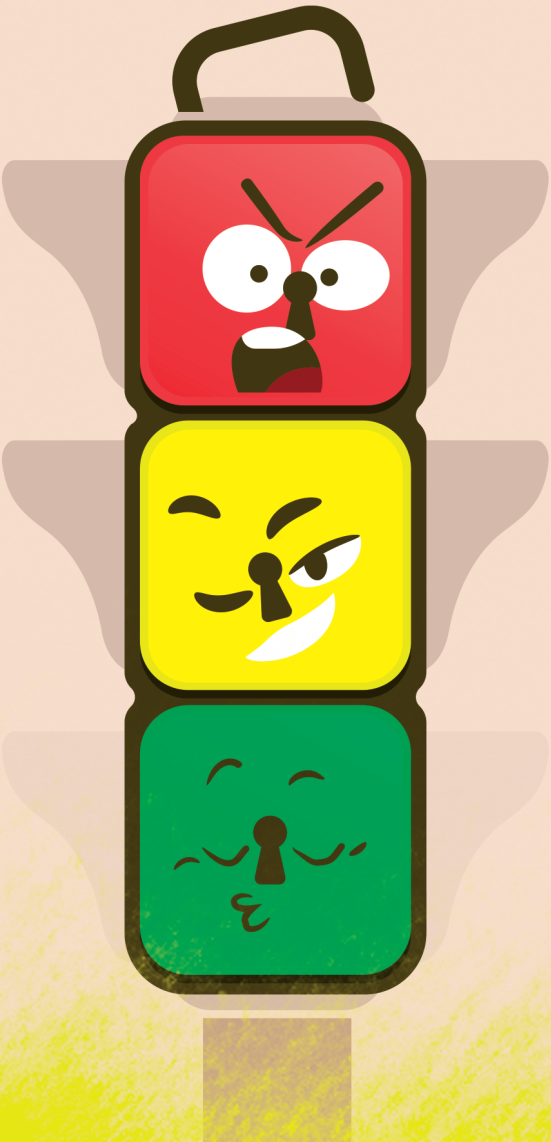


TOMANDO **CONTROL** DE MI VIDA DIGITAL

SEGURIDAD DIGITAL PARA NIÑAS, NIÑOS Y ADOLESCENTES

CONTENIDOS

INTRODUCCIÓN

Internet se ha convertido en parte fundamental en nuestra vida, sobre todo en tiempos de crisis sanitaria. En este nuevo orden de las cosas, hemos visto cómo las tecnologías de información y comunicación han transversalizado la vida cotidiana. En el caso de niñas, niños y adolescentes se ha visto un incremento en el tiempo de conexión y las actividades que se realizan en Internet.

En este sentido, se conocen las numerosas oportunidades y beneficios que brindan las tecnologías de información y comunicación a las niñas, niños y adolescentes, tanto en lo educativo como en lo social. Sin embargo, esta hiperconexión las y los expone a distintos peligros y violencias digitales. Se tiende a pensar que las niñas, niños y adolescentes, por tener mucha más familiaridad con la tecnología y, en varios casos, facilidad para usarla, cuentan con los conocimientos necesarios para defenderse e identificar situaciones de riesgo en el mundo digital, pero sabemos que está creciendo el número de niñas, niños y adolescentes que se enfrentan a violencias digitales cada día.

El objetivo de esta guía es que las niñas, niños y adolescentes puedan desarrollar estrategias de seguridad digital y aplicarlas a su vida cotidiana, identificando la importancia de incorporar hábitos de seguridad digital. Los textos están escritos de forma sencilla para que pueda ser de mejor comprensión. En la parte final se encuentran distintas actividades lúdicas para que las niñas, niños y adolescentes puedan replicar lo aprendido.

Esta guía pertenece a:

(puedes dibujarte o poner tu nombre)

TEMA 1.

ESTRATEGIAS DE DEFENSA, *HACKEANDO* LA VIOLENCIA EN LÍNEA

Existen varios tipos de violencia digital (amenazas, acoso, robo de identidad, estafas, *hackeo* de cuentas, violencia sexual en Internet, etc), y cada uno tiene sus propias características. Las personas que enfrentan violencia digital, muchas veces no solo se enfrentan a una sola violencia, sino a varios tipos de violencia digital al mismo tiempo.

La violencia digital sucede a través de medios digitales, como redes sociales, correo electrónico o aplicaciones de mensajería en los celulares; en las zonas rurales pueden utilizar la radio para difundir mensajes difamatorios, lo que también es considerado violencia digital. Las mujeres, niñas, niños, adolescentes y jóvenes, personas adultas mayores, afrodescendientes e indígenas son las poblaciones que más suelen enfrentar violencias digitales, porque históricamente han sido discriminadas.

En ese sentido, las violencias digitales no son violencias nuevas, sino una extensión de las violencias que vivimos y enfrentamos fuera de Internet. Estas violencias, que ya conocíamos, encontraron una nueva forma de expresarse, ahora mediante la tecnología. Cuando una violencia digital sucede, se tiende a pensar que la culpa la tiene la persona que está siendo agredida; surgen comentarios como “es su culpa por sacarse fotos así...” o “eso le pasa por hablar de ese tema...”. A esto se conoce como revictimización, que es cuando se le echa la culpa a la persona que en realidad es la víctima de una agresión. Debe quedar claro que la única persona culpable de la violencia cometida es el agresor o el autor de los hechos violentos.

Es importante conocer los tipos de violencia digital que existen para poder identificarlos cuando nos afecten, o quizás a alguna de nuestras amigas, para saber qué hacer. Entre los tipos de violencia digital que más enfrentan las niñas, niños y adolescentes están:[1]

Ciberacoso. Cuando te molestan o dan opiniones sobre ti sin que las hayas pedido y que te resultan molestas o intimidantes. Cuando te envían mensajes o hacen comentarios ofensivos en tus redes sociales. El objetivo del ciberacoso es dañar tu dignidad, obligarte a hacer cosas que no quieres, causar sufrimiento y ridiculizarte frente a las demás personas.

Difusión de imágenes íntimas sin consentimiento. Cuando comparten fotografías, videos o capturas de pantalla donde una persona sale en ropa interior, desnuda o semidesnuda, sin haber dado permiso para que su imagen se difunda.

Amenazas. Cuando alguien te envía un mensaje con contenido violento o también hace comentarios agresivos con la intención de dañarte, o te amenaza con causar daño a tus seres queridos.

Robo de cuentas. Cuando alguien accede a tus cuentas de redes sociales, cambia la contraseña y pierdes el acceso a ellas.

Abuso sexual facilitado por la tecnología. Un ejemplo de esto es cuando alguien te obliga a mantener alguna relación (virtual o física), a tocarla o realizar alguna práctica sexual sin que tú quieras o des tu consentimiento, y que te contactó a través de redes sociales, llamadas telefónicas o a través de cualquier dispositivo electrónico.

Violencia digital en el noviazgo. Cuando tu novio, novia o exnovio, exnovia revisa y controla tu actividad digital (lo que públicas, quiénes son tus contactos, revisa tu celular, pide tu contraseña, controla cuánto tiempo estás conectada o conectado, etc.).

1 Informe “Chidas en línea” disponible en: https://chidasenlinea.org/sin-violencia/informe-chidas-en-linea.pdf

1.1. **ESTRATEGIAS DE DEFENSA** ¡*HACKEANDO* LA VIOLENCIA EN LÍNEA!

