

# NAVEGADORES WEB

## QUÉ SON

Un **navegador web** es un programa que permite el acceso a la Web, interpretando la información de distintos tipos de archivos y sitios web para que estos puedan ser visualizados.

Su funcionalidad básica es la de permitir la visualización de textos, posiblemente con recursos multimedia incrustados. Además, permite visitar páginas web y hacer actividades en ella, es decir, enlazar un sitio con otro, imprimir, enviar y recibir correo, entre otras funcionalidades más.

Los documentos que se muestran en un navegador pueden estar ubicados en el ordenador donde está el usuario o pueden estar en cualquier otro dispositivo conectado a través de Internet, y que tenga los recursos necesarios para la transmisión de los documentos (un servidor web).

Tales documentos, comúnmente denominados páginas web, poseen hiperenlaces o hipervínculos que enlazan una porción de texto o una imagen a otro documento, normalmente relacionado con el texto o la imagen.

[Google](#)

## CUÁLES SON

Hay 5 principalmente, son: **Google Chrome, Safari, Firefox, Microsoft Edge / Internet Explorer y Opera.**



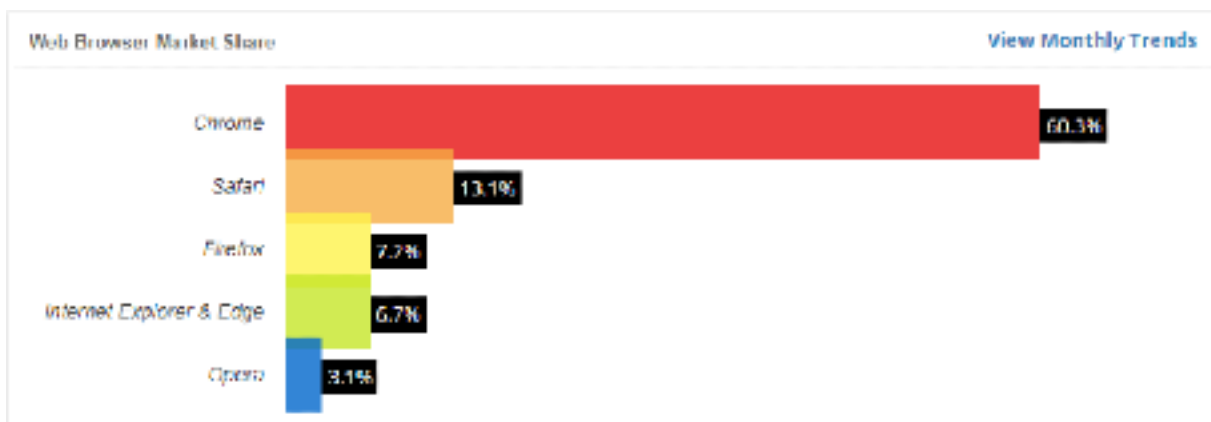
**Google Chrome:** Propiedad de Google y el más usado gracias a su rapidez y su facilidad de uso.

**Safari:** Propiedad de Apple, instalado en todos sus dispositivos como navegador característico de la marca.

**Firefox:** Navegador de software libre con una gran cantidad de complementos y opciones.

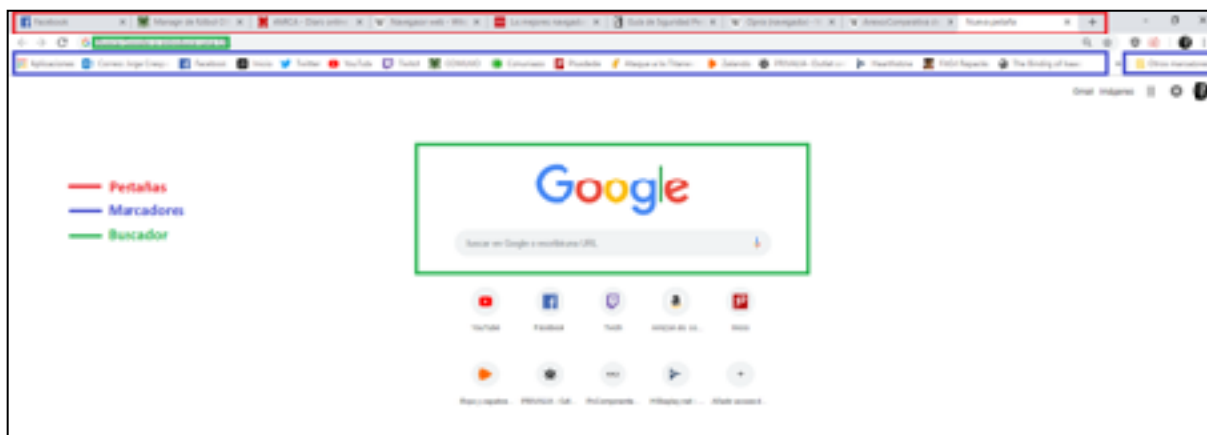
**Internet Explorer / Edge:** Propiedad de Microsoft, viene instalado en sus sistemas operativos como navegador principal. Muy popular los primeros años, pero perdió usuarios a favor de Chrome o Firefox.

