GUÍA DE

Seguridad Digital

para Mujeres en el ejercicio político público

CON EL APOYO DE:

ONU MUJERES

Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres

GUÍA DE

Seguridad Digital

para Mujeres en el ejercicio político público

CONTENIDO

INTRODUCCIÓN **AL PROBLEMA** 1

Para entender el concepto de violencia digital es importante reconocer que la violencia contra las mujeres en el entorno digital es una extensión de las violencias a las que las mujeres nos enfrentamos día a día, solo que ha encontrado una nueva forma de expresión, que es el ámbito digital. En este sentido, mujeres lideresas, candidatas y aquellas que ejercen cargos públicos se enfrentan constantemente a acoso y violencia política, que se manifiesta en el ámbito digital. El objetivo de dichas formas de violencia es excluir a las mujeres o impedir su participación en el ámbito público, afectando su dignidad y vulnerando sus derechos políticos.

Entre las formas de violencia digital que mayormente enfrentan las mujeres políticas está la manipulación, la desinformación (más conocida como noticias falsas), la difamación y las amenazas. En muchas ocasiones se tiende a minimizar las violencias digitales porque se cree que como suceden a través de una pantalla, estas no tienen efectos significativos en la vida de las mujeres, sin embargo, sí los tienen, sobre todo en la vida de mujeres lideresas y políticas.

Una consecuencia de lo anterior es la autocensura. Al reconocer que Internet es un lugar hostil, muchas mujeres decidirán callarse, no opinar y no participar en el debate público, que muchas veces sucede en Internet. Esta realidad contribuye a aumentar la brecha digital de género en nuestro país, esta brecha es la distancia entre las mujeres que pueden conectarse a Internet y saben como funciona, y las que no se conectan con frecuencia y tienen dificultades para entender el funcionamiento y los riesgos que existen.

La brecha digital de género también constituye un tipo de violencia digital, pues al no contar con una conexión estable y desconocer los múltiples beneficios que tienen las tecnologías de información y comunicación se cierran para las mujeres las posibilidades de autonomía y acceso al conocimiento, se reducen las oportunidades laborales y se incrementa el riesgo de que las mujeres sean expuestas a un espacio hostil sin herramientas de cuidado, lo cual profundiza las desigualdades de género.

En este marco, es necesario que las mujeres en función pública puedan conocer algunas formas de cuidado que existen en el mundo digital, de esta forma podrán sentirse seguras al habitar en él, lo que contribuirá a que estén conectadas a Internet sin miedo, hagan escuchar su voz y aprovechen todas las ventajas que la red ofrece. Esta guía esta diseñada para que las mujeres en función pública, de acuerdo a las tareas qué realizan en su vida política, puedan familiarizarse con aspectos básicos de la seguridad digital, para que se animen a explorar sus celulares, sus cuentas en redes sociales y tomen el control de su vida digital.

VIOLENCIAS **DIGITALES** 2

2.1. ¿Qué son las violencias digitales?

La violencia digital es cualquier agresión que pueda presentarse por las TIC (Tecnologías de Información y Comunicación como las redes sociales, aplicaciones de mensajería, páginas web,etc). Todas las violencias que enfrentamos en los espacios físicos pueden ser experimentadas en otras dimensiones y de nuevas maneras en el espacio digital. Las violencias digitales con frecuencia se ejerce contra poblaciones históricamente discriminadas (mujeres, niñas, niños, adolescentes, adulto mayores, afrodescendientes, etc.).

2.2. Tipos de violencia digital[1]

- Vigilancia e invasión a la privacidad: Ocurre cuando existe un ingreso no autorizado a nuestras cuentas en redes sociales con el objetivo de acceder a información privada sobre nosotras. Por ejemplo, cuando revisan nuestro celular para leer las conversaciones de WhatsApp.
- Acoso y amenazas: Es un conjunto de conductas qué se repiten, entre las que se cuentan las amenazas, falsas acusaciones, humillación y chantaje que resultan molestas e intimidantes. Por ejemplo, recibir mensajes en nuestra cuenta de Facebook donde nos amenazas con hacernos daño.
- Campañas de difamación y desprestigio: Son agresiones planificadas con el fin de dañar la imagen de las mujeres, este tipo de difamación tiene el fin de perjudicar a la imagen, la credibilidad, a través de información falsa, manipulada o fuera de contexto. Por ejemplo, cuando editan la foto de una mujer política para ridiculizarla en redes sociales.
- Violencia sexual digital: Tiene que ver con la invasión a la intimidad y sexualidad de una mujer. Se ejerce mediante la difusión de imágenes íntimas sin consentimiento o a través de amenazas, exigiendo el envío de contenido sexual y/o erótico, y de insultos por su actividad sexual, entre otros.

2.3 Seguridad digital y su importancia

Internet es vital para varias de las actividades que realizamos día con día, a través de Internet nos conectamos con nuestras amistades, las personas de nuestro trabajo, etc. Sin embargo, como hemos visto el mundo digital suele ser hostil para las mujeres ya qué nos enfrentamos a distintos tipos de violencia, tanto como fuera y dentro de Internet tenemos el derecho a vivir una vida libre de violencia.

La seguridad digital nos ayuda a tomar control sobre nuestra vida digital y de alguna manera reducir los riesgos de enfrentar violencias digitales. La seguridad digital es lo qué hacemos para cuidarnos cuando nos conectamos a Internet. En esta guía encontrarás varios consejos sencillos de seguridad digital qué puedes poner en práctica en tu día a día, también encontrarás enlaces qué te llevarán a videos tutoriales, los podrás identificar por qué estarán subrayados y tendrán un texto así: “sigue los siguientes pasos”.

1 Mujeres libres en política: Guía para combatir el acoso y la violencia política digital (AVP)

FORMAS LEGALES DE RESPONDER A **VIOLENCIAS DIGITALES**

3

3.1. Ley 243, Ley contra el Acoso y Violencia Política hacia las Mujeres

La Ley 243 contra el Acoso y Violencia Política hacia las Mujeres fue promulgada en 2012, tras la muerte de Juana Quispe,, concejala del municipio de Ancoraimes, quien fue asesinada después de haber recibido amenazas y agresiones durante meses. El objetivo de la ley es prevenir, atender y sancionar los actos de acoso y de violencia política cometidos contra mujeres candidatas, electas, designadas o en el ejercicio de la función político-pública.[2]

3.1.1. Mecanismos de denuncia[3]

¿A quiénes protege la Ley 243?

