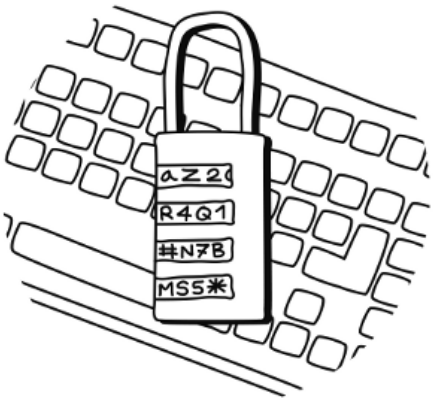
Contraseñas seguras

Por muy seguro que sea un sistema, no servirá de nada si un atacante consigue el nombre y contraseña de un usuario legítimo.



Contenidos relacionados

- Trucos para crear contraseñas seguras
- Gestión de contraseñas seguras, una tarea prioritaria
- Gestiona de forma segura tus contraseñas
- Nuevo útil gratuito en la OSI: LastPass
- Primeros pasos para proteger un ordenador recién comprado

Actualmente, el método más extendido para obtener acceso a información personal que hemos almacenado en nuestro equipo y/o servicios en línea es mediante contraseñas.

La mayoría de las veces una contraseña es la **única barrera entre nuestros datos confidenciales y los ciberdelincuentes**. Por lo que merece la pena invertir un poco de tiempo y esfuerzo para gestionarlas eficazmente.

¿Qué debe tener una contraseña para ser realmente segura?

Una buena contraseña debe cumplir, al menos, tres de estas cuatro características:

Tener números
Tener letras
Tener mayúsculas y minúsculas
Tener símbolos ($, @, &, #, etc.)

A parte, para que una contraseña sea segura también debe cumplir los siguientes requisitos:

La longitud **no debe ser inferior a siete caracteres**. A mayor longitud más difícil de adivinar.
No debe formarse con números y/o letras que estén adyacentes en el teclado. Ejemplos de malas contraseñas son: 123456, 1q2w3e o 123QWEasd.
La contraseña no debe contener información que sea fácil de averiguar, por ejemplo, nombre de usuario de la cuenta, información personal (cumpleaños, nombres de hijos, etc.)
No debe contener palabras existentes en algún idioma. Los ataques de diccionario prueban cada una de las palabras que figuran en el diccionario y/o palabras de uso común.

Buenas prácticas

No uses la misma contraseña para diferentes cuentas. Sobre todo si son de alto riesgo, como las de los servicios bancarios o comerciales.
La contraseña es algo privado, no la dejes escrita en ningún sitio, y mucho menos al lado del ordenador.
Cambia las contraseñas que traen por defecto los dispositivos y servicios en línea. Un ejemplo es el de los router WiFi, que traen por defecto contraseñas públicamente conocidas, que un atacante podría utilizar.
Limita el uso de las contraseñas almacenadas en el navegador para los servicios críticos. Si es posible el mejor sitio es la memoria de uno mismo.

Trucos para crear contraseñas seguras

Usar una frase fácil de memorizar. Una vez hecho esto, podemos hacer combinaciones con las distintas palabras que componen la frase: utilizar la primera letra de cada palabra, utilizar la última letra de cada palabra, etc.

Ejemplo: Utilizar la primera letra de cada palabra.

Frase: El 4 de Noviembre es mi cumpleaños.

Contraseña: E4dNemc

Usar una «semilla» y aplicarle un «algoritmo»: En cada lugar donde debamos crear una contraseña, pensamos en una «semilla», que no es más que una palabra que ayude a recordar ese lugar. A la semilla se le aplica un «algoritmo» que es una combinación de pasos que utilizaremos para crear las contraseñas de cualquier sitio. La ventaja de utilizar este método es que sólo será necesario recordar el algoritmo.

Ejemplo: Recordar contraseña de Hotmail.

Semilla: hotmail

Algoritmo: Quitarle las tres primeras letras, poner en mayúsculas la primera letra, añadir al principio el número 82, añadir el final los símbolos * #.