¿Cómo responder a las violencias digitales?

Recuerda que:

- No tienes la culpa de la violencia que enfrentas.
- Las culpables son las personas que nos agreden.

Pide ayuda. No tienes por qué atravesar por esto sola, solo, cuéntale a una amiga o amigo, a una persona de confianza. ¡Pedir ayuda es un acto de valentía!

Documenta. Toma captura de pantalla de los mensajes que recibes. En las imágenes se deben ver los enlaces, números de teléfono, nombres de perfiles, etc.

Denuncia. Conoce los recursos legales de nuestro país sobre difusión de imágenes íntimas sin consentimiento, *ciberbullying* o *grooming*, que es cuando una persona adulta se contacta por Internet con una niña, niño o adolescente.

Reporta. La mayoría de las redes sociales tienen procedimientos para denunciar publicaciones que vulneran nuestros derechos. Por ejemplo, si en Facebook existe una imagen humillante o burlesca de ti, puedes denunciar la publicación para que quiten el contenido.

Protege tus cuentas:

1. Cambia la contraseña de tus cuentas.
2. Activa la verificación en dos pasos.
3. Elimina a los contactos de tus redes sociales que no conozcas.
4. Configura la privacidad de las redes sociales que utilizas.
5. No des información personal en tus redes sociales.

TEMA 2.

CONTRASEÑAS **SEGURAS**

2.1. AUTODIAGNÓSTICO

Responde las siguientes preguntas, acuérdate de tus respuestas o anótalas en algún lugar. Sé sincera o sincero contigo mismo. No existen respuestas correctas o incorrectas. El resultado te ayudará a saber qué tan seguras son tus contraseñas y así podrás usar este texto para reforzar la seguridad de tus redes sociales.

1. ¿Usas la misma contraseña para todas tus cuentas?

Sí ☐ No ☐

2. ¿Usas tus datos personales (número de teléfono, fecha de cumpleaños, nombres de tus mascotas) para tus contraseñas?

a) Sí, así es más fácil acordarme de las contraseñas ☐

b) No ☐

3. ¿Has compartido tus contraseñas con alguien más?

a) Sí, mis contraseñas las saben mis amigas/amigos y/o novio/novia ☐

b) No, nadie sabe mis contraseñas ☐

Si escogiste "a" más de dos veces, es urgente qué refuerces la seguridad de tus contraseñas. Las contraseñas son la principal medida de seguridad de nuestras redes sociales, por eso debemos prestarle mucha atención. En el siguiente texto encontrarás cómo puedes hacerlo.

Si escogiste la opción "b" más de dos veces, tienes un buen cuidado de tus contraseñas. Lee el siguiente texto para aprender cómo puedes reforzar la seguridad y minimizar el riesgo de que personas desconocidas ingresen a tus redes sociales.

2.3. CONTRASEÑAS

> *¿Sabías que la contraseña más famosa es "Ábrete sésamo" y la más usada es "12345"?*

Las contraseñas de nuestras redes sociales o de nuestro celular son como las llaves de nuestra casa, nos protegen de que otras personas ingresen a ver nuestra información. Las contraseñas son la primera barrera de seguridad, si usamos una contraseña muy fácil es como si dejáramos abierta la puerta de nuestra casa para que cualquier persona entre.

Necesitamos usar contraseñas seguras y para eso no debemos:

- Utilizar datos personales como tu fecha de nacimiento, el nombre de tu perrito o tu número de celular. Esta información es predecible y fácil de adivinar.
- Poner 123456 de contraseña. Recuerda qué es la contraseña más usada.
- Compartir nuestra contraseña con nadie.
- Utilizar la misma contraseña para todas tus cuentas. Piensa que si alguien adivina esa contraseña tendrá acceso a toda tu vida en Internet.

Muchas veces una contraseña es la única medida de seguridad que nos separa de un posible ataque en Internet, por eso las contraseñas son importantes y deben ser seguras.

2.4. ¿**CÓMO SON** LAS CONTRASEÑAS SEGURAS?

Una contraseña segura es:

- Larga, tan larga como sea posible.
- Alfanumérica, tiene letras y números.
- Tiene una mezcla de mayúsculas y minúsculas.
- Usa caracteres especiales como ,!"#*_,-...
- Una contraseña segura se ve así: Est0ybuscand0unapalabraEnelumbraldetumisteri0

Recuerda cambiar las contraseñas cada seis meses. A veces tener varias contraseñas puede ser un reto para nuestra memoria; un truco sencillo para no olvidarnos de nuestras contraseñas puede ser:

- Elegir una canción que nos guste y que sepamos la letra de memoria.
- Elegir las tres o cuatro primeras palabras del coro o de la estrofa qué más nos guste y usar estas palabras como contraseña de una red social.
- Las siguientes tres o cuatro palabras de la estrofa pueden ser la contraseña de otra red social o de nuestro correo electrónico.

De esta forma siempre nos acordaremos de nuestras contraseñas porque forman parte de nuestra canción favorita.

¡Ahora que ya sabes como son las contraseñas seguras ingresa a tus redes sociales para cambiar tus contraseñas!

TEMA 3.

PROTEGIENDO MIS DATOS PERSONALES

3.1. AUTODIAGNÓSTICO

1. ¿Recuerdas haber proporcionado alguna vez tus datos en Internet?

Sí ☐ No ☐

2. ¿Qué datos crees que hay en Internet sobre ti?

Número de teléfono, nombre completo, dirección, colegio, fotos y muchas cosas más ☐

Número de teléfono, nombre completo ☐

3. Ingresa a tu celular y abre Google, busca tu nombre con la ciudad en la que vives, por ejemplo: “Ana Mendoza Oruro”. También puedes intentar buscar tu número de teléfono, por ejemplo: “7890765 Bolivia”. ¿Encontraste información personal sobre ti? ¿Qué encontraste?

Sí ☐

No ☐

Si escogiste la opción “a” dos o más veces es importante que mejores tus hábitos para cuidar tus datos personales y si seleccionaste más de dos veces la opción “b” vas por un buen camino en el cuidado de tu información personal.

3.2. ¿POR QUÉ ES IMPORTANTE **PROTEGER NUESTROS DATOS PERSONALES?**

En el tema anterior vimos cómo una contraseña puede proteger un aspecto de nuestra vida en línea: nuestras cuentas en redes sociales. Hay otra información que circula en redes sociales e Internet que también necesita de nuestra atención: los datos personales.

Los datos personales son toda la información para identificar a una persona, por ejemplo, su nombre, dirección, edad, el colegio donde estudia, número de teléfono, nombres de sus familiares o amistades. Los datos personales también son nuestras huellas digitales, nuestro rostro y el iris de nuestros ojos, porque son únicos y permiten identificar quiénes somos. Por ejemplo, existen algunos celulares que se pueden desbloquear usando la huella digital o el reconocimiento facial, estos celulares usan una tecnología que identifica la identidad de una persona a través de su huella y rostro.

Nuestros datos personales se han vuelto muy valiosos y deben ser protegidos. Si cualquier persona puede acceder a esta información puede que estemos en peligro, porque personas malintencionadas pueden utilizar nuestros datos para hacernos daño.

Si no cuidamos nuestros datos personales, otras personas pueden utilizarlos para robar nuestra identidad, amenazarnos, extorsionarnos o hasta podemos ser víctimas de secuestro. Lamentablemente, en Bolivia aún no tenemos una ley que proteja los datos personales de los y las ciudadanas que podría ayudarnos a que estén protegidos de mejor manera.

