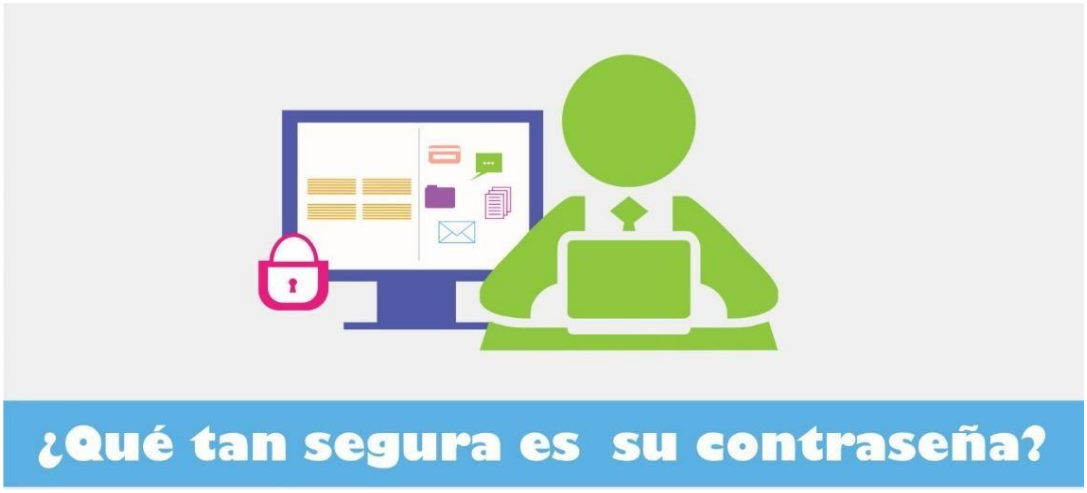


Una de las mejores maneras y la más común hoy en día para proteger la información, es asegurar que sólo las personas autorizadas tengan acceso a la misma, a este proceso se le llama "autenticación", el cual es el más importante y más difícil en el mundo cibernético, ya que se tiene que comprobar que alguien es la persona que dice ser.

Las contraseñas son el medio más común de autenticación, pero si usted no elige "buenas" contraseñas o no las trata con la confidencialidad necesaria, es casi tan ineficaz como no tener contraseña alguna.

Seguramente usted ha escuchado que a cierta estrella de Hollywood le han hackeado con éxito su cuenta de alguna red social o almacenamiento en la nube; y le han sustraído sus datos confidenciales, fotografías entre otros datos siendo expuestos a la luz pública. Muchos de estos eventos son por el uso de contraseñas inseguras o débiles.

¿Qué tan segura es mi contraseña?

Ahora se preguntará ¿Qué tan segura es mi contraseña?, la mayoría de la gente usa contraseñas que se basan en información personal y que además son fáciles de recordar. Sin embargo, eso también hace que sea más fácil para un atacante adivinar una contraseña o "hackear" una cuenta.

Las contraseñas más largar son más seguras que las más cortas debido a que hay más caracteres para adivinar; así que cuando este creando una contraseña, considere el uso de frases para generarlas. **El uso de frases** ayuda a recordar fácilmente su password volviéndolo complejo para adivinar.

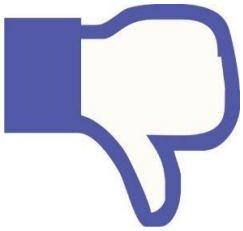
Reglas Generales:

A continuación, se lista una serie de recomendaciones a utilizar al momento de elegir o crear una contraseña:

- No utilice contraseñas que se basen en la información personal.
- No utilice palabras que se puedan encontrar en un diccionario.
- Evite frases comunes, citas famosas o letras de canciones.
- Utilice tanto minúsculas y mayúsculas.
- Use una combinación de letras, números y caracteres especiales.
- Utilice diferentes contraseñas en diferentes sistemas y cuentas.
- La longitud recomendada debe ser de al menos **8 caracteres**.
- Se recomienda cambiar su contraseña periódicamente.

Ninguno de estos consejos debe ser utilizados por si solos, la combinación de estos dará como resultado una contraseña segura.

No elija:



- **Contraseñas de menos de 6 caracteres**.
- Su nombre en cualquier forma, primer o segundo apellido, deletreado al revés, apodo o iniciales.
- Cualquier número de identificación, matricula o ID de usuario en cualquier forma.
- Parte de su ID de usuario o nombre.
- El nombre de un pariente cercano, amigo o mascota.
- Números telefónicos, dirección, cumpleaños o aniversario.
- Siglas, nombres geográficos, productos o términos técnicos.

TIP: Una forma para crear una contraseña segura es recordar una frase sencilla, pero con una extensión considerable, y tomar las letras iniciales de cada palabra contenida parara crear una contraseña, y de ser posible cambiar algunas letras por números. Por ejemplo:

"Desde que nací soy el mejor de México y del IPN"

Siguiendo las recomendaciones la contraseña que se obtenida podría ser:

Dqn53mdMyd1.

Contraseñas no seguras:

Se presentan a continuación las contraseñas más comunes y vulnerables de internet, según el sitio betech

- 123456
- password
- 123456789
- 12345678
- 12345
- 111111
- 123123
- 315023
- 000000
- qwerty

¿Qué tan sólida es su contraseña?

Una vez que ha generado su contraseña, puede comprobar su solidez a través de la siguiente liga:

https://password.kaspersky.com/mx/

¿Cómo puede proteger su contraseña?

Ahora que ha elegido una contraseña que sea difícil de adivinar, usted tiene que asegurarse de **NO** dejarla en algún lugar para que alguien la encuentre:

- No la escriba en post-it y no la pegue en la computadora.
- No la deje a la vista en su escritorio o junto a su equipo de cómputo personal.
- No revele a nadie su contraseña.
- Utilice un gestor de contraseñas.
- Si usted recibe una llamada telefónica o mensaje de correo electrónico solicitando su contraseña **NUNCA** la proporcione.

Fuentes:

https://www.us-cert.gov/sites/default/files/publications/PasswordMgmt2012.pdf
https://www.us-cert.gov/ncas/tips/ST04-002
https://password.kaspersky.com/mx/
http://windows.microsoft.com/en-us/windows-vista/tips-for-creating-a-strong-password
https://www.microsoft.com/en-us/security/pc-security/password-checker.asp
http://www.bu.edu/infosec/howtos/how-to-choose-a-password/
https://as.com/meristation/2019/02/18/betech/1550530175_884548.html
http://dsi.ipn.mx/noticias/Protege%20tu%20Pc/Contrase%C3%B1as%20seguras.pdf