Protocolo de acompañamiento frente las violencias digitales más comunes en Bolivia según 1000 mujeres encuestadas

Elaborado por SOS Digital:
Cecilia Huasebe
Lu An Méndez
Cielito Saravia
Diandra Céspedes
Djamila J. Chasqui

Versión web

Indice

0. Intro

La Internet se está convirtiendo en un lugar hostil para las mujeres. Cada día nos acosan, hackean, amenazan y vigilan, entre otras más. Estas acciones en Internet, afectan la manera en que experimentamos la realidad, e incluso, pueden tener consecuencias sobre nuestra integridad física[1].

En Bolivia, las violencias digitales más comunes según nuestro sondeo a 1000 mujeres son: el ciberacoso, intento de ingreso no autorizado a cuentas o hackeo, publicación de información sin consentimiento y amenazas de agresiones físicas, sexuales o de muerte a través de medios digitales. Este protocolo es la segunda parte de la Guía de acciones de acompañamiento para ciberbrigadistas que es un manual con información del acompañamiento preventivo y reactivo a mujeres en situación de violencia digital.

Este protocolo de acción, para enfrentar las violencias de género digitales más comunes en Bolivia, **es un intento desde la sociedad civil que busca evitar que las experiencias de las mujeres en la Internet sean violentas**, que se cuente con la información para ayudar a identificar a las personas agresoras y encararlas con técnicas y herramientas proporcionales a los ataques machistas que ahora enfrentamos en la Internet. Se divide en tres partes: la orientación en el ámbito legal, orientación tecnológica y contención psicológica.

El protocolo mostrará **casos ficticios de las principales violencias digitales de género** identificadas en el sondeo que servirán como ejemplos **para reconocer violencias digitales**. Posterior a la presentación del caso se presentará la orientación legal, tecnológica y psicológica correspondiente a la violencia digital.

Los ejemplos propuestos están basados en diversos casos de violencia digital que acompañamos el último año. Nuestro objetivo es que la persona acompañada no se sienta sola o piense que es la única que ha tenido experiencias así; al contrario, buscamos que **la experiencia de otras mujeres atacadas en línea, sirva para poder elaborar estrategias reactivas y de prevención**, algunas de las cuales, proponemos en este protocolo.

[1] Olías, Laura. CCOO denunciará a Iveco por el suicidio de una trabajadora tras la difusión de un vídeo sexual. 2019. https://www.eldiario.es/economia/CCOO-denunciara-Iveco-suicidio-trabajadora_0_904309626.html. Consultado: 4 de julio de 2020.

Se comienza con la **contención psicológica,** que se basa en la metodología de los PAP (Primeros auxilios psicológicos) usados para proporcionar apoyo emocional a las personas que han pasado por un evento traumático como una situación violenta, un accidente de coche o que han recibido información dolorosa. Esta metodología tiene un enfoque de género, ya que no se revictimiza o culpa a la persona, se acompaña el proceso dejando que la persona decida por sí misma cómo responder al ataque, y se concentra en el autocuidado emocional.

Después, se hará referencia al acompañamiento desde la **perspectiva legal** donde se sugieren preguntas para reconocer la figura legal; el paso-a-paso del proceso penal para una denuncia, que incluye la estructura del órgano judicial para entender de manera genérica el proceso en caso de que quieran iniciar medidas legales; y finalmente información legal adicional de interés sobre delitos públicos, recursos legales, medidas de protección y pruebas.

Finalmente, se verán las **estrategias reactivas** en Facebook, Twitter, Instagram, WhatsApp y Telegram como parte de la **orientación tecnológica**. Se presenta un paso-a-paso del procedimiento de denuncia con las empresas y las categorías que ofrecen para mitigar los ataques.

Es posible que la lectura de estos casos puedan rememorar experiencias sensibles para algunas personas, por lo que recomendamos que si este es el caso, se lea esta guía acompañada de amigas, amigos o te comuniques con nosotras al 62342340.

Nuestra experiencia y la de otras organizaciones denunciando agresiones en Internet, ya sea a la policía o con las mismas plataformas, no brindan razones para legitimar o confiar en estas órdenes. Sin embargo, consideramos importante que desde la sociedad civil se conozcan las acciones y estrategias que se pueden tomar, como también las restricciones a las que nos enfrentamos en el momento de experimentar una violencia digital.

0. 1 Descripción de cada área

Contención psicológica

En este apartado encontrarás información que puede ayudarte a explorar y entender mejor las emociones que pueden estar a flor de piel en estas circunstancias, para que puedas encontrar tu fortaleza interior y logres atravesar por esta situación. Encontrarás algunos consejos que podrán ser de ayuda para ti o la persona a la que estás acompañando. También veremos **técnicas de autocuidado emocional**, para que la

persona se sienta tranquila y relajada antes de entrar en la orientación legal y tecnológica, ya que en etapas posteriores **será necesario tomar una decisión consciente sobre la respuesta a los ataques.**

Asesoramiento legal

Es la ruta de denuncia en instancias estatales en caso de estar en situación de violencia digital. Creemos que cada caso amerita un análisis individual y especializado, por eso presentamos algunas preguntas iniciales que ayudarán a identificar la violencia digital y el delito correspondiente de la mejor manera posible. Las preguntas siempre deben apuntar a responder: **¿qué pasó?, ¿cuándo?, ¿dónde? y ¿quién lo hizo?**

Por otro lado, se presenta una mirada generalizada del proceso penal para entender de manera genérica el proceso en caso de que quieran iniciar medidas legales.

Entendemos que tomar la vía jurídica implica lo burocrático, que tiene amarres, arreglos y alianzas que no le favorecen a las mujeres[2]. Recurrir a la policía, es una ruta que puede funcionar, pero significa tiempo, energía, dinero, entregarles tu celular, entre otros requisitos que hemos observado. Esto puede llegar a ser un proceso frustrante para la persona que quiere iniciar una denuncia con instancias estatales; sin embargo, **la decisión de continuar esta ruta corresponde a la persona que está experimentando dicha situación.**

Orientación tecnológica

Se refiere a los pasos a seguir para realizar denuncias en aplicaciones o plataformas digitales, reportar contenidos, perfiles, grupos o bloquear en redes sociales como Facebook, Twitter, Instagram y apps de mensajería como WhatsApp y Telegram[3]. Consideramos necesario aclarar que la respuesta de estas plataformas, puede tardar o ser insatisfactoria, no obstante, pensamos que **es importante saber qué tipo de acciones pueden ser ejecutadas en estos espacios virtuales**; lo que además sirve para darnos cuenta del nivel de vulnerabilidades que podríamos experimentar en este espacio.

Por otro lado, elaboramos consejos preventivos para cada violencia digital expuesta en el protocolo, y pueden ser consultados aquí.

Al igual que la asesoría legal, la orientación tecnológica debe contemplar la particularidad de cada caso para encaminarse hacia una estrategia de seguridad digital y a **la**

[2] Soria, Estrella y Ortiz Pérez, Luisa. 2018. Hacks de vida. *(pf)*: https://archive.org/details/@hacks_de_vida
[3] Actualizado el 8 de agosto de 2020.

implementación de herramientas que se acoplen a las necesidades de cada persona. Inicialmente, proponemos interactuar con las empresas de redes sociales y apps de mensajería, realizando una denuncia, o ejecutando una restricción y un bloqueo en las configuraciones. Para información extensa sobre el uso de herramientas de seguridad digital, como creación de contraseñas seguras, tipos de malware, navegación segura, VPN, TAILS, software libre y cifrado, pueden consultar nuestro manual completo en: Guía de acciones de acompañamiento para ciberbrigadistas

1. Ciberacoso

En Bolivia, de 1.000 mujeres encuestadas, casi 900 recibieron mensajes molestos de forma repetitiva en medios digitales. 337 de las 1.000, recibieron insultos en redes por su identidad sexual.

El ciberacoso es un conjunto de conductas de carácter reiterado, entre las que se cuentan las amenazas, falsas acusaciones, humillación y chantaje, entre otros contenidos no solicitados, como material sexualizado, que resultan molestas e intimidantes[4]. Estas conductas se ejercen sobre una persona u organización mediante sus redes sociales, cuentas en plataformas web u otras representaciones digitales en Internet; y los dispositivos electrónicos, que incluyen daños al ordenador y vigilancia de la persona violentada o daños a sus dispositivos electrónicos.[5].

El ciberbullying, hace referencia a las mismas conductas, pero con enfoque a la niñez y la adolescencia vinculada al ámbito escolar. En Bolivia, el ciberbullying está mencionado en el Código niño, niña y adolescente, pero no está regulado en el Código penal, por lo que no constituye un delito.

De manera preventiva, te invitamos a leer nuestros consejos antiacoso. Si estás ya en una situación de violencia por ciberacoso, puedes seguir la ruta de orientación tecnológica. **Para asesoramiento personal, puedes comunicarte al +591 62342340.**

---

[4] Luchadoras. 2017. 13 formas de agresión relacionada con las tecnologías contra las mujeres. https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/. Consultado el 12 de julio de 2020.

[5] Marfarlene, Leroy y Bocij, Paul. 2003. An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. https://www.researchgate.net/publication/220167750_An_exploration_of_predatory_behaviour_in_cyberspace_Towards_a_typology_of_cyberstalkers. Consultado el 17 de junio de 2020.

Ruta crítica para el ciberacoso

Ejemplo: Una mujer denuncia que desde varios perfiles falsos, una persona manda mensajes molestos con insultos y amenazas con el fin de hacerle daño. Sabe que es una sola persona porque usa el mismo lenguaje, los mismos tipos de insultos y tiene la misma manera de accionar, crea perfiles falsos, manda mensajes y oculta el perfil para evitar ser bloqueada, luego abre otra cuenta para mandar mensajes nuevamente.

¿Qué se puede hacer?

1. Puedes acompañar a tu amiga que está siendo acosada, aquí algunas frases para apoyarla y el contexto para entenderla.
2. Aquí puedes ver una ruta en caso de querer hacer una denuncia formal en el sistema de justicia boliviano.
3. Puedes recopilar las pruebas, denunciar y bloquear el perfil que te acosa para parar el acoso en redes sociales o apps de mensajería.

a. **Contención psicológica**

Si estás atravesando una situación de violencia

Si quieres acompañar a una amiga

Contáctate con nosotras

¿Te gustaría hablar con alguien? Puedes contactarte con nosotras por WhatsApp, Telegram o Signal al 62342340.

b. **Orientación legal:**

Reconociendo la figura legal

Se debe tomar en cuenta que el ciberacoso, es una figura amplia y que puede llegar a relacionarse con otras figuras legales, ya que puede haber una vinculación estrecha entre acoso y amenazas.

Muchos de los delitos mencionados, no están establecidos de manera específica en un ámbito digital. Este es el caso del ciberacoso, que como figura específica no se encuentra

tipificado en el Código Penal boliviano; sin embargo, la figura que llegaría a aplicarse en éstos casos sería el delito de acoso sexual, regulado por el artículo 312 del Código Penal. De igual manera, como se menciona en la Guía de acciones de acompañamiento para ciberbrigadistas, se puede vincular el ciberacoso con las figuras de: acoso político contra mujeres (Art. 148 del Código Penal) y violencia en el sistema educativo (Art. 151 del Código niña, niño y adolescente). Dependiendo de la figura, se podrá sancionar con 2 a 8 años de privación de libertad a la persona agresora.

Preguntas para conocer los hechos

Para mayor detalle sobre las preguntas para identificar las diferentes figuras legales, se puede consultar aquí: Preguntas generales para conocer los hechos.

Sobre el ciberacoso específicamente, proponemos las siguientes preguntas para identificar esta figura dentro de los parámetros del Código Penal:

- ¿De qué manera se está realizando el acoso? ¿Qué acciones o dichos están configurando el acoso?
- ¿Dónde se ha realizado el acoso?
- ¿Las acciones tienen un contenido sexual o exigencia de acciones de tipo sexual por parte tuya? ¿Cuál es el contenido de tipo sexual?
    - Esta pregunta se realiza porque la figura de acoso sexual del Código Penal establece necesariamente ese carácter sexual.
- ¿Quién está realizando el acoso?
    - **La figura de acoso sexual también requiere que quien lo cometa tenga un posición jerárquica o de poder respecto a la persona que denuncia el hecho**, pero cabe mencionar que dicho establecimiento puede tener una interpretación amplia; así un jefe o una ex pareja puede realizar el acoso.
- ¿Es usted una persona del ámbito político o funcionaria pública?
    - La figura de acoso político requiere que la mujer pertenezca a un ámbito político o público.
- ¿El acoso ha tenido algún tipo de repercusiones en su vida privada, laboral o pública?
- ¿Desde cuándo está ocurriendo?

Si la persona decide hacer una denuncia, se puede consultar el paso-a-paso del proceso penal aquí para brindar información sobre las acciones a seguir.

c. **Orientación Tech**

¿En qué red social o app de mensajería estás siendo acosada?

Messenger y Facebook

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y fecha, el perfil que lo envía y el enlace del perfil que lo envía.
- Investiga: Ingresa al perfil falso, mira las fotos, revisa su lista de amigos y mira si tienen amigos y amigas en común, revisa sus publicaciones, la fecha de creación del perfil y asegúrate de que sea un perfil falso.
- Puedes bloquear o silenciar el perfil. Recomendamos primero denunciar el perfil en Facebook antes de bloquear o silenciar el perfil:
    - Bloquea el perfil en Messenger y lo bloquearás también en Facebook automáticamente: Ingresa a la ventana de la conversación en Messenger -> busca el ícono de un engranaje -> Bloquear -> Listo
    - Silencia el perfil en Messenger y no recibirás notificaciones de los mensajes recibidos de ese perfil: Ingresa a la ventana de la conversación en Messenger -> busca el ícono de un engranaje -> Silenciar -> Listo

Facebook

- Si el acoso proviene de un perfil falso, la razón de denuncia pueden ser las siguientes:
    - Ingresa al perfil de la persona que te acosa. Guarda el enlace de su perfil.
        - Selecciona el menú desplegable (los tres puntos en la esquina superior derecha) -> Busca ayuda/denuncia perfil -> Acoso ->
            - A mi -> Enviar.
            - A un amigo -> ingresa el nombre del contacto -> Enviar -> Reportar perfil -> Creo que este perfil infringe las normas comunitarias de Facebook -> Reportar.

Para denunciar el contenido de acoso:
Ingresa al contenido -> Selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Acoso->

- A mi -> Enviar.
- A un amigo -> ingresa el nombre del contacto -> Enviar -> Reportar perfil -> Creo que este perfil infringe las normas comunitarias de Facebook -> Reportar.

Se puede hacer seguimiento a las denuncias que hiciste en el siguiente enlace: https://www.facebook.com/support. **En esta página, encontrarás información sobre el estado de tu denuncia y Facebook te mostrará si la denuncia fue aceptada o no**. En caso de que no lo sea, también encontrarás información de las razones por las cuales Facebook no aceptó la misma.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al 62342340 o visitar nuestra guía antiacoso digital: https://internetbolivia.org/8M/

WhatsApp

En Bolivia, los números de celular son registrados con nombre, fecha de nacimiento, y carnet de identidad en la empresa de telecomunicaciones. En este caso, hay una manera de identificar al agresor, lo que facilita el proceso en el momento de hacer una denuncia a la FELCV. Para más información puede consultar el apartado denuncia de la orientación legal, aquí.

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y fecha, la foto de la cuenta, el número de celular, su estado y su perfil.
- Investiga: Ingresa al perfil, revisa si tienen grupos en común. Busca el número para ver si tiene un perfil asociado al número en Facebook y Twitter.
- Bloquea la cuenta. Esto es opcional, corresponde a una decisión personal, para más instrucciones consulta aquí: https://internetbolivia.org/8M/
- Para denunciar a un grupo (para Android y para iOS)

Android 

- En el grupo de WhatsApp, ve al menú desplegable -> Reporta el grupo y selecciona si quieres salirte del grupo.
    - Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú desplegable (3 puntos en la esquina derecha superior) de [8]WhatsApp -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

iOS 

- En el grupo de WhatsApp, ve al menú desplegable -> Reporta el grupo y selecciona si quieres salirte del grupo
    - Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú Configuración (esquina inferior derecha) -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

Instagram

- Recopila las pruebas: toma capturas de pantalla del mensaje o comentario, la hora y la fecha, la foto de la cuenta, el nombre, su descripción, publicaciones e historias.
- Investiga: Ingresa al perfil, mira sus fotos, revisa si tienen amigos o amigas en común. Mira si menciona otras redes sociales en su perfil.
- Bloquea la cuenta  : Ingresa al perfil, ve al menú hamburguesa (3 rayas en la parte superior derecha) ->
    - Denunciar -> Es inapropiado -> Bloquear.
    - Restringir -> Puedes limitar las interacciones con la cuenta sin necesidad de bloquearla o dejar de seguirla. Es una manera de silenciar a la cuenta. Los mensajes de esta cuenta serán dirigidos a “solicitud de mensajes” y no podrá ver si leíste los mensajes o no.
- Informar de un problema: En el menú hamburguesa (3 rayas a mano derecha superior) de Instagram -> Ayuda -> Informar de un problema -> Describe el problema y añade capturas de pantalla.
- Bloquear comentarios de un perfil: En el menú hamburguesa (3 rayas a mano derecha superior) de Instagram -> Privacidad -> Comentarios -> Bloquear comentarios de: selecciona la cuenta.

Twitter

- Recopila las pruebas: toma capturas de pantalla del tweet o mensaje, la hora y la fecha, la foto del perfil, el nombre, la descripción, guarda el enlace de la publicación y el perfil acosador.
- Investiga: Ingresa al perfil, mira sus fotos, la descripción, tweets, seguidores y a quienes sigue.

Para Android y iOS 

- Ingresa al perfil de Twitter -> Menú desplegable (3 puntos a mano derecha superior) -> Denunciar -> Escoge:
    - Sus tweets son abusivos o incitan al odio ->

        - Es irrespetuoso u ofensivo
        - Publica información privada
        - Participa en acoso selectivo
        - Incita al odio hacia una categoría protegida (raza, religión, género, orientación sexual o discapacidad)
        - Amenaza con violencia o daño físico
        - Expresan intenciones de suicidio o autolesiones
    - Información o imágenes de su perfil incluye contenido de odio ->
        - No apto para menores
        - Gráfico
        - Incitación al odio

- Ingresa al perfil de Twitter-> Menú desplegable (3 puntos a mano derecha superior) -> Bloquear (esto es opcional, corresponde a una decisión personal)

Telegram

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y la fecha, la foto del perfil, el número de celular, y en caso de contar con uno, el alias, es decir, el nombre de usuario que comienza con @.
- Investiga: Ingresa al perfil, revisa el nombre y número de celular, mira sus fotos de perfil, la última vez que ingresó a la app, revisa si tienen grupos en común. En Facebook y Twitter, busca el número para ver si tiene un perfil asociado al número.

Denuncia el mensaje:

- Pulsa sobre el menú desplegable -> Reportar -> Violencia.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al +591 62342340, visita nuestra guía antiacoso digital: https://internetbolivia.org/8M/ o te invitamos a leer nuestros consejos antiacoso o a consultar el siguiente manual de la Fundación Karisma, (desde la página 16), para reportar contenidos abusivos, bloquear, silenciar y otros consejos de Seguridad, Protección y Privacidad en Twitter[6].

[6] Versión 2016.

2. Intento de Ingreso no Autorizado a Cuentas de Redes Sociales por Parte de Terceros

Más conocido como hackeo, **son ataques o restricciones a las cuentas o dispositivos de una persona, de forma no autorizada**[7]. El intento de ingreso no autorizado a cuentas de redes sociales tiene varios fines, intentos de vigilancia o censura con énfasis a mujeres que expresan su posición política en redes sociales u otras plataformas de Internet, como artistas, activistas o periodistas. **También hemos presenciado casos de mujeres que fueron atacadas por sus ex parejas mediante hackeo con fines de vigilancia y hostigamiento.**

En Bolivia, de 1000 mujeres encuestadas, 813 dijeron que hubo un intento de hackeo a sus cuentas personales. Solo 350 de las 1000, fueron notificadas del intento de cambiar su contraseña en sus perfiles de redes sociales, ya sea porque tenían la verificación de dos pasos activada o porque aún tenían acceso a los números y correos electrónicos asociados a la plataforma.

De manera preventiva, te invitamos a leer nuestros consejos antihackeo. Si estás ya en una situación de violencia por hackeo, puedes seguir la ruta de orientación tecnológica. Para asesoramiento personal puedes comunicarte al +591 62342340.

Ruta crítica para el hackeo

Ejemplo: Una mujer despierta, abre su perfil en Facebook y ya no puede entrar. Alguien la dejó sin acceso a su cuenta.

¿Qué se puede hacer?

1. Puedes acompañar a una amiga que fue hackeada, aquí algunas frases para apoyarla y el contexto para entenderla.
2. proteger tu cuenta y
3. conocer la figura legal

a. Contención psicológica

[7] Luchadoras. 2017. 13 formas de agresión relacionada con las tecnologías contra las mujeres. https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/. Consultado el 12 de julio de 2020.

Si estás atravesando una situación de violencia

Si quieres acompañar a una amiga

Contáctate con nosotras

¿Te gustaría hablar con alguien? Puedes contactarte con nosotras por WhatsApp, Telegram o Signal al 62342340.

b. Orientación legal

Reconociendo la figura legal

La figura de hackeo no existe en un ámbito jurídico porque la suplantación de identidad, puede hacerse con documentos públicos (cédulas de identidad, licencias de conducir, licencia profesional, etc) pero no está determinada en relación a cuentas de redes sociales o medios de intercambio de información.

Sin embargo se podría vincular con la figura de alteración, acceso y uso indebido de datos informáticos del Art. 363 ter del Código penal. De la misma manera, se relaciona con la figura de doxxing, ya que primero debe existir un acceso a las cuentas o a los datos de una persona que están resguardados en un medio digital, para su posterior utilización.

Preguntas para conocer los hechos

- ¿Qué cuenta o cuentas fueron hackeadas?
- ¿Has podido recuperar las mismas?
- ¿Sabes si se utilizó la información contenida en tu cuenta?
    - Si ha existido un uso, o se conoce sobre el almacenamiento de dicha información, se puede relacionar la figura del hackeo con el doxxxing
- ¿Ha tenido interacción con tus contactos?
    - Las figuras son complejas, y pueden relacionarse con otras figuras, por ejemplo se puede utilizar el hackeo de cuentas para cometer delitos de fraude.
- ¿Cuándo ocurrió?
- ¿Había ocurrido antes?
- ¿Sabes quién realizó el hackeo?

Para mayor detalle sobre las preguntas para identificar las diferentes figuras legales, se puede consultar aquí: Preguntas generales para conocer los hechos.