3.3. DATOS PERSONALES **SENSIBLES**

También existen los datos personales sensibles, estos son los datos más íntimos de una persona (como estado de salud, creencias religiosas, preferencias sexuales); si los datos sensibles se usan de manera inadecuada, puede provocar discriminaciones y otros riesgos.

Por ejemplo, recordemos cuando llegó la pandemia a nuestro país. El número de personas contagiadas era muy bajo y hubo un momento en el que los nombres de las personas contagiadas se publicaron en redes sociales. Esto hizo que estas personas recibieran insultos, sean discriminadas y rechazadas por el resto de la sociedad. Por eso es importante distinguir qué datos nuestros podemos publicar sin que implique un riesgo para nosotras y nosotros.

3.4. ¿QUÉ INFORMACIÓN PUEDO **COMPARTIR EN INTERNET**? [2]

A continuación, te compartimos el semáforo de los datos personales. Podrás ver tres listas, una roja, una amarilla y otra verde.

Los datos de la lista roja son los datos personales que si los hacemos públicos nos pueden poner en peligro.

Lista roja:

- Contraseñas
- Nombre completo, el nuestro y de nuestra familia
- Dirección de tu casa o de tu escuela
- Fecha de nacimiento
- Número IP de tu computadora
- Tu ubicación (por ejemplo, si te encuentras en algún parque o restaurante o la ciudad en donde vives)
- Número de teléfono
- Nombre de colegio
- Marca o modelo de tu teléfono

Los datos de la lista amarilla son datos que no implican un riesgo mayor, pero mejor si los cuidamos, porque si son usados junto con los datos de la lista roja nos puede poner en riesgo.

Lista amarilla:

- País
- Ciudad
- Correo electrónico

Los datos de la lista verde son datos que puedes publicar en Internet y no preocuparte por nada.

Lista verde:

- Nombres o pseudónimos de nuestras cuentas en Internet.
- Fotos y videos que no te avergüencen.
- Las cosas que te gustan en general.
- Memes divertidos

Si una persona desconocida o página en Internet te pide información de la lista roja, es una señal de alerta y no debemos darle esta información.

2 The smart girl's guide to privacy: https://we.riseup.net/assets/355960/smartgirlsguidetoprivacy.pdf

3.5. ¿**QUÉ SON LOS ENLACES MALICIOSOS** Y QUÉ TIENEN QUÉ VER CON LOS DATOS PERSONALES?

Los enlaces maliciosos son esos links que podemos recibir en nuestras cuentas de WhatsApp o perfiles de Facebook, o incluso como mensaje de texto SMS o de correo electrónico. Se llama enlace malicioso porque su objetivo es engañar a la persona que recibe el enlace para robarle su información personal, es decir nuestros datos personales.

Con frecuencia, la estrategia de estos enlaces es atraer nuestra atención y generar curiosidad en nosotras y nosotros sobre el contenido que tienen. Por lo general, los mensajes hacen referencia a ofertas, premios, descuentos u otros; el objetivo es que no pensemos mucho y hagamos *click* o que ingresemos al enlace de inmediato. Una vez qué entramos al enlace, usualmente nos piden nuestros datos personales, lo que no debemos hacer.

3.6. ¿**CÓMO RECONOCER** UN ENLACE MALICIOSO?

- Pregúntate quién te envió el enlace: Si no conoces a la persona, es mejor ignorar el mensaje y no abrirlo.
- Suelen estar acompañados con mensajes relacionados a premios o intentan asustarte diciendo que ingresando al enlace encontrarás un vdeo o una foto tuya.
- Cuando ingresas usualmente te piden datos personales como tu nombre, número de teléfono, correo electrónico o contraseñas.
- Juegan con la urgencia, el mensaje puede decir que tenemos que actuar de inmediato, haciéndose pasar por un familiar lejano que se encuentra en problemas.

Si el enlace cumple con alguno de los puntos anteriores no ingreses a él.

TEMA 4.

CONFIGURACIONES DE **PRIVACIDAD Y SEGURIDAD** DE LAS REDES SOCIALES

4.1. AUTODIAGNÓSTICO

1. ¿Conoces las configuraciones de privacidad de tus redes sociales?

Sí ☐ No, nunca las vi ☐

2. ¿Cuándo fue la última vez que revisaste las configuraciones de seguridad y privacidad de Facebook?

Hace más de seis meses ☐

Nunca revisé las configuraciones de privacidad y seguridad ☐

3. ¿Sabes quiénes tienen permiso para ver las fotos publicadas en tu perfil de Facebook?

Sí, solo mis contactos ☐

No estoy segura/o, creo que todas/os pueden ver mis fotos ☐

Si escogiste la opción “a” más de dos veces conoces muy bien las configuraciones de privacidad y seguridad de tus redes sociales. Es importante que las revises cada cierto tiempo, porque estas plataformas actualizan las configuraciones sin previo aviso.

Si seleccionaste más de dos veces la opción “b” es importante qué revises las configuraciones de privacidad y seguridad de tus redes sociales de forma continua, así podrás tener un mejor control de la información que compartes con tus contactos en las redes sociales.

4.2. CONFIGURACIONES DE **PRIVACIDAD Y SEGURIDAD**

El mayor tiempo que estamos conectadas y conectados a Internet lo hacemos mirando redes sociales, podemos revisarlas desde nuestro celular, computadoras o tabletas. En ellas podemos escribir, chatear, compartir fotos, videos, memes, jugar en línea con amigas y amigos. Sin embargo, las redes sociales también pueden ser un lugar hostil para las niñas, niños y adolescentes, pues ahí enfrentan varios tipos de violencias digitales, como ciberacoso o recibir amenazas, o ser engañadas y engañados por personas desconocidas.

Una forma de protegernos de los peligros que existen en las redes sociales es revisar las **configuraciones de privacidad y seguridad**. La mayoría de las redes sociales cuentan con configuraciones de seguridad donde podemos cambiar nuestras contraseñas y **revisar desde qué celulares y lugares han ingresado a nuestra cuenta**. En las configuraciones de privacidad, podemos ajustar quiénes pueden ver la información de nuestros perfiles, es decir datos personales, fotos, videos, historias y publicaciones, entre otras cosas.

Cuando revisamos las configuraciones de privacidad de nuestras redes sociales es importante prestar atención a quiénes pueden ver nuestras publicaciones, fotos, contactos, número de celular, y quiénes son nuestras amigas y amigos en las redes sociales. Estos datos personales pueden ser usados para ejercer violencia digital contra nosotras y nosotros.

No te asustes si nunca antes has revisado las configuraciones de tus redes sociales, es una tarea muy sencilla y nunca es tarde para empezar.

4.3. CONFIGURACIONES DE **PRIVACIDAD DE FACEBOOK**

Una forma de protegernos de los peligros que existen en las redes sociales es revisar las configuraciones de privacidad y seguridad de nuestras redes. Aquí verás cómo hacerlo en Facebook.

1. Podemos revisar las configuraciones de privacidad de nuestros perfiles de Facebook desde el celular, para esto ingresamos a la aplicación y presionamos en las tres rayas horizontales superiores.
2. Nos aparecerá una larga lista de opciones; en la parte de abajo buscaremos la opción **Configuración y privacidad**.
3. Al ingresar en este apartado, buscamos la opción **Accesos directos de privacidad**. Esta parte es un acceso rápido a las opciones de configuración que más se utilizan.
4. Ingresamos a **Revisar algunas opciones de privacidad**; en esta opción podremos configurar:

- Quién puede ver lo que compartes.
- Cómo puedes proteger tu cuenta.
- Cómo pueden buscarte las personas en Facebook.

