Lo mejor son las claves aleatorias. Si se puede usar un programa generador de claves aleatorias, se estará mucho mejor protegido. La página ClaveSegura ofrece de manera gratuita uno en el que se puede escoger tanto la longitud de la contraseña como la cantidad de caracteres alfanuméricos.
Otros servicios como The Password Meter miden el nivel de seguridad de las contraseñas que se confeccionan.

No utilizar la misma contraseña para todo. Parece una obviedad, pero es lo que hace la mayoría. Hay que tener una contraseña distinta para cada servicio. También es recomendable cambiarlas cada cierto tiempo.

Guardar las claves en un documento de texto. Como las claves seguras son muy difíciles, por no decir imposibles, de recordar, lo lógico es tenerlas escritas en un documento de texto, que se usará para almacenar las contraseñas de todos los servicios personales. Cada vez que se entre a un servicio, se tendrá que recurrir a este documento. Puede que sea pesado, pero es más seguro.

Conservar el documento en un lugar seguro. Hay varias opciones para guardar el documento con las claves del usuario. La primera es emplear una **memoria USB separada** físicamente del ordenador y que solo se enchufa cuando se quiere abrir el documento con la contraseña. Hay que ser consciente de que se puede tener el terminal monitorizado por algún software malicioso (ocurre con mucha más frecuencia de la que se cree) o que alguien puede acceder a través de la conexión wifi si esta no es lo bastante segura.
La 2ª alternativa es archivar el documento en una **copia de seguridad en un servidor de la Red**, con protocolos de cifrado de 128 bits o más. Se puede guardar en plataformas diseñadas para tales usos, como Clipperz. Bastará con abrir este servicio y acceder al documento. Eso sí, la contraseña de acceso a Clipperz tiene que ser muy compleja, se debe tener escrita en una libreta, meter en un cajón y saber que si se pierde también se extraviará el resto de claves.

Cuidado con las sesiones abiertas. En muchas ocasiones, los usuarios mantienen abiertas las sesiones de diferentes servicios on line en el navegador. De esta forma, en caso de extraviar el ordenador o bien dejarse la sesión abierta en un terminal público o de un tercero, puede poner en peligro su privacidad y seguridad, al facilitar el acceso a su cuenta.
Para minimizar este riesgo, una opción recomendable es **salir de todos los servicios de uso habitual**, ya sean el correo electrónico, las distintas redes sociales donde se participa o las plataformas donde se guardan documentos para sincronizarlos, etc.

En caso de disponer de un dispositivo portátil como ordenadores, teléfonos o tabletas, es aconsejable **activar un mecanismo de seguridad de acceso al sistema cada vez que el aparato entre en hibernación o se apague la pantalla**. De esta manera, si alguien encendiera el dispositivo y el usuario no hubiera activado esta protección, el extraño podría acceder fácilmente a sus servicios con sesiones abiertas.

10 CONSEJOS
ESCRIBIR
CONTRASEÑAS

Con tu Ayuda y Colaboración
Conseguiremos como norma general
la Custodia Compartida
de nuestros hijos

Boletín de Suscripción:

Nombre:_____

Apellidos: _____

Domicilio:_____nº___

Población: _____

C.P.:_____N.I.F.:_____

e-mail.:_____

Tlf.:_____

Si, deseo pertenecer a la Asociación Padres y Madres en Acción (PAMAC) , abonando la cantidad de:

- **84´00** € Anuales ☐
- _____ € Por Donación ☐

Ingresando en la Cuenta de la Asociación Nº: **2038-1893-75-6000068701** ó domiciliando el pago en el Banco/Caja:_____

_____

Calle:_____ nº:_____

Población:_____C.P.:_____

Entidad Oficina D.C. Cuenta

☐☐☐☐ ☐☐☐☐ ☐☐ ☐☐☐☐☐☐☐☐☐☐

En _____ a ___ de _____ de 20___

Firmado:

10 consejos para escribir contraseñas seguras. Por JORDI SABATÉ|12.06.2013 -

La mayoría de los usuarios tienen claves de acceso a los servicios que cualquier 'hacker' podría romper en menos de 10 minutos ***"1234"***. Según revela un estudio, esta es la **clave más frecuente** que la mayoría de usuarios escriben para proteger sus servicios on line, donde guardan datos privados de gran importancia e, incluso, los nº de sus cuentas bancarias. Esto significa que **cualquier "hacker" puede entrar en gran cantidad de cuentas privadas** de plataformas de Internet en pocos segundos.

Algunas **pautas para confeccionar contraseñas más seguras**.
Cuando se quiere elaborar un poco más las claves, el usuario se basa, hasta de modo inconsciente, en **referencias simbólicas** como su cumpleaños, el de sus hijos o la fecha de su boda. También de esta forma uno se lo pone fácil a los "hackers", pues les basta con entrar en sitios como Facebook, ver alguno de estos datos y, a partir de ellos, buscar la combinación de entrada a los servicios personales.
Después de escribir la contraseña es importante revisar que no contenga pistas personales

Respecto al **nombre de usuario**, los "profesionales en romper claves" saben que casi todo el mundo utiliza el mismo que tiene en su dirección de correo electrónico. Conviene, por lo tanto, ser mucho más inteligentes y blindar lo que ahora se tiene casi como un libro abierto.
Buscar siempre claves que tengan más de 8 dígitos. Cuantos menos caracteres conforme una clave, más fácil es romperla para un pirata informático, puesto que el nº de combinaciones posibles son menos. Se consideran "débiles" las combinaciones menores de 8 dígitos, que pueden identificarse con programas generadores de combinaciones aleatorias (llamados robots), lo que se conoce como "la fuerza bruta".

Nunca utilizar solo números. Aunque se pongan claves de 8 o más dígitos, si se emplean solo cifras, es cuestión de tiempo que un robot encuentre la contraseña y entre en las páginas de la persona.

Tampoco usar solo letras ni palabras. Las letras se pueden combinar con robots hasta dar con la clave. Respecto a las palabras, siempre tienen una conexión simbólica con el subconsciente, por lo que alguien que conozca un poco al usuario puede adivinar las claves si piensa en el nombre de su pareja, sus hijos o sus mascotas.

Optar siempre por combinaciones alfanuméricas. Mezclar letras y nº es la solución más segura porque se juntan 2 sistemas de clasificación, lo cual amplía mucho las combinaciones. De todos modos, un "hacker" que tenga algunos datos personales sobre el usuario y mucha psicología puede adivinar las claves si no ha habido esmero en confeccionarlas. Hay que ser conscientes de que, de modo automático, siempre se buscan combinaciones fáciles de recordar y relacionadas con personas y fechas importantes. Por lo tanto, después de escribir la contraseña es importante revisar que no contenga pistas personales.

Intercalar signos de teclado. Un truco que permitirá usar letras y nº relacionados con la vida del usuario sin peligro es intercalar símbolos como "#", "$", "&" o "%" entre los caracteres de la contraseña. Su presencia es mucho más difícil de descubrir para piratas informáticos y robots.