HERRAMIENTAS

Correos	Yahoo	Gmail	Riseup
Navegadores	Internet Explorer, Safari	Chrome	Firefox
Sistema operativo	Windows	Mac	Ubuntu
Videollamadas	Skype	Google Hangout	Jitsi
Mensajería móvil	Whatsapp	Telegram chat secreto	Kik
Mensajería instantánea	MSN, Chat de Facebook	Cryptocat	Pidgin, Adium
Almacenamiento en la nube	Dropbox, Skydrive	Google Drive	Tresorit

CONSEJOS

Información básica de seguridad digital

Coloca una contraseña de bloqueo en tus dispositivos para evitar que envíen correos a tu nombre o tengan acceso a tu información.

Navegación segura

Escribe https:// antes de cada dirección, así evitarás que otros vean tu información (nota: esto servirá sólo si el sitio lo permite).
HERRAMIENTA ÚTIL: Https Everywhere es una extensión de navegador para tener https por defecto.
URL: https://www.eff.org/https-everywhere

Respaldos

Tu información es muy importante, haz un respaldo por lo menos una vez al mes y guárdalo en un lugar seguro contra daño o robo.
HERRAMIENTA ÚTIL: Cobian Backup es un sistema que automatiza el respaldo de archivos.
URL: http://www.cobiansoft.com

Contraseñas seguras

No utilices contraseñas fáciles de adivinar, como tu fecha de nacimiento. Deben incluir más de 8 dígitos, mayúsculas, minúsculas y números. ¡No uses la misma para todo!
HERRAMIENTA ÚTIL: Keepass te permite administrar tus contraseñas de forma segura.
URL: http://keepass.info

Antivirus

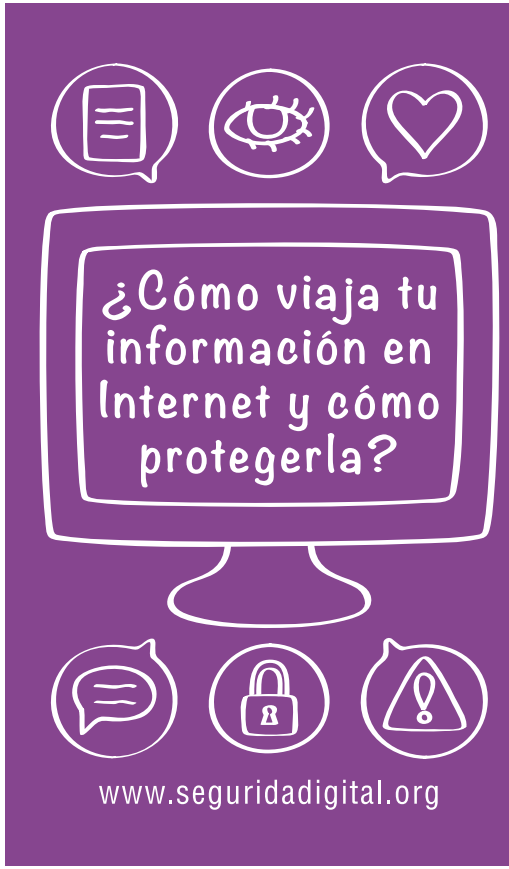
Instala un antivirus que se encargue de cuidar tu equipo y tu móvil.
HERRAMIENTA ÚTIL: Te damos dos opciones de antivirus gratuitos.
URL: AVG http://free.avg.com/mx-es/homepage
Avast https://www.avast.com/es-ww/

Privacidad

Revisa la configuración de tus redes sociales para tener claro quién puede ver lo que compartes. Recuerda siempre cerrar tu sesión al finalizar.
HERRAMIENTA ÚTIL: Terms of Service; Didn't read es una extensión para navegador que te muestra un ranking de los servicios que utilizas.
URL: www.tosdr.org

Riesgos físicos

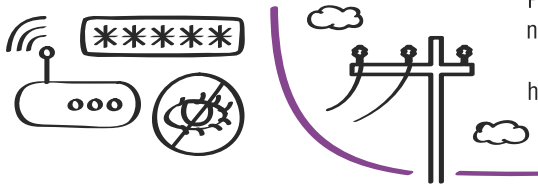
Al utilizar dispositivos digitales corremos riesgo de robo, extravío o instalación de keylogger. Un keylogger es un dispositivo que se conecta a tu computadora y graba lo que escribes a través del teclado. Haz inspecciones visuales de tu equipo, busca dispositivos extraños que tú no hayas conectado.



Te explicamos cómo viaja tu información cuando navegas en Internet

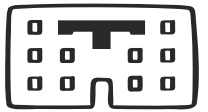
Tus dispositivos almacenan toda tu información. Para evitar que alguien haga mal uso de ella, activa contraseñas en tu celular, computadora o tablet.

El módem es tu punto de conexión a Internet. Pueden espiarte fácilmente si encuentran tu contraseña en el aparato, así que es mejor cambiarla.



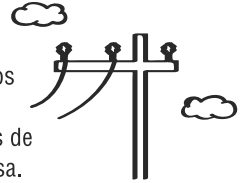
Si navegas de forma insegura, alguien puede tener acceso a tus contraseñas o incluso leer tus conversaciones. Para evitarlo siempre navega usando https. Ejemplo: https://facebook.com

Después del módem, tus datos llegan a tu proveedor de servicios de Internet.



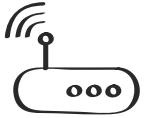
El proveedor envía tus datos a la red social que estás usando.

No todo lo que es gratis en Internet es seguro. Algunas empresas recolectan tus datos para después venderlos. Revisa con detalle los términos de servicio (ToS) de cada empresa.

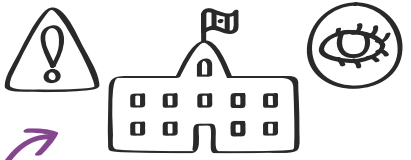


Facebook entrega tus datos a otro proveedor de Internet para que lleguen a su destino final.

El proveedor envía tus datos al módem de la destinataria.



Es importante que sepas que hay gobiernos que revisan tus datos en el trayecto. Esto desafortunadamente va en contra de una red libre y neutral.



Después de recorrer toda esta cadena, tu mensaje llega al dispositivo de la destinataria.

La seguridad es cosas de dos, ambxs deben cuidarse para tener comunicaciones más seguras.