**Opera:** El menos usado de todos y que poco a poco va perdiendo cada vez más usuarios.



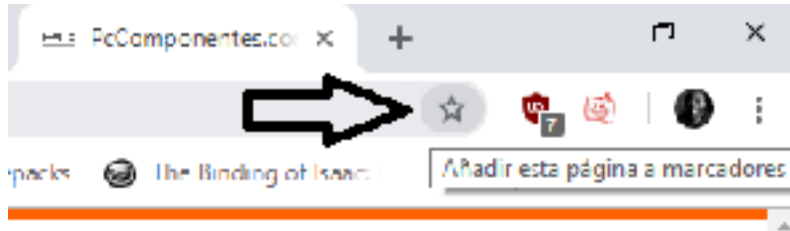
<b>Visualización</b>	Permite ver las páginas web y sus contenidos
<b>Marcadores</b>	Guardan las páginas web que queremos y pueden ser divididas por carpetas
<b>Descargas</b>	Gestionan la bajada de archivos de páginas web
<b>Contraseñas</b>	Guardan las contraseñas de las páginas web que queremos para poder usarlas sin introducir nuestros datos todo el tiempo
<b>Formularios</b>	Guardan diversos datos como dirección, teléfono, DNI etc... para introducirlos automáticamente cuando nos los pida una página web
<b>Ortografía</b>	Corrige las faltas ortográficas o gramaticales que podamos cometer
<b>Pestañas</b>	Gestionan en diversas páginas apiladas en pestañas para su mejor utilización
<b>Anti Pop-Up</b>	Evita que aparezcan ventanas emergentes, las ventanas que nos aparecen delante avisando de algo
<b>Extensiones</b>	Aplicaciones extras que cumplen una función (quitar publicidad, mejorar apariencia etc...)

(Ampliar imágenes)

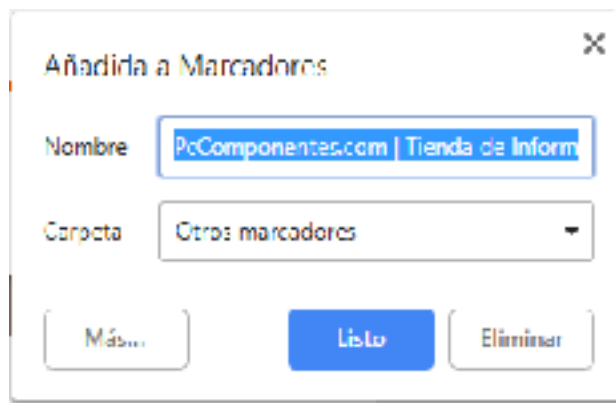


## MARCADORES

Para añadir un marcador deberemos pulsar la estrella que aparece al final de la dirección de la página web.

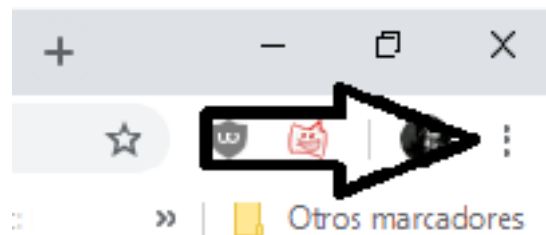


Se nos abrirá una ventana donde podremos cambiar el nombre del marcador para reconocerlo mejor y la carpeta de marcadores donde queramos guardarlo.

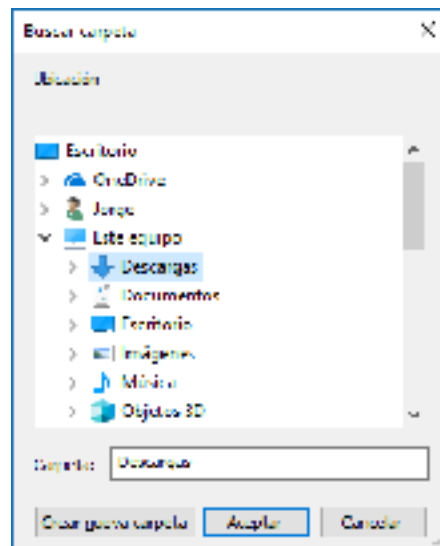
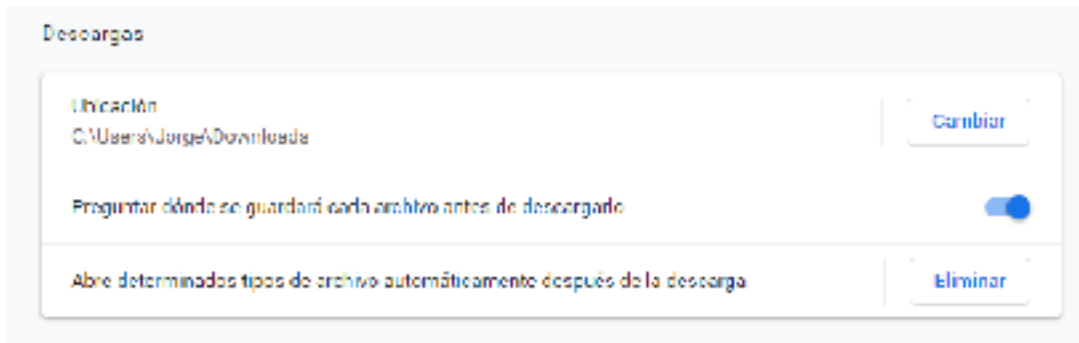


## DESCARGAS

Para gestionar el lugar donde se descargarán las cosas que nos bajemos de una página web deberemos ir a **Configuración** dentro de las opciones del navegador. En la parte superior derecha del navegador nos encontramos 3 puntos verticales; las opciones.