Si la persona decide hacer una denuncia, se puede consultar el paso-a-paso del proceso penal aquí, para conocer las acciones a seguir.

c. Orientación tech

¿En qué red social o app de mensajería fuiste hackeada?

Facebook

¿Tienes acceso al correo electrónico vinculado a tu cuenta en Facebook? Sí - No

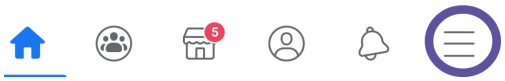
Ingresa al correo electrónico con el que normalmente inicias sesion:

- Documenta: Si recibiste notificaciones de un acceso no autorizado, saca capturas de pantallas de estas. También es importante documentar la fecha y hora del intento de ingreso a la cuenta.
- Ingresa a la página principal de Facebook ->
  - Selecciona donde dice “has olvidado los datos de tu cuenta” -> ¿Cómo quieres que te enviemos el código para cambiar la contraseña? -> Selecciona Enviar código por correo electrónico -> Continuar.

  - Se ha enviado un codigo al correo electrónico que usas para iniciar sesión en Facebook, ingresa este código en el lugar correspondiente.

- Una vez que hayas recuperado tu cuenta, es necesario actuar rápidamente para recuperar control sobre el perfil y aumentar tus niveles de seguridad para evitar ser atacada una vez más. Facebook te guiará por una serie de pasos para cambiar tu contraseña. Aquí te dejamos la ruta, por si acaso:

  - Ingresa a la Configuración de Facebook :
    - **Menú hamburguesa en la versión móvil**  **:**



    - **Menú desplegable en versión de computadora:**

Sigue estos pasos para desvincular tu cuenta de dispositivos desconocidos, activa la autenticación de dos pasos y escoge de 3 a 5 familiares, amigas o amigos cercanos para contactar en caso de que pierdas el acceso a tu cuenta otra vez.

Si las personas que ingresaron a tu cuenta cambiaron la contraseña y el correo electrónico con el que inicias sesion:

- Si se cambió el correo electrónico asociado a tu cuenta de Facebook, puedes volver a modificarla. Cuando se cambia un correo electrónico, Facebook envia un mensaje a la cuenta de correo electrónico anterior con un enlace especial. En tu correo electrónico, puedes hacer clic en este enlace para deshacer el cambio de dirección de correo electrónico y proteger tu cuenta[8].

Si seleccionaste a contactos de confianza en tu cuenta:

- Ingresa a la página principal de Facebook ->
    - Olvidaste tu cuenta -> Si se te solicita, escribe tu dirección de correo electrónico, teléfono, nombre de usuario o nombre completo y haz clic en Buscar para encontrar tu cuenta -> haz clic en ¿Ya no tienes acceso? -> Ingresa un correo electrónico o un número de teléfono nuevo, debes tener acceso a ambas -> Continuar -> Revelar mis contactos de confianza y escribe el nombre completo de uno de tus contactos de confianza -> Verás un conjunto de instrucciones con un enlace especial. El enlace contiene un código de recuperación al que solo tienen acceso tus contactos de confianza.
- Envía el enlace a contactos de confianza y para que se vincule la cuenta -> El enlace incluye un código de inicio de sesión. Debe enviar un código para recuperar la cuenta -> Usa el código de recuperación que proporcionaron los contactos de confianza para recobrar control sobre la cuenta[9].

[8] No puedo iniciar sesión. Facebook. https://es-la.facebook.com/help/105487009541643. Consultada el 8 de agosto de 2020.

[9] Cómo puedo contactar a los amigos que elegí como contactos de confianza para volver a acceder a mi cuenta de Facebook?. Facebook. https://es-la.facebook.com/help/213343062033160. Consultada 8 de agosto de 2020.

Sugerimos visitar la página de Primeros Auxilios Digitales, que tiene un paso a paso para recuperar cuentas en diversas plataformas: https://digitalfirstaid.org/es/topics/account-access-issues/questions/What_Type_of_Account_or_Service/

Si no tienes acceso al correo electrónico o número de celular con el que inicias sesion:

- Documenta: Si recibiste notificaciones del ingreso no autorizado, toma capturas de pantalla, la fecha y hora del ingreso, etc.
- Denuncia: Busca tu perfil ->
  - Selecciona el menú desplegable -> Buscar ayuda o reportar perfil -> Quiero Ayudar -> Cuenta Hackeada-> Enviar.
- Ingresa al siguiente link https://www.facebook.com/hacked-> Selecciona “mi cuenta está comprometida” -> Facebook te pedirá que ingreses tu contraseña actual o antigua para poder recuperar tu cuenta.

Si las personas que ingresaron a tu cuenta cambiaron la contraseña y el correo electrónico con el que inicias sesion:

- Si se cambió el correo electrónico asociado a tu cuenta de Facebook, puedes volver a modificarlo. Cuando se cambia un correo electrónico, Facebook envía un mensaje a la cuenta de correo electrónico anterior con un enlace especial. En tu correo electrónico, puedes hacer clic en este enlace para deshacer el cambio de dirección de correo electrónico y proteger tu cuenta[10].

Si seleccionaste a contactos de confianza en tu cuenta:

- Ingresa a la página principal de Facebook ->
  - Olvidaste tu cuenta -> Si se te solicita, escribe tu dirección de correo electrónico, teléfono, nombre de usuario o nombre completo y haz clic en Buscar para encontrar tu cuenta -> haz clic en ¿Ya no tienes acceso? -> Ingresa un correo electrónico o un número de teléfono nuevo, debes tener acceso a ambas -> Continuar -> Revelar mis contactos de confianza y escribe el nombre completo de uno de tus contactos de confianza -> Verás un conjunto de instrucciones con un enlace especial. El enlace contiene un

[10] No puedo iniciar sesión. Facebook. https://es-la.facebook.com/help/105487009541643. Consultada el 8 de agosto de 2020.

código de recuperación al que sólo tienen acceso tus contactos de confianza.

- Envía el enlace a tu amigx y pídele que lo abra -> El enlace incluye un código de inicio de sesión. Pídele que te envíe el código -> Usa los códigos de recuperación que te proporcionan tus contactos de confianza para acceder a tu cuenta[11].

Sugerimos visitar la página de Primeros Auxilios Digitales, que tiene un paso a paso para recuperar cuentas en diversas plataformas: https://digitalfirstaid.org/es/topics/account-access-issues/questions/Facebook/

Twitter

- Si tienes acceso al correo electrónico o número de celular con el que inicias sesión[12]:
  - Verifica en la bandeja de entrada del correo electrónico o en tu bandeja de spam (por si acaso) con el que inicias sesión, si recibes un mensaje informando que tu contraseña ha sido cambiada -> En el correo, encontrarás un link que dice “Recupera tu cuenta”, ingresa y sigue los pasos correspondientes.
  - Si no encuentras el correo en tu bandeja, ingresa a https://help.twitter.com/forms/restore -> Selecciona la opcion no puedo iniciar sesion.
  - Continúa con las instrucciones correspondientes.

- Si no tienes acceso al correo electrónico o al número de celular con el que inicias sesión:
  - Si no recibiste el correo electrónico -> ingresa al siguiente enlace https://help.instagram.com/149494825257596?helpref=search&sr=1&query=hacked y escoge la opción correspondiente.

[11] ¿Cómo puedo contactar a los amigos que elegí como contactos de confianza para volver a acceder a mi cuenta de Facebook?. Facebook. https://es-la.facebook.com/help/213343062033160. Consultada 8 de agosto de 2020.
[12] Digital First Aid Kits. Red de Respuesta Rápida, CiviCert. http://digitalfirstaid.org. Consultada 8 de agosto de 2020.

También recomendamos visitar la página de Primeros Auxilios Digitales, que tiene un paso a paso para recuperar cuentas en diversas plataformas: https://digitalfirstaid.org/es/topics/account-access-issues/questions/Twitter/

WhatsApp

Si sientes que alguien puede estar usando tu cuenta desde el navegador web, puedes seguir los siguientes pasos:

- En Android: Ingresa al menú con tres puntos, y En iOS: dirígete a la pestaña Ajustes
    - Presiona en WhatsApp Web -> Se verá una lista con los dispositivos vinculados al navegador, Puedes cerrar todas las sesiones, o escoger el dispositivo que quieres cerrar.

Si sospechas que otra persona está usando tu cuenta de WhatsApp, **debes notificar a tus familiares y amigos que dicha persona podría hacerse pasar por ti en tus chats individuales y de grupo.** Ten en cuenta que WhatsApp proporciona cifrado de extremo a extremo y los mensajes se almacenan en tu dispositivo, de manera que **si alguien accede a tu cuenta en otro dispositivo no podrá leer tus conversaciones pasadas.**

Para recuperar tu cuenta, puedes volver a instalar WhatsApp, se te pedirá un código de seis dígitos, que será enviado por SMS a tu celular, automáticamente la sesión abierta en el otro celular se cerrará.

También es posible que se te pida ingresar un código de verificación en dos pasos. Si no sabes ese código, es posible que la persona con acceso a tu cuenta haya activado la verificación en dos pasos. **En ese caso, debes esperar siete días para poder verificar tu número sin el código de verificación en dos pasos**. Independientemente de si sabes el código de verificación en dos pasos o no, la sesión de la persona con acceso a tu cuenta se cerrará en cuanto ingreses el código de seis dígitos enviado por SMS.[13] Aquí hay una serie de pasos para activar esta verificación.

Gmail

[13] Cuentas Robadas, WhatsApp. https://faq.whatsapp.com/general/account-and-profile/stolen-accounts?lang=es . Consultada 10 de agosto de 2020

Si tienes acceso al correo electrónico asociado [14]: -> Comprueba si recibiste un correo electrónico de "Alerta de seguridad crítica para tu cuenta de Google vinculada" de Google. -> En el correo, ingresa al link que dice ”recuperar mi cuenta”.

No tienes acceso al correo electrónico de respaldo: Ingresa a https://support.google.com/accounts/answer/7682439?hl=es -> en la sección “si otra persona está usando tu cuenta” -> Ingresa a “**recuperar cuentas pirateadas o robadas**”.-> en el apartado de “ si no puedes iniciar sesión”, ingresa a “página de recuperación de la cuenta” -> Ingresa tu correo electrónico -> Escribe la última contraseña que recuerdes haber usado con esa cuenta de Google -> Si no la recuerdas, ingresa a tu cuenta de otra manera.

También recomendamos visitar la página de Primeros Auxilios Digitales, que tiene un paso a paso para recuperar cuentas en diversas plataformas: **https://digitalfirstaid.org/es/topics/account-access-issues/questions/Google/**

Instagram

Si tienes acceso al correo electrónico o número de celular con el que inicias sesión: Comprueba si recibiste un mensaje de Instagram en tu correo electrónico, con el asunto "Tu contraseña de Instagram ha sido cambiada”-> Ingresa al enlace de recuperación -> Listo.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al +591 62342340. Te invitamos a leer nuestros consejos antihackeo.

3. Amenazas de agresiones físicas, sexuales o de muerte, a través de medios digitales

Las amenazas son contenidos violentos, lascivos o agresivos que manifiestan una intención de daño a una persona, sus seres queridos o bienes[15]. En el sondeo a 1000

[14] Digital First Aid Kits. Red de Respuesta Rápida, CiviCert. http://digitalfirstaid.org. Consultada 8 de agosto de 2020.

[15] Luchadoras. 2017. 13 formas de agresión relacionada con las tecnologías contra las mujeres.

mujeres en Bolivia, casi 500 de ellas recibieron amenazas de agresiones físicas, sexuales o de muerte, **252 de ellas eran activistas o pertenecen a alguna organización.**

Como acción preventiva a las amenazas recomendamos revisar nuestros consejos antiamenazas para tener una armadura extra contra discursos de odio, insultos y otros contenidos que buscan intimidar y censurarnos.

Ruta critica al recibir amenazas

Ejemplo: Una mujer activista recibe varios mensajes en Messenger insultándola. Son de varios perfiles falsos, ella los bloquea e ignora pero empiezan a amenazar su integridad física y quiere tomar acciones para protegerse.

¿Qué se puede hacer?

1. Para acompañar a una persona a la que le amenazaron, aquí algunos consejos de cómo apoyarla y el contexto para entenderla.
2. Puede revisar la vía legal para presentar una denuncia por amenazas,
3. Se puede reportar el mensaje, denunciar el perfil acosador y bloquearlo.

a. Contención psicológica

Si estás atravesando una situación de violencia

Si quieres acompañar a una amiga

Contáctate con nosotras

¿Te gustaría hablar con alguien? Puedes contactarte con nosotras por WhatsApp, Telegram o Signal al 62342340.

b. Orientación legal

https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/. Consultado el 12 de julio de 2020.

Reconociendo la figura legal

Las amenazas buscan en última instancia causar miedo e inseguridad, pero además buscan limitar la libertad de decisión de la persona, debido a que las amenazas usualmente se realizan buscando que una persona haga o deje de realizar determinada cuestión.

Ya que la amenaza es un anuncio de un mal futuro, de algún modo, dependiendo del caso puede relacionarse con otras figuras legales. En nuestra legislación la figura precisa es amenazas del Art. 293 en el Código Penal. El delito de amenaza también está configurado de manera genérica, no vinculado a un ámbito digital; sin embargo, las amenazas podrían realizarse desde medios informáticos o digitales.

Preguntas para conocer los hechos

Para mayor detalle sobre las preguntas para identificar las diferentes figuras legales, puede consultar aquí: Preguntas generales para conocer los hechos.

Sobre la amenaza específicamente, proponemos las siguientes preguntas para identificar esta figura dentro de los parámetros del Código Penal:

- ¿Cuál es el contenido de las amenazas?
- ¿Cuándo empezaron las amenazas y cuándo fue la última vez que fue recibida una amenaza?
- ¿Ha existido un incremento en la gravedad del contenido de las amenazas?
- ¿Dónde se han realizado las amenazas?
- ¿Quién ha realizado las amenazas?
- ¿Cree que las amenazas pueden efectivamente materializarse?

Si la persona decide hacer una denuncia, se puede consultar el paso-a-paso del proceso penal aquí, para conocer las acciones a seguir.

c. Orientación tech

¿En qué red social o app de mensajería estás siendo amenazada?

Messenger

- Recopila las pruebas: tomar capturas de pantalla del mensaje, la hora y la fecha, el perfil que te lo envía, su foto, el enlace del perfil que te lo envía, sus fotos, etc.
- Investiga: Ingresa al perfil, mira las fotos, revisa su lista de amigos y mira si tienen amigos y amigas en común, revisa sus publicaciones, la fecha de creación del perfil, asegúrate de si es un perfil falso.
- Puedes bloquear o silenciar el perfil:
    - Bloquea el perfil en Messenger y se bloqueará también en Facebook: Ingresa a la ventana de la conversación en Messenger -> busca el ícono de un engranaje -> Bloquear -> Listo
    - Silencia el perfil en Messenger y no recibirás notificación de los mensajes recibidos del perfil: Ingresa a la ventana de la conversación en Messenger -> busca el ícono de un engranaje -> Silenciar -> Listo

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al 62342340, visitar nuestra guía antiacoso digital: https://internetbolivia.org/8M/ o revisar nuestros consejos antiamenazas para tener una armadura extra ante discurso de odio, insultos y otros contenidos que buscan intimidar y censurarnos.

Facebook

- Recopila las pruebas: toma capturas de pantalla de los mensajes, hora y fecha, el perfil que te lo envía, el enlace del perfil que te lo envía.
- Investiga: Ingresa al perfil, observa si es un perfil falso, mira las fotos, revisa su lista de amigos y busca si tienen amigos y amigas en común, revisa sus publicaciones, la fecha de creación del perfil, su correo electrónico, número de celular, fecha de nacimiento.
- Denuncia el perfil:
    - Ingresa al perfil: Selecciona menú desplegable (los tres puntos en la esquina superior derecha) escoge busca ayuda/denuncia perfil -> Quiero ayudar -> Acoso -> Enviar.

Si las amenazas provienen de un perfil falso, la razón de denuncia cambiará, puedes hacer las siguientes 2 denuncias.

Para denunciar un perfil que amenaza:

1. Ingresa al perfil: -> Selecciona el menú desplegable (los tres puntos a mano superior derecha) escoge busca ayuda/denuncia perfil -> Cuenta Falso-> Siguiente -> Reportar perfil -> Creo que este perfil infringe las normas comunitarias de Facebook -> Reportar.

Para denunciar una amenaza en una publicación:

2. En la imagen -> Selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Acoso-> A mi ->Enviar

Se puede hacer seguimiento a las denuncias en el siguiente enlace: https://www.facebook.com/support, en este apartado, se encuentra información sobre el estado de la denuncia. Facebook muestra si la denuncia es aceptada o no. En el caso de que no lo sea, también hay información de las razones por la cual Facebook no aceptó la misma.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al 62342340, visitar nuestra guía antiacoso digital: https://internetbolivia.org/8M/ o revisar nuestros consejos antiamenazas para tener una armadura extra ante discurso de odio, insultos y otros contenidos que buscan intimidar y censurarnos.

Instagram

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y la fecha, la foto de la cuenta, el nombre, su descripción, publicaciones e historias.
- Investiga: Ingresa al perfil, mira sus fotos, revisa si tienen amigos o amigas en común. Mira si menciona otras redes sociales en su perfil.

Tienes varias opciones para dejar de recibir amenazas en Instagram, entre ellas recomendamos:

- Reportar el mensaje:
  - Entra a la conversación -> Pulsa 3 segundos sobre el mensaje -> Reportar -> Violencia o amenaza de violencia -> Reportar
- Reportar el comentario:
  - Pulsa 3 segundos sobre el comentario -> Presiona en el ícono de la parte superior derecha -> Reportar este comentario -> Es inapropiado -> Violencia u organizaciones peligrosas -> Enviar reporte
- Reportar el perfil:
  - Ingresa al perfil -> Ve al menú desplegable -> Reportar -> Es inapropiado -> Reportar cuenta -> Publica contenido que no debería estar en Instagram -> Violencia u organizaciones peligrosas -> Reportar
- Bloquear el perfil:
  - Ingresa al perfil -> Ve al menú desplegable -> Bloquear. Recomendamos bloquear el perfil después de haber reportado el comentario y perfil.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al 62342340, visitar nuestra guía antiacoso digital: https://internetbolivia.org/8M/ o revisar nuestros consejos antiamenazas para tener una armadura extra ante discurso de odio, insultos y otros contenidos que buscan intimidar y censurarnos.

Twitter

- Recopila las pruebas: toma capturas de pantalla del tweet o mensaje, la hora y fecha, la foto del perfil, el nombre, la descripción, el nombre de la cuenta @, si menciona otras cuentas en Twitter o redes sociales, etc.
- Investiga: Ingresa a la cuenta, mira sus fotos, la descripción, tweets, seguidores, a quienes sigue, sus menciones y listas.

Recomendamos que reportes el tweet, el perfil y bloquees la cuenta. Aquí los pasos a seguir:

- Reporta el tweet: Pulsa encima del Tweet-> Pulsa en la flecha (mano derecha superior) -> Denunciar tweet -> Comete abusos o es perjudicial -> Amenaza con violencia o daño físico -> ¿Esta amenaza contiene información privada?
    - Sí -> Marca las opciones con las que te sientas identificada ->Esta información pertenece a:
        - A mí o a alguien a quien represento -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).
        - Otra persona -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).
    - No -> ¿A quién ataca @agresor?
        - A mí -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).
        - Otra persona -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).

- Reporta el perfil: Ingresa al perfil -> Ve al menú desplegable -> Denunciar -> Sus tweets son abusivos o incitan al odio -> Amenaza con violencia o daño físico -> ¿Esta amenaza contiene información privada?
    - Sí -> Marca las opciones con las que te sientas identificada ->Esta información pertenece a:
        - A mí o a alguien a quien represento -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).

        - Otra persona -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).
    - No -> ¿A quién ataca @agresor?
        - A mí -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha)
        - Otra persona -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha)

- Bloquea el perfil (opcional): Ingresa al perfil -> Ve al menú desplegable -> Bloquear

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al 62342340, visitar nuestra guía antiacoso digital: https://internetbolivia.org/8M/ o revisar nuestros consejos antiamenazas para tener una armadura extra ante discurso de odio, insultos y otros contenidos que buscan intimidar y censurarnos.

WhatsApp

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y fecha, la foto de la cuenta, el número de celular, sus estados y descripción.
- Investiga: Ingresa al perfil, revisa si tienen grupos en común. Busca el número en Facebook y Twitter para ver si tiene un perfil asociado al número.

Recomendamos reportar al contacto o grupo de dónde provienen las amenazas, enviar un reporte a WhatsApp y bloquear al contacto. Aquí las instrucciones para Android y iOS:

Android

- Ingresa a la conversación -> presiona sobre el Menú desplegable (tres puntos) -> Ajustes -> Reporta.
- Para denunciar a un grupo en WhatsApp en Android -> En el grupo de WhatsApp, ve al menú desplegable -> Reporta el grupo y selecciona si quieres salirte del grupo.
- Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú desplegable (3 puntos a mano derecha superior) de WhatsApp -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

iOS

- Para denunciar a un grupo en WhatsApp en iOS ->

- Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú Configuración (lado derecho inferior) de WhatsApp -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al 62342340, visitar nuestra guía antiacoso digital: https://internetbolivia.org/8M/ o revisar nuestros consejos antiamenazas para tener una armadura extra ante discurso de odio, insultos y otros contenidos que buscan intimidar y censurarnos.

Telegram

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y fecha, la foto del perfil, el número de celular, y en caso de contar con uno, el alias, el nombre de usuario que comienza con @.
- Investiga: Ingresa al perfil, registra el nombre y número de celular, mira sus fotos de perfil, la última vez que ingresó a la app, revisa si tienen grupos en común. En Facebook y Twitter, busca el número para ver si tiene un perfil asociado al número.

Denuncia el mensaje:

- Pulsa sobre el menú desplegable -> Reportar -> Violencia.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al 62342340, visitar nuestra guía antiacoso digital: https://internetbolivia.org/8M/ o revisar nuestros consejos antiamenazas para tener una armadura extra ante discurso de odio, insultos y otros contenidos que buscan intimidar y censurarnos.

4. Difusión de información íntima sin consentimiento (DIISC):

Esto se refiere a robar u obtener información personal de alguien con el fin de difundirla para que afecte a una persona o grupo de personas[16]. Este tipo de agresión no es aislada, generalmente viene acompañada por otras violencias con las que coexiste, superponen y

[16] https://www.takebackthetech.net/es/blog/13-formas-de-agresion-en-linea-contras-las-mujeres

se fortalecen entre sí[17] Esa violencia suele ir de la mano de la manipulación de la información con el fin de desprestigiar, extorsionar y amenazar[18].

En Bolivia, de 1000 mujeres encuestadas, 450 indicaron que alguien publicó información falsa para desprestigiarlas. 264 mujeres dijeron que fueron publicadas fotos de ellas sin su consentimiento. 214 mujeres dijeron que fueron publicadas fotos suyas en su círculo cercano.