Contraseña: 82Mail* #

Aplicaciones que nos pueden ayudar

Comprobador de contraseñas:

Cuando no estés seguro de si la contraseña que has elegido es lo suficientemente segura, puedes utilizar un medidor de fortaleza de la contraseña:

Comprobador de contraseñas / Password

Gestores de contraseñas:

Cuando manejamos muchas cuentas se vuelve complicado recordar la contraseña asociada a cada una de ellas. Lo peor que podemos hacer en ese caso es optar por utilizar la misma contraseña para todos los sitios, ya que si se descubre la contraseña de acceso a alguna de estas cuentas, un atacante podrá fácilmente acceder al resto de ellas. Para solucionar este problema, existen los gestores de contraseñas.

Un gestor de contraseñas es un programa que se utiliza para almacenar contraseñas. Nos permite recordar todas las contraseñas, claves de acceso y nombres de usuario que necesitamos para acceder a una cuenta o página de Internet. La información se almacena cifrada y sólo se puede acceder a través de una clave.

Puedes obtener más información sobre herramientas de gestión de contraseñas en los siguientes enlaces:

Aplicaciones para almacenar contraseñas en Windows
Cinco herramientas para gestionar contraseñas online
Aplicaciones para almacenar contraseñas en Mac OS X

Cómo proteger las contraseñas en el navegador

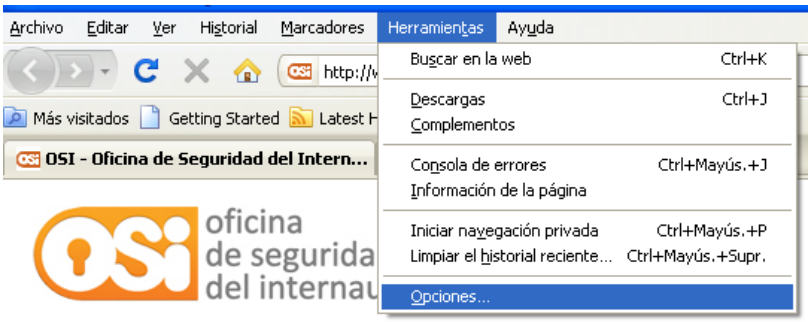
Seguramente el navegador sea el programa que utilizamos para acceder a la mayoría de nuestras cuentas: ver el correo electrónico, acceder a nuestro banco o conectarnos a las redes sociales. Utilizar una contraseña diferente para cada cuenta puede resultar algo lioso, pero actualmente los navegadores disponen de gestores de contraseñas capaces de almacenar los nombres de usuarios y contraseñas utilizados para acceder a los distintos sitios.

Sin embargo, si compartes el ordenador, guardar en el navegador las contraseñas hace que las personas que también vayan a utilizar tu equipo puedan acceder a diferentes sitios Web en tu lugar con las cuentas que tengas almacenadas; es posible evitar este inconveniente y seguir almacenando las contraseñas en el navegador utilizando una **contraseña maestra**, que se solicitará que escribas cada vez que quieras acceder a alguna cuenta que tengas almacenada en el navegador. La importancia de utilizar dicha contraseña es muy grande, ya que sin ella, cualquier persona que acceda a tu ordenador podrá ver todas las parejas de nombre de usuario/contraseñas que utilizas habitualmente para navegar por Internet.

