educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 5

Gestión de contraseñas

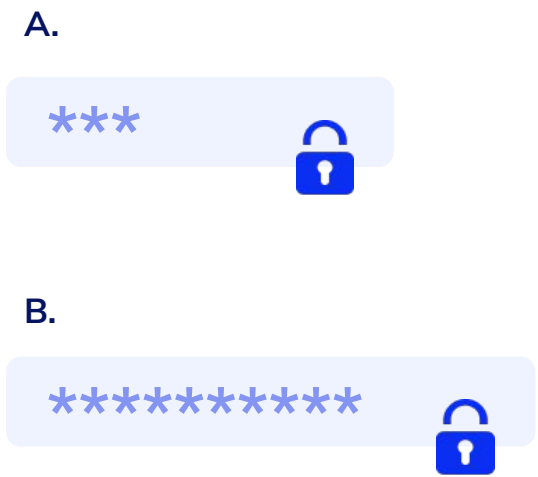
Gestión de contraseñas

A día de hoy, las ***contraseñas*** siguen siendo la **principal forma de protección para nuestros datos y cuentas de usuario**, es por eso que debemos tener ciertas consideraciones para seleccionar contraseñas que nos protejan de manera adecuada. Dependiendo del sistema en el cual se almacene la contraseña, **existen varias formas en las que un atacante podría intentar conseguirla y obtener acceso a nuestra información privada**. Independientemente del sistema que intentamos proteger, los siguientes son consejos prácticos para seleccionar y gestionar nuestras contraseñas.

Consejos generales

1. Separación

Utiliza una contraseña distinta para cada una de tus cuentas importantes, como la cuenta de correo electrónico y la del servicio online del banco. Reutilizar contraseñas conlleva un riesgo. Si alguien averigua tu contraseña para una cuenta, podría acceder a tu dirección de correo electrónico, o incluso a tu dinero y saber dónde vives. Las contraseñas que utilizamos para cuentas que no son de nuestra importancia y que no permiten acceso a datos confidenciales, pueden ser reutilizadas.



2. Renovación periódica

Si alguien ha averiguado tu contraseña, puede estar accediendo a tu cuenta sin tu conocimiento. Si cambias tu contraseña de forma periódica, podrás limitar este tipo de acceso no autorizado.

3. Complejidad

Si utilizas **números, símbolos y combinaciones de mayúsculas y minúsculas** en tu contraseña, conseguirás que sea más difícil averiguarla.

Por ejemplo, una contraseña de 8 caracteres compuesta por números, símbolos y letras mayúsculas y minúsculas es más difícil de averiguar que una que sólo esté compuesta por 8 letras en minúscula, ya que la primera tiene más de 30.000 combinaciones posibles.

4. Evitar la Inclusión de datos personales

Crea una contraseña exclusiva que no esté relacionada con tu información personal y que utilice una combinación de letras, números y símbolos. Por ejemplo, puedes seleccionar una palabra o una frase al azar e insertar letras y números en el principio, en el medio y en el final para conseguir que sea muy difícil de averiguar (por ejemplo, *FeL1C3s@Fi3StAs*).

No utilices palabras o frases simples, como *contraseña* o *quieroentrar*, ni patrones de teclado como *qwerty* o *qazwsx*, ni patrones secuenciales como *abcd1234*, ya que, si lo haces, tu contraseña será más fácil de averiguar.

5. Actualizar los métodos de recuperación

Algunos sistemas permiten la funcionalidad de *Olvidé mi contraseña*, y en la mayoría de los casos se basan en enviar una contraseña temporal a la dirección de correo electrónico que hayamos configurado para tal propósito. Siempre debemos mantener actualizada esta información.