De manera preventiva, te invitamos a hacer este divertido test sobre sexting seguro, el Calentómetro. Para asesoría personal puedes comunicarte al +591 62342340.

Ruta crítica para la publicación de fotos sin consentimiento

Ejemplo: Una mujer recibe un mensaje de su amiga, es una captura de pantalla de una conversación de un grupo en una app de mensajería o red social con una foto suya desnuda que fue compartida por un expareja.

¿Qué se puede hacer?

1. Se puede acompañar a la persona, aquí algunas frases para entender y apoyar a una persona, cuyas fotos han sido publicadas.
2. Conocer las acciones legales que puedes tomar.
3. Se puede denunciar el contenido y el perfil que lo publicó.

a. Orientación legal

Reconociendo la figura legal

La difusión de información íntima sin consentimiento (DIISC) se relaciona estrechamente con el consentimiento, y está establecido con la figura de pornografía tipificada en el Art.

[17] Fuente: Asociación Civil Hiperderecho, Conocer para resistir: https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf

[18] Para más información sobre la distribución de imágenes, íntimas o sexuales sin consentimiento: qué es, cómo ocurre y cómo defenderte, consulta la guía urgente de tecnoresistencias: https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/11/guia_pornografia_no_consentida_peru.pdf

323 bis del Código Penal en Bolivia. Este delito será sancionado con pena privativa de libertad de diez (10) a quince (15) años. Esta figura reconoce el delito si la persona agresora reproduce o almacena, distribuye o vende material pornográfico.

Preguntas para conocer los hechos

- ¿Qué es lo que fue difundido? ¿Fotografías o videos?
- ¿Qué contenía de manera específica el medio difundido?
- ¿Quién es la persona que tiene acceso a esa fotografía o video?
    - Pueden ocurrir distintos supuestos, el más común que una ex pareja difunda imágenes o videos íntimos, pero también podría ocurrir que nadie haya tenido acceso específico a la información sino que se haya tenido acceso indebido a un medio digital y se haya extraído de dicho lugar, las imágenes íntimas. En este caso también se podrían vincular las figuras de hackeo y doxxxing.
- ¿Cómo supo de la difusión de las imágenes o videos?
- ¿Sabe en qué lugares puede encontrarse dichas imágenes o videos?
    - Se debe tomar en cuenta que si la imagen fue compartida con la ex pareja, y posteriormente el grupo de amigos tuvo acceso a la imagen, puede que incluso haya llegado a una página web de difusión de pornografía.

Para mayor detalle sobre las preguntas para identificar las diferentes figuras legales, puede consultar aquí: Preguntas generales para conocer los hechos.

Si la persona decide hacer una denuncia se puede consultar el paso-a-paso del proceso penal aquí para conocer las acciones a seguir.

b. Contención psicológica

Si estás atravesando una situación de violencia

Si quieres acompañar a una amiga

Contáctate con nosotras

¿Te gustaría hablar con alguien? Puedes contactarte con nosotras por WhatsApp, Telegram o Signal al 62342340.

c. Orientación tecnológica

¿En qué red social o app de mensajería se publicó tu información?

Facebook

El contenido publicado en Facebook solo será eliminado si incumple sus Normas comunitarias. Se restringen los desnudos y la exhibición de actividades sexuales, a menos que se publique con fines educativos, humorísticos o satíricos[19].

Algunos de los contenidos que no permiten, sobre contenido sexual, son:

- Actividad sexual
- Ofrecimiento o solicitud de actividad sexual
- Pezones femeninos (excepto en el contexto de lactancia, salud y actos de protesta) Desnudos en los que se muestran genitales
- Lenguaje sexual explícito

A continuación recomendamos las siguientes acciones reactivas ante la difusión de imágenes íntimas sin consentimiento:

- Recopila las pruebas: toma capturas de pantalla de la publicación o mensaje, la hora y fecha de publicación, el perfil que lo publicó, guarda el enlace de la publicación, etc.
- Investiga: Ingresa al perfil que publicó tu información, mira sus fotos, revisa su lista de amigos y mira si tienen amigos y amigas en común, revisa sus publicaciones, la fecha de creación del perfil, verifica si es un perfil falso. A continuación, sugerimos reportar el contenido y el perfil.
- Denunciar el contenido con el administrador del grupo: Si se comparte contenido en un grupo.
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación a administradores del grupo -> Desnudos -> Enviar.
- Denuncia el contenido:
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Desnudos ->
        - Desnudos de adultos -> Siguiente.
        - Contenido sexualmente sugerente -> Siguiente.
        - Actividad sexual -> Siguiente.
        - Explotación sexual -> Siguiente.

[19] Facebook. 2020. Desnudos u actividad sexual de adultos. https://www.facebook.com/communitystandards/adult_nudity_sexual_activity. Consultada el 8 de agosto de 2020.

        - Contenido relacionado a un menor -> Siguiente.
        - Se comparten imágenes privadas -> Siguiente.
            - Reportar publicación -> Siguiente
                - Sí, quiero enviar el reporte -> Siguiente -> Reportar al administrador (si se hizo en un grupo) -> Listo.
            - Reportar al administrador -> Siguiente.
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Otros -> Se Propiedad Intelectual -> Siguiente -> Reportar foto -> Creo que esta foto infringe las normas comunitarias de Facebook -> Reportar.
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Otros -> Se Imágenes íntimas sin consentimiento -> Siguiente -> Reportar foto -> Creo que esta foto infringe las normas comunitarias de Facebook -> Reportar.
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Otros -> Se comparten imágenes privadas -> Siguiente -> Reportar foto -> Creo que esta foto infringe las normas comunitarias de Facebook -> Reportar.
- Denuncia el perfil: puedes hacerlo por la publicación de contenido inapropiado, si proviene de un perfil falso y por publicación de imágenes íntimas sin consentimiento.
    - Ingresa al perfil -> Abre el menú desplegable -> Buscar ayuda o reportar perfil ->Publica contenido inapropiado -> Enviar.
    - Ingresa al perfil: -> Selecciona menú desplegable (los tres puntos a mano superior derecha) escoge busca ayuda/denuncia perfil -> Quiero ayudar -> imágenes íntimas sin consentimiento -> Enviar.
    - Ingresa al perfil: -> Selecciona el menú desplegable (los tres puntos a mano superior derecha) escoge busca ayuda/denuncia perfil -> Perfil Falso--> Enviar.
- Reportar casos de chantaje, fotos de carácter sexual o amenazas con compartir fotos de carácter sexual:
    - Llena el formulario en: https://www.facebook.com/help/contact/567360146613371

    Si prefieres, también puedes bloquear al perfil, pero esto te inhabilitaría desde la plataforma para monitorearlo, verificar si el contenido fue removido o asegurarte de que el perfil no vuelva a publicar más imágenes tuyas. Aquí los pasos por si decides bloquear el perfil:

Para Android y iOS 

- Ingresa al perfil de la persona que quieras bloquear -> Presiona en “Más”  -> Bloquear -> ¡Listo!

Para Escritorio 

- Ingresa al perfil de la persona que quieras bloquear -> Haz clic en ••• -> Bloquear -> ¡Listo!

Para más detalles consulta nuestra guía aquí[20] o sigue los pasos de Facebook para reportar perfiles falsos: https://www.facebook.com/help/306643639690823?helpref=uf_permalink

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al +591 62342340. También te invitamos a hacer este divertido test sobre sexting seguro, el Calentómetro.

Se puede hacer seguimiento a las denuncias que hiciste en el siguiente enlace: https://www.facebook.com/support, en este apartado encontrarás información sobre el estado de tu denuncia, Facebook te mostrará si la denuncia fue aceptada o no. En el caso de que no lo sea, también encontrarás información de las razones por las cuales Facebook no aceptó la misma.

WhatsApp

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y la fecha, la foto de la cuenta, el número de celular, etc.
- Si no conoces a la persona, investiga: ingresa a su perfil, registra el nombre y número de celular, su estado, descripción y revisa si tienen grupos en común. Busca el número en Facebook y Twitter para ver si tiene un perfil asociado al número.
- Recomendamos reportar al contacto o grupo de dónde provienen las amenazas, enviar un reporte a WhatsApp y bloquear al contacto. Aquí las instrucciones para Android y iOS:

[20] Manual paso a paso actualizada el 23 de octubre de 2019.

ANDROID 

- Ingresa a la conversación -> presiona sobre el Menú desplegable (tres puntos) -> Ajustes -> Reporta.
- Para denunciar a un grupo en WhatsApp-> En el grupo de WhatsApp, ve al menú desplegable -> Reporta el grupo y selecciona si quieres salirte del grupo.
- Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú desplegable (3 puntos a mano derecha superior) de WhatsApp -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

iOS 

- Para denunciar a un grupos en WhatsApp en iOS ->
    - Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú desplegable (3 puntos a mano derecha superior) de WhatsApp -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al +591 62342340. También te invitamos a hacer este divertido test sobre sexting seguro, el Calentómetro.

Instagram

- Recopila la información: toma capturas de pantalla de la publicación o mensaje, la hora y fecha de publicación, el perfil que lo publicó, guarda el enlace de la publicación, etc.
- Reporta el contenido:
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar -> Es inapropiado (puedes reportar en cualquiera de las siguientes 5 opciones):
        1. Desnudos o actividad sexual:
            - Desnudos o pornografía
            - Explotación o servicios sexuales
            - Se comparten imágenes privadas
                - Si gustas puedes bloquear la cuenta

2. Violencia u organizaciones peligrosas: Para denunciar publicaciones que fomentan la violencia por razones de religión, etnia o sexo. Daño físico, robo o vandalismo.
3. Bullying o acoso -> ¿Quién es la víctima del acoso o bullying?
    - Yo
    - Alguien que conozco
    - Otra persona
4. Infracción de la propiedad intelectual: Denunciar robo de identidad, es mejor si la persona afectada hace la denuncia con la plataforma -> Listo.
5. Información falsa -> Listo

- Reporta la cuenta:
    - En su perfil -> Selecciona el menú desplegable -> Reportar -> Es inapropiado -> Reportar cuenta -> Publica contenido que no debería estar en Instagram -> Desnudos o actividad sexual -> Imágenes íntimas sin consentimiento -> Enviar reporte.

Si necesitas ayuda, comunícate con nosotras al 62342340 para que te ayudemos en el proceso de denunciar el contenido o si necesitas asesoría personal. Te invitamos a hacer este divertido test sobre sexting seguro, el Calentómetro.

Buscador Google

- Recopila las pruebas: toma capturas de pantalla de las páginas donde están publicando tus imágenes o contenido con el objetivo de difamarte.
- Google te da 2 opciones para hacer la denuncia en su página: desvincular el URL o enlace de las búsquedas de Google o hablar con los administradores de la página web donde se encuentra el contenido.
  1. Puedes enviar una petición a Google para pedir que se baje el contenido si tiene que ver con:
    - Ingresa a este enlace para retirar de Google pornografía falsa publicada sin consentimiento, lee atentamente las indicaciones y restricciones, al finalizar te pedirán llenar este formulario, una solicitud para retirar tu información personal de Google.

        - Qué quieres hacer? -> Eliminar información que aparece en la Búsqueda de Google.
        - La información que quiero eliminar es -> En los resultados de búsqueda de Google y en un sitio web
        - ¿Te has puesto en contacto con el webmaster del sitio? -> No, prefiero no hacerlo.
        - Quiero eliminar -> Imágenes sexualmente explícitas o de desnudos, o nombres en sitios web pornográficos -> Una imagen o un video en la que aparezco.
        - ¿Apareces tú (o alguien que estés autorizado a representar) en las imágenes o vídeos, estás desnudo o en situaciones sexualmente explícitas? -> Sí
        - ¿Alguna vez has dado tu consentimiento para distribuir las imágenes o los vídeos? -> No
        - Llena el formulario para enviar la solicitud a Google.

    2. Es importante notar que, si bien el enlace o URL específicas será removido de la Búsqueda de Google, la página web que aloja el contenido puede seguir existiendo. Para eliminar el contenido en la página web debes contactarte con los administradores de la página web. Para más información puedes ver aquí.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al +591 62342340. También te invitamos a hacer este divertido test sobre sexting seguro, el Calentómetro.

Twitter

- Recopila las pruebas: toma capturas de pantalla del tweet o mensaje, la hora y fecha, la foto del perfil, el nombre, la descripción.
- Pulsa encima del Tweet-> Pulsa en la flecha (mano derecha superior) -> Denunciar Tweet -> Escoge:
    - Muestra una foto o un video de carácter delicado ->
        - No apto para menores
        - Violento
        - Incitación al odio
        - Una foto o un video no autorizados ->
            - Incluye contenido no autorizado de carácter íntimo sobre mí o sobre otra persona ->

    - A mí o alguien a quien represento -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).
    - Otra Persona-> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).
  - Incluye información privada
  - Me muestra a mí y no quiero que este contenido esté en Twitter

- Ingresa al perfil de Twitter-> Menú desplegable (3 puntos a mano derecha superior) ->Reportar -> Sus tweets son abusivos y promueven el discurso de odio -> Ingresa los enlaces de los tweets que quieres reportar.
- Recomendamos llenar el formulario que provee Twitter para proteger tu información personal: https://help.twitter.com/forms/private_information

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al +591 62342340. También te invitamos a hacer este divertido test sobre sexting seguro, el Calentómetro y consultar la siguiente guía de la Fundación Karisma (desde la página 16) para reportar contenidos abusivos, bloquear, silenciar y otros consejos de Seguridad, Protección y Privacidad en Twitter[21].

Telegram

- Recopila las pruebas: toma capturas de pantalla del mensaje, la hora y fecha, la foto del perfil, el número de celular, y en caso de contar con uno, el alias, el nombre de usuario que comienza con @.
- Investiga: Ingresa al perfil, registra el nombre y número de celular, mira sus fotos de perfil, la última vez que ingresó a la app, revisa si tienen grupos en común. En Facebook y Twitter, busca el número para ver si tiene un perfil asociado al número

Denuncia el mensaje:

- Pulsa sobre el menú desplegable -> Reportar -> Pornografía

[21] Versión 2016.

¿La información que te dimos fue de ayuda? Si necesitas más orientación, puedes comunicarte al +591 62342340. También te invitamos a hacer este divertido test sobre sexting seguro, el Calentómetro o revisar nuestra guía antiacoso digital: https://internetbolivia.org/8M/

5. Obtención y publicación de información personal - Doxxing

Este tipo de violencia tiene que ver con el robo u obtención y publicación de información personal y privada, como fotografías, número de celular, fecha de nacimiento, domicilio, lugar de trabajo, nombres, información de familiares, etc. para afectar a la persona[22]. **Podemos entenderlo como la pérdida de control sobre nuestros datos personales**. Como acción preventiva, te invitamos a leer nuestros consejos antidoxxing para evitar estar en una situación de violencia como esta.

En Bolivia, 300 mujeres de 1000 encuestadas dijeron que en algún momento se publicó información personal sin su consentimiento como: nombre completo, número de celular, correo electrónico, entre otros.

Ruta crítica para el doxxing

Ejemplo: Una mujer se percata de que una fotografía con su nombre, apellido, número de celular y lugar de trabajo es publicada en redes sociales. La imagen es publicada en varios lugares, acusandola y difamándola. Ella está siendo atacada por doxxing, pues sus datos personales han sido publicados.

¿Qué se puede hacer?

1. Para acompañar a una persona de la que publicaron su información: fotos, número de celular, domicilio, etc. aquí te dejamos algunas frases para apoyarla y el contexto para entenderla.
2. Puedes informarte sobre la figura legal en Bolivia
3. Puedes denunciar el contenido y el perfil que lo publicó.

[22]Luchadoras. 2017. 13 formas de agresión relacionada con las tecnologías contra las mujeres. https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/. Consultado el 12 de julio de 2020.

a. **Contención psicológica**

Si estás atravesando una situación de violencia

Si quieres acompañar a una amiga

Contáctate con nosotras

¿Te gustaría hablar con alguien? Puedes contactarte con nosotras por WhatsApp, Telegram o Signal al 62342340.

b. **Orientación legal**

Reconociendo la figura legal

La figura del doxxxing como tal no está en nuestra legislación, pero puede vincularse con la alteración, acceso y uso indebido de datos informáticos que se encuentra en el Art. 363 ter del Código penal. A la vez, con los delitos en contra del honor como difamación, calumnia, ofensa a la memoria de los difuntos e injuria en los Arts. 282, 283, 284 y 287 del Código Penal. Para información más detallada puede consultar nuestra Guía de acciones de acompañamiento para ciberbrigadistas

Preguntas para conocer los hechos

- ¿Cómo fue obtenida la información?
  - Notar que podría existir un acceso a información privada a través de medios indebidos como ser el ingreso a cuentas en redes sociales o aparatos digitales personales, pero también podría existir la averiguación de información obtenida en medios de acceso público, como la información en perfiles de redes sociales: Facebook, Twitter, Instagram etc.
- ¿Qué información ha sido difundida?
- ¿Dónde fue difundida?
- ¿Quién difundió la información?
- ¿Qué efectos ha tenido la difusión en su vida personal, laboral o pública?

Para mayor detalle sobre las preguntas para identificar las diferentes figuras legales, puede consultar aquí: Preguntas generales para conocer los hechos.

Si la persona decide hacer una denuncia, se puede consultar el paso-a-paso del proceso penal aquí para conocer las acciones a seguir.

c. Orientación tecnológica

¿En qué red social o app de mensajería está pasando?

Facebook

- Recopila las pruebas: toma capturas de pantalla de la publicación o mensaje, la hora y fecha de publicación, el perfil que lo publicó, guarda el enlace de la publicación, etc.
- Investiga: Ingresa al perfil que publicó tu información, mira sus fotos, revisa su lista de amigos y mira si tienen amigos y amigas en común, revisa sus publicaciones, la fecha de creación del perfil, revisa si es un perfil falso.
- Denuncia el contenido: Facebook no te permite hacer una denuncia específica sobre la publicación de información personal a pesar de estar reconocido como una infracción de privacidad en sus normas comunitarias. Es por eso que recomendamos denunciar el contenido de la siguiente manera:
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Otro -> Imágenes íntimas sin consentimiento -> Siguiente -> Reportar foto -> Creo que esta foto infringe las normas comunitarias de Facebook -> Reportar.
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Otros -> Se comparten imágenes privadas-> Siguiente -> Reportar foto -> Creo que esta foto infringe las normas comunitarias de Facebook -> Reportar.
    - En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Otro -> Acoso -> Siguiente -> Reportar foto -> Creo que esta foto infringe las normas comunitarias de Facebook -> Reportar.

- Denuncia el perfil: puedes hacerlo por la publicación de datos personales, si proviene de un perfil falso y por publicar imágenes íntimas sin consentimiento.
    - Ingresa al perfil -> Abre el menú desplegable -> Buscar ayuda o reportar perfil -> Publica contenido inapropiado -> Enviar.
    - Ingresa al perfil: -> Selecciona menú desplegable (los tres puntos a mano superior derecha) escoge busca ayuda/denuncia perfil -> Quiero ayudar -> imágenes íntimas sin consentimiento -> Enviar.

- Ingresa al perfil: -> Selecciona el menú desplegable (los tres puntos a mano superior derecha) escoge busca ayuda/denuncia perfil -> Perfil Falso -> Enviar.

Se puede hacer seguimiento a las denuncias que hiciste en el siguiente enlace: https://www.facebook.com/support, en este apartado encontrarás informacion sobre el estado de tu denuncia, Facebook te mostrará si tu denuncia es aceptada o no. En el caso de que no lo sea, también encontrarás información de las razones por las cuales Facebook no aceptó la misma.

WhatsApp

- Documenta
- Denunciar un contacto o grupo:
  Ingresa a la conversación -> presiona sobre el Menú desplegable (tres puntos) -> Más -> Reporta.
  - Decide si quieres eliminar la conversación y bloquear al contacto -> Listo.
  - Decide si quieres eliminar la conversación de tu celular del grupo -> Listo.

Instagram

- Documenta
- Reporta el mensaje: Entra a la conversación -> Presiona 3 segundos sobre el mensaje -> Reportar -> Acoso o Bullying -> Reportar
- Reporta el comentario: Pulsa 3 segundos sobre el comentario -> Presiona en el ícono de la parte superior derecha -> Reportar este comentario -> Es inapropiado -> Acoso o bullying -> ¿Quién es víctima de acoso o bullying?
  - Yo ->Enviar reporte
  - Alguien que conozco ->Listo
  - Otra persona ->Listo
- Reporta el perfil: Ingresa al perfil -> Ve al menú desplegable -> Reportar -> Es inapropiado -> Reportar cuenta -> Publica contenido que no debería estar en Instagram -> VIolencia u organizaciones peligrosas -> Reportar
- Bloquea el perfil: Ingresa al perfil -> Ve al menú desplegable -> Bloquear

Twitter

- Documenta
- Reporta el tweet: Pulsa encima del Tweet-> Pulsa en la flecha (mano derecha superior) -> Denunciar tweet -> Comete abusos o es perjudicial -> Incluye

información privada -> Marca las opciones con las que te sientas identificada -> Esta información privada pertenece a:
    - A mí o a alguien a quien represento -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha)
    - Otra persona -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha)
- Reporta el perfil: Ingresa al perfil -> Ve al menú desplegable -> Denunciar -> Sus tweets son abusivos o incitan al odio -> Publicar información privada -> Marca las opciones con las que te sientas identificada -> Esta información privada pertenece a:
    - A mí o a alguien a quien represento -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).
    - Otra persona -> Agrega hasta 5 tweets a esta denuncia -> Escoge los tweets -> Presiona en agregar -> Listo (Parte superior derecha).

- Bloquea el perfil: Ingresa al perfil -> Ve al menú desplegable -> Bloquear.

Google

- Recopila las pruebas, toma capturas de pantalla de las páginas donde están publicando tus imágenes o contenido.
- Ingresa a https://support.google.com/, en la parte donde pide que "definamos el problema", se sugiere escribir; "Retirar información de Google"- > Te mostrará un menú de varios pasos, ingresa al Paso 2: Tomar medidas -> **Retirar información de los resultados de búsqueda de Google** -> No tengo control sobre la página web-> En la opción 2 te muestra dos opciones,
- 1: Cómo retirar contenido de Google ->
    - Escoge en qué plataforma se difunde el contenido -> Te mostraran las siguientes opciones:
    - Me gustaría informar sobre software malintencionado, suplantación de identidad, divulgación de datos privados u otras incidencias similares.
    - Quiero informar de un blog que suplanta mi identidad.
    - Quiero informar sobre la divulgación de información o imágenes de desnudos.
    - Quiero informar de contenido intimidatorio y acosador ->Listo

Google te mostrará un link donde podrás hacer la denuncia correspondiente.

