Contraseña

Una **contraseña** o **clave** es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. Con la contraseña se concede o se niega el acceso a algún recurso.

La longitud de las contraseñas no debe ser inferior a ocho caracteres. A mayor longitud mayor seguridad se obtiene.

Construir las contraseñas con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas, número y caracteres especiales como: @, ¡, +, &).

Tips para tener en cuenta a la hora de crear una contraseña:

Un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y acortarla aplicando alguna regla sencilla.

Se deben cambiar las contraseñas regularmente.

Usted debe evitar:

C

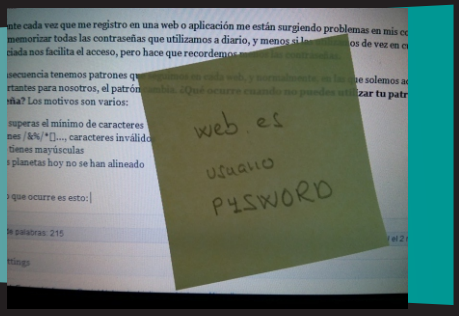
La contraseña no debe contener el nombre de usuario de la cuenta, o cualquier otra información personal fácil de averiguar (cumpleaños, nombres de hijos, cónyuges, ...). Tampoco una serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)

O

No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea.

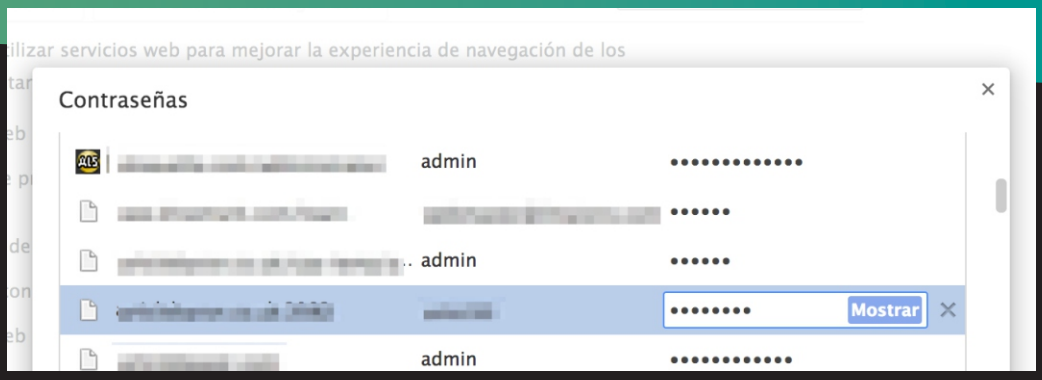
Password1

N No se deben almacenar las contraseñas en un lugar público y al alcance de los demás (encima de la mesa escrita en papel, etc…).



T No compartir las contraseñas en Internet (por correo electrónico) ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que le soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla. Casi con total seguridad se tratará de un fraude.

R No utilizar la opción de "Guardar contraseña" que en ocasiones se ofrece, para evitar reintroducirla en cada conexión.

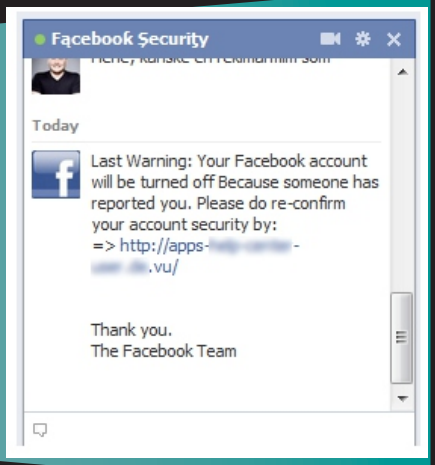


A Las **contraseñas son privadas**. No reveles tu contraseña a nadie, ni siquiera a tus amigos. Las amistades cambian y no tendría ninguna gracia que otro se haga pasar por ti. Elige una contraseña que te sea fácil de recordar pero nadie más pueda adivinar. Un truco: crea una frase del tipo "Me fui del colegio de primaria en 2005" para extraer la contraseña "Mfdcdpe05".

S Sea precavido al hacer clic en vínculos que recibe en mensajes de sus amigos en su sitio web social. Trate los vínculos en los mensajes de estos sitios de la misma forma que los vínculos en los mensajes de correo electrónico. El objetivo de los ciber-delincuentes es que a usted "le guste".)

E

No confíe en que un mensaje realmente es de la persona que dice ser. Los hackers pueden entrar en cuentas y enviar mensajes que parecen de sus amigos, pero no lo son. Si sospecha que un mensaje es fraudulento, use un método alternativo de comunicarse con su amigo para saber si lo es. Esto incluye invitaciones a unirse a nuevas redes sociales. Para obtener más información, consulte Los estafadores se aprovechan de las amistades de Facebook.



Ñ

Escriba la dirección de su sitio de redes sociales directamente en el explorador o use su marcador personal. Si hace clic en un vínculo al sitio a través del correo electrónico u otro sitio web, podría estar introduciendo su nombre de cuenta y su contraseña en un sitio falso donde se podría robar su información personal.

A

Sea selectivo a la hora de decidir a quién acepta como amigo en una red social. Los ladrones de identidades pueden crear un perfil falso para obtener su información, fotos, direcciones, teléfono, etc.

Integrantes: Aporta, Estefania; Arce, Marcelo; La Rosa, Valeria; Persia, Nicolás.
Seguridad Informática - Instituto San Vicente de Paul PT-26 - 2014