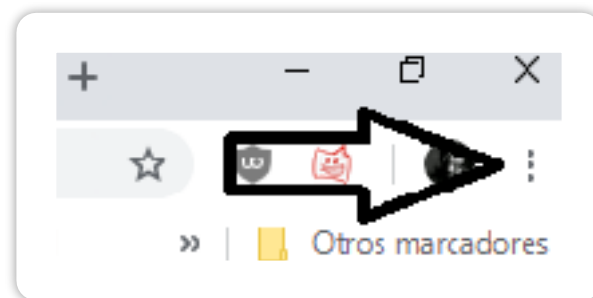
Dentro de las opciones hay un apartado para las descargas. Aquí podremos indicar la carpeta en la que queremos que nos guarde aquello que descarguemos.

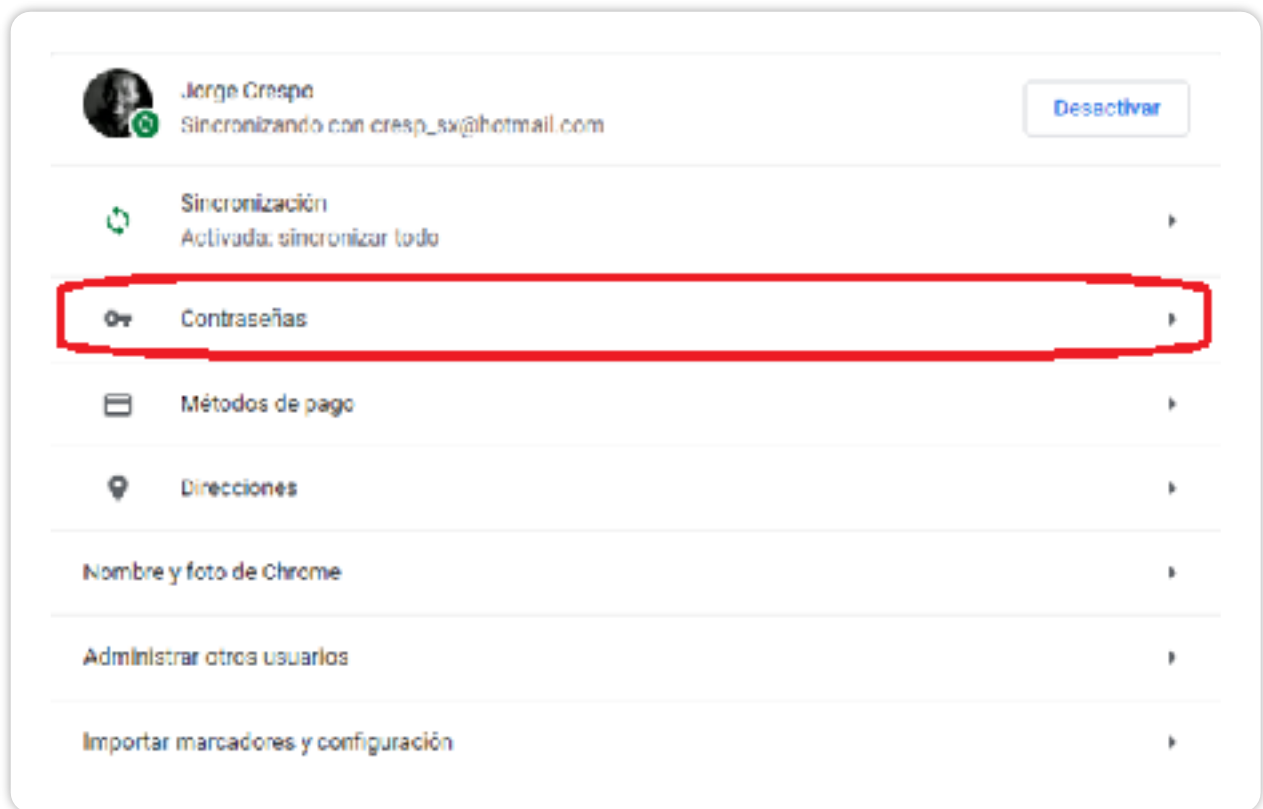


## CONTRASEÑAS

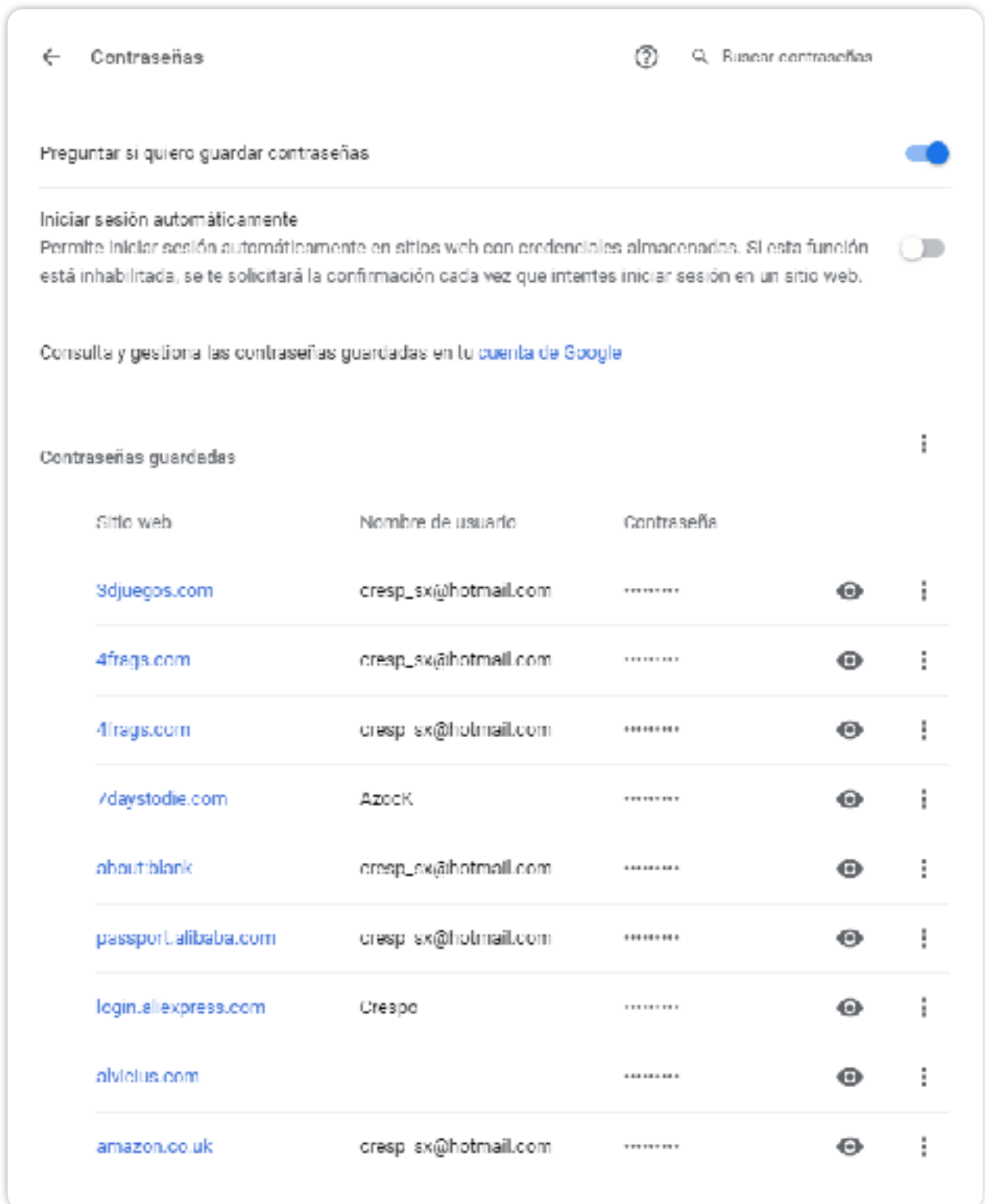
Para no tener que recordar cada usuario y contraseña con el que accedemos a una web el navegador nos permite almacenar estos datos en el ordenador de una manera segura.

Para poder gestionar las contraseñas deberemos conocer la contraseña del equipo, estas opciones se encuentran en las opciones del navegador.