2. **S**olucionar problemas con la retirada de contenido de páginas de terceros**:** En la sección de: Información personal que retirará Google, te aparecen las siguientes opciones:

   - Retirar de Google imágenes personales explícitas y no deseada
   - Retirar de Google pornografía falsa publicada sin consentimiento
   - Retirar de Google contenido sobre mí de sitios web en los que se llevan a cabo prácticas de retirada de contenido explotador.
   - Retirar de Google información financiera, médica y de identificación nacional.
   - Retirar contenido de "doxxing"; es decir, contenido que expone información de contacto con intención de perjudicar a alguien -> Listo

   Google te mostrará un link donde podrás hacer la denuncia correspondiente.

6. **Ataque de denuncias por contenido no apropiado en redes sociales: intento de censura.**

Esta violencia se refiere al ataque de cuentas personales y perfiles de organizaciones con el intento de censura, ejercido normalmente a medios de comunicación, medios alternativos, artistas, organizaciones y activistas.

Esto no ha sido incluido en el sondeo, por lo tanto no tenemos datos sobre esta violencia. Sin embargo, por la cantidad de casos recibidos con el intento de restringir acciones en redes sociales desde octubre 2019, hemos decidido incluirla en nuestro protocolo.

Ruta crítica para el intento de censura

Ejemplo: Recibes un correo electrónico que dice que tu cuenta en Facebook ha sido temporalmente deshabilitada (3 días, 3 semanas o 6 meses). Aún puedes ingresar a Facebook, publicar y ver las publicaciones de los y las demás, pero tus publicaciones no son públicas.

¿Qué se puede hacer?

- Puedes acompañar a una persona u organización a quien le restringen acceso a publicar aquí algunos consejos.
- Puedes informarte sobre la figura legal en Bolivia
- Puedes denunciar el contenido y el perfil que lo publicó.

a. **Contención psicológica**

Si estás atravesando una situación de violencia

Si quieres acompañar a una amiga

Contáctate con nosotras

¿Te gustaría hablar con alguien? Puedes contactarte con nosotras por WhatsApp, Telegram o Signal al 62342340.

b. **Orientación legal**

Reconociendo la figura legal

En el intento de censura, se ve que en el trasfondo es una vulneración al derecho a la libertad de expresión, el cual se encuentra resguardado tanto a nivel nacional como internacional; a nivel nacional, la Constitución Política del Estado determina el misma en el artículo 106.

A pesar de dicha protección, como todo derecho, se debe tener en cuenta que no es absoluto, que tiene límites; en ese sentido, **están prohibidos los mensajes que inciten al odio o a la violencia**, por lo que no se puede alegar libertad de expresión en mensajes con dicho contenido.

En esta figura el protocolo legal, no sería aplicable, debido que no hay un delito referido a que hayan eliminado un contenido por ser inapropiado. Podría acudirse a otra vía, como la Constitucional, pero la dificultad se establece en el hecho de que será difícil determinar quién realizó la denuncia del contenido, porque finalmente es la plataforma, la que determinará si el contenido es o no eliminado, ello en relación a sus términos de uso.

Preguntas para conocer los hechos

- ¿Cuándo ocurrió la caída del contenido por denuncia?
- ¿En qué plataforma ocurrió la bajada de contenido?

    - Se debe tomar en cuenta que cada plataforma tiene términos de uso, y hay que revisar los mismos, para ver si era o no justificable, bajar el contenido de una publicación.
- ¿Cuál era el contenido del mensaje que ha sido sacado de la plataforma?
    - Como se mencionó, existe un límite a la libertad de expresión, y puede establecerse una línea delgada entre un discurso de protesta y uno que incite a la violencia; dichos criterios son bastante subjetivos, y deben ser analizados caso por caso.
    - Cabe mencionar que en algunos casos, a las personas censuradas, se les puede iniciar algún tipo de proceso, por ejemplo, los relacionados con los delitos en contra de la dignidad humana, vinculados a temas de racismo y discriminación. Sin embargo, muchas veces se inician procesos penales, justamente para hacer más fuerte la censura.
- ¿Sospechas que alguien en específico haya podido realizar la denuncia del contenido?
- ¿Por qué crees que se hizo la denuncia?
- ¿Ha ocurrido antes?
- ¿Además de la denuncia y posterior eliminación del contenido, han ocurrido otras acciones como ser amenazas?
    - Si se realiza la denuncia de un contenido, debido a que por ejemplo es una persona opositora al gobierno, quizás han existido otras acciones, y debe analizarse de manera conjunta.

Para mayor detalle sobre las preguntas para identificar las diferentes figuras legales, puede consultar aquí: Preguntas generales para conocer los hechos.

Si la persona decide hacer una denuncia se puede consultar el paso-a-paso del proceso penal aquí para conocer las acciones a seguir.

c. Orientación tecnológica

Si eres una persona de perfil público, artista, crítica, política, activista, influencer, puedes hacer que tu cuenta personal sea verificada por la plataforma. Esto te da una capa extra de seguridad ante las denuncias de grupos disidentes. Aquí pasos para cada red social.

Facebook

1. Confirmación de identidad en Facebook[23]:

Además de respetar las Condiciones del servicio de Facebook, tu cuenta debe cumplir los siguientes requisitos:

- Debe ser auténtica. Tu cuenta debe representar a una persona, un negocio registrado o una entidad real.
- Debe ser única, debe ser la única presencia de la persona o el negocio que representa. Solo se puede verificar una cuenta por persona o negocio, con excepciones en el caso de cuentas con versiones en distintos idiomas. No verifican cuentas de interés general (por ejemplo, Memes de perritos).
- Debe estar completa, debe estar activa y tener una sección de información, una foto de perfil y al menos una publicación.
- Debe ser notable, esto quiere decir que debe representar a una persona, una marca o una entidad conocida a la que las personas busquen con frecuencia.
- Ten en cuenta que, si proporcionas información falsa o engañosa durante el proceso de verificación, perderás la insignia verificada y quizá tomen medidas adicionales para eliminar tu cuenta.

2. Pasos y enlace para solicitar la verificación

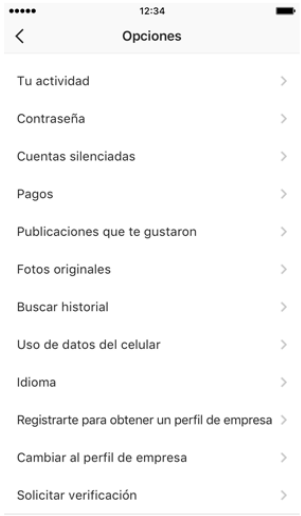
Una vez que el perfil o página esté lista, se debe solicitar la verificación de la insignia Facebook.

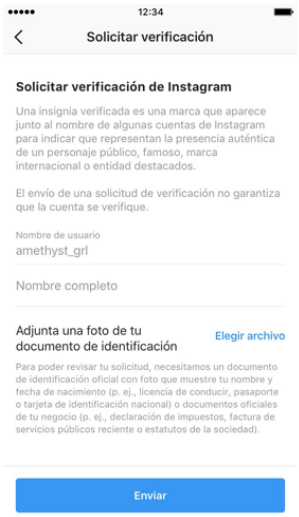
1. Dirígete al enlace oficial para solicitar una verificación azul: https://www.facebook.com/help/contact/342509036134712
2. Selecciona si estás verificando tu perfil personal o una página.
3. Para una página, selecciona la página en el menú desplegable. Para un perfil, proporciona tu enlace de perfil (es decir, https://www.facebook.com/XxxxxXxxxx)
4. Adjunta una identificación oficial emitida por el gobierno (perfil) o declaración de impuestos, documentos de constitución, factura de servicios públicos (página de la empresa o institución).
5. En el cuadro de texto Información adicional, escribe una presentación y la razón convincente de por qué debe verificarse. Aquí debes incluir tu sitio web y enlaces a artículos de prensa relevantes o una página de Wikipedia. Es mejor si mantienes esta información corta y de fácil lectura.
6. Pulsa Enviar y espera de 2 a 30 días para recibir respuesta de Facebook.

---

[23] Facebook. *Servicio de ayuda.* Disponible en: https://www.facebook.com/help/1288173394636262. Consultado: 4/06/2020

Instagram





- Ve a tu perfil -> Vé al menú hamburguesa -> Configuración -> Cuenta -> Solicitar verificación -> Llena el formulario -> Enviar

El formulario es muy sencillo: solo debes agregar tu nombre de usuaria (que se coloca automáticamente), tu nombre completo y adjuntar una foto de alguna identificación oficial que tenga tu foto, fecha de nacimiento y otros datos que corroboren tu identidad. Al enviar la información, Instagram analizará los datos para concluir si se activa o no el membrete de autenticidad.[24]

Al ser propiedad de empresa de Facebook Inc, Instagram tiene los mismos requisitos que los expuestos anteriormente.

Twitter

Actualmente, el programa de verificaciòn de cuentas de Twitter está en pausa, debido a una polémica al haber verificado la cuenta de un supremacista blanco. Aún así, se han registrado cuentas verificadas después de que Twitter anunciara dicha pausa[25].

---

[24] Instagram. 2020. Servicio de ayuda. Disponible en https://www.facebook.com/help/instagram/312685272613322?helpref=uf_permalink. Consultado el 4 de julio de 2020

[25] Marketin4Ecommerce. Jack Dorsey quiere que tú también puedas verificar tu cuenta en Twitter. Disponible en: https://marketing4ecommerce.net/verificar-cuenta-en-twitter/ Consultado del 13 de febrero de 2020

CONTENCIÓN PSICOLÓGICA

Efectos psicológicos de la violencia digital

Las violencias que ocurren en Internet son reales, y como todo tipo de violencia, tiene efectos en la vida de las personas. Es bastante común que se minimicen estas experiencias, porque existe una computadora o un teléfono celular que sirve de mediador entre atacante y víctima, lo que fácilmente nos hace pensar que porque no hay una interacción directa, estos ataques en Internet no lastimarán o no tendrán efectos en las personas que los reciben.

Esta clase de argumentos ignoran o no toman en cuenta, que estos tipos de violencias responden a un orden estructural más grande, como el patriarcado; es decir, la causa de las violencias de género que se viven en las calles, escuelas, trabajos u hogar, es la misma causa de las violencias que ocurren en Internet y que tienen como blanco a las mujeres.

En ese sentido, que personas extrañas tengan acceso a tus cuentas de redes sociales, que revisen tus conversaciones, que te acosen en redes sociales o publiquen un video tuyo sin tu consentimiento, por mencionar algunas formas de violencia digital, representan vulneraciones a la intimidad y a la privacidad y sus efectos pueden ser serios a nivel psicológico y físico.

Efectos psicológicos

- Ansiedad y miedo
- Desprendimiento, como si fuera una extraña en su propia vida.
- Angustia
- Inseguridad, incluso cuando no tiene sentido sentirse de esta manera
- Irritabilidad
- Enfado
- Culpabilidad, vergüenza y culpa de una misma.
- Depresión y desesperanza.
- Vergüenza

• Pensamientos o recuerdos intrusivos y molestos que pueden venir de repente.

• Memoria poco confiable, como dificultad para recordar exactamente detalles.

• Pesadillas e Insomnio

• Suicidio a causa de la revictimizacion o por sentimiento de exposicion.

•Cambio de hábitos

Efectos físicos[26]

• Latidos cardíacos acelerados

• Respiración acelerada

• Náuseas

• Tensión muscular

• Sudoración

• Dificultad para concentrarse

• Tendencia a evitar personas, eventos o situaciones.

Es posible que las personas atacadas por este tipo de violencias puedan sentir algunos de los efectos mencionados, o todos, dependiendo de la gravedad del caso y de los recursos emocionales de cada persona. No todos, ni todas respondemos a la violencia de la misma forma y no todos los casos son iguales.

Sobre la revictimización

Se centra en la culpabilización que es el acto de responsabilizar a la persona por lo que le ha ocurrido, algo muy frecuente en casos de violencia de género y un común denominador de las violencias digitales.

La culpabilización, (culpar a la víctima por lo que ha ocurrido), un aspecto en común en distintos casos de violencia de género, también se observa cuando se habla de violencias

26 Violet Blue. The Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online. Disponible en: https://we.riseup.net/assets/355960/smartgirlsguidetoprivacy.pdf

digitales. Comentarios como “no debiste compartir esta foto” o “es tu culpa por haberte expuesto así en Facebook”, son bastante comunes.

Responsabilizar a la víctima por la violencia que ha sufrido o está sufriendo tiene como efecto la revictimización. Es decir, la persona que está viviendo una situación de violencia, además de afrontar la misma, se enfrenta a que la sociedad, el Estado, amigos/as y familiares le culpen por lo que está pasando o pongan en duda su palabra.

La revictimización incrementa los efectos psicológicos de la violencia, existe mayor angustia, mayores niveles de depresión, y es probable que la persona que sufre la re victimización no denuncie futuros episodios de violencia por temor a no que no le crean.

En ese sentido, es de gran importancia tratar estos casos con mucha empatía. A continuación, veremos algunas formas de poder responder de forma empática y respetuosa en el marco del acompañamiento a una amiga o compañera que esté pasando por una situación de violencia en línea. También veremos algunos consejos de bienestar si es que eres tú la que está sufriendo violencia digital.

Si estás atravesando una situación de violencia

Cuando vivimos algún tipo de violencia, tendemos a culpabilizarnos o responsabilizarnos por lo sucedido: “es mi culpa” o “me lo merezco por…”, y no existe nada más alejado de la realidad, nadie tiene derecho a violentarnos en nuestros espacios digitales ni en ningún otro lugar, la culpa siempre será del agresor y no al contrario.

Situaciones como esta, despiertan un sin fin de sentimientos y emociones, es importante que las escuches y valides. Recurre a tu círculo de confianza cercano, amigos(as) o familiares para poder expresarte. Cuéntales cómo te sientes, qué necesitas, y menciona cómo pueden ayudarte.

Identificar, reconocer, nombrar nuestros sentimientos y malestares físicos, es necesario, muchas veces los negamos, ignoramos o subestimamos por miedo a ser juzgadas, esto a la larga nos produce estrés, ansiedad y tensión emocional etc.

La rabia, el enojo, el miedo y la impotencia, son sentimientos que puedes tener hacia quienes dañaron tu integridad, tienes derecho a sentirte así. Es recomendable darle paso a estas emociones cuando vengan de visita, entendiendo qué son temporales y no llegan para quedarse.

Recuerda que cada persona enfrenta la violencia de forma diferente, no existe una manera "correcta" o " incorrecta" de responder.

Si sientes que estás en peligro, busca ayuda de tus vínculos familiares más cercanos, cuentales la situación y establezcan acciones de seguridad, por ejemplo; mandar ubicación en tiempo real cuando estés camino algún lugar, o avisar cada vez que llegues a tu destino.

Mensajes de Bienestar y Autocuidado

Cuando hablamos de autocuidado, nos referimos a lo que hacemos por nuestra salud física y mental, te dejamos algunos consejos para que los puedas poner en práctica.

1. Intenta descansar y dormir lo suficiente. Si notas que tienes problemas para dormir, intenta realizar ejercicios de relajación antes de acostarte.
2. No te atormentes con pensamientos de cosas que no puedes controlar, enfócate en lo que sí están bajo tu control.
3. Recuerda las estrategias que hayas utilizado en otros momentos de estrés y que te ayudaron. !Usalas ahora¡
4. Aléjate de las redes sociales unos minutos para despejar tu mente y escuchar tus emociones.
5. Todos reaccionamos a las situaciones de estrés de forma diferente, no existe una solo forma de enfrentarse o una forma correcta.
6. Reconoce que a veces es necesario pedir ayuda. No tengas miedo de hacerlo.
7. Puedes buscar grupos u organizaciones feministas, el acompañamiento colectivo muchas veces es poderoso. Compartir nuestra experiencia puede ayudarnos a quitarnos culpas y eso nos fortalece.
8. No te culpes a ti misma, por lo que ha ocurrido, la persona que te ha hecho daño es la única culpable.
9. Es comprensible que no quieras continuar con tus actividades diarias, trata de recuperar tu rutina poco a poco, realiza actividades que te causen satisfacción.
10. Una técnica sencilla que puedes utilizar cuando sientas ansiedad, es mantenerte consciente de tu respiración. Un ejercicio sencillo es el siguiente:

    Inspira profundamente mientras cuentas mentalmente hasta 5, mantén la respiración mientras cuentas mentalmente hasta 4, suelta el aire mientras cuentas lentamente. (Repítelo varias veces hasta que te sientas más relajada).

Si quieres acompañar a una amiga

Si tu amiga está pasando por este tipo de situación, es importante que encuentre en ti un espacio seguro, ya que lo que más se necesita en estos casos es confidencialidad, confianza y validación. También puedes ayudarla a recolectar las pruebas y hacer las denuncias en las plataformas correspondientes. Recuérdale que ella tiene un problema, que no es el problema. Si tu amiga se siente muy angustiada, usar los primeros auxilios psicológicos puede ser de utilidad.

Primeros Auxilios Psicológicos

Son técnicas que se utilizan con personas que acaban de sufrir el impacto de una noticia, un accidente o han sido víctimas de violencia, personas **que están en shock, que se sienten vulnerables y que están tratando de entender lo que les ha ocurrido y las consecuencias de lo que ha pasado.**

La duración de una sesión puede variar de minutos a horas y su objetivo principal es **proporcionar apoyo, facilitar la expresión de sentimientos y emociones, y escuchar y comprender a la persona afectada.**

Es importante tomar en cuenta; ¿Estoy en condiciones?: Es necesaria una auto-evaluación de la condición personal frente a la crisis. Si nos encontramos afectadas por alguna situación personal (ej. duelo, crisis familiar, experiencia traumática reciente), es recomendable no aplicar la contención con otra persona. **De esta manera, evitamos consecuencias negativas sobre nosotras mismas y sobre la persona afectada.**

<u>Tres aspectos importantes de los primeros auxilios psicológicos</u>

1. **Escucha activa:** Es demostrar con nuestro comportamiento que estamos escuchando a la persona que habla. No simplemente estamos oyéndole, sino que estamos entendiendo, comprendiendo, dando sentido a lo que escuchamos.
2. **Qué se debe hacer:** El lenguaje no verbal debe dar el mensaje de que estamos respetando lo que ella nos está diciendo. Hacerle entender que no solo la estamos escuchando para obtener su testimonio, sino que nos importa lo que le está pasando.
3. **Qué no se debe hacer: C**uando alguien nos cuenta algo doloroso no se debe dar la contra. Cuando alguien está comunicando su dolor, no se debe interrumpir esta

expresión pasándole un pañuelo, dándole un vaso de agua, porque se da el mensaje de que queremos que pare de llorar.

Empatía

Es la capacidad de contactar emocionalmente, en este caso, con la víctima. Sería como la habilidad de ser capaces de ponernos en su lugar e intentar llegar a sentir lo que ella siente: Las personas que no están entrenadas para hablar con sobrevivientes de violencia, suelen decir algo equivocado aunque tengan buenas intenciones. Es importante entender que la violencia en línea es igual que la violencia fuera de línea. Las personas sobrevivientes se enfrentan muchas veces a la misma situación de trauma psicológico y se encuentran frente a verdaderos peligros en ambas instancias.

Por lo tanto, es importante hablar **en un entorno seguro, generar confianza, utilizar el respeto, evitar juicios y suposiciones.** No queremos caer en culpabilizar a alguien por lo que está pasando. Muchas veces, sin querer responsabilizamos a una persona que queremos ayudar y no a las personas que le agreden, cuyo comportamiento está normalizado y aceptado por la sociedad.

"Ella tiene un problema, ella no es el problema"

Evita juzgar sus decisiones o presionarla para llevar a cabo acciones como levantar una denuncia, hablar con el agresor, hacer una denuncia pública en redes sociales… Todas estas son opciones válidas, y al acompañar es posible sugerirlas, más no presionar a una opción que consideremos “correcta”.

Respeta que la decisión de hacerlo o no es de ella. En ocasiones, se puede presionar para ayudar o pensando en lo que nosotras desearíamos si nos ocurriera algo similar.

Se debe evitar

- El culpabilizar a la víctima:

  -*¿Por qué hiciste eso?*, *¿Por qué mandaste esa foto?*

- El recriminar:

  -*Deberías habernos contactado antes*; L*a decisión que ha tomado está mal, si no denuncia no le volveremos a ayudar la próxima vez*; *Encima, ¿cómo puede disculpar lo que ha hecho?*; *No sé cómo no se da cuenta*…

- Mostrar indiferencia:

    -*Aunque denuncies, no va a pasar nada*.

- Dar falsas esperanzas.
- Minimizar la situación.

    -*No es para tanto; No te preocupes*.

- Abstenerse de dar consejos:

    -*Yo, en tu lugar*…

- No se debe forzar a las personas a hablar, ni ser intrusiva o agresiva.
- No hacer que repita una y otra vez su testimonio. Puede resultar muy doloroso para ella o él por cuanto se revictimiza.
- Evitar cualquier interrupción, ya sea por llamadas telefónicas o intervención de terceras personas ajenas..
- Acusar a las víctimas: Las personas que atraviesan por esta situación pueden encontrarse con otras personas que minimizan su experiencia o que las acusan de haber estado en situaciones de violencia por estar visibles en línea. Las mujeres tienen derecho a trabajar, jugar y ejercer sus opiniones en línea. Esto no puede usarse como “razón” para excusar la violencia.

Respiración

Algunas personas que han vivido una crisis pueden mostrarse ansiosas o alteradas, sintiendo confusión o encontrándose sobrepasadas por la situación, observándose temblorosas, teniendo dificultades para respirar o sintiendo su corazón muy agitado. Los ejercicios de respiración son necesarios, porque la forma como respiramos modifica nuestras emociones. Cuando exhalamos nos relajamos más que cuando inspiramos.

Ejercicio de respiración

Consiste en inspirar, exhalar y luego esperar un momento con los pulmones vacíos hasta volver a inspirar… lo importante es la pausa luego de vaciar los pulmones.

Para empezar, pídele a la persona que adopte una postura relajada y cómoda, poniendo los pies en el piso y sintiendo ese contacto. Si la persona lo desea o se siente cómoda, puede cerrar los ojos o mirar un punto fijo con la mirada baja.

Acompañamiento

En caso de que estés acompañando un caso, para generar un clima de confianza, puedes utilizar la siguientes frases:

- Muchas gracias por confiar en mí/nosotras y por compartir lo que te esta pasando .
- Eres muy valiente, por tomar la decisión de hablar sobre lo que estás viviendo.
- Hemos asesorado varios casos de violencia digital, haremos todo lo posible para poder ayudarte.
- Siento mucho por lo que estás pasando, se ve que es una situación muy complicada.
- Me imagino que puede ser muy duro vivir una situación así.
- No te preocupes si ahora no sabes bien qué decisión tomar, es es una decisión importante y toma su tiempo.
- Si necesitas hablar en otro momento, estaré aquí para ti.
- Es normal que te sientas asi.
- Tú, no hiciste nada malo, nada justifica el accionar de esta/estas personas.

