Fuente: OSI

Contraseñas

Si alguien conoce nuestro usuario y contraseña tendrá acceso a toda nuestra información: podrá publicar en nuestro nombre en las redes sociales, leer y contestar a correos electrónicos o ver el saldo de nuestra cuenta bancaria, entre otros.

DEBEMOS TENER MUCHO CUIDADO Y SEGUIR LAS SIGUIENTES RECOMENDACIONES

Las contraseñas deben ser secretas

La primera recomendación para que nuestra contraseña sea segura es mantenerla en secreto. Una clave compartida por dos o más personas ya no es segura.

Es muy importante transmitir esta recomendación a los menores, acostumbrados a compartir las claves con amigos o parejas. Si esa relación se rompe o se produce una enemistad, la otra persona tendrá acceso a toda su información.

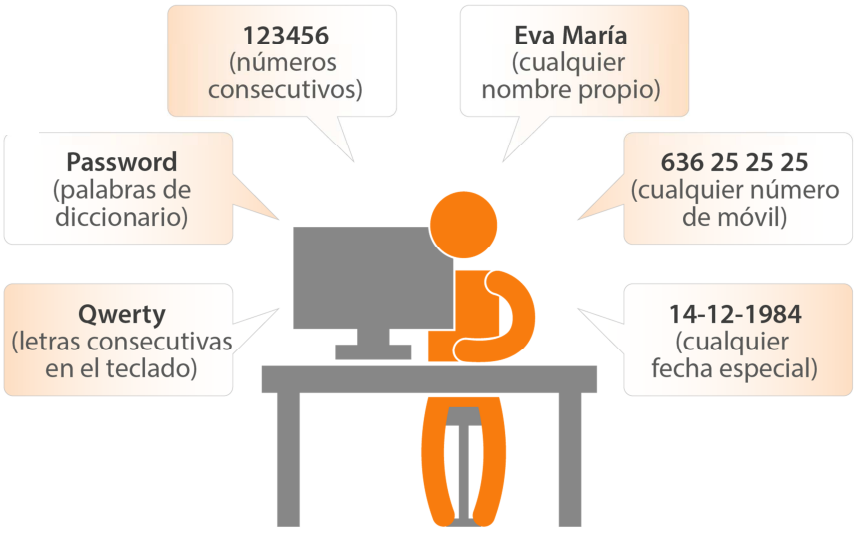
Las contraseñas deben ser robustas

Siempre debemos elegir una contraseña robusta: longitud mínima de ocho caracteres, que combine mayúsculas, minúsculas, números y símbolos.

No debemos utilizar palabras sencillas en cualquier idioma, nombres propios, lugares, combinaciones excesivamente cortas, fechas de nacimiento, etc. Esto incluye claves formadas únicamente a partir de la concatenación de varios elementos. Por ejemplo, “Juan1985”.

Fuente: OSI

EJEMPLOS DE CONTRASEÑAS QUE NO DEBEMOS UTILIZAR



Uno de los problemas de utilizar claves demasiado simples es que existen programas diseñados para probar millones de contraseñas por minuto. La tabla siguiente muestra el tiempo que tarda un programa de este tipo en averiguar una contraseña en función de su longitud y los caracteres que utilicemos.

Longitud	Todos los caracteres	Sólo minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

Fuente: OSI

Las contraseñas deben ser únicas

Debemos utilizar claves diferentes en servicios diferentes, dado que el robo de la clave en uno de ellos permitiría el acceso a todos.

En ocasiones, recordar todas las contraseñas que utilizamos (correo electrónico, redes sociales, mensajería instantánea, foros, etc.) puede resultar complicado. Para facilitar la tarea, podemos utilizar algunas sencillas reglas:

- **Cambiar las vocales por números**. Por ejemplo:
  - Mi familia es genial → M3 f1m3l31 2s g2n31l
- **Utilizar reglas mnemotécnicas**. Por ejemplo, elegir la primera letra de cada una de las palabras de una frase que sea fácil de recordar para nosotros:
  - Con 10 cañones por banda… → C10cpb…
- **Para hacer más sencillo el trabajo, podemos utilizar claves basadas en un mismo patrón, introduciendo ligeras variaciones para cada servicio**. Por ejemplo, tomando como base la contraseña anterior, añadir al final la última letra del servicio utilizado en mayúscula:
  - Facebook → C10cpb…K
  - Twitter → C10cpb…R
  - Gmail → C10cpb…L
- **Dependiendo del servicio y de su importancia podemos utilizar claves más robustas o menos, para facilitar su memorización.** Para los servicios más sensibles, siempre podemos utilizar un generador aleatorio de contraseñas. La mayoría de los gestores de contraseñas ofrecen esta funcionalidad.

Lo mejor es utilizar estas reglas como inspiración para crear contraseñas personales y secretas.

Cuidado con las preguntas de seguridad

Algunos servicios ofrecen la opción de utilizar preguntas de seguridad para que, en caso de olvido, podamos recuperar la contraseña.

Sin embargo, muchas de estas preguntas son simples y cualquier persona que nos conozca mínimamente o que disponga de acceso a nuestras redes sociales podría averiguar la respuesta. Por ejemplo: *¿Cómo se llama tu mascota?*

Por ello, no debemos utilizar las preguntas de seguridad con respuestas obvias. Podemos facilitar una respuesta compleja o bien una respuesta falsa y sólo conocida por nosotros.

Utiliza gestores de contraseñas

Para almacenar las claves de los diferentes servicios podemos utilizar un gestor de contraseñas. Éstos almacenan nuestras claves de manera segura y las protegen con una clave de acceso maestra.

Fuente: OSI

Debemos tener en cuenta lo siguiente antes de utilizar este tipo de programas:

- La contraseña que utilicemos para el acceso debe ser segura y robusta ya que nos da acceso al resto de claves.
- Si olvidamos esta clave no podremos acceder al resto de nuestras contraseñas.
- Debemos realizar copias de seguridad del fichero de claves, para evitar perder las claves almacenadas.

Consejos finales

Hagamos un repaso rápido a los consejos que debemos tener en cuenta a la hora de gestionar nuestras claves:

- No compartas tu clave con otras personas. Una vez la compartes, deja de ser secreta.
- Utiliza una clave robusta y segura. Hay muchas formas de tener una clave robusta fácil de memorizar.
- No utilices la misma clave en diferentes servicios. Siempre claves diferentes para servicios diferentes.
- Cuidado con las preguntas de seguridad. Si las utilizas, que sólo tú y nadie más sepa las respuestas.
- Utiliza gestores de contraseñas. Si te cuesta memorizar o utilizas muchos servicios, utiliza uno de estos programas. Son muy útiles y sencillos de usar.