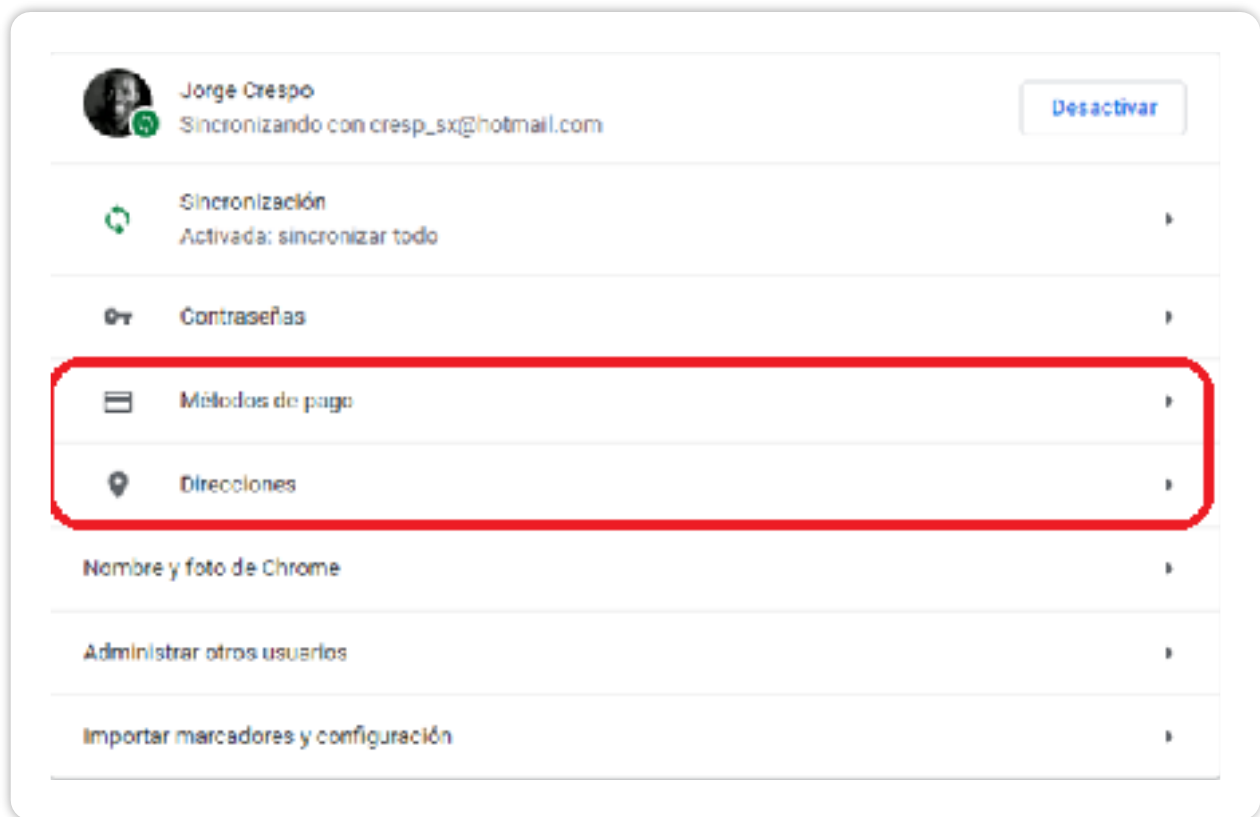
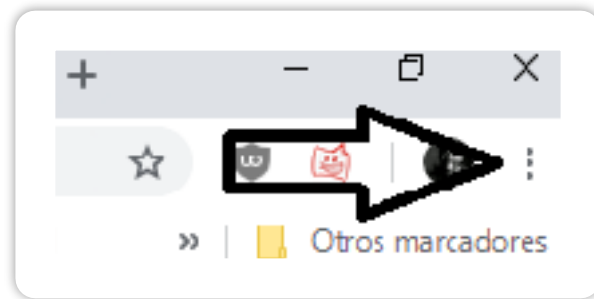
Aquí podremos gestionar algunas opciones. Si queremos guardar automáticamente las contraseñas, iniciar sesión automáticamente en aquellas páginas web donde tengamos nuestros datos de acceso guardados o poder ver las contraseñas que tenemos guardadas.



## FORMULARIOS

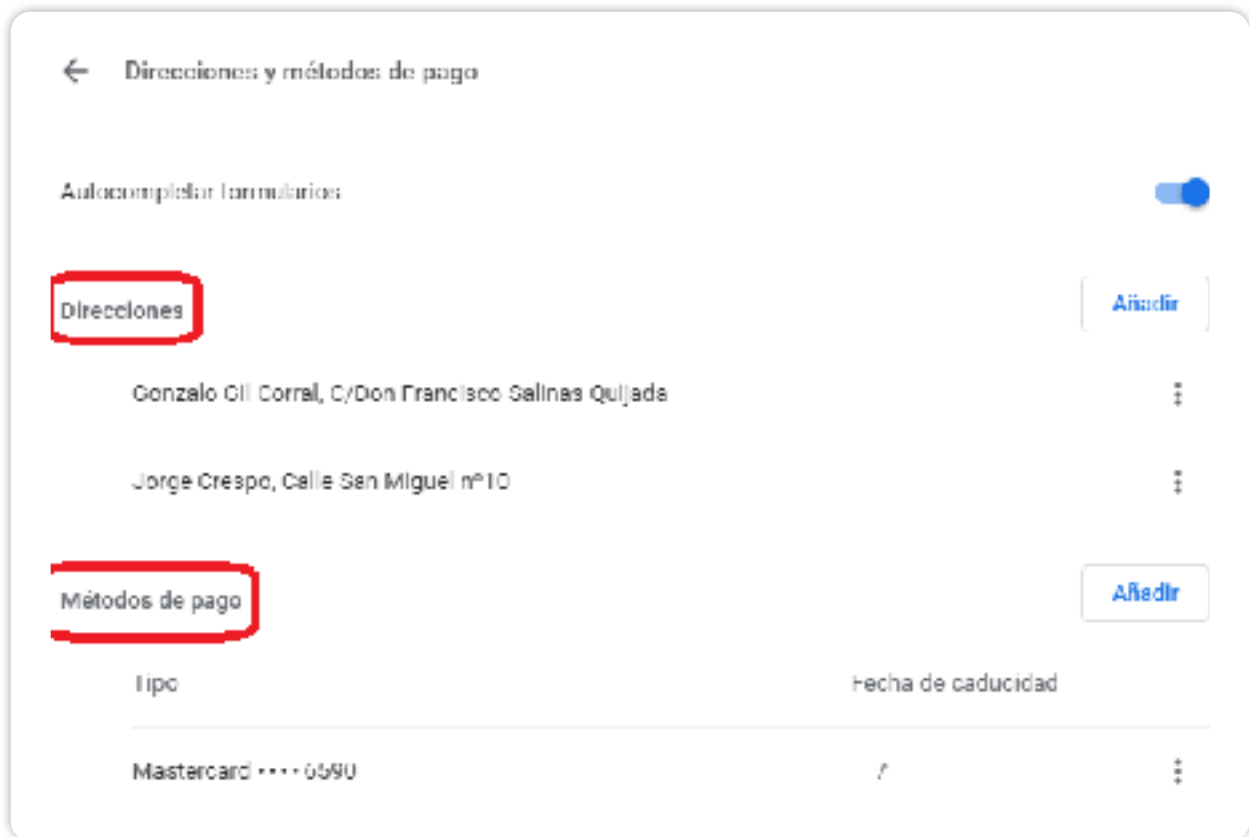
Los formularios nos sirven para autocompletar los datos que nos pidan y tengamos guardados en el formulario. Estos datos pueden ser datos de pagos para tarjetas de crédito, direcciones, nombres etc...