Si te gustaria hablar con alguien sobre los efectos de la violencia digital puedes contactarte con nosotras por WhatsApp, Telegram o Signal al 62342340.

ORIENTACIÓN LEGAL

A continuación, se hará la descripción de los aspectos legales que son parte de un proceso en relación a una posible vulneración a los derechos digitales. En el protocolo legal se podrán encontrar preguntas para conocer los hechos, el paso-a-paso con instancias judiciales y algunas figuras jurídicas que son descritas con mayor detalle en la guía de ciberbrigadistas.

Lo primero que debe tomarse en cuenta, es que las distintas acciones: técnica, psicológica y legal, por más que tengan sus propios ámbitos de actuación, se relacionan. En el aspecto legal, sobre todo en la primera intervención, existe una estrecha relación con la contención psicológica, porque ayuda a conocer los hechos que han dado lugar a la situación jurídica correspondiente. La contención psicológica es importante para que la persona se encuentre tranquila. También es importante que la persona se sienta en confianza para que se puedan realizar las preguntas y poder contar la experiencia vivida.

Los aspectos desarrollados se constituyen en un panorama general de lo que ocurre en un proceso penal, y tienen la finalidad de que las ciberbrigadistas puedan explicar cuál sería el desarrollo del proceso en el caso de que las mujeres que están acudiendo a ellas decidan iniciar acciones legales.

Es importante que las ciberbrigadistas den a conocer la importancia de que se cuente con una abogada o abogado para que pueda hacer la defensa, porque muchas de las actuaciones requieren del servicio de un profesional de derecho. Por otro lado, es importante mencionar a la denunciante que debe haber un seguimiento a la actuación de la abogada o abogado y que podrá contar con la colaboración de la ciberbrigadista.

Con el conocimiento de estos aspectos legales, se podrá realizar un mejor seguimiento, porque aunque no sea desde una condición de especialista en derecho, el conocimiento del acompañamiento podrá permitir entender mejor los aspectos que se están desarrollando.

Preguntas generales para conocer los hechos

Primero, dejar que relate los hechos, sin ninguna presión para poder identificar las conductas y otros aspectos, tomar nota de aquello que se crea relevante o que se quiera preguntar posteriormente. Durante su relato, procurar identificar a qué figura legal puede referirse e identificar con el mayor detalle posible las acciones y hechos acontecidos.

Algunas de las preguntas que se pueden realizar son:

- ¿Cuándo sucedió el hecho? Se debe tener en cuenta que debemos tener claro el momento en que se inició, y la última vez que dicho acto haya sido realizado (por ejemplo: una mujer que haya recibido amenazas, las cuales empezaron en junio de 2019, pero no les dio importancia, y han continuado, teniendo el último mensaje de amenaza el 20 de mayo de 2020).
- ¿Cada cuánto tiempo suceden los hechos? Servirá para identificar patrones de tiempo.
- ¿Dónde ocurrió el hecho? Para identificar los medios o plataformas en los cuales los actos pudieron realizarse.
- ¿Quién ha realizado el acto? Se debe procurar identificar a la persona que ha realizado la vulneración; esto no siempre será posible, si la persona no sabe exactamente quién cometió el acto, se debe preguntar ¿Sospechas de alguien? ¿Por qué sospechas de esa persona?
- Podría ocurrir que no exista una sospecha concreta, en ese caso, se puede consultar sobre conflictos o roces con personas ¿Has tenido una pelea, discusión o problema con alguna persona? ¿cuándo ocurrieron dichos hechos? Esto servirá para intentar identificar algún tipo de relación, entre el problema

personal o de otra índole, con la vulneración de un derecho digital. Se debe tener cuidado con este último aspecto, y procurar ser lo más objetiva posible, porque en muchos casos serán simples suposiciones las relaciones de causalidad.

- Se debe consultar: ¿ya hubo una denuncia o haz tomado una medida legal?
- Para definir la relación entre el ámbito digital y el no digital: ¿Estos actos se han dado de manera física o material o solo de forma digital? (Por ejemplo, que alguien nos diga que su ex la está amenazando y que lo hace a través de medios digitales, pero también la espera fuera del trabajo).

Cuando deciden hacer una denuncia

Si la persona expresa interés en hacer una denuncia a instancias formales, el seguimiento deberá ser continuo. El primer encuentro serviría para tener un panorama general que luego debe completarse, además sirve para empezar el análisis y tratar de identificar la figura jurídica a la que puede pertenecer. Por lo tanto, deberían coordinar más reuniones.

En los distintos encuentros, se debe poner atención a la coherencia de los relatos, la primera versión no tendría por qué variar drásticamente. Pueden existir nuevos detalles que se hayan ido recordando, pero la historia no tendría que cambiar. También es posible que existan denuncias falsas, los distintos encuentros podrán ayudar a identificarlos.

Será bueno plasmar todos estos cuestionamientos, ya sea a través de una libreta de apuntes, o si es posible, a través de una grabación, siempre que exista el consentimiento, por lo que debe pensarse en hacer un documento de consentimiento y registro. Todo ésta indagación servirá para poder responder:

¿QUÉ PASÓ? ¿CUÁNDO? ¿DÓNDE? ¿QUIÉN LO HIZO?

Estructura del órgano judicial

Es importante que las ciberbrigadistas conozcan la estructura del órgano judicial, para poder explicar de manera genérica a las denunciantes cómo será el proceso judicial en caso de que quieran iniciar medidas legales. Esto es importante para poder visualizar la manera en la que será el desarrollo de la denuncia.

Juzgados Públicos y Tribunales

El órgano judicial tiene 3 grandes instancias. La 1ra instancia, está conformada por los Juzgados Públicos y Tribunales, y estos existen en las distintas áreas del derecho: penal, civil, familiar, laboral, etc.

En la 1ra instancia se desarrollarán la gran parte de los procesos y terminarán con una **Sentencia**. La Sentencia, en caso de que alguna de las partes no esté de acuerdo con ella, puede ser revisada a través de la denominada *Apelación*, donde se solicita que la Sentencia sea revisada por un ente jerárquicamente superior. Las *apelaciones* son revisadas por los Tribunales Departamentales de Justicia.

Tribunales Departamentales de Justicia

Como su nombre lo indica, cada departamento tiene un Tribunal departamental y todas las apelaciones de los distintos juzgados y tribunales de ese departamento, son resueltas por el Tribunal Departamental correspondiente.

El Tribunal Departamental de Justicia, revisará la sentencia y decidirá a través de un *Auto de Vista* si confirma o cambia la Sentencia.

Si uno no está de acuerdo con la decisión del Tribunal Departamental, tiene la posibilidad de otro recurso, que es la *Casación*, que se interpone ante el Tribunal Supremo de Justicia.

Tribunal Supremo de Justicia

Es el mayor órgano de la denominada Jurisdicción Ordinaria, se encuentra en el departamento de Chuquisaca.
Esta instancia resuelve todos los recursos de *casación* provenientes de los distintos departamentos.

A través de un *Auto Supremo,* resuelve los recursos de casación, y a través de los mismos, puede confirmar o modificar la Sentencias y Autos de Vista.

Inicio de procesos en el ámbito penal

Se debe tener en cuenta, que cada área del derecho tiene un procedimiento específico, el cual tiene varios pasos y requisitos. Por dicha amplitud, a continuación se hará referencia solo al proceso penal con una explicación genérica procurando identificar los aspectos más relevantes.

Un proceso penal se puede iniciar por tres maneras:

1. Denuncia: Policía o fiscalía
2. Querella: Fiscal
3. Acción directa de la policía

Denuncia

Se presenta ante la policía o el Ministerio Público (Fiscalía). A continuación se establecen algunos aspectos a tomar en cuenta:

- Puede ser de forma escrita o verbal.
- Si es verbal, se registrará en un formulario.
- Se deja la constancia de la identidad de la persona denunciante, su domicilio, incluyendo un croquis.
- Se puede solicitar la reserva de información, para aspectos de protección.
- Se habilitará el buzón de ciudadanía digital, para que puedan recibirse las notificaciones.
- La denuncia debe contener la relación de hechos, el tiempo, el lugar, la identificación de autores, víctimas y testigos. Para esto, servirá el registro que las ciberbrigadistas tienen gracias al contacto con la denunciante.

Querella

Es presentada ante el Ministerio Público, de manera escrita y debe contener[27]:

1. El nombre y apellido del querellante;
2. Su domicilio real, adjuntando el formulario único del croquis;
3. El buzón de notificaciones de ciudadanía digital del abogado y del querellante si lo tuviera;
4. En el caso de las personas jurídicas, la razón social, el domicilio y el nombre de su representante legal;

[27] Fuente: Art. 290 del Código de Procedimiento Penal

5. La relación circunstanciada del hecho, sus antecedentes o consecuencias conocidas y, si fuera posible, la indicación de los presuntos autores o partícipes, víctimas, damnificados y testigos;
6. El detalle de los datos o elementos de prueba; y,
7. La prueba documental o la indicación del lugar donde se encuentra.

La diferencia principal entre la denuncia y la querella, es que la **denuncia** puede ser presentada por cualquier persona que tenga conocimiento de la comisión de un delito, independientemente de que esté implicada o no; en cambio, la **querella**, puede presentarse solo por la víctima o un representante de la misma y permite que se pueda tener una participación más activa en el proceso.

Acción directa

Hace referencia a actuaciones de los policías. Por ejemplo, que por una investigación policial se tome conocimiento de una red de difusión de pornografía con imágenes que no han sido consentidas para hacerse públicas y se intervenga el lugar de distribución.

Paso-a-paso del Proceso Penal

El proceso penal tiene tres etapas:

1. Investigación preliminar que es parte de la etapa preparatoria
2. Preparatoria: el desarrollo final y la revisión de los actos conclusivos. Se suele denominar etapa intermedia
3. Juicio oral

Investigación Preliminar

- Inicia desde que la policía o el Ministerio Público ha tomado conocimiento del hecho delictivo, es decir, a partir de la presentación de la denuncia o querella.

- A partir de las modificaciones del Código de Procedimiento Penal, realizadas a través de la Ley de modificaciones al Sistema Normativo Penal (Ley 007 del 18-Mayo-2010), se ha establecido que esta etapa debe tener una duración de **20 días.**
- Cada caso tendrá un investigador (policía) y fiscal asignado.
- El investigador asignado al caso deberá realizar las acciones correspondientes como ser tomar declaraciones, realizar el registro de personas, objetos y lugares, recoger y conservar objetos e instrumentos vinculados con el delito, entre otras. Es en esta etapa que las denunciantes deben entregar su celular al investigador como parte del proceso de investigación. Con estas acciones, se permitirá identificar a los presuntos autores, partícipes o cómplices.
- Dichas actuaciones policiales, serán recibidas por el Fiscal y en caso de que se requiera complementarlas, se puede extender el plazo, **no debiéndose sobrepasar los 60 días.**
- En casos complejos dicho plazo puede incrementarse, pero necesariamente debe informarse de aquello al Juez de Instrucción en lo Penal, quien realiza el denominado control jurisdiccional de las actuaciones investigativas.
- Esta etapa concluye con: la **imputación formal** o el **rechazo** de la denuncia o querella.

Preparatoria

- Esta etapa, como su nombre lo indica sirve para preparar el juicio oral a través de la recolección de todos los elementos de convicción para establecer la verdad sobre los hechos. Por lo tanto, se continuarán realizando el proceso investigativo.
- Tiene una duración máxima **de 6 meses.**
- En casos complejos, la o el Fiscal podrá solicitar la ampliación de dicho plazo al Juez de Instrucción, **por un máximo de 18 meses.**
- Esta etapa concluye con la **acusación**, cuando hay fundamentos suficientes para el enjuiciamiento; o el **sobreseimiento** cuando se ha comprobado que el hecho no existió, que no es delito, que el imputado no participó o no se han recabado suficientes elementos para acusar.
- Existe una etapa denominada *Intermedia*, en la cual se procedía a revisar los actos conclusivos. Sin embargo, han existido algunos cambios, pero cabe mencionar, que también es posible aplicar salidas alternativas o iniciar un proceso de conciliación, en los casos que sea posible, o así lo decida la denunciante.

Juicio Oral

- Se considera la fase esencial del proceso. Se realizará sobre la base de la acusación, buscando la comprobación del delito y la determinación de las responsabilidades emergentes.
- Se lleva a cabo a través de audiencias orales, en la que las partes implicadas plantean sus posiciones.
- Es en ésta etapa, en la cual los elementos recabados en la investigación se convierten en **pruebas** a través de su judicialización.
- Ésta etapa se realiza a través de **una autoridad judicial diferente** a la que realizó el control jurisdiccional anteriormente. Así, el juicio oral se sustancia ante un Juzgado de Sentencia o ante un Tribunal de Sentencia.

Información legal adicional de interés

Delitos públicos de materia penal

De los delitos identificados en la Guía, a excepción de algunos que se mencionan a continuación, todos se desarrollan en el juicio oral en los Juzgados de Sentencia.

- Los delitos de trata de personas (Art. 281 bis del Código Penal), tráfico de personas (Art. 321 bis del Código Penal) y pornografía (Art. 323 bis del Código Penal) serán conocidos en juicio oral por los Tribunales de Sentencia.
- Los Tribunales de Sentencia, se componen de 3 jueces técnicos, por lo que actualmente se ha eliminado la figura de los jueces ciudadanos.
- Ya sea el Juez o Tribunal de Sentencia, dictará una **Sentencia**, la cual puede ser **absolutoria** donde se declara inocente al procesado o **condenatoria** donde se declara la culpabilidad.

Recursos legales

- Apelación que serán conocidos por los Tribunales Departamentales de Justicia
- Casación, que será resuelto por el Tribunal Supremo de Justicia.
- Cada uno de ellos, tiene sus plazos y un procedimiento específico.

Medidas de protección

- Existen medidas de protección que pueden ser solicitadas y se aplicarán dependiendo de las características del caso. También se disponen medidas de protección especiales en el caso de mujeres.

Pruebas

- Existen distintos medios de prueba. Pueden ser documentales, testificales, periciales (trabajo de expertos en cierta área, en este caso podría ser informáticos, que emiten un determinado informe), reconocimiento de personas, reconstrucción de hechos, entre otros.
- Los medios de prueba, dependen de la naturaleza del caso.
- En este caso, se debe procurar los medios de prueba que se tengan sean resguardados, por ejemplo, a través de capturas de pantalla.
- Se debe mencionar que en algunos casos, cuando se esté realizando la investigación, se podrán requerir de algunos medios, como ser el celular o la computadora, para recabar elementos que puedan servir como pruebas, realizando las pericias informáticas que correspondan.
- De igual manera, se puede solicitar que un Notario, pueda dar fe de un documento electrónico, según los establece el Artículo 19, inciso J[28] de la Ley del Notariado Plurinacional (Ley 483).
- Dichos medios de prueba servirán para poder demostrar la responsabilidad de la persona a la cual se la está procesando penalmente.

ORIENTACIÓN TECNOLÓGICA

Consideramos que Facebook, Google y otras redes sociales privativas no son espacios de libertad de expresión, acceso a información, ni permiten el ejercicio de nuestros derechos o libertades plenamente, por lo tanto, nos gustaría invitarte a reflexionar sobre tu presencia en dichas plataformas…

La smartphonización de la vida

Sin ánimo de alarmarse, vale la pena reconocer que el hecho de que toda nuestra información esté concentrada en un mismo lugar, es un riesgo. Esto significa que basta un solo ataque para acceder a la totalidad de nuestras vidas digitales. Existen varios motivos (comodidad, falta de conocimiento, etc.) por los que se suele tratar como uno, a un dispositivo que es un ensamblaje de muchos otros: cámara, mapa, agenda, bolígrafo, calendario, calculadora; que tienen una utilidad en nuestro cotidiano, pero que además

[28]: Ley de Notariado Nacional. 2014. https://bolivia.infoleyes.com/articulo/74959. Consultado el 8 de agosto de 2020.

están conectados a Internet, estableciendo una localización precisa y recolectando información sobre nuestros comportamiento y hábitos.

Son 5 verificaciones de donde estamos, dando como resultado una ubicación cada vez más exacta. Esto nos hace pensar en una dimensión social de los teléfonos inteligentes, más allá de su aspecto tecnológico, **pues al ser tantos dispositivos en uno, supone que estaremos más tiempo con ellos, y que más de nuestras interacciones sociales pasarán por allí.**

La seguridad de nuestros dispositivos es la última barrera entre nosotrxs y quien realice algún tipo de ataque en nuestra contra, ya que si hay un ataque a un dispositivo personal, quiere decir que la identidad de su propietaria y/o ubicación, probablemente han sido determinadas, y a la vez, que es posible que conozcamos a nuestrx atacante.

En este orden de ideas, reconocemos 3 actores, que por distintos motivos perpetúan y promueven las violencias digitales a mayor escala. A continuación, los presentamos destacando una de tantas características que los convierten en factores determinantes en la existencia de las violencias digitales.

- El Estado, al no implementar políticas que conduzcan hacia la reducción de la brecha digital. Es responsable del desconocimiento en el manejo y acceso a tecnologías de la información, que afecta principalmente a mujeres mayores del área rural[29].

- Las corporaciones de redes sociales y apps de mensajería, ya que no permiten que las denuncias de violencias ocurridas en su interior, sean tratadas con celeridad o reportadas fácilmente. En el mismo sentido, la estructura misma de estas plataformas permite que dichas violencias se magnifiquen y expandan sin control por sus algoritmos. Si alguna vez te has propuesto a denunciar un contenido en alguna plataforma privativa, sabrás de qué estamos hablando.

- El patriarcado, como paradigma civilizatorio, es el caldo de cultivo propicio para formar trolls que personifican el machismo, por lo que destaca una particular insensibilidad al momento de crear un contenido, acceder a él o difundirlo, generando altas cifras de violencias digitales, dirigidas específicamente a mujeres y otras expresiones de sexo y género no binarias, de todas las edades.

[29] Mercado Andira, Karen; Bazoberry Chali, Oscar. 2019. https://www.sudamericarural.org/images/impresos/archivos/Acceso-a-internet-y-Ruralidad-Machareti.pdf.Conusltado: 8 de agosto de 2020.

A menudo, no se piensa en cómo podría sentirse la persona a quien el contenido busca perjudicar, o quizás no importa. Además, son ejercicios que se refuerzan por las prácticas de relaciones tóxicas; y el castigo (pornovenganza) está "plenamente justificado", por lo que un contenido puede ser difundido como una suerte de respaldo a la fratría (orgullo masculino) con la que se genera una identificación activa.

Retomando, ahora que hemos identificado a algunos de los actores en la larga lista de perpetradores y promotores de violencias digitales, veamos algunas estrategias de prevención.

Paso-a-paso de la orientación tecnológica

Este apartado está dividido en tres: **acciones preventivas** con consejos para enfrentar las violencias digitales más comunes identificadas en el sondeo a 1000 mujeres bolivianas y las configuraciones de seguridad y privacidad en redes sociales y apps de mensajería; **acciones reactivas**; **consejos de cuidado físico en nuestra interacción con la tecnología**. Estas tres están divididas para que se puedan ejecutar acciones en Facebook, WhatsApp, Instagram, Twitter, Telegram y Messenger.

Acciones preventivas

En general, las configuraciones de privacidad y seguridad en las plataformas de redes sociales son muy parecidas. Recomendamos que se revisen estas configuraciones en cada una de las cuentas en redes sociales y apps de mensajería. En promedio, y dependiendo de la familiaridad con las plataformas, esto tarda de 15 a 30 minutos.

Las configuraciones de privacidad y seguridad se modifican con frecuencia y sin notificación, por lo que es necesario revisar estas configuraciones, **con la misma regularidad que se hace la limpieza profunda de la casa.** A continuación, mostraremos características de las configuraciones de seguridad y privacidad de las plataformas más usadas y posteriormente el paso-a-paso, de acuerdo a cada plataforma, para activar estrategias de seguridad digital preventivas.

Las **configuraciones de privacidad**, son la suma de características que damos a nuestras cuentas en redes sociales o plataformas web, que determinan la información personal que tenemos de manera pública en nuestros perfiles.

Presentamos una lista general de las configuraciones de privacidad que pueden modificar en los perfiles de redes sociales. El paso-a-paso para las configuraciones de privacidad se encuentra más adelante.

- Revisa quién puede ver la información personal del perfil (foto de perfil en el caso de WhatsApp o número de celular en Facebook): Todo el mundo, amigos de amigos, amigos o nadie.

- Se puede limitar el acceso a información personal como: número de celular, cumpleaños, cuidad de origen, estudios, lista de amigos, gustos y páginas a las que sigues; limitar las publicaciones anteriores, perfiles bloqueados, etc.

- Protege la cuenta con una contraseña fuerte, verificación de dos pasos y alertas de inicio de sesión de dispositivos no conocidos.

- En Telegram, oculta tu número de celular de manera que sólo el nombre de usuaria (@nombre) sea visible. Recomendamos que si es necesario empezar un una conversación en alguna app de mensajería con un desconocido o desconocida sea en Telegram, tomando en cuenta que puedes ocultar tu número de celular .

- Revisa quienes pueden enviar solicitudes de amistad en Facebook.

- En Facebook, configura la privacidad de las cuentas para que los motores de búsqueda fuera de esta red social no vinculen tu nombre con tu perfil en Facebook.

- Revisa si el correo electrónico y celular asociado a los perfiles en redes sociales son públicas, esto puede contribuir a identificar a una persona con facilidad.

- Mira las apps que acceden a información personal mediante Facebook, Google u otras: Pedidos Ya, Tinder, etc.

- Considera necesario tener el reconocimiento facial, ubicación, registro de actividad, entre otra información personal activada en redes social como en tus dispositivos.

Las **configuraciones de seguridad,** son las características en las redes sociales o plataformas que ajustamos a nuestras necesidades como medidas de prevención y alerta en caso de ser atacadas.

Más adelante detallaremos los pasos para mejorar las configuraciones de seguridad en cada plataforma. Para resumir la información, aquí les dejamos una lista corta de los

aspectos generales a tomar en cuenta cuando configuran los aspectos de seguridad en sus redes sociales

- Habilitar la autenticación de dos pasos.
- Revisar si aún se tiene acceso a los correos electrónicos que están asociados a tu perfil de la red social. Si no tienes acceso a ellos, elimínalo. Si aún tienes acceso a ellos, **¿cuándo fue la última vez que cambió la contraseña?** Actualízalo con una contraseña alfanumérica, de al menos 10 caracteres y única.
- Al igual que los correos, revisa si tienes acceso al número de celular asociado a tu perfil. Si aún tienes ese número en tu posesión, activa la autenticación de dos pasos. Si no tienes ese número en tu posesión, elimínalo.
- Observa si todos los dispositivos conectados a tu cuenta son tuyos. Si no lo son, toma una captura de pantalla de los dispositivos desconocidos, elimínalos y cambia la contraseña de tu cuenta.
- Elige a amigos para contactar en caso de que pierdas el acceso a tu cuenta.