5. Ahora sigue las instrucciones de Facebook y decide qué información quieres que sea pública y qué información no.

4.4. VERIFICACIÓN EN **DOS PASOS WHATSAPP**

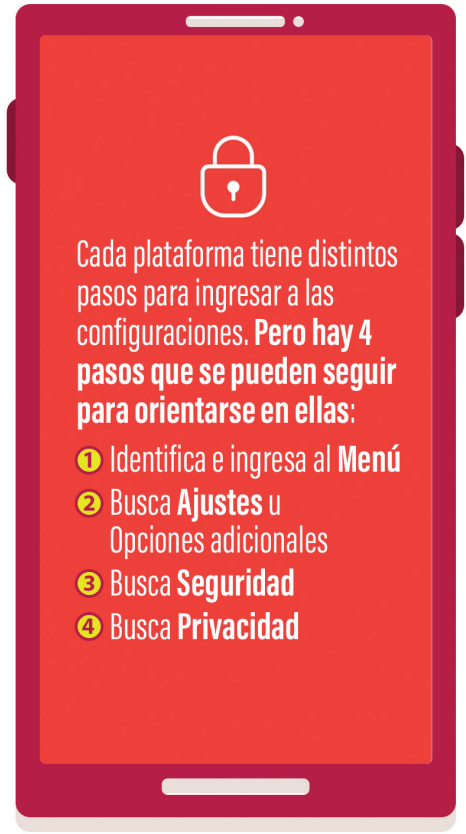
Una medida de seguridad en WhatsApp es la verificación en dos pasos. Existen varias formas en que pueden robar nuestra cuenta de WhatsApp y de esta manera ver nuestras conversaciones, la verificación en dos pasos nos protege de esto. Activar la verificación en dos pasos nos permite agregar una capa de seguridad a nuestra cuenta, con esto nos aseguramos de que nadie pueda registrar nuestro número de teléfono en otra cuenta de WhatsApp. Te mostramos cómo hacerlo:

1. Ingresa a **Whatsapp** en tu teléfono celular.
2. Toca en el botón de menú (son tres puntos que se encuentran en la parte superior) de WhatsApp y elige **Ajustes**.
3. Selecciona la primera opción de la lista, **Cuenta**.
4. Una vez ahí, busca la opción **Verificación en dos pasos**.
5. Se abrirá la configuración de verificación en dos pasos. Para comenzar el proceso toca en **Activar**.
6. Una vez ahí tendremos que crear un **código PIN (contraseña hecha con números)**, este código es importante y no debes olvidarlo porque te lo pedirán la próxima vez que quieras usar este número de teléfono en WhatsApp.
7. El siguiente paso es agregar **una dirección de correo electrónico**, que se usará en caso de que olvides el código PIN; por eso, el correo que escribas debe ser uno al que tengas acceso.

4.5. CONFIGURACIONES DE **PRIVACIDAD Y SEGURIDAD** EN OTRAS PLATAFORMAS

Recomendamos revisar las configuraciones en otras apps, hay cuatro pasos que se pueden seguir para orientarse en ellas:

1. Identifica e ingresa al **Menú**.
2. Busca **Ajustes** u Opciones adicionales.
3. Busca **Seguridad**.
4. Busca **Privacidad**.



TEMA 5.

PORNOGRAFÍA EN MIS CLASES **¿QUÉ HACER?**

5.1. AUTODIAGNÓSTICO

1. ¿Qué aplicaciones utilizas o utilizaste para pasar clases?

a) Zoom ☐
b) Google Meet ☐
c) Zoom y Google Meet ☐
d) WhatsApp ☐
e) Todas las anteriores ☐

2. ¿Alguna vez ingresaron personas desconocidas a tus clases en línea para molestar?

a) Sí ☐
b) No, nunca ☐

Si respondiste sí a la pregunta anterior, ¿recuerdas cómo reaccionaste, qué hicieron tus compañeras y compañeros? En el siguiente tema podrás leer algunos consejos que te ayudarán a entender, prevenir y responder a estos ataques en nuestras clases en línea.

5.2. CLASES EN **PANDEMIA**

Desde que empezó el confinamiento causado por el covid-19 hubo muchos cambios en la forma en la que hacíamos las cosas, uno de los principales cambios fue que pasamos de la educación presencial a pasar clases a través de Internet sin salir de nuestras casas.

Las escuelas empezaron a utilizar plataformas de videoconferencia como Zoom, Google Meet y Teams para pasar clases. Este cambio dejó ver varios problemas, por ejemplo, que no todas las personas en nuestro país tienen acceso a computadoras o celulares inteligentes para conectarse, también que a las niñas, niños y adolescentes se les hace más fácil el uso de la tecnología que a las personas mayores.

Un gran problema que surgió en esta migración de nuestras clases al mundo digital fue lo que se llama *zoombombing*. Esta palabra en inglés se traduce al español como "bombardeo en Zoom" y hace referencia al momento en que personas desconocidas ingresan a una clase y comienzan a compartir su pantalla mostrando contenido gráfico molesto e inapropiado, como contenido racista, discriminatorio o videos pornográficos. Esto obliga a las personas a cerrar las reuniones y perjudica sobre todo a la educación en línea.

Además de las imágenes que comparten, estas personas intrusas pueden ver los nombres de las y los estudiantes, el nombre de la profesora o profesor y los rostros de las personas que tienen activada la cámara. Estos son datos sensibles y, como habíamos mencionado en otro tema, pueden ser usados para hacernos daño.

Zoom es una plataforma de videoconferencias que ha sido objeto de muchas críticas por los problemas de seguridad y privacidad que se han detectado, como robo de listas con nombres de usuarios y contraseñas, que luego han sido puestas a la venta. También se identificaron varios errores en su programa que pone en riesgo la seguridad de sus usuarios y usuarias, algunas de estas situaciones terminaron en demandas legales por violaciones a la privacidad y la seguridad.

Para evitar incidentes de z*oombombing,* recomendamos:

- No compartir los enlaces de las clases virtuales en grupos de WhatsApp o Facebook públicos. Existen buscadores especiales para enlaces de Zoom que permiten encontrar salas sin contraseña; es así que personas malintencionadas ingresan a la sala a sabotear las sesiones en línea. Toma en cuenta que las y los profesores están aprendiendo a usar estas herramientas y es posible que acciones como el zoombombing violenten sus derechos y afecten su salud mental, como también la de nuestras compañeras y compañeros.
- Revisa las configuraciones de privacidad y seguridad antes de crear los enlaces donde puedes: crear una sala de espera, encuestas para los y las participantes, evitar que entren antes que el anfitrión, apagar el video y micrófono de la persona, entre muchas, otras cosas más.

5.3. ¿QUÉ HACEMOS SI EN NUESTRAS CLASES COMPARTEN PORNOGRAFÍA?

- Desconectarnos. El objetivo de estas personas es tener nuestra atención. Si comparten contenido agresivo y sexual no tenemos por qué verlo.
- Estas situaciones afectan de forma diferente a cada una de nuestras compañeras y compañeros, algunas personas pueden sentirse molestas y sensibles por lo que ha ocurrido, no los juzgues, muéstrales tu apoyo y empatía.
- Habla con tu mamá, papá o una persona adulta de confianza sobre lo ocurrido, tu sentido de seguridad y confianza se vio amenazada. Cuéntale cómo te sientes. ¿Tienes miedo de que vuelva a pasar?

