

Paso 3



Familiarízate con las configuraciones de privacidad y seguridad



- Para proteger información y datos personales en redes sociales y apps de mensajería.
- Busca en tu aplicación la opción **Ajustes**, allí están las opciones de **Privacidad y Seguridad**.
- **Decide quién puede ver tu perfil personal**, lista de amigos, publicaciones pasadas, etc.
- Quién puede etiquetarte en publicaciones.
- **Limita** a las y los usuarios que pueden enviarte mensajes directos.



- **Activa la verificación de dos pasos.** Así, si hay un intento de ingreso a una cuenta (más conocido como hackeo), recibirás un mensaje de texto o correo electrónico para denegar el ingreso.

Paso 4

Aprende a reconocer enlaces maliciosos

Porque pueden dirigir a una web falsa para robar tu información personal, tus contraseñas o para instalar algún virus en tu dispositivo.



Tu cuenta de banco ha sido bloqueada por cambios fuera de lo normal. Debido a dichos cambios nos vemos obligados a pedirle que autentique su identidad dentro de las próximas 24 horas o su cuenta quedará inactiva. Para autenticar su cuenta, ingrese en el siguiente enlace: www.autenticarmicuentabolivia.bo

Los **enlaces maliciosos** pueden llegarte en forma de mensaje (por correo electrónico, SMS, chat, etc.)

Antes de hacer clic sobre un enlace, chequea si:

- ¿**Conoces** a la persona que envió el mensaje?
- El mensaje ¿hace mención a **premios, ofertas o regalos**?
- ¿Recibiste un mensaje que dice que ganaste el premio de un concurso en el que nunca participaste?
- ¿El mensaje te invita a que instales o descargues algún documento?

Paso 5

Revisa si tus datos personales están disponibles en Internet

Abre un buscador y en la barra de búsqueda ingresa tus datos personales como:



- Es posible que esta información esté publicada en Internet.
- Si quieres borrar tu información de una página web, **puedes solicitar a la página que lo haga.**

Para conocer más detalles de cómo hacerlo, comunícate a nuestra **línea de ayuda:**

623 42430

Paso 6

Separa tu identidad pública de la privada

- Intenta tener **dos líneas en tu dispositivo**, uno para la vida personal y otro para la vida pública y laboral. Así reduces riesgos de acceso no deseado a tus datos.
- Usa **perfiles distintos** para publicar información. Uno puede ser para tu trabajo político y otro para compartir información privada con tu círculo cercano.
- **Verifica tus cuentas de redes sociales.** Este es un servicio que autentica que la persona dueña de la cuenta es quien dice ser. Sirve para evitar el robo de identidad.
- **Elimina** las publicaciones antiguas masivamente de tus redes sociales y desactiva las cuentas que ya no usas.



Si no entendiste alguno de estos consejos, comunícate con nosotras, te orientaremos.

Paso 7

Cuida tus comunicaciones sensibles



Opta por apps de mensajería que tienen encriptado de punta a punta como **Signal o WhatsApp**.

El **cifrado de extremo a extremo** disfraza un mensaje para que no sea interceptado y que solo la persona receptora del mensaje pueda ver su contenido.

- Activa las opciones de **autodestrucción**.
- Recuerda **deshabilitar la previsualización** de los mensajes en la pantalla de tu celular. De esta forma las personas que estén cerca de ti no podrán leer tus mensajes.
- **Borra el historial** de tus conversaciones que consideres sensibles o muy privadas.

Paso 8

Documenta las agresiones



- **Toma captura de pantalla** de la publicación que quieres documentar.
- **Guarda el enlace o link** de la publicación y del perfil de la persona agresora.
- Crea una **bitácora** de lo que ocurrió, **incluyendo fechas y contexto del ataque.** Es decir, pregúntate si las agresiones ocurrieron en el marco de un evento en particular (una protesta, una entrevista, etc).

Hacer esto sola puede generar ansiedad, **puedes pedirle a alguna persona de confianza que lo haga por ti.**

Guarda esta información en un lugar seguro.

Paso 1

Cuida tus dispositivos

- **Actualiza** el sistema operativo de tus celulares, tablets o computadoras.
- **Desactiva** el Wi-Fi y el bluetooth si no están en uso.
- **Activa el bloqueo de pantalla** de tu celular. Usa un PIN o contraseña y evita usar patrones o el reconocimiento de huella dactilar o facial.
- **Si usas un PIN no uses números que puedan asociarse contigo** como tu año de nacimiento o que se puedan adivinar fácilmente.

Tu celular, computadora y tablet tienen mucha información privada como conversaciones, fotos, datos bancarios, historial de búsqueda, etc. **por lo que perder un dispositivo sin una contraseña puede poner en riesgo esta información.**

Paso 2

Usa contraseñas seguras

Ayuda a obstaculizar el **robo de tus cuentas.**

Muchos de los robos de cuentas ocurren porque las contraseñas son débiles como "12345678" o porque utilizamos la misma contraseña para varias redes sociales.

NO USES

Fecha de nacimiento, nombre de hijos, carnet de identidad, número de celular u otras palabras predecibles.

Ques0!T0m@t3

- Que tenga al menos 12 caracteres.
- Debe ser única.
- Debe ser una mezcla de números y letras.
- Usa mayúsculas, minúsculas, caracteres especiales.



Las contraseñas deben ser secretas

Si compartes una contraseña con tu equipo que maneja tus redes sociales. **No repitas esta contraseña en otros servicios.**

Recordar una contraseña para cada cuenta puede ser difícil. Puedes usar una parte distinta de una canción que nadie sabe que te gusta como contraseña para cada una de tus cuentas en Internet.

Explora la opción de usar un **administrador de contraseñas**. Se trata de una aplicación que sirve como un llavero donde puedes guardar de forma segura las contraseñas de todas tus cuentas.



Cambia tus contraseñas cada 3 meses.



CONSEJOS DE SEGURIDAD DIGITAL PARA MUJERES POLITICAS

Este material pedagógico ha sido elaborado por el **Centro S.O.S. Digital** equipo de respuesta a violencias digitales de género de la Fundación InternetBolivia.org.

Y su reimpresión es posible gracias al proyecto RECIFE cofinanciado por la Unión Europea. Su contenido es responsabilidad exclusiva de los autores y socios en la ejecución y no reflejan necesariamente las opiniones de la Unión Europea.

FRENTE A LA VIOLENCIA DIGITAL, NOS ORGANIZAMOS.



ESCRÍBENOS A LA LÍNEA DE APOYO

+591 **62342430**



Signal



Telegram



WhatsApp



Cofinanciado por la Unión Europea



WWW.SOSDIGITAL.INTERNETBOLIVIA.ORG