<u>Consejos de prevención a violencias digitales basados en el sondeo a 1000 mujeres bolivianas</u>

1. No hables con extraños, ni agregues a perfiles falsos. 200 mujeres de 1000 encuestadas dijeron ser contactadas por medios digitales con mentiras para ser abusadas física, psicológica o sexualmente.
2. Cuídate de las personas que quieren mirar conversaciones privadas. Nadie tiene derecho a ver estas conversaciones sin tu permiso, no porque estés escondiendo algo, sino porque **es parte de tu privacidad**. Más de la mitad de las mujeres que respondieron al sondeo manifestaron que les borraron información de sus redes personales, o fueron obligadas a borrarla. Esto incluye conversaciones, fotos o personas (eliminar contactos de Facebook, por ejemplo), esta pregunta sitúa a la violencia en el círculo cercano a la víctima. Se trata de una forma de monitoreo y acecho.
3. Contesta mensajes cuando gustes. Nadie tiene derecho a obligarte a contestar inmediatamente. 855 de 1000 mujeres encuestadas dijeron que las personas con las que están chateando se enojan porque no les contestan con prontitud.
4. Ten control de tus perfiles en redes sociales, nadie puede obligarte a publicar, agregar amigos, presionarte a enviar contenido erótico (365 de 1000 dijeron que estuvieron en esta situación) u otros. Las cuentas en redes sociales son la representación en la vida digital. Es como si alguien dijera lo que debes hacer con tu cuerpo.
5. Prepárate para una respuesta tardía de las plataformas de redes sociales. Es común que estas no respondan de manera pronta y oportuna a la denuncia de

contenido ofensivo. 539 mujeres encuestadas de 1000 denunciaron sin respuesta. Esto evidencia el poco interés de estos actores para tomar acciones en contra de la violencia digital experimentada.

Consejos anti-acoso

WhatsApp

- No contestar llamadas de desconocidos.
- Configura los parámetros de privacidad y seguridad para limitar la cantidad de información que das a desconocidos.
- Busca tu número en Facebook y otros buscadores, para asegurarte de que el número no sea de fácil acceso para cualquier persona.
- Configura quién puede agregarte a grupos de Whatsapp
    - Menú desplegable de WhatsApp (3 puntos a mano derecha superior) -> Ajustes -> Privacidad -> Grupos -> Seleccionar Quién puede añadirte a los grupos.

Facebook y Messenger

- Generalmente los perfiles falsos, porque fueron creados recientemente, tienen poco contenido y puedes ver su fecha de creación, después de unos minutos revisándolos.
- Facebook y Messenger tienen un buzón de ayuda para hacer seguimiento a la cuenta que reportaste, para consultar el estado del reporte, pulsa aquí: https://www.facebook.com/support/
- Configura los parámetros de privacidad y seguridad.

Instagram

- Configura los parámetros de privacidad y seguridad en https://www.instagram.com/accounts/privacy_and_security/ para limitar la cantidad de información que das a desconocidos.
- Puedes configurar una cuenta como privada para evitar recibir mensajes molestos. Ingresa a tu perfil -> Haz clic en el menú hamburguesa (3 rayas en la parte superior derecha) -> Ingresa a Configuración -> Privacidad -> Privacidad de la cuenta -> Activa la Cuenta Privada.

Telegram

- No contestar llamadas de desconocidos.
- Configura los parámetros de privacidad y seguridad para limitar la cantidad de información que das a desconocidos.
- Busca tu número de celular en Facebook y otros buscadores para asegurarte de que el número no sea de fácil acceso para cualquier persona.
- Configura quién puede agregarte a grupos:
    - Menú hamburguesa -> Ajustes -> Privacidad y Seguridad -> Grupos y canales
        - ¿Quién puede añadirme?
            - Todos
            - Mis contactos
            - Añadir excepciones: Los usuarios que añadas en estas listas, serán la excepción a las reglas de arriba
                - No permitir -> Añadir usuarios

Twitter

- Se puede configurar una cuenta para que sea privada y elegir quienes pueden seguirla ingresando al panel de Privacidad y Seguridad disponible en https://twitter.com/settings/safety.
- Se pueden denunciar perfiles y mensajes y elegir bloquear a los perfiles que envían dichos mensajes.

Consejos anti-hackeo

- Tener acceso a las cuentas de correo electrónico y el número de celular asociado al perfil.
- Cambiar contraseñas, al menos una vez al año. Las mejores contraseñas son una mezcla de números, letras, contienen al menos 10 caracteres y no tienen información personal.
- No permitas que nadie tenga acceso, ni instale apps en tus dispositivos. Con esto nos referimos al momento en que compramos un smartphone y empezamos a usarlo. Es requerido que ingresemos información personal, registrar el equipo, activar algunas configuraciones, etc. Hemos identificado que algunas personas prefieren darle el dispositivo a su pareja para que configure el dispositivo, es así que se inicia el primer riesgo, ya que en este proceso se establecen contraseñas y

se da acceso a cuentas de correo electrónico. Si no conocemos estos detalles, no podremos recuperar las cuentas o dispositivos en caso de hackeo.

- No permitas que terceros configuren tus perfiles en redes sociales. Esto se refiere al momento de la creación de un perfil personal o de la configuración de privacidad y seguridad. Recomendamos que se tenga conocimiento pleno de estos aspectos para poder recuperar la cuenta en caso de hackeo.
- Para personas que no quieren perder su información, pueden hacer un respaldo: Menú hamburguesa -> Seguridad -> Descarga información -> Ingresa tu correo electrónico -> Tu información (fotos, comentarios, información de perfil, etc.) será enviada en 48 horas a tu correo.

Aquí una lista de acciones preventivas que puedes tomar en redes sociales, apps de mensajería y gmail.

Facebook

- Configura las opciones de seguridad en Facebook. Puedes ingresar pulsando: https://www.facebook.com/settings?tab=security o ve al menú hamburguesa -> Configuración y privacidad .> Configuración -> Seguridad e inicio de sesión:
  - Ver todos
  - Salir de todas las sesiones
  - Autenticación de dos pasos -> Usar la autenticación de dos pasos:
    - Para la versión con aplicación: Descarga DuoMovile ->
      - En Facebook, una vez descargada la aplicación, te aparecera un codigo QR, entra a -> Configurar en el mismo dispositivo.
      - DuoMovile mostrará un código que debe ser ingresado en Facebook después de darle continuar. Ahora la autenticación de dos pasos está activada. Cada vez que inicies sesión desde un dispositivo desconocido, Facebook te pedira un codigo que será emitido por DuoMobile -> Listo.
    - Para la versión con mensajes de texto (sms): Facebook pedirá ingresar o verificar el número de celular -> Te mandará un mensaje de texto con un código que deberás ingresar en la casilla correspondiente -> Ahora la autenticación de dos pasos está activada. Cada vez que inicies sesión desde un dispositivo

desconocido, Facebook te enviará un código a tu celular -> Listo.

WhatsApp

- Revisa si la cuenta está abierta en otros dispositivos (para Android):
  - En la barra de notificaciones, revisa si existe alguna que diga “WhatsApp Web está actualmente activo”
  - Ingresa a WhatsApp -> Ve al menú desplegable -> WhatsApp Web -> Revisa los dispositivos en los que se inició sesión, si no reconoces alguno -> Pulsa encima del dispositivo -> Cerrar Sesión.
  - Si al abrir WhatsApp aparece el mensaje de verificar tu número -> pulsa en Confirmar -> Ingresa tu número de WhatsApp

- Revisa si la cuenta está abierta en otros dispositivos (para iOS):
  - En la barra de notificaciones, revisa si existe alguna que diga “WhatsApp Web está actualmente activo”.
  - Ingresa a WhatsApp -> Ve a Ajustes o Configuración -> WhatsApp Web -> Revisa los dispositivos en los que se inició sesión, si no reconoces alguno -> Pulsa encima del dispositivo -> Cerrar sesión.
  - Si al abrir WhatsApp aparece el mensaje de verificar tu número, esto quiere decir que tu cuenta está abierta en otro celular, para cerrarla -> pulsa en Confirmar -> Ingresa tu número de WhatsApp -> Ingresa el código de seis dígitos, y automáticamente se cerrará la sesión en el otro dispositivo y se abrirá en el que usas actualmente.

Gmail

Para ingresar a las configuraciones de seguridad, pulsa aquí https://myaccount.google.com/?utm_source=OGB&utm_medium=act o ingresa a la cuenta que deseas configurar -> Haz clic sobre la foto de tu perfil -> Gestiona tu cuenta de Google -> Seguridad -> Asegura tu cuenta ->

- Desvincula los dispositivos inactivos que están asociados a tu cuenta.
- Iniciando tu sesión desde otros dispositivos -> Habilita la verificación de dos pasos -> Sigue las instrucciones si tienes tu celular a la mano para recibir códigos de seguridad y habilitar la verificación de dos pasos.

Es posible que las cuentas en los dispositivos vinculados se hayan des-sincronizado cuando se completa este paso. Por eso es importante saber las contraseñas para poder volver a acceder a las cuentas que fueran des-sincronizadas.

- Revisa las últimas actividades que realizaste ingresando a: https://myaccount.google.com/security

    - Actividad de inicio de sesión. Ingresa a: https://myaccount.google.com/device-activity -> Revisa si algún dispositivo desconocido a los que usas tienen acceso a tu perfil. Para desvincular -> presiona sobre los 3 puntos -> Cerrar sesión.
    - Mejora tu contraseña -> Ingresa la contraseña actual y una nueva.
    - Habilita la autenticación de dos pasos -> Mensaje de texto -> Ingresa el código enviado a tu número de celular -> Listo.

Instagram

- Para revisar las últimas actividades que realizaste puedes ingresar aquí: https://www.instagram.com/session/login_activity/. Si se accede desde un móvil o tablet pulsa sobre el Menú hamburguesa -> Seguridad ->
    - Actividad de inicio de sesión -> Revisa si algún dispositivo desconocido a los que usas tienen acceso a tu perfil. Para desvincular -> presiona sobre los 3 puntos -> Cerrar sesión.
    - Contraseña -> Ingresa la contraseña actual y una nueva.

- Confirma tener acceso al número de celular y correo electrónico asociado a la cuenta. Pulsa aquí: https://www.instagram.com/accounts/edit/. Si se accede desde un móvil o tablet pulsa sobre el Menú hamburguesa -> Seguridad -> Editar perfil.
- Habilita la autenticación de dos pasos. Pulsa aquí: https://www.instagram.com/accounts/edit/. Si se accede desde un móvil o tablet, pulsa sobre el Menú hamburguesa -> Privacidad y seguridad - Autenticación en dos pasos -> Envía código a celular -> Ingresa el código-> Guarda los códigos de respaldo en caso de no poder recibir mensajes de texto al número de celular asociado.

Telegram

Para evitar el ingreso a tu cuenta de Telegram, o que se abra la sesión en otros dispositivos se recomienda lo siguiente:

- Código de bloqueo -> Al activar esta opción  Cada vez que entres a la App de Telegram se te pedirá el PIN que configures -> Ingresa un PIN -> Confirma el PIN.

        - *Nota: SI te olvidas el PIN de bloqueo, será necesario que desinstales Telegram y lo vuelvas a instalar. Debido a que tenías el bloqueo de PIN activado, se borrarán todos los chats secretos.*
    - Cambiar código: Si ya lo tienes configurado, puedes cambiar el PIN
    - Desbloquear con huella digital
    - Autobloqueo -> Telegram se bloqueará con PIN automáticamente, transcurrido el tiempo que elijas.
- Verificación en dos pasos: Cuando se inicia sesión en un nuevo dispositivo, se requerirá ingresar la contraseña para verificar la identidad de la dueña.o de la cuenta. -> Ingresa una contraseña -> Confirma la contraseña -> Ingresa una pista para tu contraseña -> Ingresa tu correo electrónico: *Te llegará un código de verificación a tu bandeja de entrada, si no, revisa la carpeta de Spam.* -> Ingresa el código en la App.
- Sesiones Activas
    - Sesión Actual: Te mostrará la informaciòn del dispositivo que estés usando en ese momento.
    - Cerrar todas las sesiones: Puedes cerrar las sesiones de todos los dispositivos donde usaste Telegram, excepto el que estés usando para realizar este proceso.
    - Sesiones activas: Te aparecerá una lista donde estarán todos los dispositivos donde utilizas Telegram, si no reconoces algún dispositivo presiona encima del nombre -> Cerrar Sesión.

Twitter

Para que solo tu puedas iniciar sesión en otros dispositivos, habilita la autenticación en dos fases:

-  Presiona en tu foto de perfil en la parte superior izquierda -> Configuración ->Cuenta ->Autenticación en dos fases
    - Mensaje de texto -> Comenzar -> Inserta tu contraseña -> Enviar código (*Si no tienes agregado tu número de celular, vincula este a tu cuenta*) -> Ingresa el código -> Listo, al finalizar te mostrará un código en caso de que no puedas iniciar sesión.
    - App de autenticación -> Ingresa tu contraseña -> “Link the App” *Si no tienes una app de autenticación, descarga Duo Mobile u otra App* -> En Twitter: Ingresa el código que te da la aplicación -> Entendido.
    - Llave de seguridad (*Solo funciona para navegadores*)

En caso de que alguien quiera restablecer tu contraseña, sin tu autorización puedes pedir una confirmación a tu celular

-  Presiona en tu foto de perfil en la parte superior izquierda -> Configuración ->Cuenta ->Protección de restablecimiento de contraseña -> Marca la casilla para confirmar con el número o correo electrónico cada vez que se restablezcas la contraseña

Para revisar en qué dispositivos está iniciada tu sesión, puedes seguir los siguientes pasos:

-  Presiona en tu foto de perfil en la parte superior izquierda -> Configuración ->Cuenta ->Aplicaciones y sesiones
    - Aplicaciones: Aparecerán listadas todas las aplicaciones que estén vinculadas con la cuenta de Twitter, si no se reconoce algún dispositivo, pulsa el menú desplegable al lado de la aplicación -> Revocar acceso.
    - Sesiones: Primero aparecerá el dispositivo que se está usando en ese momento.
        - Cerrar todas las sesiones -> Cerrar sesión.
        - Verás un listado de los dispositivos donde iniciaste sesión.
            - Para cerrar sesión en un dispositivo -> ve al menú desplegable al lado del dispositivo -> Cerrar la sesión que se muestra -> Cerrar sesión.

Consejos anti-amenazas

Facebook

Se pueden configurar la siguientes opciones para limitar el contacto con personas desconocidas. Puedes ingresar pulsando aquí: https://www.facebook.com/settings?tab=privacy

Si se accedes desde un móvil o tablet, pulsa sobre el Menú hamburguesa -> Configuración y privacidad -> Configuración -> Privacidad ->

- ¿Quién puede enviarte solicitudes de amistad? -> Elige la opción que prefieras
    - Todos
    - Amigos de amigos
- ¿Quién puede ver tu lista de amigos? -> Elige la opción que prefieras
    - Público
    - Amigos
    - Amigos excepto ...
    - Amigos concretos

    - Solo yo
- ¿Quién puede buscarte con la dirección de correo que proporcionaste? -> Elige la opción que prefieras
    - Todos
    - Amigos de amigos
    - Amigos
    - Solo yo
- ¿Quién puede buscarte con el número de teléfono que proporcionaste? -> Elige la opción que prefieras
    - Todos
    - Amigos de amigos
    - Amigos
    - Solo yo
- ¿Quieres que los motores de búsqueda fuera de Facebook se vinculen con tu perfil? -> Si esta opción está activada, quiere decir que si alguien en el buscador de Google, DuckDuckGo, Startpage, etc. inserta tu nombre, podrá encontrar tu perfil de Facebook.

Messenger

Desactiva los mensajes de personas desconocidas o que no tengas como seguidores o amigos en la red social, los mensajes de estas personas irán a la bandeja de solicitud de mensajes.

- Solicitudes de mensajes: En esta sección se mostrarán todos los mensajes que te hayan enviado personas que no estén en tu lista de contactos.

WhatsApp

Pon la foto disponible sólo para tus contactos, estado y ultima vez conectada en sólo amigos o privado. La configuración de privacidad y seguridad no es posible desde el WhatsApp Web, por lo tanto es necesario configurar estas opciones desde el móvil.

- Para ingresar a los ajustes, abre la aplicación, ve a la parte superior derecha de la pantalla -> Configuración
-  Para ingresar a los ajustes, ve al menú desplegable en la parte superior derecha de tu pantalla -> Ajustes
    - Cuenta
        - Privacidad

- Hora de últ. vez: Elige quién puede ver la última hora de tu conexión.
    - Todos (*Cualquier persona que tenga tu número de celular, aunque tú no la tengas en tu lista de contactos*)
    - Mis contactos
    - Nadie
- Foto del perfil: Elige quién puede ver tu foto de perfil
    - Todos (*Cualquier persona que tenga tu número de celular, aunque tú no la tengas en tu lista de contactos*)
    - Mis contactos
    - Nadie
- Info: Elige quién puede ver la info (*El mensaje pequeño que sale bajo tu foto de perfil*)
    - Todos (*Cualquier persona que tenga tu número de celular, aunque tú no la tengas en tu lista de contactos*)
    - Mis contactos
    - Nadie
- Estado: Elige quién puede ver tus estados
    - Mis contactos
    - Mis contactos, excepto… (*Escoge los contactos que no quieres que vean tu estado*)
    - Solo compartir con...(*Escoge los contactos que quieres que vean tu estado*).
- Confirmaciones de lectura -> Activa o desactiva  si deseas que otras personas sepan que viste sus mensajes (*Al activar esta opción tampoco podrás ver si vieron tus mensajes*).
- Grupos: Elige quién puede agregarte a grupos
    - Todos
    - Mis contactos
    - Mis contactos, excepto…(*Elige los contactos que no pueden añadirte a grupos*).

Instagram

- Se puede elegir quienes siguen, comentan y escriben a la cuenta personal en Instagram pulsando aquí: https://www.instagram.com/accounts/privacy_and_security/. Si se accede desde un móvil o tablet, pulsa sobre el Menú hamburguesa -> Privacidad y seguridad -> Privacidad -> Editar configuración de comentarios:

- Filtro de comentarios: Agrega palabras o frases para que éstas sean ocultadas en las publicaciones.
- Usar palabras clave predeterminadas: Oculta las publicaciones con comentarios que incluyan palabras clave que se suelen reportar como ofensivas.

- Toma un descanso de Instagram. Inhabilita temporalmente la cuenta en: https://www.instagram.com/accounts/remove/request/temporary/. Si se accede desde un móvil o tablet, pulsa sobre el Menú hamburguesa -> Privacidad y seguridad -> Privacidad -> Editar perfil -> Inhabilita temporalmente mi cuenta -> Selecciona las razones -> Inhabilitar cuenta temporalmente.

- Restringe a la cuenta: Limita las interacciones no deseadas sin necesidad de bloquear o dejar de seguir a personas que conoces.
  - Busca el perfil de la persona -> Menú desplegable -> Restringir. Podrás controlar si otra persona puede ver nuevos comentarios en tus publicaciones. Sus chats se moverán a "Solicitudes de mensajes", por lo que no verá si leíste sus mensajes.

  - Bloquea a la cuenta: No podrá encontrar tu perfil, publicaciones ni historias en Instagram. Instagram no le avisará a esta persona que la bloqueaste.
    - Busca el perfil de la persona -> Menú desplegable -> Bloquear.

  Para configurar desde la computadora ingresa a: https://www.instagram.com/accounts/privacy_and_security/
  - Etiquetas:
    - Aprobar etiquetas manualmente : te ayuda a revisar las publicaciones donde te etiquetan.
  - Estado de actividad -> Las personas con las que te conectaste mediante mensajes en Instagram pueden ver cuando fue la última vez que usaste la aplicación
  - Privacidad de la cuenta -> Al activar esta opción, solo las personas que tú apruebes podrán ver tu perfil.

  - Cuentas restringidas -> Si no quieres bloquear, o dejar de seguir a algunas cuentas, puedes añadir a estas personas a la lista, por ejemplo: los mensajes que te manden se moverán a la carpeta de solicitudes de mensajes, por lo que no sabrán si leíste o no su mensaje.

- Cuentas bloqueadas -> Te aparecerá la lista de personas que bloqueaste. -> Para bloquear una cuenta ve a su perfil -> Ve al menú desplegable -> Bloquear.
- Cuentas silenciadas -> Te aparecerá la lista de personas que Silenciaste. Para bloquear una cuenta, ve a su perfil -> Presiona en "*Siguiendo"* -> Silenciar
  - Publicaciones
  - Historias

Twitter

Puedes tomar las siguientes recomendaciones para proteger tu cuenta de Twitter.

- Ingresa a Privacidad y seguridad pulsando aquí https://twitter.com/settings/safety. Si se accede desde un móvil o tablet pulsa sobre el Menú hamburguesa -> Configuración y privacidad -> Privacidad y seguridad ->
  - Protege tus tweets: Para mostrar los tweets publicados sólo a las cuentas que te siguen. Al activar esta opción, las personas que no siguen la cuenta tendrán que enviar una solicitud.
  - Etiquetado de fotos ->
    - Cualquiera te puede etiquetar
    - Solo las personas a las que sigues te pueden etiquetar
    - Desactivado
  - Mensajes Directos
    - Recibir solicitudes de mensajes -> Al activar esta opción, podrás recibir mensajes de cualquier usuario de Twitter, incluso si no lo sigues.
    - Mostrar confirmaciones de lectura
  - Visibilidad y contactos
    - Permite que otros te encuentren por tu correo electrónico.
    - Permite que otros te encuentren por tu número de teléfono.
    - Sincronizar contactos de las libreta de direcciones: Si se marca esta opción, Twitter sincronizará automáticamente los contactos de tu celular para que puedas seguirles. Esto es solo posible si vincularon sus números con sus cuentas.
    - Eliminar todos los contactos: borrará toda la información de los contactos anteriormente sincronizados.

Telegram

- Esconde tu número de teléfono: Ingresa a la app de Telegram -> Pulsa al menú hamburguesa-> Configuración -> Privacidad y seguridad -> Número de celular:
    - Quién puede ver mi número de celular:
        - Todos
        - Mis contactos
        - Nadie
    - Quién puede encontrarme con mi número de celular:
        - Todos
        - Mis contactos
    - Agrega excepciones
        - Permite a: contactos y grupos. Esto anulará las configuraciones anteriores.
- Asigna un nombre de usuario a tu cuenta. Ingresa a la app de Telegram -> Pulsa al menú hamburguesa-> Configuración -> Nombre de usuario -> Crea un alias. Esta opción permite que terceros puedan encontrarte en Telegram a través de éste alias.