- Mujeres candidatas
- Mujeres electas como titulares o suplentes
- Mujeres que acceden a la función político-pública nombradas para el cargo
- Mujeres lideresas de organizaciones políticas sociales

3.1.1.1 ¿Quiénes pueden denunciar?

La denuncia puede ser presentada por la víctima, sus familiares o cualquier otra persona natural o jurídica, como también por las autoridades electorales, servidores públicos u otras autoridades en forma verbal o escrita.

3.1.1.2. ¿Dónde presentar una denuncia?

- Órgano Electoral (Responsable de Género del Tribunal Supremo Electoral, los Tribunales Electorales Departamentales o jueces electorales).
- Policía (FELCV o FELCC donde no exista la primera).
- Ministerio Público o Fiscalía.
- Comisiones de ética de los GAM y GAD

3.1.1.3. ¿Cuáles son los tipos de denuncia?

De acuerdo a la Ley 243, las mujeres en política tienen cuatro caminos para realizar una denuncia por acoso y violencia política:

Vía constitucional: Se refiere a las acciones de defensa establecidas en la Constitución Política del Estado encargadas de preservar los derechos políticos de las mujeres.

Vía electoral: La denuncia puede ser presentada de forma verbal o escrita por la candidata, mujer electa o en función político pública, familiares o una persona natural o jurídica ante los Tribunales Electorales Departamentales.

Vía administrativa: Si se conoce a la persona atacante, se puede denunciar ante la misma institución a la que pertenece la persona agresora o grupo agresor. Se buscarán sanciones administrativas o disciplinarias de acuerdo al procedimiento dispuesto en la norma vigente.

Vía penal: Los delitos de acoso político y/o violencia política pueden ser denunciados ante la FELCV o el Ministerio Público. Si la vida de la persona agredida está en riesgo, se deben dar medidas de protección.

2 Módulo 3. Mujeres en la política: prevención y actuación frente al acoso y violencia política. Coordinadora de la Mujer.

3 Módulo 3. Mujeres en la política: prevención y actuación frente al acoso y violencia política. Coordinadora de la Mujer.

SEPARANDO NUESTRA VIDA **PERSONAL Y LABORAL** 4

4.1. La importancia de separar **nuestra vida personal de la laboral**

Las redes sociales se han convertido en parte de la vida cotidiana, están cambiando las formas tradicionales de comunicarnos y de consumir información, lo cual ha tenido un impacto en los procesos electorales y en las estrategias de comunicación de autoridades electas, partidos políticos, etc. Las tecnologías de la información y comunicación (TIC) ofrecen un espacio para ejercer el derecho a la libertad de expresión y participar en la vida pública.[4]

El uso efectivo de las redes sociales puede ayudar a las mujeres políticas a mejorar sus estrategias de comunicación durante la campaña electoral o durante sus gestiones en cargos públicos. Sin embargo, se han convertido en un espacio hostil para las mujeres en la política, donde a menudo tienen que enfrentar acoso, difamación y amenazas, solo por mencionar algunos tipos de violencia digital. Para poder responder a estas agresiones en las redes es necesario conocer algunos aspectos que nos permitan tomar el control de la información que compartimos en Internet, para reducir el riesgo de enfrentar violencias digitales.

Para retomar el control de la información que compartimos en Internet, se recomienda separar las comunicaciones e información que tenemos en la vida laboral y en la personal. En la vida fuera de Internet, todo el tiempo decidimos qué información compartimos con algunas personas y qué información no, por ejemplo: cuando estamos con ciertas amigas(os) es posible que les contemos algunas situaciones personales que no compartiríamos con otras personas que no son tan allegadas.

Esta misma distinción la podemos hacer en nuestra vida digital. Si bien existe cierta información que podemos compartir con varias personas cercanas, la misma puede estar también a la mano de personas desconocidas, lo cual nos pone en riesgo de enfrentar violencias digitales y también violencias fuera de Internet.

4 "Social Media: A Practical Guide for Electoral Management Bodies"IDEA Internacional (2014):.
Ver: https://www.idea.int/publications/catalogue/social-media-practical-guide-electoral-management-bodies?lang=en

4.2. ¿Por dónde comenzar?

4.2.1. En el teléfono

Para poder separar nuestra vida personal de nuestra vida laboral primero debemos pensar en nuestras comunicaciones. Sería de gran ayuda contar con dos celulares; sin embargo, esa es una situación ideal en nuestro contexto económico. No obstante, es más viable contar con dos líneas telefónicas y un número de teléfono para asuntos laborales y el otro para asuntos personales.

Si es posible tener dos teléfonos móviles diferentes, en el celular asignado a la vida personal se puede guardar los contactos de la familia, fotos personales y conversaciones privadas. Mientras, en el número asignado al ámbito laboral, todo lo que concierna a este espacio. Separar nuestra información de esta manera es de mucha ayuda en caso de perder uno de nuestros celulares, si esto pasa habremos perdido el 50% de nuestra información y no toda, como hubiera pasado si solo guardamos nuestros datos en un solo dispositivo.

Así, en caso de que nos veamos imposibilitadas de contar con dos celulares, una forma de separar nuestra vida privada de nuestra vida política es tener dos líneas de teléfonos distintas. En la actualidad, la mayoría de los celulares con conexión a Internet tiene la opción de poner dos chips, es decir, tener dos líneas telefónicas funcionando al mismo tiempo en el mismo celular. Una línea telefónica puede ser de gran ayuda para dividir nuestra vida pública de la privada. Una línea telefónica puede ser destinada para asuntos políticos y laborales y el otro número para asuntos personales, es importante que este último número sea manejado en reserva, solo personas cercanas a ti deberían saberlo.

4.2.2. En Facebook

Usar una página de Facebook para nuestra vida profesional es una forma de separar nuestra identidad personal de la pública. En una página de Facebook, cualquier persona puede darle “Me gusta” tras ver lo que se publica en la misma, exclusivamente, y no en la cuenta de perfil personal. De esta forma, activando las medidas de privacidad adecuadas, se puede publicar en el perfil aspectos más personales que se desee compartir con familiares y amistades. Siempre revisando que conocemos a todos a nuestros contactos, y así en nuestra página podemos publicar aspectos más relacionados con el trabajo político.