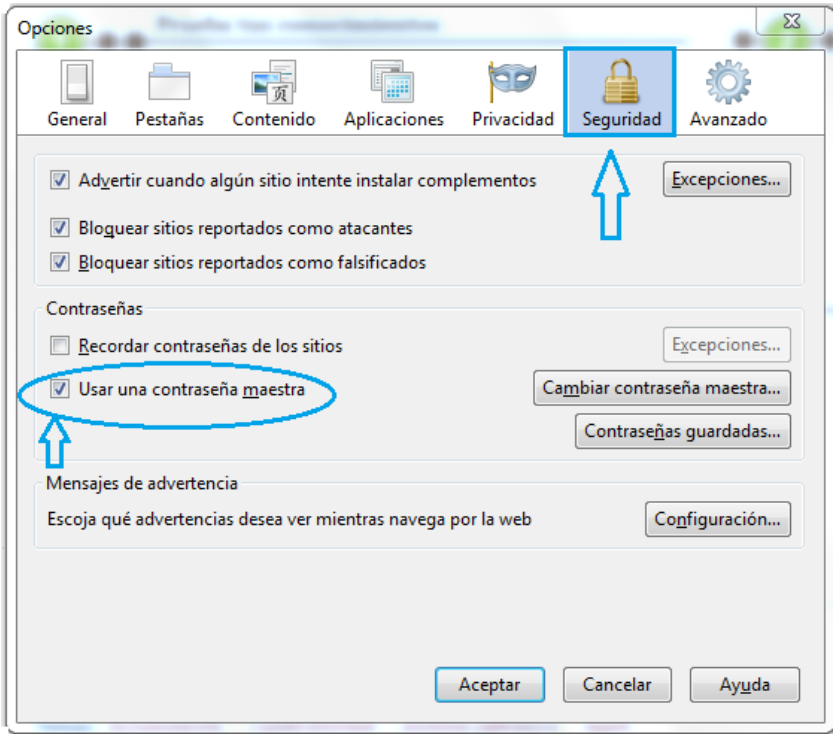
Firefox:

Para proteger las contraseñas almacenadas en el navegador Firefox con una contraseña maestra hay que realizar los siguientes pasos:

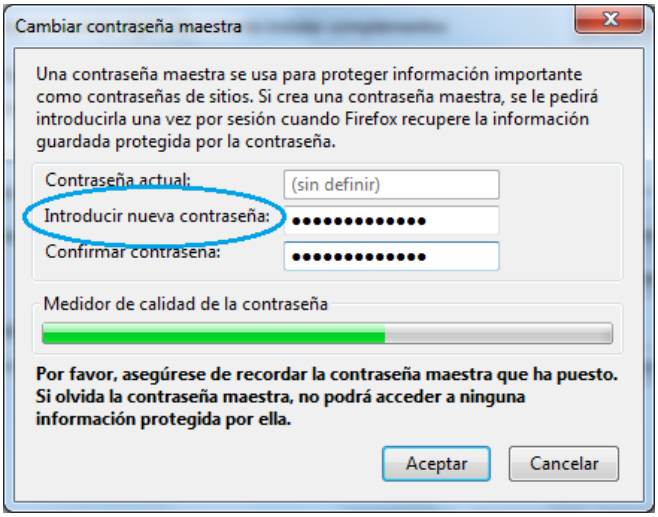
1. Iniciar Firefox
2. Ir al menú «Herramientas», y hacer clic en «Opciones»



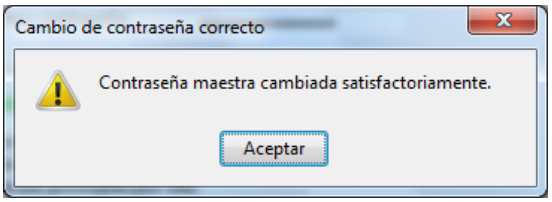
3. Seleccionar el icono «Seguridad» y activar la casilla «Usar contraseña maestra».



4. En el cuadro de diálogo que aparece, debemos introducir la contraseña. Para que la contraseña sea lo más segura posible Firefox proporciona un Medidor de la calidad.



5. Aceptamos los cambios realizados. Aparecerá una ventana indicando que la contraseña maestrea se ha cambiado correctamente.



6. Reiniciar el navegador para que se hagan efectivos los cambios.

Después de seguir estos pasos, cada vez que se quiera acceder a un sitio del que Firefox tenga guardada la contraseña, nos pedirá introducir la contraseña maestra para poder acceder a dicho sitio.

Recuerda

“Las contraseñas son como la ropa interior. No puedes dejar que nadie la vea, debes cambiarla regularmente y no debes compartirla con extraños”.

“Una contraseña es un secreto que no hay que contar a nadie”.

“Si las llaves de casa no se las dejas a nadie, ¿por qué vas a dejar tus contraseñas a alguien?”.

“Para evitar que te atraquen por la calle tomas ciertas medidas de seguridad: no caminas por sitios extraños, llevas bien guardada la cartera, etc. Si quieres evitar que te roben por Internet información personal, dinero, etc. toma también las medidas de seguridad necesarias.”