Consejos anti-doxxing

Un paso importante cuando se exponen nuestros datos personales, es buscar si es que los mismos se encuentran publicados en otras plataformas, para esto se pueden utilizar distintos motores de búsqueda como Google, DuckDuckgo, Startpage con el objetivo de prevenir o tomar medidas para eliminar u ocultar **esos datos que pueden ponernos en peligro.**
Una forma sencilla de empezar con este proceso, es buscar los siguientes datos en distintos buscadores

- Nombre, usando comillas, “Ana Pérez”
- Número de teléfono
- Dirección
- No. de Carnet de Identidad

Anti-machitrolles

- Activa la verificación de dos pasos.
- Ingresa a Privacidad en Facebook: https://www.facebook.com/settings?tab=privacy
    - Revisa quién puede ver las publicaciones

Configuraciones de seguridad y privacidad en redes sociales

Facebook

-  En la pantalla principal -> Ve al menú hamburguesa -> Configuración y privacidad -> Configuración de la cuenta ->
-  Para ingresar a los ajustes, ve al menú desplegable en la parte superior derecha de tu pantalla -> Configuración de la cuenta

Seguridad

Seguridad e inicio de sesión ->

- Dónde iniciaste sesión -> Al lado derecho, ve a la opción de “Ver todos” -> Aparecerá una lista de todos los dispositivos en donde iniciaste sesión, Si no reconoces alguno,
  - ve al menú de desplegable a lado del dispositivo ->
    - Cerrar sesion
    - Proteger cuenta ->
      - No eres tu? -> Proteger cuenta
      - Salir
  - Al final de la lista de los dispositivos aparecera la opcion de cerrar todas las sesiones
- Inicio de sesión
  - Cambiar contraseña -> Actualiza tu contraseña

Autenticación en dos pasos

Puedes activar estas opciones para recibir notificaciones cuando se inicia sesión en tu cuenta, evitando así el ingreso no autorizado a tu cuenta.

- Seguridad e inicio de sesión ->
  - Usar autenticación en dos pasos ->
    - App de autenticación -> Descarga Duo Mobile del Play Store -> En la app de facebook: Configurar en el mismo dispositivo -> Listo

- Mensaje de texto (SMS) -> Escoge un numero de telefono o agrega uno nuevo -> Ingresa el código del SMS que facebook te envió a tu número celular -> Listo

- Inicios de sesión autorizados -> Lista los dispositivos que inician sesión sin pedir contraseña -> Si no reconoces alguno, al lado del dispositivo presiona en el ícono “X”

Configurar seguridad adicional

- Seguridad e inicio de sesión ->

    - Recibir alertas sobre inicios de sesión no reconocidos ->
        - Notificaciones -> Elige la mejor opción para ti
        - Messenger -> Elige la mejor opción para ti
        - Correo electrónico -> Elige la mejor opción para ti
    - Elegir de 3 a 5 amigos para contactar en caso de que pierdas el acceso a tu cuenta -> Elige mínimo 3 personas (*mejor si son familiares de confianza*) para que te ayuden a acceder a tu cuenta en caso de que pierdas el correo o número vinculados.

Descarga tu información de facebook

- Registro de actividad: Filtrado por categoría y año, todas las actividades que realizas en Facebook
- Propiedad y control de la cuenta.
- Descargar tu información: En esta sección puedes realizar una copia y descargar los datos que tiene almacenados Facebook sobre tu cuenta. Desde tu información básica, hasta las páginas que administras. La última es útil en caso de que pierdas o te cierren tu página de Facebook.
    - Solicitar copia -> Marca todas las opciones que consideres necesarias -> Al final de la lista encontrarás:
        - Intervalo de fechas: Elige un intervalo de fechas o descargar todo.
        - Formato: El formato de descarga se encuentra en HTML, es aconsejable dejarlo en esta opción.
        - Calidad: Elige en qué calidad descargar los datos
        - Crear Archivo -> Listo!
          Facebook te enviará un mensaje cuando tu copia esté lista, y podrás descargarla en el dispositivo que prefieras.

Privacidad

- Información Personal -> Nombre -> Puedes cambiar tu nombre y agregar apodos.
- Dirección de correo electrónico ->
  - Puedes agregar otro correo electrónico que quieras vincular a tu cuenta
  - En el icono al lado de tu correo, escoge la mejor opción para ti respecto a quién puede ver la dirección de correo electrónico :
    - Publico
    - Amigos
    - Solo yo
    - Más opciones… -> Mejores Amigos
- Número de teléfono ->
  - Puedes agregar otro número que quieras vincular a tu cuenta
  - En el icono al lado de tu número, escoge la mejor opción para ti respecto a quién puede ver tu número :
    - Público
    - Amigos
    - Solo yo
    - Más opciones… -> Mejores Amigos
- Confirmación de identidad -> Sigue los pasos para confirmar tu identidad. Facebook te pregunta si publicarás contenido o publicidad acerca de temas políticos, ya que esta confirmación está dirigida a ese público. Recomendamos no dar esta información a la plataforma, ya que pide nuestro carnet de identidad y otros datos personales adicionales.

- Administrar cuenta
  - Contacto delegado -> Esta opción sirve para delegar a un contacto de confianza tu cuenta de facebook cuando falleces, para que pueda hacer una copia de tus datos.
  - Desactiva tu cuenta -> Esta opción no elimina de forma permanente tu perfil

  - Configuración de la privacidad
    - Administrar tu perfil -> Se muestra la información que proporcionas en tu perfil. Para editar quién puede ver, presiona en el botón editar ✎ ->
      - Editar opción…

    - Compartir con -> Elige la opción que prefieras
        - Público
        - Amigos
        - Solo yo
        - Mejores amigos
- ¿Quién puede ver tus publicaciones futuras? -> Facebook te mostrará cómo se ven tus publicaciones antes de publicarlas y elegir a quienes llega actualmente.
- Limitar quién puede ver tus publicaciones anteriores -> Te dará la opción para que, a partir de ahora todas tus publicaciones anteriores sean visibles solo para tus amigos.
- ¿Quién puede ver las personas, páginas y listas que sigues? > Elige la opción que prefieras
    - Público
    - Amigos
    - Solo yo
    - Mejores amigos
- ¿Quién puede ver tu historia? -> Elige la opción que prefieras
    - Público
    - Amigos y conexiones
    - Personalizado
    - Ocultar historia a ...
- ¿Quién puede ver tus historias destacadas? -> Elige la opción que prefieras
    - Público
    - Amigos
    - Personalizado
    - Ocultar historias destacadas a …
- ¿Quién puede enviarte solicitudes de amistad? -> Elige la opción que prefieras
    - Todos
    - Amigos de amigos
- ¿Quién puede ver tu lista de amigos? -> Elige la opción que prefieras
    - Público
    - Amigos
    - Amigos excepto ...
    - Amigos concretos
    - Solo yo

- ¿Quién puede buscarte con la dirección de correo que proporcionaste? -> Elige la opción que prefieras
    - Todos
    - Amigos de amigos
    - Amigos
    - Solo yo
- ¿Quién puede buscarte con el número de teléfono que proporcionaste? -> Elige la opción que prefieras
    - Todos
    - Amigos de amigos
    - Amigos
    - Solo yo
- ¿Quieres que los motores de búsqueda fuera de Facebook se vinculen con tu perfil? -> Si esta opción está activada, quiere decir que si alguien en el buscador de Google, DuckDuckGo, Startpage, etc. inserta tu nombre, podrá encontrar tu perfil de Facebook.

- *Reconocimiento Facial*
    - ¿Quieres que Facebook pueda reconocerte en fotos y videos? -> Esta opción crea una plantilla de tu cara a partir de las fotos que **TÚ** subiste (foto de perfil, fotos en las que te etiquetaron), la usan para reconocerte en fotos y videos en los que puedas aparecer y te notifica acerca de estos.
- *Biografía y etiquetado*
    - ¿Quién puede buscarte con el número de teléfono que proporcionaste? -> Elige la opción que prefieras
        - Amigos
        - Solo yo
    - ¿Quién puede ver lo que otros publican en tu biografia? -> Elige la opción que prefieras
        - Todos
        - Amigos de amigos
        - Amigos
        - Amigos excepto…
        - Amigos concretos
        - Solo yo
    - ¿Permitir que otras personas compartan tus publicaciones en sus historias? -> Elige la opción que prefieras.

- ¿Quién puede ver las publicaciones en las que te etiquetan en tu biografia? -> Elige la opción que prefieras
    - Todos
    - Amigos de amigos
    - Amigos
    - Amigos excepto…
    - Amigos concretos
    - Solo yo
- Cuando alguien te etiquete en una publicación, ¿a quién quieres agregar al público, si es que aún no puede verla? -> Elige la opción que prefieras
    - Amigos
    - Solo yo
- ¿Quieres revisar las etiquetas que las personas agregan a tus publicaciones antes de que aparezcan en Facebook? -> Esta opción te permite aceptar que alguno de tus amigos te etiqueten en una publicación
- ¿Quieres revisar las etiquetas que las personas agregan a tus publicaciones antes de que aparezcan en Facebook? -> Esta opción te permite escoger si una publicación en la que te etiquetan aparece o no en tu perfil.

- *Bloqueos*
    - Agregar a la lista de bloqueados
        - Ingresa el nombre de la persona que deseas bloquear.
    - Te aparecerá una lista de las personas que bloqueaste.

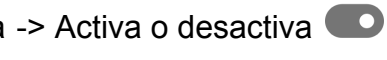
Otra manera de bloquear a una persona es la siguiente:

- Ingresa al perfil de la persona que quieras bloquear -> Presiona en “Más”  -> Bloquear -> ¡Listo!

WhatsApp

-  Para ingresar a los ajustes, ve a la parte inferior derecha de tu pantalla -> Configuración o Ajustes
-  Para ingresar a los ajustes, vé al menú desplegable en la parte superior derecha de tu pantalla -> Ajustes
    - Cuenta

- Seguridad
    - Verificación en dos pasos: Cuando vuelvas a registrar tu numero de celular en otros dispositivo o en el mismo, te pedirá un pin como forma de autentificar que eres tú -> Activar-> Inserta un pin de 6 dígitos -> Confirma el pin -> Añade tu correo -> Confirma tu correo -> Listo.

- Privacidad
    - Hora de últ. vez: Elige quién puede ver la última hora de tu conexión.
        - Todos (*Cualquier persona que tenga tu número de celular, aunque tú no la tengas en tu lista de contactos*)
        - Mis contactos
        - Nadie
    - Foto del perfil: Elige quién puede ver tu foto de perfil
        - Todos (*Cualquier persona que tenga tu número de celular, aunque tú no la tengas en tu lista de contactos*)
        - Mis contactos
        - Nadie
    - Info: Elige quién puede ver la info (*El mensaje pequeño que sale bajo tu foto de perfil*)
        - Todos (*Cualquier persona que tenga tu número de celular, aunque tú no la tengas en tu lista de contactos*)
        - Mis contactos
        - Nadie
    - Estado: Elige quién puede ver tus estados
        - Mis contactos
        - Mis contactos, excepto… (*Escoge los contactos que no quieres que vean tu estado*)
        - Solo compartir con...(*Escoge los contactos que quieres que vean tu estado*)
    - Confirmaciones de lectura -> Activa o desactiva  si deseas que otras personas sepan que viste sus mensajes (*Al activar esta opción tampoco podrás ver si vieron tus mensajes*)
    - Grupos: Elige quién puede agregarte a grupos
        - Todos
        - Mis contactos

        - Mis contactos, excepto…(*Elige los contactos que no pueden añadirte a grupos*)
    - Contactos bloqueados: En el ícono  añade a los contactos que no quieres que te envíen mensajes o vean cualquier información tuya en WhatsApp

Instagram

-  Ve a tu perfil -> Menú desplegable -> Configuración ->
    - Seguridad
        - Contraseña -> Cambia tu contraseña
        - Actividad de inicio de sesión: Te muestra los lugares y los dispositivos donde iniciaste sesión ->
            - Si no reconoces el dispositivo, al lado de cada dispositivo en el menú desplegable -> Cerrar sesión
        - Info. de inicio de sesión guardada -> Al activar esta opción, cada vez que cierres sesión en tu dispositivo, la info (*usuario y contraseña*) se guardarán para que no vuelvas a introducirlas.
        - Autenticación en dos pasos -> Empezar
            - App de autenticación -> Descarga Duo Mobile del Play Store -> En la app de Instagram: Siguiente -> Listo
            - Mensaje de texto (SMS) -> Escoge un número de teléfono o agrega uno nuevo -> Ingresa el código del SMS que Instagram te envió a tu número celular -> Listo.
        - Correos electrónicos de Instagram: Al entrar en esta sección, puedes revisar la lista de correos que Instagram te envió respecto a inicios de sesión o temas relacionados con la seguridad de tu cuenta
    - Privacidad
        - Comentarios
            - Permitir comentarios de
                - Todos
                - Personas que sigues y tus seguidores
                - Personas que sigues
                - Tus seguidores
            - Bloquear comentarios de -> Busca y elige quienes no podrán comentar en tus publicaciones
            - Ocultar comentarios ofensivos 
            - Filtro manual 

        - Inserta palabras que no quieras leer en los comentarios de tus publicaciones.
        - Filtrar palabras más reportadas: Oculta los comentarios que contengan palabras que son reportadas por otros usuarios.
    - Etiquetas
        - Aprobar etiquetas manualmente : te ayuda a revisar las publicaciones donde te etiquetan.
    - Estado de actividad -> Las personas con las que te conectaste mediante mensajes en Instagram pueden ver cuando fue la última vez que usaste la aplicación.
    - Privacidad de la cuenta -> Al activar esta opción, solo las personas que tú apruebes podrán ver tu perfil.
    - Cuentas restringidas -> Si no quieres bloquear, o dejar de seguir a algunas cuentas, puedes añadir a estas personas a la lista; por ejemplo: los mensajes que te manden se moverán a la carpeta de solicitudes de mensajes, por lo que no sabrán si leíste o no su mensaje.
    - Cuentas bloqueadas -> Te aparecerá la lista de personas que bloqueaste. -> Para bloquear una cuenta, ve a su perfil -> Ve al menú desplegable -> Bloquear.
    - Cuentas silenciadas -> Te aparecerá la lista de personas que Silenciaste. Para bloquear una cuenta ve a su perfil -> Presiona en "*Siguiendo"* -> Silenciar
        - Publicaciones
        - Historias

Twitter

 Presiona en tu foto de perfil en la parte superior izquierda -> Configuración -> Cuenta

Cuenta

- Teléfono -> Ingresa la contraseña -> Se puede cambiar el número de teléfono vinculado a la cuenta.
    - Existe la opción para que las personas que buscan un número de celular, puedan encontrar la cuenta vinculada a ella.
- Correo electrónico -> Ingresa la contraseña -> Se puede cambiar el correo vinculado a la cuenta.

        - Existe la opción para que las personas que buscan un correo electrónico, puedan encontrar la cuenta vinculada a él.
    - Contraseña -> Cambia tu contraseña

Seguridad

- Autenticación en dos fases
    - Mensaje de texto -> Comenzar -> Ingresa tu contraseña -> Enviar código (*Si no tienes agregado tu número de celular, vincula este a tu cuenta*) -> Ingresa el código -> Listo, al finalizar te mostrará un código en caso de que no puedas iniciar sesión.
    - App de autenticación -> Ingresa tu contraseña -> "Link the App" *Si no tienes una app de autenticación, descarga Duo Mobile u otra App* ->
      En Twitter: Ingresa el código que te da la aplicación -> Entendido.
    - Llave de seguridad (*Solo funciona para navegadores*)
- Protección de restablecimiento de contraseña -> Marca la casilla para confirmar con el número o correo electrónico cada vez que se restablezcas la contraseña
- Aplicaciones y sesiones
    - Aplicaciones: Aparecerán listadas todas las aplicaciones que estén vinculadas con la cuenta de Twitter, si no se reconoce algún dispositivo, pulsa el menú desplegable al lado de la aplicación -> Revocar acceso.
    - Sesiones: Primero aparecerá el dispositivo que se está usando en ese momento.
        - Cerrar todas las sesiones -> Cerrar sesión.
        - Verás un listado de los dispositivos donde iniciaste sesión.
            - Para cerrar sesión en un dispositivo -> ve al menú desplegable al lado del dispositivo -> Cerrar la sesión que se muestra -> Cerrar sesión.

 Presiona en tu foto de perfil en la parte superior izquierda -> Configuración y privacidad -> Privacidad

Privacidad

- Protege los tweets: Al activar esta opción, solo los seguidores actuales podrán ver los Tweets publicados, las personas que no sigan a la cuenta, te tendrán que enviar una solicitud.
- Etiquetado de fotos ->
    - Cualquiera te puede etiquetar
    - Solo las personas a las que sigues te pueden etiquetar
    - Desactivado

- Mensajes Directos
    - Recibir solicitudes de mensajes -> Al activar esta opción, podrás recibir mensajes de cualquier usuario de Twitter, incluso si no lo sigues.
    - Mostrar confirmaciones de lectura
- Visibilidad y contactos
    - Permite que otros te encuentren por tu correo electrónico: Marca esta opción si deseas que te encuentren de esta forma.
    - Permite que otros te encuentren por tu número de teléfono: Marca esta opción si deseas que te encuentren de esta forma.
    - Sincronizar contactos de las libreta de direcciones: Si marcas esta opción, Twitter subirá automáticamente tus contactos para que puedas seguirlos, solo si vinculan sus números con sus cuentas.
    - Eliminar todos los contactos: borrará toda la información de los contactos anteriormente sincronizados.
- Mostrar fotos y videos que puedan incluir contenido delicado: Activa la opción para ocultar fotos o vídeos sensibles.
- Marcar el contenido multimedia que se twittea para indicar si podría incluir material delicado.
- Cuentas bloqueadas: Mostrará la lista de cuentas que se haya bloqueado. Para bloquear una cuenta:
    - Entra al perfil de la cuenta -> menú desplegable -> Bloquear
- Cuentas silenciadas: Mostrará la lista de cuentas que se haya silenciado. Para bloquear una cuenta:
    - Entra al perfil de la cuenta -> menú desplegable -> Silenciar
- Palabras silenciadas -> Entendido -> Ve al 'icono ⊕ -> Ingresa solo una palabra, frase o Hashtag a la vez -> Marca si quieres silenciar en la Cronología de inicio y Notificaciones, o solo en una de ellas -> Elige por cuanto tiempo quieres silenciar.
- Ubicación exacta -> Si marcas esta opción, Twitter recopilará la ubicación del dispositivo mediante el GPS.

<u>Telegram</u>

-  Ve al menú hamburguesa -> Ajustes

-  En la esquina inferior derecha-> Ajustes
    - Presiona sobre el número de teléfono para cambiarlo
    - Nombre de usuario -> Elige un nombre de usuario, para que puedan encontrarte en Telegram a través de este.

    Seguridad

        - Llamadas
            - Quién puede llamarme?
                - Todos
                - Mis contactos
                - Nadie
            - Añadir excepciones: Los usuarios que añadas en estas listas, serán la excepción a las reglas de arriba.
                - No permitir -> Añadir usuarios
            - Usar peer-to-peer con: *Las llamadas a través de Telegram están configuradas por defecto en "Punto a Punto", es decir, directamente de usuario a usuario. Esta configuración hace que la IP de los usuarios en llamada sea visible en los registros de consola de Telegram. Para que no suceda esto, es recomendable cambiar la opción de "Todos" o "Mis Contactos" a "Nadie", para que la llamada vaya a través de los servidores de Telegram, donde se ocultará la IP de los usuarios, la única desventaja es que la calidad del audio bajará un poco*[30].
                - Todos
                - Mis contactos
                - Nadie
                - Añadir excepciones: Los usuarios y usuarias que añadas en estas listas, serán la excepción a las reglas de arriba.
                    - Permitir -> Añadir usuarios.
                    - No permitir -> Añadir usuarios.
        - Grupos y canales
            - ¿Quién puede añadirme?
                - Todos
                - Mis contactos

[30] Betech. La app Telegram filtra tus datos IP sin permiso. Cómo solucionarlo en móviles y en PC. 2018. https://as.com/meristation/2018/10/01/betech/1538384856_883385.html Consultado el: 19 de febrero de 2020.

        - Añadir excepciones: Los usuarios y usuarias que añadas en estas listas, serán la excepción a las reglas de arriba.
            - No permitir -> Añadir usuarios
- Código de bloqueo -> Al activar esta opción  Cada vez que entres a la App de Telegram se te pedirá el PIN que configures -> Ingresa un PIN -> Confirma el PIN.
        - *Nota: Si te olvidas el PIN de bloqueo, será necesario que desinstales Telegram y lo vuelvas a instalar. También se borrarán todos los chats secretos ya que se tenía el PIN activado.*
    - Cambiar código: Si ya está configurado, se puede cambiar el PIN
    - Desbloquear con huella digital. Esto no lo recomendamos.
    - Autobloqueo -> Telegram se bloqueará con PIN automáticamente, transcurrido el tiempo que elijas.
    - Mostrar contenido en la multitarea -> Al activar esta opción, se ocultará el contenido en la pantalla de aplicaciones en uso (Multitarea) y a su vez se restringirá la captura de pantalla en los chats.
- Verificación en dos pasos: Esta opción permite la autorización a la cuenta desde un nuevo dispositivo, por lo tanto se pedirá la contraseña para verificar a la persona que ingresa -> Ingresa una contraseña -> Confirma la contraseña -> Ingresa una pista para la contraseña -> Ingresa el correo electrónico: *Se enviará un código de verificación a la bandeja de entrada, si no, revisa la carpeta de Spam.* -> Ingresa el código en la App.
- Sesiones Activas
    - Sesión Actual: mostrará la información del dispositivo que se está usando en ese momento.
    - Cerrar todas las sesiones: Se puede cerrar las sesiones activas de todos los dispositivos conectados a la cuenta de Telegram, excepto el que estés usando para realizar este proceso.
    - Sesiones activas: Aparecerá una lista donde estarán todos los dispositivos donde se utiliza Telegram, si no se reconoce algún dispositivo presiona encima del nombre -> Cerrar sesión.

- Eliminar borradores: Cuando se escribe un mensaje, y por alguna razón no se lo envía, Telegram lo almacena en la nube como borrador. Presiona en esta opción para eliminar todos los borradores que Telegram tiene almacenados.
- Eliminar mi cuenta si estoy fuera: Si la cuenta de Telegram se encuentra inactiva por 6 meses, se eliminará la cuenta.