CONFIGURACIÓN DE **PRIVACIDAD Y SEGURIDAD EN WHATSAPP**

5

WhatsApp es una de las aplicaciones que usamos a diario. Muchas veces, nuestra vida laboral, personal, fotos, historias y documentos importantes se encuentran en WhatsApp, es por eso que la seguridad y la privacidad que tenemos en esta aplicación nos debe importar.

La mayoría de las aplicaciones de mensajería, así como de las redes sociales, cuentan con un apartado donde podemos configurar la seguridad y privacidad de nuestra información. Usualmente, cuando se hace referencia a las configuraciones de seguridad, se trata de la protección de las cuentas, aquí podremos cambiar la contraseña y asegurar el ingreso de nuestra cuenta. En privacidad podemos configurar quiénes pueden ver los permisos sobre quienes pueden ver la información de las y los usuarios (datos personales, fotos de perfil, hora de última conexión, estados), entre otras cosas.

5.1. ¿**Qué información** sobre mí pueden ver mis contactos?

Cuando usamos WhatsApp nuestros contactos y cualquier persona que tenga nuestro número de teléfono puede ver, entre otras cosas, la siguiente información:

- La última vez que nos conectamos
- Foto de perfil
- Confirmaciones de lectura (Si hemos leído o no el mensaje)

WhatsApp nos da la opción de elegir que estos datos sean compartidos con:

- Todos (todas las personas que tengan nuestro número aunque nosotras no tengamos guardado el suyo)
- Mis contactos (solo personas de las cuales tenemos guardado el número)
- Nadie

Para proteger nuestra privacidad recomendamos seleccionar “Mis contactos”, de manera que solo determinadas personas puedan encontrar visible la información en WhatsApp. Para configurarlo de esta manera, ingresar al menú de opciones que está simbolizado con tres puntos verticales; seleccionar ajustes > cuenta > privacidad y seguir los siguientes pasos.

5.2. **Controlar quién** puede agregarme a grupos

Es común ser añadida en grupos de WhatsApp sin que nos pidan permiso para ello, sobre todo cuando nuestro número de teléfono está al alcance de varias personas por el trabajo que realizamos. Esta situación suele ser muy molesta porque de un minuto al otro nos encontramos con varias notificaciones de mensajes que no son de nuestro interés.

En WhatsApp podemos elegir a quienes nos pueden agregar a grupos:

- Todos
- Mis contactos
- Mis contactos excepto... (Si elegimos esta opción podemos seleccionar los contactos específicos que no queremos que nos agreguen a grupos de forma automática)

Es importante saber que si conFiguramos esta opción, WhatsApp nos avisará cuando alguien nos quiera agregar a algún grupo y nosotras tendremos que aceptar si queremos formar parte del grupo o no. Para controlar quién puede agregarte a grupos sigue los siguientes pasos.

5.3. **Protegiendo mi cuenta** de WhatsApp con la verificación en dos pasos

En WhatsApp, como en la mayoría de las redes sociales, una medida de seguridad es la verificación en dos pasos. Si activas esta opción te proteges de que personas desconocidas roben tu cuenta; es decir, si alguien quiere instalar la WhatsApp con tu número de teléfono, no podrá hacerlo si esta opción está activada.

Al activar esta opción debemos crear un código PIN de seis cifras, es importante que recordemos este código porque WhatsApp nos lo pedirá la próxima vez que instalemos la aplicación con nuestro número, como cuando cambiamos de modelo de celular.

También nos pedirá que agreguemos un correo electrónico que se usará en caso de que olvidemos el código PIN, por eso debemos ingresar un correo electrónico al que tengamos acceso.

Para activar la verificación en dos pasos debemos ingresar al menú de opciones qué está simbolizado con tres puntos verticales, seleccionar ajustes > cuenta > verificación en dos pasos y seguir los siguientes pasos.

CONFIGURACIÓN DE **PRIVACIDAD Y SEGURIDAD EN FACEBOOK**

6

La mayoría de las violencias digitales que enfrentan las mujeres ocurren en Facebook, esto se debe a una variedad de factores, como que es una de las redes sociales que más se usa las formas en las que responden a las violencias en sus plataformas son deficientes. En ese sentido, una forma de reducir los riesgos de enfrentar estas violencias es revisar las configuraciones de seguridad para que reduzcamos la posibilidad de que nos roben o ingresen sin permiso a nuestra cuenta y las configuraciones de privacidad para asegurarnos que nuestra información personal no sea visible para todo el mundo.

6.1. Configuraciones de **seguridad**

6.1.1. ¿**Cómo verificar** si alguien ingresó a mi cuenta de Facebook sin mi permiso?

Facebook te muestra un registro de todos los lugares desde donde te conectaste a tu cuenta, en el registro existen datos como modelo de celular, ubicación, fecha, hora y región desde donde te conectaste. En ese sentido, si sospechas que alguien ingresó o tiene acceso a tu cuenta en Facebook puedes acceder a este listado para verificar si existe algún inicio de sesión que no hayas realizado.

Para revisar el listado puedes dirigirte al menú de opciones que se encuentra en la parte superior de tu pantalla y que está simbolizado con tres rayas horizontales, selecciona la opción **configuraciones de seguridad y privacidad >configuración >seguridad >dónde iniciaste sesión** o sigue los siguientes pasos.

Si encuentras un inicio de sesión que no hiciste tú, por ejemplo si en este listado aparece un modelo de celular que no corresponde al tuyo, puedes cerrar la sesión en ese dispositivo siguiendo los siguientes pasos:

6.1.2. ¿**Cómo evitar** que otras personas ingresen a nuestra cuenta de Facebook?

En Facebook también tenemos la opción de activar la verificación de dos pasos, que brinda una mayor capa de seguridad a nuestra cuenta. La verificación en dos pasos es una función de seguridad que, junto a la contraseña, ayuda a proteger tu cuenta de Facebook. Si activamos esta opción, cuando queramos ingresar a nuestra cuenta desde otro celular o computadora que no sea el usual, Facebook mandará un código a través de SMS a nuestro celular y nos pedirá que lo ingresemos después de escribir la contraseña.

