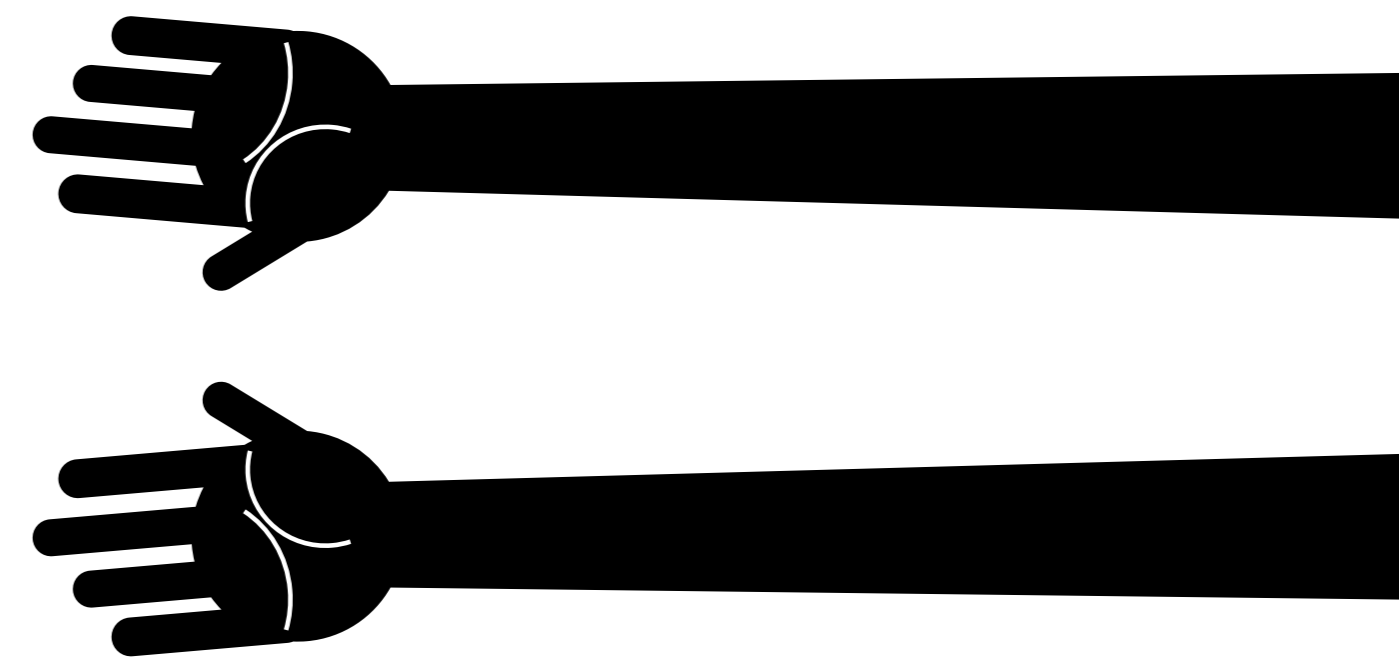


10 Tips de seguridad digital para líderes sociales



Protegemos nuestros celulares. Nuestros celulares tienen clave o patrón de acceso. Además, hacemos copias de seguridad con regularidad.

Más seguro: Si nuestros celulares lo permiten, ciframos sus contenidos.



Nos aseguramos de no dejar información en los computadores de terceros.

Cuando nos conectamos desde un café internet, un espacio público o el computador de otra persona, usamos siempre el modo de navegación incógnita y recordamos borrar los documentos descargados.

Más seguro: Preferimos usar Firefox.



Nos comunicamos con herramientas seguras y ni siquiera las chuzadas nos escuchan.

Preferimos usar aplicaciones de mensajería que cifran las comunicaciones (ej. WhatsApp), que hacer una llamada telefónica o enviar un SMS.

Más seguro: Usamos las aplicaciones Signal o Wire, que son aún más seguras, y también les pedimos a nuestros contactos que lo hagan.



Nuestra navegación en internet es segura.

Revisamos la configuración de seguridad del navegador para deshabilitar rastreo y cookies de terceros, y borrar el historial. Además, mantenemos nuestro navegador actualizado.

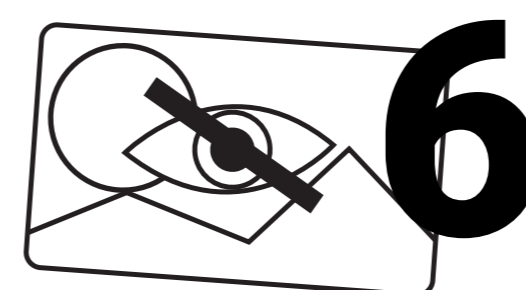
Más seguro: Usamos una red virtual privada (VPN) o el navegador TOR^[1] cuando queremos proteger nuestra identidad digital.



Tenemos copias de respaldo de nuestra información digital.

Con regularidad respaldamos la información que tenemos en computadores, celulares y en la nube.

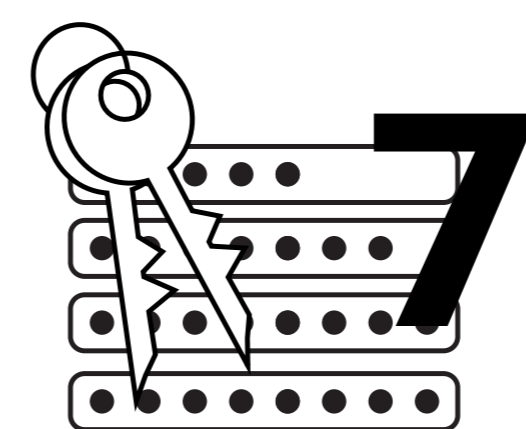
Más seguro: Mantenemos más de una copia de respaldo y/o ciframos las copias de respaldo.



Cuidamos lo que publicamos en internet.

Protegemos nuestra privacidad y la de otras personas en internet evitando publicar fotos, información personal (números de identificación, teléfonos, direcciones, etc.) y ubicación. Además, tenemos cuidado al momento de decidir si etiquetamos fotos y mensajes.

Más seguro: Establecemos con cuidado quienes pueden ver o no cada publicación.



Cuidamos nuestras contraseñas.

Creamos contraseñas complejas, largas y diferentes para cada cuenta. Las cambiamos de vez en cuando, sobre todo, cuando sospechamos que pueden estar comprometidas (ej. si las usamos en un café internet).

Más seguro: Usamos un gestor de contraseñas como KeePass^[2].



Protegemos la información sensible.

Los archivos con información sensible los protegemos con contraseñas de acceso.

Más seguro: Ciframos nuestros archivos sensibles con programas especializados como 7-Zip o Veracrypt.^[3]



Protegemos nuestras cuentas en Facebook y otras redes sociales.

Usamos contraseñas seguras en nuestras cuentas. Para el fanpage de Facebook asignamos los roles (administrador, editor, moderador, etc.) y permisos con cuidado.

Más seguro: Utilizamos la autenticación de dos pasos.



Tenemos una vida digital saludable y segura.

Nos cuidamos en internet y en el mundo físico. Actualizamos las versiones de los programas que usamos en todos nuestros dispositivos, y revisamos con regularidad sus configuraciones de seguridad y privacidad.

Más seguro: Limpiamos nuestros equipos eliminando programas, aplicaciones, archivos e información no necesarios.

[1] <https://www.torproject.org/projects/torbrowser.html>

[2] <https://keepass.info/>

[3] <https://www.7-zip.org/>
<https://www.veracrypt.fr/en/Home.html>