Privacidad

- Bloqueados -> En el icono  -> Elige los contactos que se quiere bloquear
- Número de teléfono ->
    - ¿Quién puede ver mi número?
        - Todos
        - Mis contactos
        - Nadie
    - Añadir excepciones: Los usuarios y usuarias añadidas en estas listas, serán la excepción a las reglas de arriba.
        - Permitir -> Añadir usuarios
        - No permitir -> Añadir usuarios
- Última vez y en línea
    - ¿Quién puede ver mi última vez?
        - Todos
        - Mis contactos
        - Nadie
    - Añadir excepciones: Los usuarios y usuarias que se añada en estas listas, serán la excepción a las reglas de arriba.
        - Compartir con -> Añadir usuarios
        - No compartir con -> Añadir usuarios
- Foto de perfil
    - Quién puede ver mi foto de perfil
        - Todos
        - Mis contactos
    - Añadir excepciones: Los usuarios y usuarias que se añada en estas listas, serán la excepción a las reglas de arriba.
        - Compartir con -> Añadir usuarios
        - No compartir con -> Añadir usuarios
- Mensajes reenviados: cuando un mensaje se reenvía, este mensaje aparecerá con el nombre de usuario que lo escribió.

- ¿Quién puede añadir un enlace a mi cuenta al reenviar mis mensajes?
    - Todos
    - Mis contactos
    - Nadie
- Añadir excepciones: Los usuarios y usuarias que se añada en estas listas, serán la excepción a las reglas de arriba.
    - No compartir con -> Añadir usuarios

Messenger

Las configuraciones de privacidad de Messenger son las que hayas establecido en Facebook. Por lo tanto, solo veremos las configuraciones de seguridad en esta sección. Recomendamos activar las conversaciones secretas para tener un encriptado de punto a punto, modificar la configuración de los archivos multimedia para no saturar la memoria de tu celular y no brindar más información privada que la necesaria a la plataforma.

Seguridad

-  Presiona sobre tu foto de perfil
-  En la esquina inferior derecha-> Ajustes
    - Solicitudes de mensajes: En esta sección se mostrarán todos los mensajes que hayan enviado personas que no estén en la lista de contactos.
    - Estado activo: Al desactivar esta opción, el estado y la última conexión serán ocultas. Al mismo tiempo, tampoco se podrá ver esta información de los contactos.
    - Historia ->
        - ¿Quién puede ver tu historia?
            - Público
            - Amigos y conexiones
            - Solo amigos
            - Personalizado
        - Ocultar mi historia a… *Elige al contacto que no quieras que vea la historia.*
        - Historias que silenciaste: *Lista de las personas de las cuales no quieres ver sus historias.* Para silenciar una historia:

            - Ingresa a la historia -> Ve al menú desplegable -> Silenciar historia.
        - Archivar historias: Si la opción está activada, todas las historias que se publicó serán guardadas en un archivo.
        - Ver archivo de historias: Es el archivo de todas las historias guardadas
    - Configuración de mensajes -> Personas que tienen el número de celular.
    - SMS: Al activar esta opción, los SMS que lleguen se abrirán a traveś de Messenger. Recomendamos no activar esta opción para limitar la cantidad de información personal que se brinda a la plataforma.
    - Personas
        - Subir contactos -> Sincronizar los números de contacto del celular con Messenger.
        - Cuenta de Instagram -> En esta sección se puede desconectar Messenger de Instagram. Recomendamos que las cuentas no estén vinculadas entre sí.
        - Administrar contactos -> Aparecerá la lista de contactos que Messenger sincronizó, se puede elegir eliminar toda la lista de contactos almacenados en Facebook
        - Personas Bloqueadas
            - Agregar Personas: Elige los contactos que se desea bloquear
            - Lista de personas bloqueadas: Si quieres desbloquear algún contacto, presiona en desbloquear.
    - Fotos y archivos multimedia
        - Guardar al capturar: Activa esta opción, si deseas que las fotos tomadas a través de la App se guarden en tu galería
        - Abrir enlaces en navegador predeterminado: Esta opción permite que los enlaces que te envíen sean abiertos por tu navegador y no a través de Facebook
    - Conversaciones secretas
        - Conversaciones secretas -> Habilita el dispositivo para intercambiar mensajes con cifrado de extremo a extremo. Para habilitar las conversaciones secretas
            - Dirígete al chat, o el contacto con quien quieras iniciar el chat secreto -> ve al ícono de la parte superior -> Ir a conversación Secreta y ¡Listo!
        - Eliminar todas las conversaciones secretas: Al presionar esta opción se eliminarán de manera permanente todas las conversaciones secretas que hayas iniciado.

- Configuración de la cuenta: Te dirigirá a las configuraciones de Facebook
- Reportar problema técnico: Si presentas algún problema, adjunta capturas de pantalla del problema, descríbelo -> Enviar.

Acciones reactivas

Son aquellas opciones que tenemos para reportar contenidos o acciones de los perfiles que nos violentan o desagradan. Nuestra experiencia y la de otras organizaciones denunciando agresiones en Internet, ya sea a la policía o con las mismas plataformas, no brindan razones para legitimar o confiar en estas órdenes. Sin embargo, presentamos algunas estrategias de resistencia que pueden minimizar los daños.

Sobre el proceso de denuncia en general, hay muchas percepciones sobre cómo se manejan las denuncias de contenido en Facebook. Por un lado, está la idea de que mientras más personas denuncian, mejor. Por otro lado, se dice que si denuncias al menos 6 veces, la denuncia recién es remitida a una persona para revisarla. Sin embargo, Facebook nunca ha reconocido ni desmentido el funcionamiento real de estas políticas.

El proceso en general consiste en:

- Documentar: recopila las pruebas y guárdalas en un lugar seguro
- Investiga al agresor o agresora e identifica si es un perfil falso: Ingresa al perfil falso, mira las fotos, revisa su lista de amigos y fíjate si tienen amigos o amigas en común, verifica sus publicaciones, la fecha de creación del perfil y asegúrate de que sea un perfil falso.
- Denuncia: Denunciar por razones de copyright o derechos de autor con las plataformas tiene más eficacia que denunciar por perfil falso, por ejemplo.
- Decide si se comparte la denuncia.

A continuación, presentamos el paso-a-paso para denunciar un perfil o contenido en cada red social.

Facebook

La denuncia con la plataforma puede ser a perfiles, páginas, grupos o contenidos. A continuación un desglose de las opciones que puedes elegir:

Denuncia de perfil

- Ingresa al perfil: Selecciona menú desplegable (los tres puntos a mano superior derecha) escoge busca ayuda/denuncia perfil.
- Puedes denunciar un perfil por las siguientes opciones:
  -> Se hace pasar por otra persona -> yo, un amigo famoso -> Enviar
  -> Cuenta Falsa -> Enviar
  -> Nombre Falso -> Enviar
  -> Publicación de contenido inapropiado ->Enviar
  -> No puedo acceder a mi cuenta -> Enviar
  ->Quiero ayudar->suicidio, autolesion, cuenta hackeada -> Enviar
  ->Otro -> Enviar

Denuncia de página

- Ingresa a la página: Selecciona menú desplegable (los tres puntos a mano superior derecha) escoge *busca ayuda o reportar página*.
- Puedes denunciar una página por las siguientes opciones:
  - Lenguaje que incita al odio -> Siguiente ->
    - Bloquear la página
    - Ocultar todo de la página (no ver publicaciones)
    - Reportar página ->
      - Creo que infringe las normas comunitarias de Facebook-> Reportar
  - Contenido sexual o desnudos:
    - Desnudos de adultos-> Siguiente ->
    - Contenido sexualmente sugerente-> Siguiente ->
    - Actividad sexual-> Siguiente ->
    - Explotación Sexual-> Siguiente ->
    - Servicios Sexuales-> Siguiente ->
    - Contenido relacionado con un menor-> Siguiente ->
      - Bloquear la página
      - Ocultar todo de la página (no ver publicaciones)
      - Reportar página ->
        - Creo que infringe las normas comunitarias de Facebook-> Reportar
  - Violencia :
    - Amenaza creíble de violencia-> Siguiente ->
    - Robo o Vandalismo-> Siguiente ->

- Suicidio o autoagresión-> Siguiente ->
- Violencia gráfica-> Siguiente ->
    - Bloquear la página
    - Ocultar todo de la página (no ver publicaciones)
    - Reportar página ->
        - Creo que infringe las normas comunitarias de Facebook-> Reportar

- Acoso :
    - Yo-> Siguiente ->
    - Otra persona -> Siguiente ->
        - Bloquear la página
        - Ocultar todo de la página (no ver publicaciones)
        - Reportar página ->
            - Creo que infringe las normas comunitarias de Facebook-> Reportar
- Estafas y páginas falsas:
    - Me solicitó información financiera -> Siguiente ->
        - Bloquear la página
        - Ocultar todo de la página (no ver publicaciones)
    - Se hace pasar por otro negocio -> Siguiente ->
        - Por qué negocio o persona se hace pasar esta página (ingresar el perfil del otro negocio)->Enviar
            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)
    - Se hace pasar por otra persona -> Siguiente ->
        - Por que negocio o persona se hace pasar esta página (ingresar el perfil del otro negocio)->Enviar
            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)
    - Página falsa -> Siguiente ->
        - Bloquear la página
        - Ocultar todo de la página (no ver publicaciones)
    - Cambio de nombre de página engañoso-> Siguiente ->
        - Bloquear la página
        - Ocultar todo de la página (no ver publicaciones)
    - No es una figura pública, una empresa de medios o una marca real-> Siguiente ->
        - Explica con más detalle por que esta página no cumple los requisitos de la insignia verificada azul -> Enviar

            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)
    - El tema de esta página cambió
        - Explica con más detalle por que esta página no cumple los requisitos de la insignia verificada azul -> Enviar
            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)
- Ventas no autorizadas:
    - Fomenta el consumo de drogas-> Siguiente ->
    - Compraventa de armas o drogas-> Siguiente ->
    - Venta de productos farmacéuticos con receta médica-> Siguiente ->
    - Promociona las apuestas online
    - Otro-> Siguiente ->
        - Bloquear la página
        - Ocultar todo de la página (no ver publicaciones)
        - Reportar página ->
            - Creo que infringe las normas comunitarias de Facebook-> Reportar
- Propiedad Intelectual:
    - Bloquear la página
    - Ocultar todo de la página (no ver publicaciones)
    - Reportar página ->
        - Creo que infringe las normas comunitarias de Facebook-> Reportar
- La página no debe tener insignia
    - No es una figura pública, una empresa de medios o una marca real-> Siguiente ->
        - Explica con más detalle por que esta página no cumple los requisitos de la insignia verificada azul -> Enviar
            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)
    - El tema de esta página cambió-> Siguiente ->
        - Explica con más detalle por que esta página no cumple los requisitos de la insignia verificada azul -> Enviar
            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)
    - Se hace pasar por otra cosa-> Siguiente ->

        - Por que negocio o persona se hace pasar esta página (ingresar el perfil del otro negocio)->Enviar
            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)
    - Otro-> Siguiente ->
        - Explica con más detalle por que esta página no cumple los requisitos de la insignia verificada azul -> Enviar
            - Bloquear la página
            - Ocultar todo de la página (no ver publicaciones)

Denuncia de grupos

- Ingresa al grupo: Selecciona menú desplegable (los tres puntos a mano superior derecha) selecciona *Reportar*.
- Puedes denunciar un grupo por las siguientes opciones:
    - Desnudos o actividad sexual
        - Reportar grupo
    - Acoso o bullying: ¿Quién es víctima de acoso?
        - Yo
        - Amigo o miembro de un grupo
        - Otra persona
            - Reportar grupo
    - Lenguaje que incita al odio
        - Reportar grupo
    - Ventas no autorizadas
        - Reportar grupo
    - Violencia
        - Reportar grupo
    - Spam

Denuncia de contenido

- En la imagen o publicación -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar publicación o buscar ayuda -> Desnudos -> Desnudos de adultos -> contenido sexualmente sugerente ->actividad sexual -> explotación sexual -> servicios sexuales ->contenido relacionado con un menor -> se comparten imágenes privadas -> Enviar.
    -> Violencia -> Enviar
    -> Acoso -> A mi, un amigo -> Enviar
    -> Suicidio o autolesiones -> Enviar

-> Noticias Falsas -> Enviar
-> Spam -> Enviar
-> Ventas no autorizadas ->Drogas ->Armas ->Animales en peligro de extinción -> Otros animales -> Otro problema -> Enviar
-> Incitación al odio -> Raza o etnia -> Nacionalidad -> Afiliación religiosa -> Clase Social ->Orientación sexual -> sexo o identidad de género
-> Terrorismo -> Otro motivo -> Enviar

WhatsApp

Cuando se reporta un contacto en WhatsApp, esta plataforma puede expulsar a este usuario por violar los términos y condiciones de la aplicación. Se puede reportar un usuario, o a un grupo y comunicarse con la plataforma para describir el problema de la siguiente manera:

Android

- Ingresa a la conversación -> presiona sobre el Menú desplegable (tres puntos) -> Ajustes -> Reporta.
- Para denunciar a un grupo en WhatsApp-> En el grupo de WhatsApp, ve al menú desplegable -> Reporta el grupo y selecciona si quieres salirte del grupo.
- Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú desplegable (3 puntos a mano derecha superior) de WhatsApp -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

iOS

- Para denunciar a un grupo en WhatsApp en iOS ->
    - Puedes también comunicarte con WhatsApp y explicar el problema: desde el menú desplegable (3 puntos a mano derecha superior) de WhatsApp -> Ayuda -> Contáctanos -> Describe el problema y añade capturas de pantalla.

Telegram

En Telegram solo se pueden reportar grupos, y por las siguientes razones.

- Ingresa al grupo -> Pulsa sobre el menú desplegable -> Reportar ->
    - Spam
    - Violencia
    - Abuso Infantil
    - Pornografía
    - Otros -> Describir la denuncia

Twitter

Te permite realizar varias acciones dependiendo de la agresión cometida. Antes de comenzar con la denuncia, recomendamos primero recopilar las pruebas: toma capturas de pantalla del tweet o mensaje, la hora y fecha, la foto del perfil, el nombre, la descripción. Segundo, investiga: Ingresa al perfil, mira sus fotos, la descripción, tweets, seguidores y a quienes sigue.

Si se decide denunciar un perfil o contenido, Twitter envía reportes del estado de la denuncia. Aquí mostramos un desglose de todas las opciones de denuncia con la plataforma, para que puedas escoger con antelación una ruta. También puedes consultar la plataforma del Centro de Ayuda de Twitter [31].

- Ingresa al perfil de Twitter-> Menú desplegable (3 puntos a mano derecha superior) -> Denunciar ->
    - No me interesa esta cuenta -> dejar de seguir, silenciar, o bloquear.
    - Es sospechoso o spam -> Es una cuenta falsa. Para denunciar bots.
        - Comparte enlaces a sitios web que podrían ser maliciosos
        - Usa una tendencia o un hashtag para enviar spam
        - Usa las funciones de respuesta, retweet o me gusta para enviar spam.
        - Es otra cosa.
    - Parece que su cuenta está hackeada -> Listo.
    - Fije que soy yo u otra persona -> A quién está suplantando ->
        - a mí
        - a alguien que represento
        - mi empresa o marca registrada
        - otra persona.
    - Sus tweets son abusivos o incitan al odio ->
        - Es irrespetuoso u ofensivo
        - Publica información privada
        - Participa en acoso selectivo
        - Incita al odio hacia una categoría protegida (raza, religión, género, orientación sexual o discapacidad)
        - Amenaza con violencia o daño físico
        - Fomenta al suicidio o a las autolesiones

31 Twitter. 2020. Centro de ayuda: Denunciar comportamientos abusivos. https://help.twitter.com/es/safety-and-security/report-abusive-behavior. Consultado: 2 de julio de 2020

- Información o imágenes de su perfil incluye contenido de odio ->
  - No apto para menores
  - Gráfico
  - Incitación al odio
- Expresan intenciones de suicidios o autolesiones ->
  - Agrega hasta 5 tweets a tu denuncia -> selecciona los tweets -> listo.

Instagram

Antes de comenzar con la ruta de denuncia, recomendamos primero recopilar las pruebas: toma capturas de pantalla del contenido o mensaje, la hora y fecha, la foto del perfil, el nombre, la descripción. Segundo, investiga. Ingresa al perfil, mira sus fotos, la descripción, publicaciones, seguidores y a quienes sigue.

A continuación mostramos un desglose de las opciones de denuncia de contenido y de perfiles para que puedas escoger una ruta con antelación.

Denuncia de perfil

En el perfil, selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar usuario -> Es inapropiado -> Reportar cuenta -> Se hace pasar por otra persona -> Yo. Denunciar robo de identidad, es mejor si la persona afectada hace la denuncia con la plataforma.

Denuncia de contenido

- En la imagen -> selecciona el menú desplegable (los tres puntos a mano superior derecha) -> Reportar -> Es inapropiado ->
  - Desnudos o actividad sexual ->
    - Desnudos o pornografía
    - Explotación o servicios sexuales
    - Se comparten imágenes privadas
      - Si gustas puedes bloquear la cuenta
  - Lenguaje o símbolos que incitan al odio: Para denunciar amenazas específicas de daños físicos, robo o vandalismo.
  - Violencia u organizaciones peligrosos: Para denunciar publicaciones que fomentan a la violencia por razones de religión, etnia o sexo. Daño físico, robo o vandalismo.
  - Venta de artículos ilegales o regulados
    - Drogas, alcohol o tabaco
    - Armas de fuego

        - Productos para bajar de peso o cirugías estéticas
        - Animales
    - Bullying o acoso -> ¿Quién es la víctima del acoso o bullying?
        - Yo
        - Alguien que conozco
        - Otra persona
    - Infracción de la propiedad intelectual: Denunciar robo de identidad. Es mejor si la persona afectada hace la denuncia con la plataforma.
    - Suicidio o autolesión: Publicaciones que identifican y se burlan de víctimas que autolesión.
    - Fraude -> Listo
    - Información falsa -> Listo
    - Simplemente no me gusta ->
        - Bloquear
        - Deja de seguir

Google

Google ha habilitado un formulario en línea para solicitar al buscador no mostrar contenidos que te violenten: una fotografía íntima, contenido difamatorio, información personal entre otros.

A continuación, puedes seleccionar la opción que más se relacione con el problema y Google mostrará un link para hacer la denuncia correspondiente. Para retirar información de Google es necesario proporcionar: nombre, correo electrónico, enlace del contenido que quieres retirar, la página de resultados de búsqueda de Google, la información del webmaster del sitio, capturas de pantalla y otra información personal.

En este enlace de solucionar problemas con la retirada de contenido de páginas de terceros puedes solicitar eliminar de la búsqueda en Google las siguientes, bajo los estos parámetros:

- Retirar de Google imágenes personales explícitas y no deseada
- Retirar de Google pornografía falsa publicada sin consentimiento
- Retirar de Google contenido sobre mí de sitios web en los que se llevan a cabo prácticas de retirada de contenido explotador.
- Retirar de Google información financiera, médica y de identificación nacional.

- Retirar contenido de "doxxing"; es decir, contenido que expone información de contacto con intención de perjudicar a alguien.

Otras

Para otras plataformas como Youtube, Pinterest, Flickr, WordPress, Tumblr, Blogger puedes ver información detallada en acoso.online.

Cuidados físicos

Consejos para cuidar los ojos

El esfuerzo de mirar una pantalla puede variar mucho dependiendo al entorno.

- Se recomienda usar el modo oscuro para lectura de textos cortos y si el entorno está poco iluminado. Si la principal fuente de luz es la pantalla, esto provoca mayor tensión ocular por una pantalla iluminada[32]. Se puede configurar el modo oscuro en las siguientes redes y apps de mensajería:

    - Facebook
        - Ingresa a Facebook -> Configuraciones -> Modo oscuro ->Activar.
            - Esta opción no funciona en todos los celulares.
    - Twitter
        - Ingresa a Twitter -> Pulsa en tu foto de perfil -> En la parte inferior izquierda pulsa en el foco 💡
            - Activado
            - Automático al atardecer
    - WhatsApp
        - Ingresa a Whatsapp -> Pulsa en el menu desplegable (los 3 puntos) -> Ajustes -> Chats -> Presiona “Tema” -> Oscuro
    - Telegram
        - Ingresa a la app de Telegram -> Pulsa al menú hamburguesa-> Encuentra la luna en la parte superior derecha dentro del menú ->

32Clark, Laurie. 2019. Dark mode isn't as good for your eyes as you believe. https://www.wired.co.uk/article/dark-mode-chrome-android-ios-science. Consultado: 2 de julio de 2020.

Pulsa la luna. Esto ayudará a la lectura de mensajes en entornos poco iluminados.

- Se recomienda usar el modo claro, si se debe realizar lecturas extensas, si es de día o si se encuentra en un entorno bien iluminado.
- En caso de experimentar dolor, cansancio de ojos, percatarse de expresiones de tensión facial por la lectura en computadoras, etc. recomendamos visitar a un oculista para realizar una evaluación y ver la necesidad de usar lentes con filtro para la lectura en computadoras o dispositivos móviles.

Consejos para cuidar el cuerpo

- Mantener a los celulares alejados mientras realizamos llamadas. Los celulares emiten altos niveles de ondas de radiación magnética que pueden ser dañinas para la salud[33].Las computadoras, celulares, tablets y otros dispositivos emiten ondas radiación electromagnética La exposición constante a estas ondas puede tener consecuencias cancerígenas[34].
- Se recomienda no guardar estos dispositivos en zonas del cuerpo como el torso, bolsillos de los pantalones (delanteros y traseros).

Glosario (agregar a la guía)

Menú hamburguesa: Lo encuentras abriendo la aplicación, son las 3 rayas en la parte superior derecha. Se la llama así porque tiene 3 capas, como una hamburguesa.

Menú desplegable: Lo puedes encontrar abriendo la aplicación en la parte superior derecha, son 3 puntos.

Bloquear

Silenciar

Cifrado de extremos a extremo: Es un sistema de comunicación donde solo los usuarios que se comunican pueden leer los mensajes. Garantiza que un mensaje sea

33 Davis, Devras. 2015. The truth about mobile phone and wireless radiation. https://www.youtube.com/watch?v=BwyDCHf5iCY. Consultado: 2 de julio de 2020.

34 Organización Mundial de la Salud. 2011. IARC CLASSIFIES RADIOFREQUENCY ELECTROMAGNETIC FIELDS AS POSSIBLY CARCINOGENIC TO HUMANS. https://www.iarc.fr/wp-content/uploads/2018/07/pr208_E.pdf Consultado: 2 de julio de 2020.

convertido en un mensaje secreto por parte de su emisor original y descifrado solo por su receptor final.

Más guías de resistencia:
https://hiperderecho.org/tecnoresistencias/resiste/recursos/
https://hiperderecho.org/sexting/
https://acoso.online/bo/4-resiste-y-toma-control-sobre-la-tecnologia/
https://www.criptica.org/blog/resistencia-digital/