De esta forma, si alguien está intentando ingresar a tu cuenta no podrá hacerlo porque necesitará el código que te ha llegado a tu celular. En ese sentido, si usamos la verificación en dos pasos, junto con nuestra contraseña, tendremos dos métodos de seguridad, es como cuando tenemos dos llaves para ingresar a nuestra casa, una para cada cerradura.

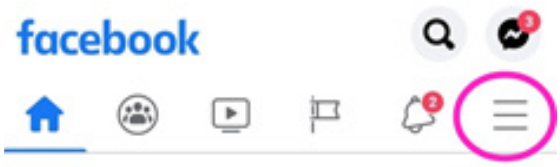
Para poder activar la verificación en dos pasos en Facebook sigue los siguientes pasos.

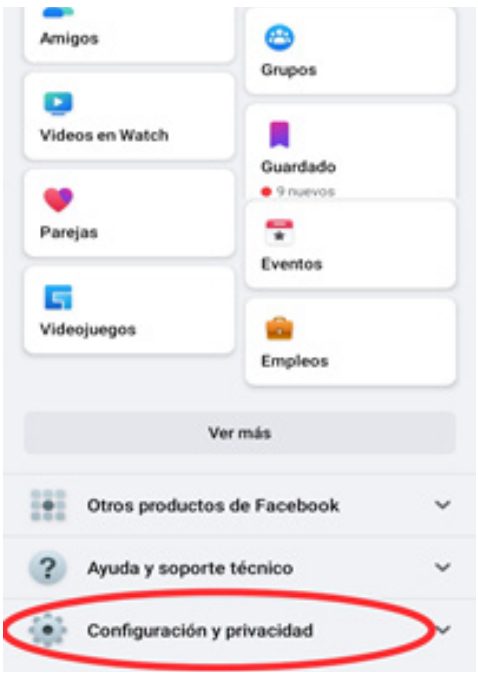
6.2. Configuraciones de **privacidad en Facebook**

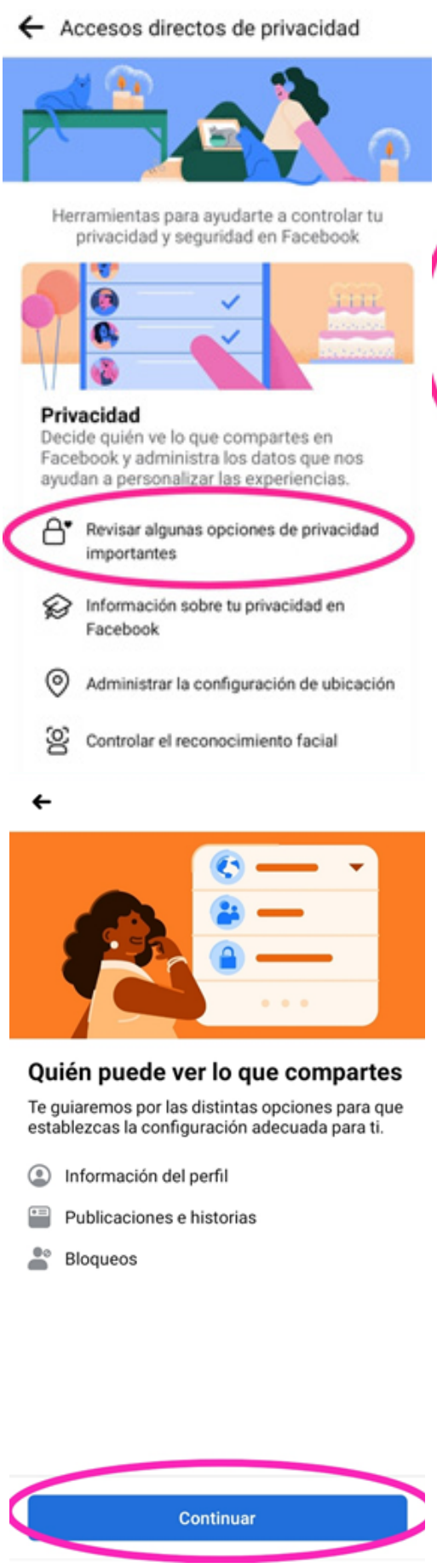
En el sector donde se encuentran las configuraciones de privacidad de Facebook podemos encontrar una lista larga de todos los aspectos referentes a privacidad, que podemos personalizar, es importante que recibamos todas para conocer todas las formas en las que podemos cuidar nuestra información en esta plataforma. En esta guía nos centraremos en tres secciones importantes: ¿Quién puede ver tu información?, ¿Quién puede encontrarte en Facebook? y ¿Quién puede mandarte mensajes?.

6.2.1. ¿**Quién puede** ver tu información?

Para configurar quién puede ver nuestra información, nuestras publicaciones pasadas y futuras, debemos ingresar al menú de configuraciones de Facebook. Para esto necesitamos presionar en las tres rayas horizontales de la parte superior, una vez ahí buscamos las siguientes opciones: Configuración de privacidad y seguridad> Comprobación rápida de privacidad> ¿Quién puede ver lo que compartes? > Continuar