Para poder gestionar los formularios deberemos ir a las opciones del navegador.



Desde aquí podremos editar las direcciones que tenemos guardadas, nuestros datos o los datos de pago.

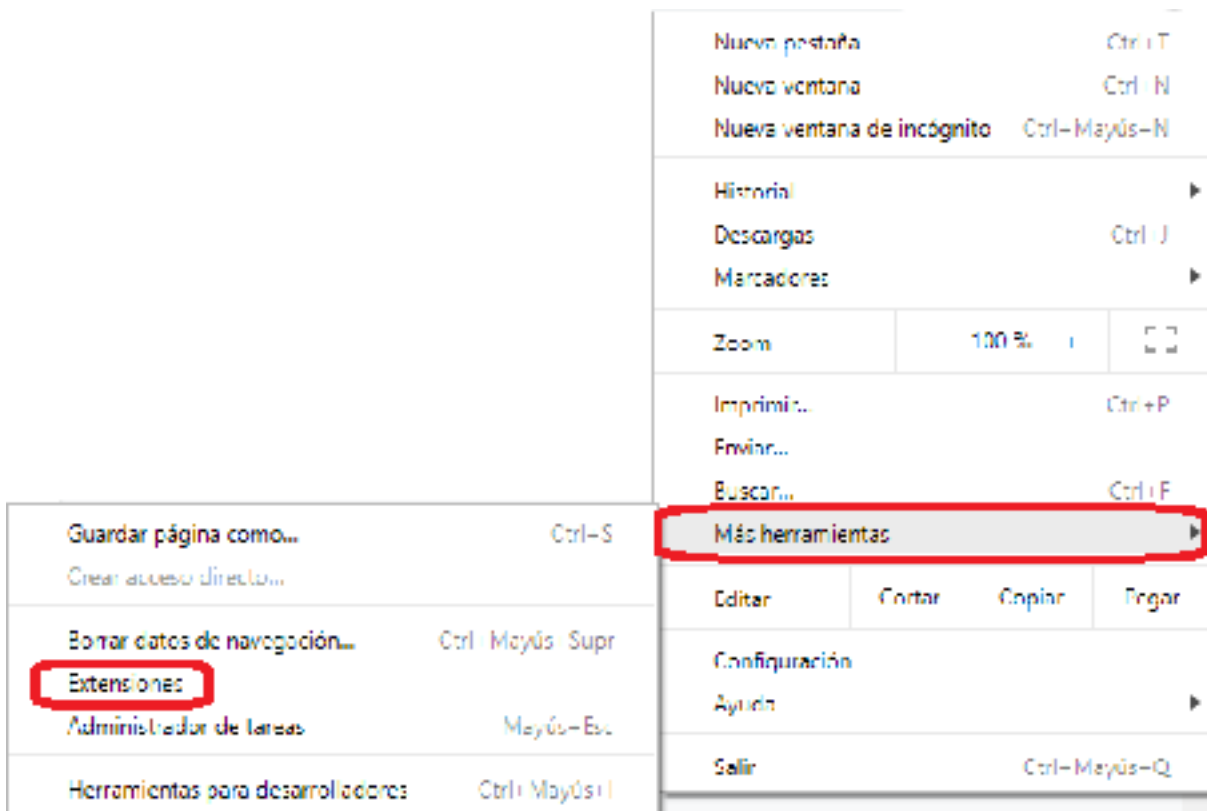
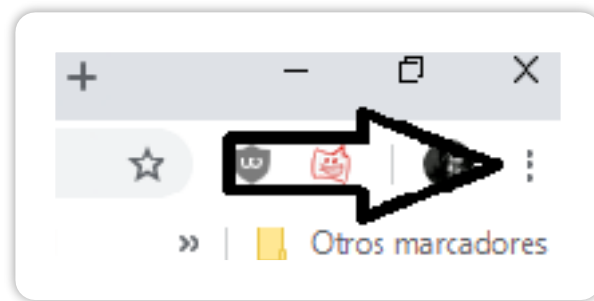