5.3.1. ¿QUÉ PODEMOS HACER PARA **PREVENIRLO**?

- Presta atención a las interrupciones no deseadas, si ves algo extraño en el chat. Si se están escribiendo insultos o palabras ofensivas, alerta a tu profesor o profesora.
- Debemos alertar si vemos que alguien extraño, con un nombre que no conocemos, entró a la sala de Zoom. Nuestra profesora o profesor deberá pedir a esta persona que se identifique.
- Pídeles a tus profesoras y profesores que no publiquen los enlaces de las clases virtuales en lugares públicos como las redes sociales.
- No compartas el enlace de tu clase en ningún lugar y con nadie que no sea tu compañera o compañero de estudio.
- Explora las configuraciones de seguridad y privacidad de Zoom en su página zoom.us antes de crear un enlace.

TEMA 6.

ME HABLÓ UN EXTRAÑO, **¿QUÉ HAGO?**

6.1. AUTODIAGNÓSTICO

1. ¿Alguna vez aceptaste la solicitud de amistad de una persona que no conocías en Internet?

a) Sí, de eso se tratan las redes sociales ☐

B) No, nunca ☐

2. ¿Si una persona qué no conoces te contacta por redes sociales?

Le respondo, me gusta hacer nuevos amigas y amigos ☐

No le respondo ☐

3. ¿Intercambiaste datos personales (número de teléfono, dirección de casa, etc.) con personas desconocidas por redes sociales?

Sí ☐ No ☐

Si escogiste la opción “a” más de dos veces te recomendamos leer el siguiente texto para conocer cómo protegerte de personas malintencionadas en Internet y saber cómo identificar a quienes fingen ser algo qué no son. También es importante que protejas tus datos personales, ya que esta información te puede poner en riesgo si llega a manos de personas desconocidas.

Si seleccionaste la opción “b” más de dos veces quiere decir que cuidas tu información personal en Internet al no aceptar conversaciones con personas desconocidas, te invitamos a leer el siguiente tema para aprender más sobre cómo cuidarte en Internet.

6.2. ¿CÓMO **IDENTIFICAR UN PERFIL FALSO**?

Internet se ha vuelto un espacio público, es como una calle o una plaza donde las personas se encuentran para intercambiar opiniones, relacionarse, estudiar y hasta buscar trabajo. De la misma manera que en la calle o en cualquier otro espacio público no hablaríamos con personas extrañas, no deberíamos hablar a personas extrañas en Internet, sobre todo si son de un perfil falso.

Identificar un perfil falso puede tomar algunos minutos, la idea general es revisar en el perfil:

1. Si tiene comentarios en sus publicaciones. Si no tiene es una mala señal.
2. Si comparte contenido original (selfis, fotos con amigos o familia, videos que haya producido) no solo fotos sacadas de Internet. Si no tiene contenido original es también una mala señal.
3. Revisa cuántos amigos tiene agregados. Si tiene pocos amigos agregados y estos también son perfiles falsos, es una señal de que este perfil también podría ser un perfil falso.
4. Fíjate hace cuánto fue creada la cuenta. Por lo general, las cuentas creadas recientemente son un indicador de una cuenta falsa.

Al revisar estos detalles podrás tener una idea de si se trata o no de un perfil falso y decidir si quieres hablar con una persona que no conoces. Recuerda que revisar si es un perfil falso es un paso para evitar a personas malintencionadas. Pero también es posible que no identifiquemos si es un perfil falso y comencemos a hablar con una persona que no conocemos; en este caso te recomendamos leer el siguiente acápite para saber qué información no debemos darle a extraños.

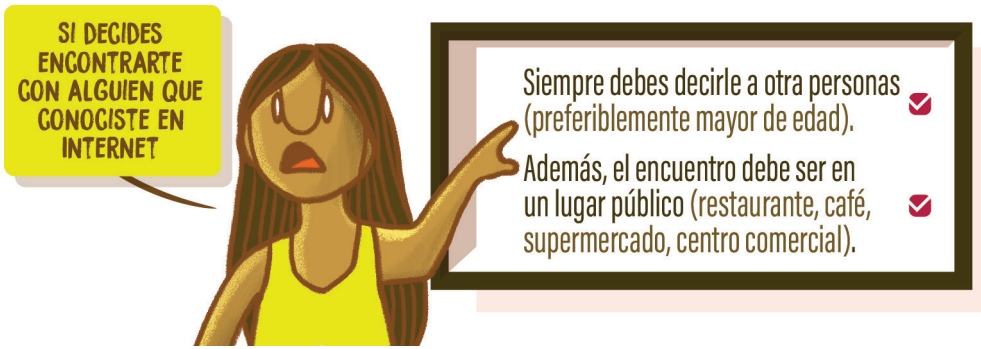
Las personas desconocidas se contactan con niñas, niños y adolescentes para primero ganar su confianza, **después te pueden ofrecer su amistad y hasta tener una relación amorosa.**

Recuerda que **en Internet es fácil fingir** ser alguien que no eres. No caigas en la trampa.

6.3. **RECOMENDACIONES** POR SI UNA PERSONA DESCONOCIDA SE PONE EN CONTACTO CONTIGO

1. Evita aceptar solicitudes de amistad de personas qué no conoces.
2. Evita enviarle fotos o selfis (fotos de nuestra cara) a extraños.
3. No menciones dónde te encuentras o los lugares que frecuentas.
4. No compartas muchos datos con personas desconocidas, como el nombre de tu colegio, tu dirección, número de teléfono, quiénes son tus amigas y amigos y sus números de teléfono, entre otra información personal.
5. Si la persona que te contactó te pide dinero o que le recargues crédito, no lo hagas. Cuéntale lo qué está pasando a una persona adulta de tu confianza.
6. Las personas desconocidas se contactan con niñas, niños y adolescentes para primero ganar su confianza, después te pueden ofrecer su amistad y hasta tener una relación amorosa. Recuerda que en Internet es fácil fingir ser alguien que no eres. No caigas en la trampa.
7. Si decides encontrarte con alguien que conociste en Internet, siempre debes avisarle a otras personas (con preferencia, adultas). Además, el encuentro debe ser en un lugar público (restaurante, café, supermercado, centro comercial).

Por último, recuerda tener cuidado con la información que publicas y más todavía con la que envías a personas desconocidas, porque pueden usarla para extorsionarte y acosarte.



TEMA 7.

SEXTING **SEGURO**

7.1. AUTODIAGNÓSTICO

Escoge la respuesta correcta	
1. El consentimiento es...	
Aceptar algo	☐
Aceptar hacer algo, de forma libre y sin presiones	☐
2. El *sexting* es...	
Práctica sexual que consiste en el envío de fotos o videos íntimos	☐
Un delito	☐

La respuesta correcta de la pregunta 1 sobre consentimiento es "b".

El consentimiento es aceptar algo de forma libre y sin presiones; para tomar una decisión es importante estar informada o informado de los pros y contras. También el consentimiento es reversible, podemos aceptar hacer algo y después cambiar de opinión, nadie nos puede obligar a hacer cosas qué no queremos. Te invitamos a leer este capítulo para conocer la relación del *sexting* con el consentimiento.