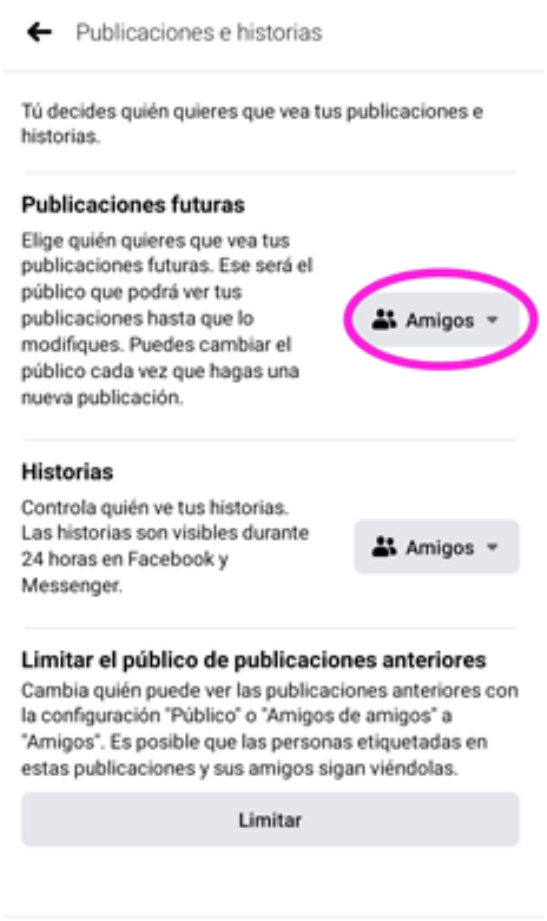





Accesos directos de privacidad
Herramientas para ayudarte a controlar tu privacidad y seguridad en Facebook
Privacidad
Decide quién ve lo que compartes en Facebook y administra los datos que nos ayudan a personalizar las experiencias.
Revisar algunas opciones de privacidad importantes
Información sobre tu privacidad en Facebook
Administrar la configuración de ubicación
Controlar el reconocimiento facial
Quién puede ver lo que compartes
Te guiaremos por las distintas opciones para que establezcas la configuración adecuada para ti.
Información del perfil
Publicaciones e historias
Bloqueos
Continuar
Comprobación rápida de privacidad
Te mostraremos algunas opciones de configuración para que puedas tomar las decisiones correctas para tu cuenta.
¿Con qué tema quieres empezar?
Quién puede ver lo que compartes
Hace aproximadamente 5 meses
Cómo proteger tu cuenta
Hace un año
Cómo pueden buscarte las personas en Facebook
Hace aproximadamente 12 meses
Tu configuración de datos en Facebook
Hace una semana
Información del perfil
Revisa esta información de tu perfil y decide quién puede verla. Es posible que tu perfil tenga más información de la que se muestra aquí.
Número de teléfono
Solo yo
Correo electrónico
Solo yo
Fecha de nacimiento
Amigos de amig...
Solo yo
Ciudad de origen
La Paz
Público
Intereses
Siguiente

El primer aspecto que debemos configurar es seleccionar qué información personal queremos que sea visible para cualquier persona en Facebook y cuál no. En la lista de los datos que podemos configurar están:

- **Número de teléfono**: Recomendamos que esta información solo sea visible para ti, de esta forma las personas en Facebook no podrán tener acceso al número de celular con el que probablemente inicias sesión.
- **Correo electrónico:** De la misma forma que en el punto anterior, es recomendado que esta información sea visible solo para ti.
- **Fecha de nacimiento:** Solemos creer que esta información no nos puede poner en riesgo, sin embargo, nuestra fecha de nacimiento es una dato que nos piden para autenticar que somos nosotras en diferentes trámites, por ejemplo, cuando queremos recuperar nuestro chip o cuando nos comunicamos con el banco por teléfono, por esta razón recomendamos que esta información sea privada y en Facebook solo esté disponible para nosotras.
- **Ciudad de origen:** Esta información no nos pone en riesgo y puede estar de forma pública si así lo deseamos.



La siguiente opción que nos aparece es: publicaciones e historias. En este apartado podremos configurar quién tiene acceso a nuestras publicaciones futuras y pasadas. Nos aparecerán las siguientes opciones:

- **Publicaciones futuras:** Podemos seleccionar quienes van a ver las publicaciones que hagamos de ahora en adelante, podemos elegir que sean nuestros amigos (contactos en Facebook), solo nosotras o el público en general (todos los y las usuarias de Facebook) quienes vean estas publicaciones. Recomendamos que se seleccione la opción de que solo nuestros amigos puedan ver.
- **Historias:** De la misma manera, en este apartado recomendamos seleccionar que solo “Amigos” puedan ver nuestras historias.
- **Limitar las publicaciones anteriores:** Es probable que desde la fecha que hemos creado nuestro perfil en Facebook hasta hoy hayan pasado muchos años. Es decir, durante todo este tiempo hemos realizado varias publicaciones sin percatarnos quienes podían verlas (si solo estaban disponibles para nuestros contactos o para el público en general). En ese sentido, si seleccionamos esta opción, automáticamente todas nuestras publicaciones anteriores que estaban disponibles para el público en general se volverán disponibles solo para nuestros contactos en Facebook. Es decir, si alguien que no es nuestro contacto en Facebook quisiera buscar y leer antiguas publicaciones de nuestro perfil no encontrará mucha información.

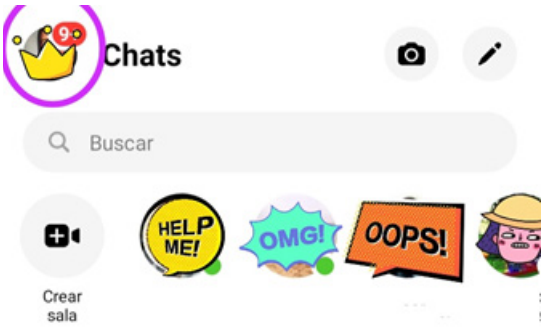
Para activar la opción, solo debemos presionar en **“Limitar”**, nos aparecerá el siguiente mensaje y nuevamente presionamos **“Limitar”**.

6.2.2. ¿**Quién puede** mandarte mensajes?

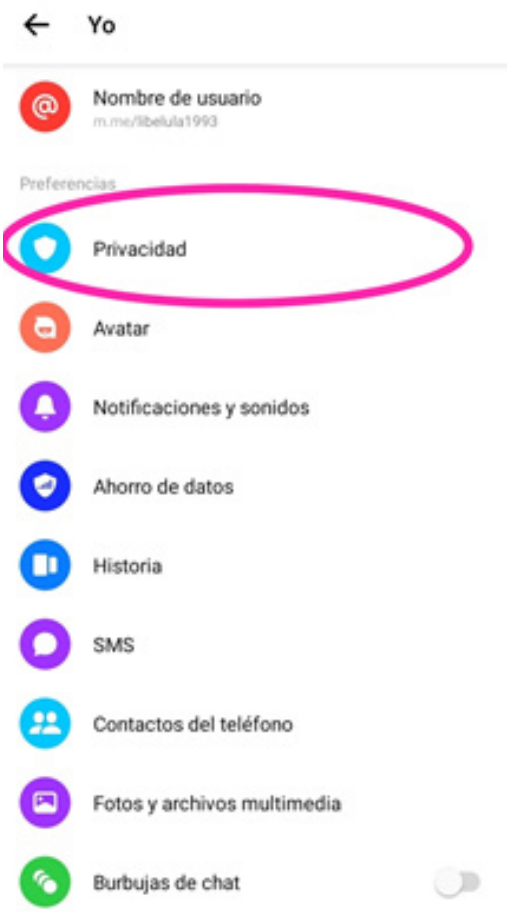
Para configurar quienes pueden mandarnos mensajes debemos ingresar a la aplicación de Facebook Messenger desde nuestro celular. En esta aplicación podemos elegir quienes en Facebook nos pueden mandar mensajes. A veces, las mujeres políticas o lideresas solo por el hecho de opinar, denunciar vulneraciones o estar activas en la vida política enfrentan ciberacoso y amenazas en sus perfiles de Facebook. El objetivo de estas violencias es silenciar a estas mujeres, ya que desde una concepción patriarcal las mujeres no pertenecen al ámbito público.

