugar de utilizar contraseñas fáciles es mejor utilizar **contraseñas complejas**. Ejemplo, para nuestro correo de Gmail, en lugar de utilizar como contraseña 'manzana', podemos utilizar 'z86O#?ik/+z9i4IQWqb' que es mucho más dificil de averiguar. La ventaja es que es muy improblable que alguien pueda averiguar nuestra contraseña haciendo pruebas, aunque la desventaja es que **dependemos de KeePass**, porque ni nosotros mismos podremos aprendernos de memoria una contraseña tan compleja, pero esto no es problema porque podemos tener nuestro KeePass Portable en el pendrive USB u oculto en alguna URL dentro de nuestra página web.

Opciones de KeePass

KeePass permite personalizar algunas opciones. Para ello, debemos ir a **Herramientas > Opciones** .

Entre otras opciones, podemos por ejemplo ir a Herramientas > Opciones > Avanzado y establecer las opciones que se ven en la siguiente figura, para que al ejecutar KeePass.exe abra automáticamente nuestra base de datos y al cerrar el programa guarde los posibles cambios que hayamos podido hacer.



Opciones de KeePass

Otra opción interesante es la combinación de teclas para realizar la Escritura Automática que se puede personalizar desde **Herramientas > Opciones > Avanzado > Autocompletar**.

Seguridad de KeePass

KeePass guarda toda la información en la base de datos de KeePass, en un archivo que normalmente se llama **Database.kdb** aunque podemos darle otro nombre.

KeePass guarda en el archivo Database.kdb toda la información: URLs, nombres de usuario, contraseñas, información adicional, secuencias Auto-Type, etc... Para hacer copia de seguridad de KeePass, tan solo debemos salvaguardar el archivo Database.kdb.

El archivo Database.kdb se puede cifrar mediante el sistema **AES o el sistems Twofish**, reconocicos como dos de los mejores sistemas de cifrado. La
contraseña maestra no se almacena
en ningún lugar ni cifrada ni sin cifrar sino que es utilizada en el proceso de cifrado, lo que incrementa la seguridad.

La base de datos se guarda cifrada

Cada vez que se guarda el archivo Database.kdb en el disco duro, se aplica el algoritmo de cifrado un número elevado de veces consecutivas, **en torno a un millón**, para dar más fortaleza al cifrado. Si alguien consiguiera robarnos el archivo Database.kdb y quisiera tratar de descifrarlo por fuerza bruta probando todas las contraseñas posibles, debería aplicar el algoritmo de cifrado un millón de veces por cada clave, lo que tarda aproximadamente en torno a un segundo utilizando un PC rápido. Si elegimos una contraseña maestra que tenga letras mayúsculas, minúsculas y números (60 caracteres distintos), de 6 caracteres de longitud (60^6 =46.656.000.000 contraseñas posibles), harían falta unos
mil quinientos años

para que un PC pudiera probar todas las contraseñas posibles aplicando el algoritmo un millón de veces por contraseña (46.656.000.000 segundos = 1.500 años). Para elegir el algoritmo de cifrado y establecer el número de veces que queremos que se aplique, debemos ir al **Menú Archivo > Configuración de la base de datos**
.

Para incrementar la seguridad, podemos además utilizar un **archivo llave** (Key File). El archivo llave es un archivo de 64 bytes de longitud que almacena una contraseña de 64 caracteres generada aleatoriamente. Sería como utilizar una contraseña de 64 caracteres y se puede utilizar como una seguridad extra además de la contraseña maestra. El inconveniente es que deberíamos guardar el archivo llave en el disco USB y si alguien nos lo roba, tendría la base de datos y el archivo llave.

Conclusiones

Si queremos incrementar la seguridad de nuestras contraseñas o manejamos un número tan elevado de diferentes nombres de usuario y contraseña que nos cuesta recordar, KeePass es una herramienta excelente que nos facilitará el trabajo incrementando la seguridad. Recomiendo a todos aquellos que tengan dificultades para acordarse de sus contraseñas, que antes de utilizar una contraseña demasiado sencilla o tenerla anotada en un post-it en el monitor del PC, se animen a probar esta herramienta.