Almacenamiento seguro de contraseñas

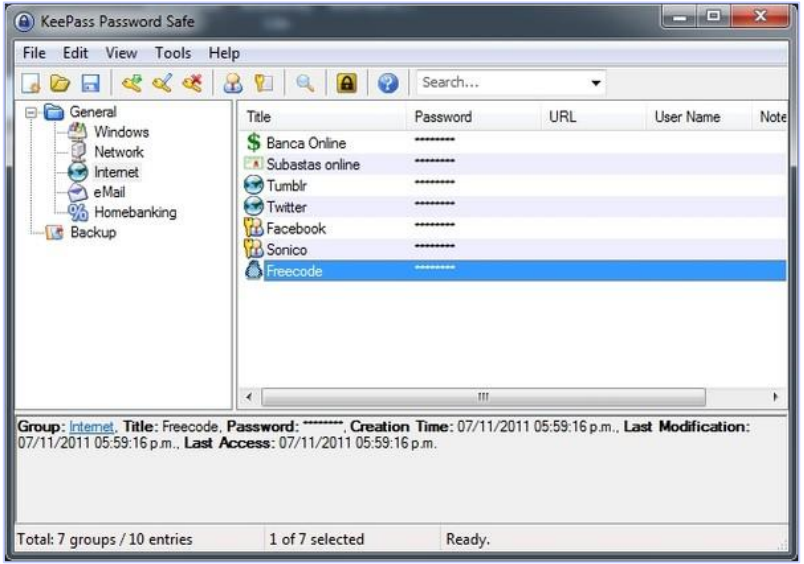
Una vez seleccionadas las contraseñas para nuestras cuentas, es muy posible que nos veamos en la tarea de memorizarlas, lo cual muchas veces resulta imposible, por la complejidad y cantidad de las mismas. Es por eso que se recomienda almacenar las mismas en algún sistema **gestor de contraseñas**, y se desaconseja terminantemente el escribir las contraseñas en algún lugar que pueda ser visto por otras personas.

KeePass

KeePass (keepass.info) es una aplicación de administración de contraseñas, de código abierto y con un potente abanico de características.

Viene en **dos versiones**, las que empiezan con **1** (1.x) y las que empiezan con **2** (2.x). Las primeras prácticamente no requieren librerías especiales de Windows; las 2.x, en cambio, dependen de las bibliotecas de la plataforma .NET 2.0 de Microsoft (incluídas por defecto a partir de Windows Vista, e instalables en versiones anteriores a Vista).

En el siguiente enlace podemos ver un cuadro comparativo de ambas versiones: KeePass Edition Comparison.



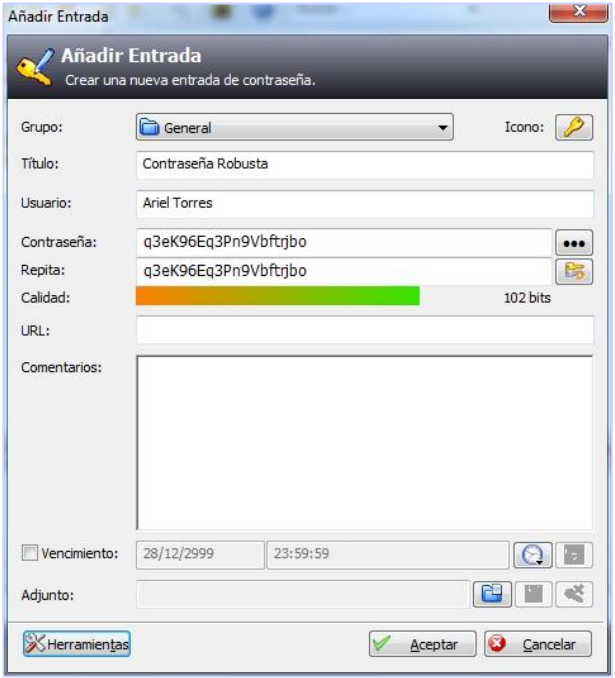
Ventana principal de KeePass.

Utilización de KeePass

Primero, se crea una **nueva base de datos de contraseñas** (podemos tener varias bases de datos). KeePass solicita entonces la creación de una clave para proteger las contraseñas que almacenaremos en esa base de datos. Suena circular, cierto, pero de ahora en más (al menos, en teoría), sólo tendremos que recordar esta única contraseña para acceder a las demás.

Aceptada la **contraseña maestra**, el programa produce una serie de **subcarpetas** (o **subgrupos**) del grupo *General*, con nombres como *Windows*, *Homebanking* e *Internet*.

Desde luego, es posible crear más grupos y subgrupos. Ahora, basta seleccionar un grupo o, más probablemente, un subgrupo, y apretar el ícono de la llave con la flechita verde (o presionar ***Ctrl+Y*** o ir al menú ***Editar > Añadir Entrada***). Esto abre un cuadro de diálogo como el que se muestra en la figura. Los campos son bastante obvios, con el añadido de que además miden la fortaleza de la contraseña.



Podemos inventar nuestras propias contraseñas, o dejar que KeePass lo haga por nosotros.

> KeePass protege su base de datos con ***AES*** (Advanced Encryption Standard - Wikipedia).

educación IT
CODE YOUR FUTURE

¡Sigamos trabajando!