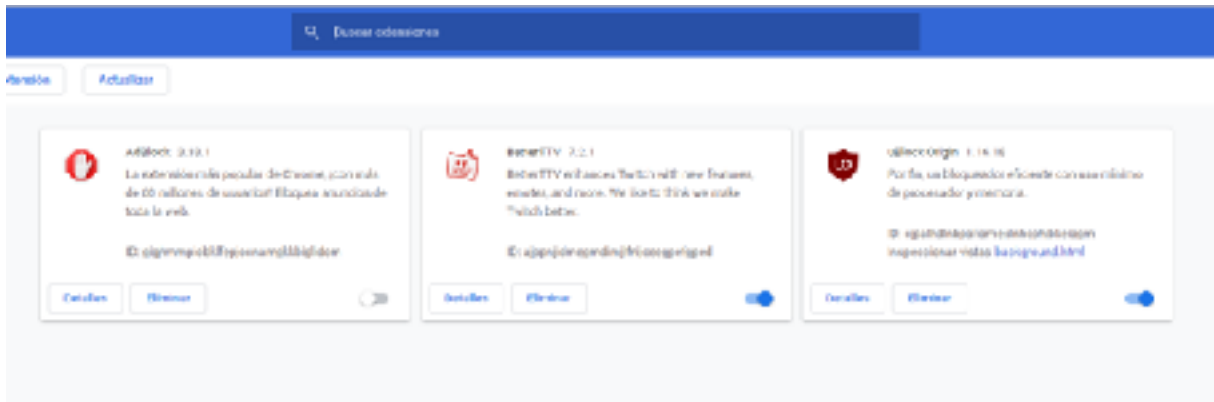
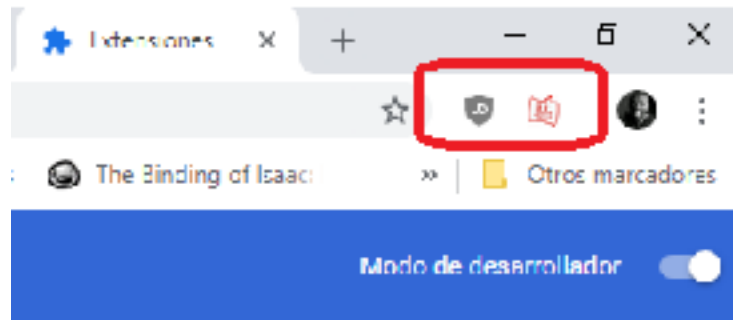


## EXTENSIONES

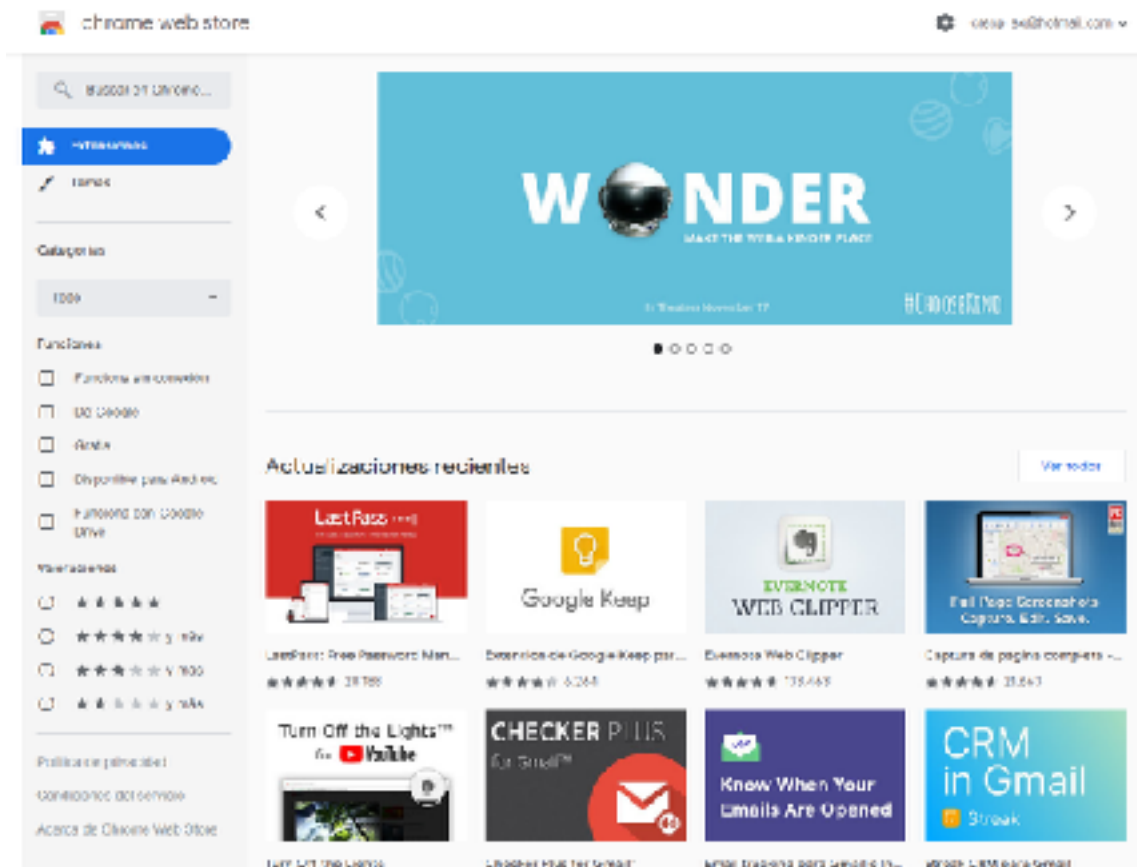
Las extensiones son programas que podemos descargar desde las plataformas de descarga de los navegadores para añadir funciones. Para poder acceder a ellas deberemos ir a las