La respuesta correcta a la pregunta 2 sobre el sexting es "a"

Sexting es el intercambio de imágenes, videos eróticos a través de nuestros celulares, computadoras, tablets, etc. Muchas personas dicen que el *sexting* es una práctica sexual placentera qué fomenta la creatividad, pero es muy importante saber que existen algunos riesgos.

7.2. **¿QUÉ ES** EL *SEXTING*?

El *sexting* es una palabra en inglés que se refiere a la actividad de enviar fotos, videos o mensajes de contenido íntimo, sexual y erótico, a través de dispositivos tecnológicos (celulares, computadoras, tablets), utilizando aplicaciones de mensajería instantánea (Whatsapp, Messenger), redes sociales u otra herramienta de comunicación. La palabra *sexting* es un acrónimo en inglés formado por *sex* (sexo) y *texting* (escribir mensajes). En la actualidad, las y los jóvenes también utilizan la palabra *packs* para referirse al envío de imágenes íntimas. Esta práctica implica varios riesgos, porque si se envían fotos, audios o videos de contenido íntimo estos pueden ser compartidos de forma pública y perjudicar a las personas que aparecen en las imágenes, pues afecta su privacidad y su dignidad.

Asegúrate de qué conoces los riesgos de esta práctica y **toma una decisión informada.**

1. **Analiza** si la persona a la que le enviarás es digna de **tu confianza.**

¿Confías en esta persona?

↓

¿Esta persona **respeta la privacidad** de l@s demás?

↓

⚠ SI NO ES ASÍ, **NO LE ENVÍES NADA.**

Compartir contenido sin consentimiento y bajo presión es un acto de violencia sexual, esto es un delito en Bolivia y puede ser denunciado ante la Fuerza Especial de Lucha contra la Violencia (FELCV) como delito de pornografía. Si las personas afectadas tienen menos de 18 años, el delito sería pornografía infantil y se puede denunciar ante la Defensoría de la Niñez y Adolescencia.

El *sexting* es seguro cuando se hace con el consentimiento de ambas partes. Es decir, cuando no se hace bajo presión, ni con amenazas.

El *sexting* seguro se realiza cuando conocemos todos los riesgos asociados a esta práctica, cuando hemos tomado la decisión informada y estamos seguras y seguros de qué queremos hacerlo.

Algunos de los riesgos a los que nos exponemos cuando practicamos el *sexting* son:

- Que la persona a la que le enviaste las imágenes le muestre o reenvíe ese contenido a sus amigas o amigos.
- Que la persona a la que le enviaste las imágenes o tú extravíen el dispositivo (celular/ computadora) donde están guardadas las imágenes.
- Que personas extrañas revisen tu celular o el celular de la persona a la que le enviaste tus fotos.
- Que tus fotos sean publicadas en páginas para adultos.
- Que tus fotos sean difundidas en grupos de WhatsApp, Telegram, Facebook sin tu consentimiento.

Una aclaración importante: el *sexting* practicado bajo las condiciones adecuadas, es decir con consentimiento de ambas partes y tomando las medidas de seguridad adecuadas, es un ejercicio de libertad y expresión sexual que forma parte de nuestros derechos sexuales.

Es posible que la sociedad culpe a las personas que aparecen en las fotos y en videos íntimos que han sido difundidos sin su consentimiento, a esto se llama revictimización. Las personas que intercambiaron el contenido no tienen culpa alguna. La persona culpable siempre será la que compartió, publicó o incitó a publicar ese contenido sin el consentimiento de las involucradas. Estigmatizar el *sexting* refuerza estereotipos de género y quita la responsabilidad a los agresores.

7.3. **¿CÓMO ES** EL *SEXTING* SEGURO?

1. Asegúrate de qué conoces los riesgos de esta práctica y toma una decisión informada.
2. Analiza si la persona a la que le enviarás es digna de tu confianza. ¿Confías en esta persona? ¿Esta persona respeta la privacidad de las y los demás? Si no es así, no le envíes nada.
3. Crea acuerdos, cuéntale a la otra persona lo qué esperas de esta práctica (que no comparta las fotos con nadie más, que no se enviarán fotos sin avisar antes, imagínate que te envíe fotos íntimas mientras estás viendo tu celular con alguien más).
4. Cuando tomes fotos o videos intenta cubrir tu cara y los rasgos qué te identifican. Esto reduce los riesgos de que te puedan reconocer si ese contenido es publicado en Internet.
5. Selecciona una aplicación segura para el envío de tus fotos o videos. Signal es una buena opción porque tiene autodestrucción de mensajes (no mandes por Messenger ni Instagram, son aplicaciones inseguras).
6. Concéntrate antes de enviar el contenido, no querrás enviar las fotos y videos a otras personas.
7. Elimina las fotos que te enviaron y enviaste de tu celular.

TEMA 8.

TIKTOK, INSTAGRAM Y WHATSAPP, SI SON GRATIS, **QUIZÁS EL PRODUCTO ERES TÚ**

8.1. AUTODIAGNÓSTICO

1. ¿Te ha pasado que, sin darte cuenta, pasas muchas horas viendo redes sociales?

a) Sí ☐ b) No ☐

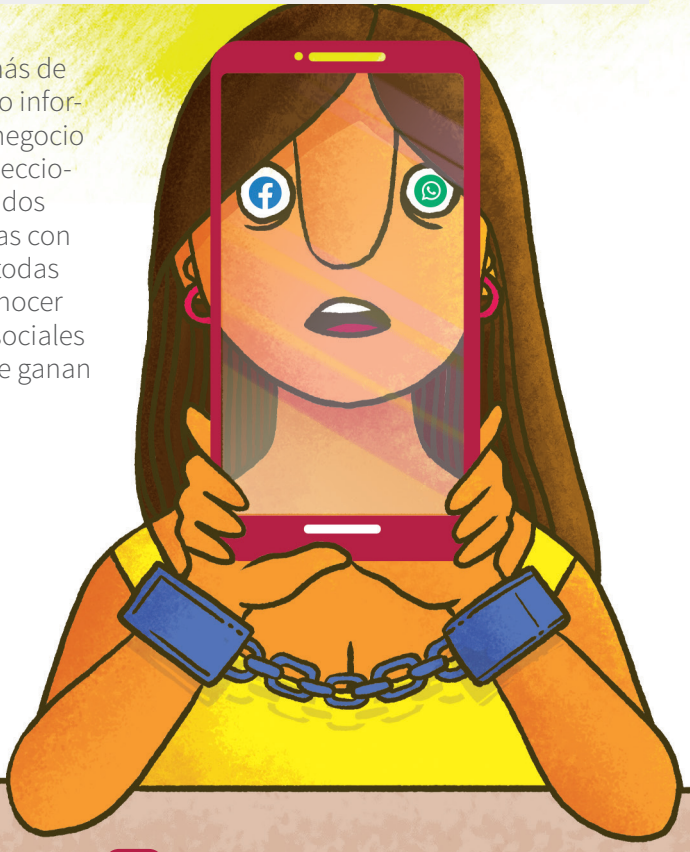
¿Sabías qué las redes sociales ganan dinero a partir de tus datos?

a) Sí ☐ b) No ☐

¿Aceptas los términos y condiciones de las aplicaciones sin leerlas?

a) No ☐ b) Sí ☐

Si escogiste la opción “a” más de dos veces estás informada o informado sobre el modelo de negocio de las redes sociales. Si seleccionaste la opción “b” más de dos veces es importante que leas con atención este capítulo. De todas maneras, es importante conocer cómo funcionan las redes sociales y de lo que verdaderamente ganan dinero



8.2. **¿CÓMO GANAN DINERO** FACEBOOK, TIKTOK, INSTAGRAM Y LAS DEMÁS REDES SOCIALES?

