



Gestionando y creando contraseñas con KEEPASS



Tener contraseñas fuertes es muy importante para proteger nuestra información en internet. Cada contraseña tiene que ser **diferente** a las demás, así, si perdemos alguna perdemos el acceso sólo a una de nuestras cuentas. También deben ser **difíciles de adivinar**, por ejemplo no deberíamos usar nuestro nombre o fecha de nacimiento, porque esa es información personal que se puede averiguar. Usar la frase de una canción, o un conjunto de palabras que juntas nos recuerden algo gracioso (por ejemplo: *tomatesdebilescantabantristemente*) no es

suficiente, porque una contraseña segura no solo debe ser larga, sino una mezcla de letras mayúsculas, minúsculas, símbolos, y números. Así es como se ve una contraseña fuerte y segura:



Contraseñas como esta no se pueden memorizar; lo aconsejable es guardarlas en un lugar seguro. KeePass es un gestor de contraseñas gratuito y de código abierto que **guarda** y nos ayuda a administrar nuestras contraseñas.



Instalación y uso

Existen diferentes versiones de KeePass, antes de instalarlo es importante verificar en el sitio web oficial si esa versión sigue siendo **mantenida y actualizada**.

- **GNU/Linux** → Desde el gestor de software principal o la terminal ([Milpa 19](#)) está disponible **KeePassXC**
- **Windows** → **KeePass** <https://keepass.info/download.html>
- **MacOS** → **MiniKeePass** <https://itunes.apple.com/app/id451661808>

Para usar KeePass en el celular tenemos **KeePassDroid** para Android (disponible en F-Droid) y **MiniKeePass** para iOS.



Recordemos que es aconsejable guardar en nuestra base de datos del celular sólo las contraseñas que necesitemos usar en ese dispositivo.

Una vez instalado KeePass creamos una base de datos (un archivo que terminará en la extensión .kdbx) donde guardaremos las contraseñas, los datos de nuestras cuentas, URLs de los servicios que usamos, etc. Esta base de datos estará cifrada y protegida por una contraseña maestra, que será la única que tendremos que recordar.



Copias de seguridad

Si perdemos el acceso a nuestra base de datos no hay forma de recuperar la información. Por eso es recomendable hacer una copia de seguridad y guardarla en un dispositivo diferente (si nuestra base de datos está en la computadora, guardamos la copia de seguridad en un USB, no en la misma computadora), que a su vez guardaremos en un lugar seguro.



Con KeePass también podemos generar contraseñas seguras, en lugar de tener que inventarnos contraseñas largas y complejas continuamente.

Al momento de guardar nuestra base de datos podemos darle al archivo un nombre ingenioso para que no sea tan obvio que contiene nuestras contraseñas, también podemos cambiar la extensión del archivo para ocultarlo mejor.



Suscríbete a ResistenciaDigital en
Telegram @CanalResistenciaDigital

También podemos imprimir una hoja de emergencia, donde escribiremos en que parte de nuestra computadora hemos creado la base de datos (en el escritorio, en la carpeta Documentos, etc.), y nuestra clave maestra, o una descripción que nos ayude a recordarla, y esta hoja la guardaremos en otro lugar seguro.

El nombre de la canción que me cantaba mi abuela, pero cambiando la vocal E por un 7, todas las A con mayúscula, y poniendo un signo de exclamación entre cada palabra, sin espacios.



¡No olvides que puedes imprimir tu propia MilpaDigital y compartirla!



CódigoSur
EDICIONES