Una forma de evitar que estas personas puedan ponerse en contacto con nosotras, es configurando quienes pueden escribirnos mensajes a través de Facebook. Una vez dentro de la aplicación de Facebook Messenger debemos seguir los siguientes pasos:

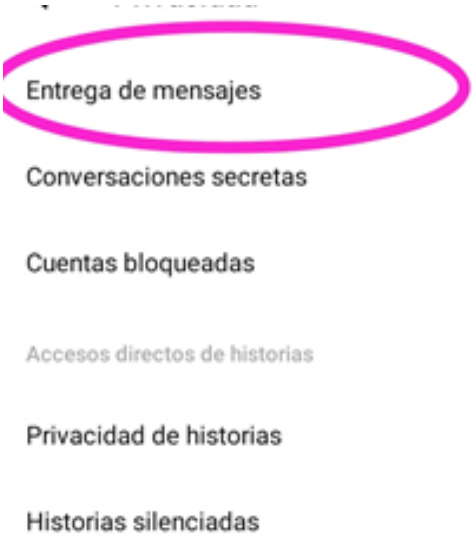
1. Presionar en el círculo pequeño en el extremo superior donde se encuentra nuestra foto.



2. Se abrirá un menú de opciones, buscamos la opción de privacidad e ingresamos.



3. Ingresamos a entrega de mensajes



4. Nos aparecerán varias opciones sobre quienes pueden mandarnos mensajes. Es importante saber que en varias de las opciones mencionan a Instagram, porque éste y Facebook pertenecen a la misma empresa y además comparten información entre ambas aplicaciones. Las opciones son:
   - Personas que tienen mi número: En esta opción podemos decidir si las personas que tienen nuestro número guardado en su celular nos pueden escribir mensajes. Facebook tiene acceso a nuestra agenda de contactos de nuestro celular, es por eso que puede saber quién tiene guardado nuestro teléfono. Entre las opciones que nos muestran están:
     - **Chat:** Si seleccionamos chats, las personas que tienen nuestro número guardado podrán mandarnos mensajes, nos llegará una notificación y los mensajes aparecerán junto con todos los otros chats de la aplicación.
     - **Solicitudes de mensajes:** Si seleccionamos esta opción, la aplicación de Messenger nos preguntará si queremos leer estos mensajes y entablar una conversación con esta persona.
     - **No recibir solicitudes:** Con esta opción este grupo de personas no podrán escribirnos mensajes.
   - **Amigos de amigos en Facebook:** En este apartado podemos elegir si los que son amigos en Facebook de nuestros contactos pueden escribirnos. De la misma forma que la opción anterior, podemos elegir entre chat, solicitudes de mensajes o no recibir solicitudes.
   - **Cuentas que sigues o con las que chateaste en Instagram:** Si tenemos una cuenta en Instagram y chateamos con otras cuentas, en esta opción podemos elegir si queremos que estas personas se contacten con nosotras. En este apartado podemos elegir si los que son amigos en Facebook de nuestros contactos pueden contactarnos. De la misma forma que la opción anterior. Podemos elegir entre chat, solicitudes de mensajes o no recibir solicitudes.
   - **Tus seguidores en Instagram:** Si tienes un perfil en Instagram en esta opción puedes seleccionar si quieres que tus seguidores puedan enviarte mensajes.
   - **Otras personas en Facebook:** Aquí podemos seleccionar si queremos que cualquier persona en Facebook nos pueda mandar mensajes.
   - **Otras personas en Instagram:** Aquí podemos seleccionar si queremos que cualquier persona en Instagram nos pueda mandar mensajes.

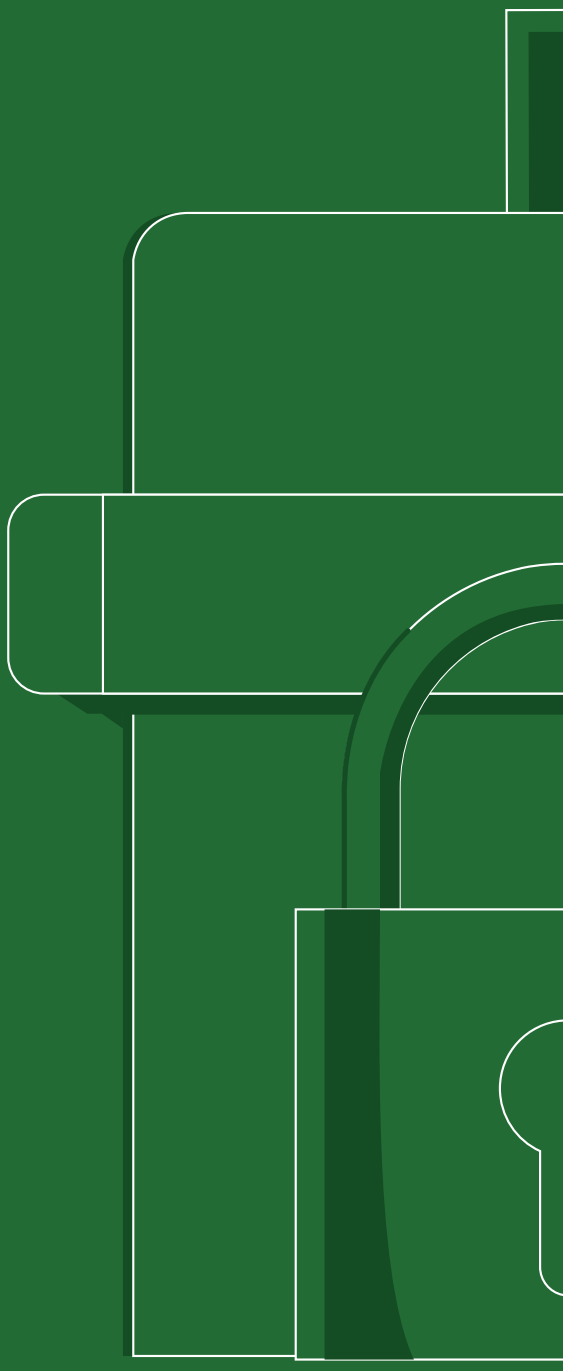
NAVEGACIÓN EN **MODO INCÓGNITO**

7

7.1. ¿**Qué es** la navegación en modo incógnito?