"Hace unos años, los usuarios de servicios de Internet empezaron a darse cuenta de que cuando un servicio en línea es gratuito, es porque tú eres el producto" (Tim Cook, director ejecutivo de Apple en 2014).[3]

"Sabemos dónde estás. Sabemos dónde has estado. Podemos saber más o menos en qué piensas" (Eric Schmidt, director ejecutivo de Google en 2010).[4]

Estos dos personajes son las cabezas de dos de las empresas tecnológicas más grandes del mundo. Ambas son frases un tanto polémicas, ya que admiten que, por un lado, nos ven como un producto y no como personas, y, por otro lado, que pueden predecir hasta nuestros pensamientos por la cantidad de información que tienen sobre nosotras y nosotros.

Nos dicen que somos el producto porque recolectan nuestros datos personales (nombre, gustos, lugares frecuentados) para luego venderlos. ¿Cómo acceden a nuestros datos? Pues estas empresas dicen que les dimos permiso para recolectar y guardar nuestros datos cuando aceptamos los "Términos y Condiciones" de uso de sus aplicaciones. El objetivo de las redes sociales es recolectar la mayor cantidad de datos posible, entre más tiempo pasamos viendo Facebook, TikTok, Instagram, más datos recolectan sobre nosotras y nosotros para después venderla a otras empresas.

Las redes sociales están diseñadas para que pasemos la mayor cantidad de tiempo viendo el contenido que nos ofrecen. Por ejemplo, las notificaciones de las redes sociales son una de las herramientas más eficaces para atraer a las y los usuarios que no están viendo la red social y mantenerlos conectadas/os. De igual manera, el celular Smartphone es una herramienta perfeccionada para mantener nuestra atención. Es por eso que cada vez que suena una alarma o se activa una notificación las personas tienden a mirarlo de inmediato, porque sus diseños están hechos para atrapar nuestra atención.

3 https://gadgets.ndtv.com/internet/news/tim-cook-to-google-users-youre-not-the-customer-youre-the-product-594242

4 https://www.stateofdigital.com/top-15-of-eric-schmidts-remarkable-quotes/

Por otro lado, las redes sociales también están diseñadas para qué las noticias falsas se propaguen más rápido que las noticias reales. La información falsa rinde más dinero a las empresas, ya que las usuarias y usuarios tienden a leer más con estas noticias. Los titulares sensacionalistas están diseñados para mantener nuestra atención y robar datos personales mientras leemos. Títulos como; "Cinco celebridades que evitan la lactosa, no podrás creer por qué" o "¿Cuál es tu espíritu animal?" o "¿Qué personaje de Los Simpson eres?" están diseñados para mantener nuestra interacción con páginas y así ganar más dinero por el tiempo que nos hicieron invertir. El dinero les motiva para crear más contenido e incluso para convencer de compartirlo con tus amigos y amigas, es por eso que es mejor ignorar este tipo de artículos.

Ya que las empresas de tecnología ganan dinero de los datos que obtienen, entonces les conviene que permanezcamos conectadas y conectados.

Las redes sociales están diseñadas para qué pasemos la mayor cantidad de tiempo posible en ellas porque ganan dinero de nuestra atención.

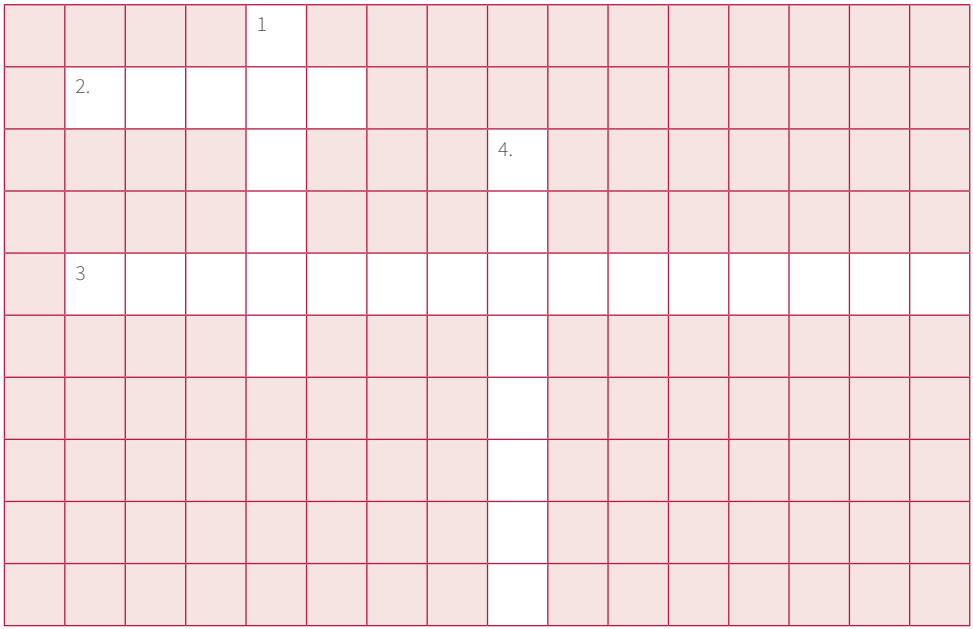
8.3. ¿CÓMO PODEMOS COMBATIR EL **MODELO DE NEGOCIO** DE LAS REDES SOCIALES?

- **Desactiva** las notificaciones de las redes sociales que utilizas, así entrarás a ellas solo cuando tengas tiempo libre y te distraerá menos durante el día.
- **Valora tu tiempo**. Entre más tiempo pases en las redes, más información sobre ti les das. Intenta establecer horarios de ingreso.
- **No te enganches a noticias sensacionalistas**. Recuerda que las noticias falsas se propagan rápido. Verifica en las páginas de medios de comunicación y otras fuentes de noticias para confirmar si se trata de una noticia real.
- **Explora en Internet**. Las redes sociales solo son una pequeña muestra de todo lo que se puede hacer en la red.
- **Desconéctate** una hora antes de dormir.
- **Libérate de las aplicaciones**. Los juegos, las redes sociales y otras ocupan valioso espacio de almacenamiento de tu dispositivo, consumen batería y recolectan datos personales aun cuando no las estás usando, por ello te recomendamos eliminar las aplicaciones que ya no usas.