opciones del navegador y seleccionar **Más Herramientas**, donde nos aparecerá la opción de **Extensiones**.





Para obtener estas aplicaciones deberemos ir, en el caso de Chrome, a la [Chrome Store](#).



## NAVEGACIÓN SEGURA

### ACTUALICE DE FORMA REGULAR EL SISTEMA OPERATIVO.

Actualice de forma regular el sistema operativo y las aplicaciones que utilice más a menudo, especialmente las de las familias Java, Adobe, y Office.

### UTILICE UN NAVEGADOR ACTUALIZADO.

Considere el empleo de extensiones que bloqueen la ejecución de Scripts automáticos. Además, evite cualquier enlace que pudiera parecer sospechoso, sobre todo aquellos cuyo certificado digital no es correcto.

### ELIJA CONTRASEÑAS SEGURAS Y DIFERENTES PARA CADA SERVICIO DE INTERNET.

Las contraseñas deben ser largas y alfanuméricas (contener letras y números) ; y al menos una distinta para los diferentes ámbitos de su actividad en Internet, una para las cuentas de correo personal, otra para actividades económicas, otra para las Redes sociales,...etc. De esta forma le será más sencilla que recordar decenas de contraseñas diferentes y evitar reutilizar la misma contraseña para todo

### VERIFIQUE REGULARMENTE LOS MOVIMIENTOS DE SU CUENTA BANCARIA.

De esta forma detectará rápidamente los fraudes y podrá bloquearlos. Si su entidad lo permite, establezca alertas de aviso a su móvil de transacciones extrañas o cuantiosas. Haga lo mismo con sus tarjetas de crédito.

### UTILICE UN ANTIVIRUS CON LICENCIA Y ACTUALIZADO, E INSTALE UN FIREWALL.

Existen varios que son gratuitos (muchos SO' s lo traen por defecto), con ellos evitará accesos no autorizados. Aun así, no los remplace por su sentido común y no ejecute archivos sospechosos.

### CONSIDERE LA POSIBILIDAD DE UTILIZAR UN ÚNICO DISPOSITIVO PARA LAS TRANSACCIONES DE BANCA Y COMERCIO ELECTRÓNICOS (PC, SMARTPHONE, ... ETC.).

Así podrá localizar fácilmente el equipo infectado o comprometido por cualquiera de los cientos de troyanos bancarios que existen en la actualidad. Y de esta manera desinfectarlo de una forma rápida y sencilla.

### DESCONFÍE DE LOS MENSAJES CORTOS Y EXTRAÑOS QUE PUEDA RECIBIR POR REDES SOCIALES, SOBRE TODO SI INCLUYEN UN ENLACE PARA ACCEDER A OTRO CONTENIDO.

Incluso si provienen de contactos conocidos pueden resultar peligrosos. Compruebe que sus contactos son los auténticos remitentes del mensaje, y no introduzca sus datos personales en formularios dudosos o sospechosos.

**NO PIENSE QUE ES INMUNE AL SOFTWARE MALICIOSO PORQUE UTILICE UN DETERMINADO SISTEMA OPERATIVO O UN DISPOSITIVO PORTÁTIL**

Las aplicaciones de Smartphone se han convertido en un objetivo para los desarrolladores de virus y troyanos. Los proveedores están constantemente revisando sus "markets" para limpiarlos de aplicaciones maliciosas.

No confíe ciegamente en las aplicaciones de seguridad instaladas, éstas no remplazan a la navegación responsable ni a la prudencia del usuario.

**SI DISPONE DE UN ROUTER INALÁMBRICO PARA CONECTARSE A INTERNET, CAMBIE LAS CONTRASEÑAS POR DEFECTO Y ESTABLEZCA UNA MÁS SEGURA.**

No utilice el cifrado WEP, es vulnerable y puede ser fácilmente comprometido. Si es posible, configure el router para que solo se puedan conectar al mismo determinados ordenadores.