Cuando nos conectamos a Internet, ya sea para buscar alguna información o noticias, usualmente lo hacemos a través de un navegador. Un navegador es el programa que nos permite acceder a Internet, los más usados son Google Chrome y Firefox; en nuestro celular es más común que utilicemos el primero. Un navegador te lleva a cualquier lugar de Internet, permitiéndote ver texto, imágenes y vídeos de cualquier parte del mundo. Recupera información de otras partes de la web y la muestra en tu computadora o celular. Estos navegadores tienen la opción de **"navegar en modo incógnito"**, lo que significa que usando este modo no se guardará información sobre los sitios web a los que accedemos en la computadora o en el celular desde donde nos estamos conectando, es decir que, de alguna manera, protege nuestra privacidad porque:

- No se guardan las páginas visitadas en el historial
- No se guardan las contraseñas



7.2. **En qué** momentos utilizar la navegación en modo incógnito

El modo incógnito de navegación es un buen aliado para cuando tengamos que conectarnos desde computadoras o celulares que no nos pertenecen; por ejemplo, cuando nos conectamos en un café Internet, cuando nos conectamos a nuestras redes sociales para descargar un documento e imprimirlo o a revisar nuestro correo electrónico. Otra situación donde podemos usar la navegación en modo incógnito es cuando usamos computadoras del trabajo o de un amigo o amiga.

Si activamos la navegación en modo incógnito en estas situaciones no deberíamos preocuparnos de que nuestras contraseñas o correo electrónico con el que ingresamos a nuestras redes sociales queden guardados en estas computadoras.

7.3. ¿**Cómo hacerlo** desde mi celular?

Para activarlo sigue las instrucciones.

7.4. ¿**Cómo hacerlo** desde una computadora?

Para activarlo sigue las instrucciones.

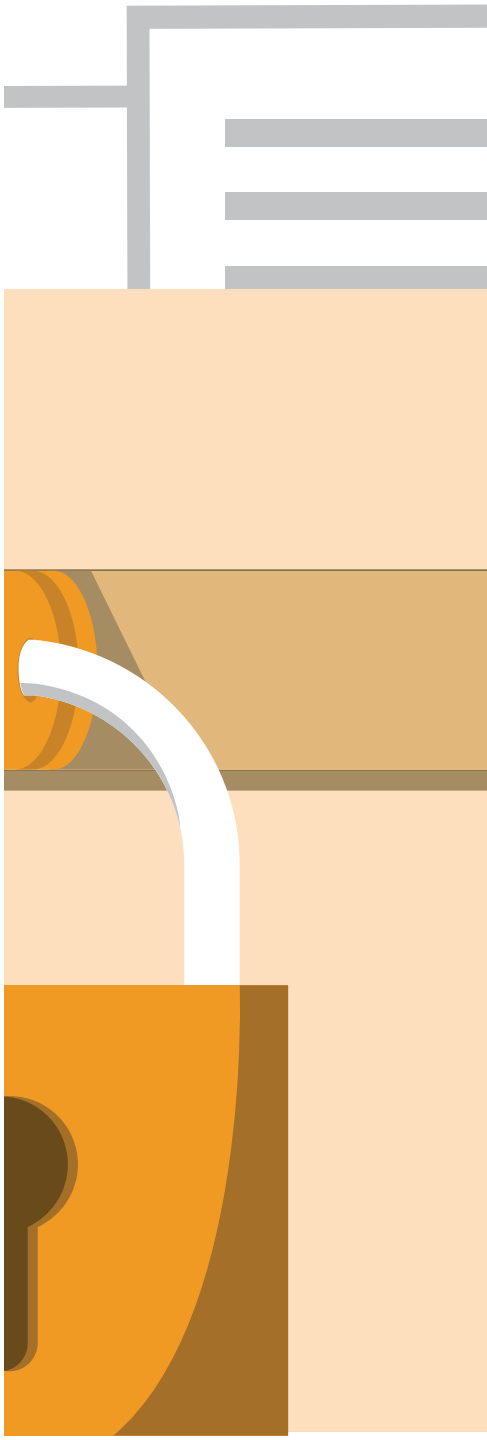
COMUNICACIONES **SEGURAS**

8

8.1. ¿Qué es información sensible y **por qué debemos cuidarla**?

La información sensible es información privada de una persona, empresa, institución o organización política, etc. La información sensible son los datos que si caen en manos equivocadas puede perjudicarnos.

Algunos ejemplos de información sensible pueden ser: datos personales (nombre, fecha de nacimiento, carnet de identidad, dirección, cuentas bancarias, saldo en cuentas bancarias, diagnóstico de salud, creencias religiosas, etc.) contraseñas de nuestras cuentas en Internet o cualquier otra información que consideremos que debemos proteger y mantener privada. En la actualidad mucha de esta información la compartimos por aplicaciones de mensajería, sin preguntarnos si las mismas son seguras para el envío de nuestra información sensible.



8.2. Aplicaciones que me ayudan a **cuidar mi información**

En la actualidad existen varias aplicaciones de mensajería instantánea, como WhatsApp (que es la más usada), Facebook Messenger, Telegram, Signal, también podemos mandar mensajes por Instagram, etc. Para saber cuál es la aplicación que nos ofrece mejores opciones de seguridad y privacidad debemos conocer sus características. Usualmente elegimos la aplicación de mensajería que vamos a usar por ser la más popular, pero es importante conocer las características que hacen que una aplicación de mensajería tenga mejores niveles de seguridad.

Una aplicación de mensajería con altos niveles de seguridad reduce la posibilidad de que nuestras conversaciones puedan ser interceptadas por terceros, es decir que solo tú y la persona receptora del mensaje puedan leer el mismo. Una característica de seguridad que tiene que ver con esto es el cifrado de extremo a extremo.