9. ACTIVIDADES PARA **EVALUAR EL CONOCIMIENTO**

9.1. CRUCIGRAMA

1. Cuando una violencia sucede, es culpa del _____
2. Una contraseña segura debe ser _____
3. Son lo más valioso que tenemos en Internet.
4. En Internet también tenemos_____



9.2. SOPA DE **LETRAS** 1

Encuentra las ocho palabras clave para responder a las violencias digitales.

o	h	f	e	r	a	t	h	j	a	l	i	r	t	f	l	o	q	r	s
e	b	d	h	a	c	k	s	d	a	w	p	i	d	e	r	t	y	i	i
q	g	t	o	d	e	v	i	d	a	o	r	a	y	u	d	a	o	g	v
a	d	c	o	s	e	t	d	f	h	l	i	l	a	r	t	f	q	e	e
d	o	c	u	m	e	n	t	a	d	e	v	o	p	ñ	g	q	w	g	r
e	q	e	r	t	y	u	u	y	u	t	a	a	f	r	y	r	j	l	i
h	a	e	r	e	s	e	a	n	f	g	c	r	e	t	i	d	f	a	f
j	k	e	a	g	e	e	r	t	c	i	o	p	u	i	o	p	q	g	i
c	o	n	f	i	g	u	r	a	c	i	o	n	a	d	g	y	j	f	c
ñ	k	p	s	a	u	y	u	i	a	r	a	r	y	u	o	q	e	r	a
m	a	ñ	b	s	r	c	a	p	t	u	r	a	e	r	t	i	q	y	c
i	a	t	a	q	i	e	l	a	r	t	y	u	t	y	u	u	i	q	i
q	d	q	w	r	d	c	o	n	s	e	n	t	i	m	i	e	n	t	o
v	w	r	t	u	a	y	i	t	l	v	c	w	e	r	t	y	u	i	n
x	g	h	a	w	d	d	b	a	l	o	t	q	w	e	t	u	i	p	v
a	h	j	e	v	j	u	i	l	w	e	r	t	u	i	m	a	t	u	i
t	e	v	g	h	u	a	e	l	a	l	g	y	f	r	a	a	r	n	t
o	y	u	p	k	a	r	p	a	l	e	q	y	j	k	i	w	e	i	h

Si encontraste las nueve palabras, ¡felicidades! ya estás en camino a reconocer la seguridad en tu cotidianidad.

1. Pide ayuda
2. Documenta
3. Configuración
4. Captura
5. Consentimiento
6. Verificación
7. Privacidad
8. Seguridad

9.3. **CONECTA LA CONTRASEÑA** CON SU CARACTERÍSTICA

Contraseña	**Característica**
SeMe4c4b4e14rgumentoyL4Metodo1ogí4	Contraseña débil
admin	
cachuchin2015	Contraseña segura
eseldiadelplatanoChiCheñol	

Respuesta:

SeMe4c4b4e14rgumentoyL4Metodo1ogí4 ▸ Contraseña segura
admin ▸ Contraseña débil
cachuchin2015 ▸ Contraseña débil
eseldiadelplatan0ChiChen0l ▸ Contraseña segura

Si respondiste de forma correcta, de seguro tus contraseñas son a prueba de cualquier *hacker*.

9.4 SOPA DE **LETRAS** – CONFIGURACIÓN DE **PRIVACIDAD Y SEGURIDAD** DE REDES SOCIALES

L	O	R	T	W	C	B	I	E	N	T	H	S	D	I	G	S	T	R
V	U	A	C	C	E	S	O	D	R	O	A	E	R	V	T	E	M	N
T	D	E	V	I	O	R	E	D	V	R	E	A	U	R	T	G	B	N
W	H	A	N	S	T	N	A	W	S	B	U	E	R	T	G	U	V	Q
H	I	R	T	A	D	V	F	T	B	C	R	W	A	B	A	R	G	W
A	L	E	C	O	T	R	V	I	A	R	E	N	D	K	R	I	A	G
T	R	E	A	G	S	T	B	Q	G	U	R	O	A	C	V	D	L	E
S	E	G	Y	C	T	Z	A	F	V	U	A	R	V	A	E	A	L	S
A	W	R	D	A	D	I	C	A	V	I	R	P	L	U	X	D	S	E
P	R	I	V	A	T	R	K	Q	S	X	N	A	K	Q	Z	O	W	H
P	X	S	F	C	Q	V	B	I	R	U	P	S	C	A	S	V	R	E
S	E	C	O	N	T	R	A	S	E	Ñ	A	S	M	I	N	R	Y	S
V	E	R	C	S	E	G	Q	W	V	K	G	A	M	R	O	B	S	R
L	I	R	A	K	O	O	B	E	C	A	F	R	C	E	A	N	B	R
J	H	S	W	Q	E	R	A	S	C	P	E	L	O	V	C	Z	A	R
S	A	M	R	O	F	A	T	A	L	P	H	C	O	N	V	A	E	T
F	O	R	C	Q	C	U	E	N	T	A	C	O	S	D	E	C	B	W
S	O	M	Q	X	K	A	E	R	A	W	E	C	F	E	S	A	D	C
E	I	N	F	O	R	M	A	C	I	O	N	A	P	R	E	Z	S	A

Respuestas:

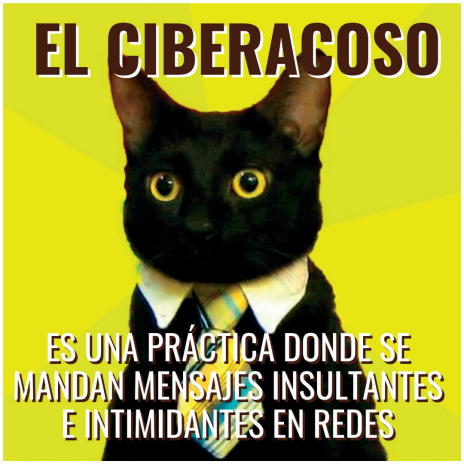
- Configuración
- Acceso
- Información
- Privacidad
- Seguridad
- Cuenta
- Permisos
- Contraseñas
- Facebook
- Datos
- Whatsapp
- Plataformas

9.5. **UNIENDO** CONCEPTOS

Une con una línea los conceptos que corresponden a un riesgo del *sexting* o a una característica del *sexting* seguro.

Riesgo del sexting	Que tus fotos sean difundidas en grupos de WhatsApp, Telegram, Facebook sin tu consentimiento.
Sexting seguro	Que tus fotos sean publicadas en páginas para adultos.
Riesgo del sexting	Cuando tomes fotos o videos intenta cubrir tu cara y los rasgos que te identifican.
Sexting seguro	Que personas extrañas revisen tu celular o el celular de la persona a la que le enviaste tus fotos.
Riesgo del sexting	Selecciona una aplicación segura para el envío de tus fotos o videos.
Sexting seguro	Crea acuerdos, cuéntale a la otra persona lo qué esperas de esta práctica.
Riesgo del sexting	Que la persona a la que le enviaste las imágenes le muestre o reenvíe este contenido a sus amigas o amigos.
Sexting seguro	Analiza si la persona a la que le enviarás es digna de tu confianza. ¿Confías en esta persona? ¿Esta persona respeta la privacidad de las y los demás?

10. STICKERS


EL CIBERACOSO
ES UNA PRÁCTICA DONDE SE MANDAN MENSAJES INSULTANTES E INTIMIDANTES EN REDES


¿ACEPTA LOS TÉRMINOS Y CONDICIONES DE USO?
SI


YO VIENDO COMO TODOS SE QUEJAN DE LOS TÉRMINOS Y CONDICIONES DE #WHATSAPP Y YO LE PUSE ACEPTAR SIN LEER NADA


SI UNA CUENTA DE FACEBOOK USAR QUIERES
TUS DATOS PERSONALES PUBLICAR NO DEBES


MI CARA DESPUES QUE ME ROBEN LA CUENTA
POR NO PONER UNA CONTRASEÑA SEGURA


VAMO´ A
REVISAR LAS CONFIGURACIONES DE PRIVACIDAD DE NUESTRAS REDES SOCIALES

terre des hommes suisse

Con el apoyo de

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Agencia Suiza para el Desarrollo y la Cooperación COSUDE

www.tdhsbolivia.org
@tdhsbolivia
@TerredesB
terredeshommessuissebolivia
Terre des Hommes Suisse Bolivia