UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO. RECUPERADO DE LA REVISTA UNAM DEL 10 DE FEBRERO DE 2018.

10 tips para elegir una contraseña segura

*Por*[*Alejandro Martínez Notte*](http://www.grupodeboss.com/blog/author/admin/)*,*

Un estudio realizado a las claves con las cuales las personas protegen sus correos electrónicos, sus cuentas bancarias y cuentas registradas en sitios Web, entre muchas otras variantes, demuestra que la contraseña más utilizada a nivel mundial es: “1234”.

Para la gente especializada en hackear cuentas ajenas, ingresar la clave 1234 y descubrir que es la que permite el ingreso al lugar de supuesta privacidad resulta muy sencillo, incluso máquinas llamadas “robots” hacen ese trabajo, generar constantes combinaciones de números hasta encontrar la clave correcta.

A continuación te daremos 10 razones por las cuales las contraseñas que utilices para tus sitios no sean simples de hackear.

1. Utilizar claves que superen los ocho dígitos, de esta manera existirán muchas más combinaciones que se deberán utilizar para poder hallar la indicada y violar la seguridad de la cuenta.

2. Si se utilizan sólo números se le simplificará el trabajo al hacker o robot que intente detectar la clave.

3. Elegir contraseñas formuladas con palabras o letras que hagan referencia a fechas como la de nacimiento, casamiento, etc. son aún más sencillas de adivinar debido a que esos datos son de fácil acceso para cualquier persona.

4. Muchos sitios en Internet, a la hora de crear cuentas personales y exclusivas sugieren la creación de contraseñas que incluyan letras y números entre sus dígitos, generando mayor privacidad debido a que el ingreso a esta cuenta sería más complicado.

5. El uso de los símbolos en las claves las hace casi inviolables debido a que dígitos que representen símbolos como @, #, $, %, &, /, etc., son casi imposibles de descifrar dentro de una contraseña aunque muchos sitios no las permitan.

6. La página <http://www.clavesegura.org/> genera contraseñas con la variante de que el usuario pueda elegir si desea letras, números, símbolos o combinación de ellos.

7. No utilizar la misma contraseña en todos aquellos sitios que la soliciten, ya que al descubrir una, bastará para que le puedan hackear el resto de la cuentas.

8. Mantener en lugares seguros, ya sean documentos de texto que sólo usted pueda observar, escribirlos en un bloc de notas o documentos de texto, todas las contraseñas indicando a que página de Internet pertenece cada una.

9. El documento creado anteriormente, guardarlo en algún dispositivo USB, CD o DVD y que no sea de uso compartido con otras personas.

10. Jamás tildar la casilla que dice recordar usuario y/o contraseña y renovar la misma con una frecuencia de un mes.

**PREGUNTAS**

Para validar la información que encontramos en la Internet, hay que tomar en cuenta, entre otros, los siguientes aspectos:

1) ¿Quién es el autor del documento?

Respuesta:

2) ¿Qué institución respalda al autor?

Respuesta:

3) ¿Es seria esta institución?

Respuesta:

4) ¿Cuál es la fecha en la que se publicó?

Respuesta:

5) ¿Esta publicación se actualiza constantemente?

Respuesta:

6) La información que leíste ¿crees qué es verdadera?

Respuesta:

7) ¿Por qué?

Respuesta:

8) ¿Cuál es tu conclusión de lo que leíste?

Respuesta:

**Resumen del artículo:**

Contraseña segura Ejemplo: 1234

Incluye letras y números

Nunca usa símbolos especiales

Es mayor de 8 dígitos

Incluye fecha de nacimiento, casamiento, etc.

Contraseña NO segura Se utiliza en todos los sitios

Se guarda en un lugar seguro

Ejemplo: t5JDEK%5n

Se renueva cada mes

Se almacena tildando la casilla “RECORDAR”