El cifrado de extremo a extremo significa que solo tú y la persona a la que le envías el mensaje pueden leer el contenido. Lo que el cifrado de extremo a extremo hace a tus mensajes es que los vuelve indescifrables, es decir, nadie que intercepte tus comunicaciones podrá entender lo que dice el mensaje, solo el destinatario al que le enviaste lo puede "descifrar".

Es importante reconocer que migrar todas nuestras conversaciones a estas otras aplicaciones de mensajería es bastante complicado, porque la mayoría de las personas con las que nos comunicamos solo usan WhatsApp, por eso es importante que aprendamos a distinguir e identificar nuestra información sensible, por si llega el momento que debamos compartir esta información lo hagamos por un canal seguro. Es decir, podemos determinar que toda la información sensible que tengamos que comunicar lo hagamos por Signal o en el chat secreto de Telegram y el resto de nuestras comunicaciones que no impliquen un peligro para nosotras, lo hagamos en la aplicación que usamos en nuestro día a día. De esta forma, avanzamos en el cuidado de nuestra información y poco a poco vamos migrando nuestras conversaciones a canales más seguros.

8.3. **Signal**, cómo usarla y aprovechar sus opciones

Signal es una de las aplicaciones que cuida mucho la privacidad de sus usuarios y en el último tiempo ha adquirido mucha popularidad. Signal tiene cifrado de extremo a extremo, el cual ha sido comprado por WhatsApp, lo que quiere decir que WhatsApp también cuenta con este cifrado, sin embargo esta aplicación no es de código abierto por lo cual no conocemos ni podemos comprobar que hace lo dice que hace.

Volviendo a Signal, esta aplicación tiene un diseño muy sencillo y es similar a otras aplicaciones. Una vez que instalas Signal en tu teléfono, la aplicación detectará quienes de tus contactos utilizan también la aplicación. Dentro de la aplicación se pueden realizar llamadas, videollamadas, enviar emojis, stickers, audios y videos.

Una opción importante para maximizar el cuidado de la privacidad de nuestras conversaciones es la autodestrucción de los mensajes. Esta opción la podemos activar cuando necesitamos enviar información sensible que no queremos que se guarde en el teléfono de nuestro destinatario, es decir, mensajes que solo queremos que se vean una vez y no más. Para instalarla y saber cómo usar sigue los siguientes pasos.

8.4. **Estafas por Internet**. ¿Cómo reconocerlas?

En Internet existen varios peligros relacionados con estafas, como robo de identidad, de dinero, de información, entre otros. Estas estafas, al igual que las noticias falsas, tienen el objetivo de llegar a nuestro lado emocional para que caigamos en ellas. Para poder identificar estas estafas debemos prestarle atención a los siguientes aspectos:

- Las personas que estafan a través de Internet en algunas ocasiones estudian la información que existe en la red sobre ti. Los estafadores pueden encontrar los datos que has publicado o se han publicado de ti en Internet, desde tu dirección de correo electrónico, tu número de teléfono, el nombre de tu mascota, dónde vives, hasta los nombres de tus familiares. Por esta razón, aunque estas personas te den mucha información relacionada con tu vida privada, no debes creerles.
- Cuando se realizan estafas por Internet, se intenta meter presión a las usuarias y usuarios; para esto utilizan el sentido de urgencia, te dan el mensaje de que si no actúas en ese instante te vas a perder de un premio, de una oferta, etc. De esta forma se aseguran que actúes de forma impulsiva y sin pensar mucho en las consecuencias.
- Los mensajes que se envían suelen estar acompañados con información relacionada a premios o intentan asustarte diciendo que ingresando al enlace encontrarás un vídeo o una foto tuya. Estos mensajes se envían por WhatsApp, por Messenger Facebook, por mensajes de texto (SMS), etc.
- Es importante no abrir enlaces desconocidos (un enlace es algo como esto: www.bolivia.com.bo), si una persona que conoces te envía un enlace sin explicarte de qué se trata, es mejor no abrirlo y preguntarle al respecto. Si no conoces a la persona, es mejor ignorar el enlace y no abrirlo.
- Cuando ingresas a uno de estos enlaces usualmente te piden datos personales, como tu nombre, número de teléfono, correo electrónico o contraseñas, bajo ninguna circunstancia debemos proporcionarles estos datos.

8.5. ¿Cómo identificar **noticias falsas**?

Las noticias falsas manipulan el relato de lo que pasa y tienen el objetivo de dañar la percepción que nos hacemos de la realidad. Una noticia falsa es un mensaje falso difundido con el objetivo de engañar y/o desinformar y en las redes sociales se difunden de manera muy rápida porque la mayoría de los usuarios y usuarias no verifican la información antes de compartirla.

Para poder reconocerlas debemos prestar atención a los siguientes puntos:

- Las noticias falsas apelan al lado emocional para viralizarse, ya que las emociones son más convincentes para las personas que los datos o estadísticas. Si una publicación nos produce una emoción fuerte debemos preguntarnos si estamos siendo manipuladas.[5]
- Duda de información que confirma tus creencias y desacredita la opinión de los demás.
- Desconfía de textos que comienzan con:
  1. "Nos han llegado reportes", "Fuentes han confirmado", "Mi primo que trabaja en... me dijo...".
  2. Usualmente, las fuentes de desinformación presentan textos incompletos, sacados de contexto, poco claros.
  3. Desconfía de las publicaciones con mala ortografía.
- Pregunta la fuente; es importante qué cuestiones de dónde viene la información que estás leyendo. ¿Es un periódico o un portal de noticias en el que confías? Si es así, la información que estás leyendo estará publicada en otros sitios de noticias.
- Pregunta a las plataformas que se dedican a la verificación de noticias: https://www.chequeabolivia.bo/ y https://boliviaverifica.bo/ Estos portales tienen el objetivo de desmentir noticias falsas, si tú estás dudando si la información que estás leyendo es cierta o no, puedes consultar con estas plataformas.

5 Noticias falsas y desinformación: ¿Qué son noticias falsas? Disponible en: https://uned.libguides.com/noticias_falsas

AMADBOL

35 años coordinadora de la mujer

CON EL APOYO DE:

ONU MUJERES

Entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres