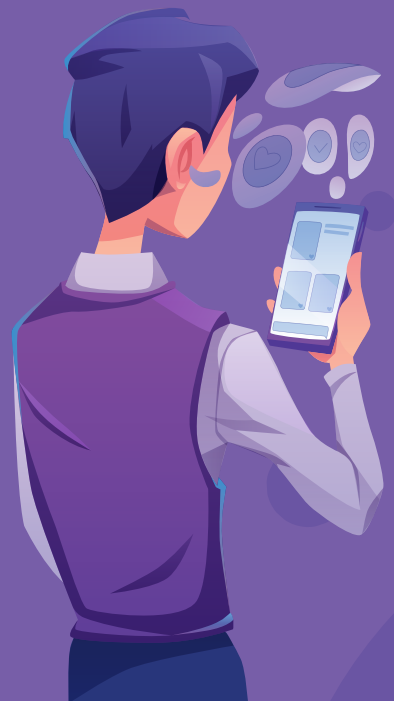


CÓDIGO DE ÉTICA

PARA LA PREVENCIÓN DE LA VIOLENCIA DIGITAL CONTRA LAS MUJERES.

Uso y consumo seguro de los servicios de telecomunicaciones.

GOBIERNO DE MÉXICO | ECONOMÍA SECRETARÍA DE ECONOMÍA | INMUJERES INSTITUTO NACIONAL DE LAS MUJERES | PROFECO PROCURADURÍA FEDERAL DEL CONSUMIDOR

Presentación

El Gobierno de México, comprometido con el ejercicio de los derechos de las mujeres, principalmente con el derecho a vivir una vida libre de violencia, impulsó –a través de la Procuraduría Federal del Consumidor (PROFECO) y del Instituto Nacional de las Mujeres (INMUJERES)– la elaboración de un código de ética que promueva la prevención de la violencia digital contra las mujeres mediante el uso y consumo responsable, informado, sostenible, seguro y saludable de los servicios de telecomunicaciones.

Derivado del trabajo coordinado entre estas dos instituciones, se presenta este *Código de ética para la prevención de la violencia digital contra las mujeres* que describe acciones y prácticas que constituyen violencia digital, así como algunas recomendaciones para prevenirlas. Su difusión se apoya en alianzas entre empresas e instituciones que conforman el ecosistema de las telecomunicaciones en México que, con compromiso y responsabilidad social, informan a sus usuarias y usuarios sobre estos temas.

Se trata de un documento que apuesta al cambio cultural en el ámbito del uso y consumo de servicios de telecomunicaciones.

El Gobierno Federal refrenda su compromiso con las mujeres, al sumar esfuerzos entre los sectores público y privado para sentar las bases que posibiliten una vida libre de violencia hacia las mujeres en el mundo digital.

Introducción

Violencia digital son todas aquellas formas de agresión contra la integridad de una mujer que se realizan mediante el uso de tecnologías de la información y la comunicación.

Se trata de la exposición, distribución, difusión, exhibición, transmisión, comercialización, oferta o intercambio de imágenes, audios, videos –reales o simulados– de contenido íntimo sexual de una mujer sin su consentimiento, aprobación o autorización.

La violencia contra las mujeres en medios digitales se manifiesta mediante la difusión de fotografías y datos personales, sin su consentimiento; amenazas, difamaciones, acoso o cualquier forma de humillación y ataques a su integridad, identidad e intimidad.

Tales actos generan daño psicológico y/o emocional, y ponen en riesgo la intimidad, privacidad y dignidad de las mujeres[1] en cualquier ámbito de su vida privada, o pública, y en su imagen.

Las redes sociales son los espacios más comunes donde ocurren estas formas de violencia contra las mujeres, pero también en plataformas de internet y videojuegos, en aplicaciones de teléfonos móviles, a través de correos electrónicos, mensajes de texto y/o de voz.

[1] Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (DOF).

Las personas que cometen este tipo de agresiones utilizan el anonimato que ofrecen algunas aplicaciones y plataformas, generando perfiles o identidades falsas, aunque también es muy común que ocurra a través de perfiles reales y por medios de comunicación registrados y verificados.

En este tipo de violencias se han popularizado términos como:

Ciberbullyng

También conocido como ciberacoso, se utiliza para describir cuando una persona es molestada, amenazada, acosada, humillada, avergonzada o abusada por otra persona, mediante las tecnologías digitales.[2]

Trolear

En foros de internet y redes sociales, publicar mensajes provocativos, ofensivos o fuera de lugar con el fin de boicotear algo o a alguien, o entorpecer la conversación.[3]

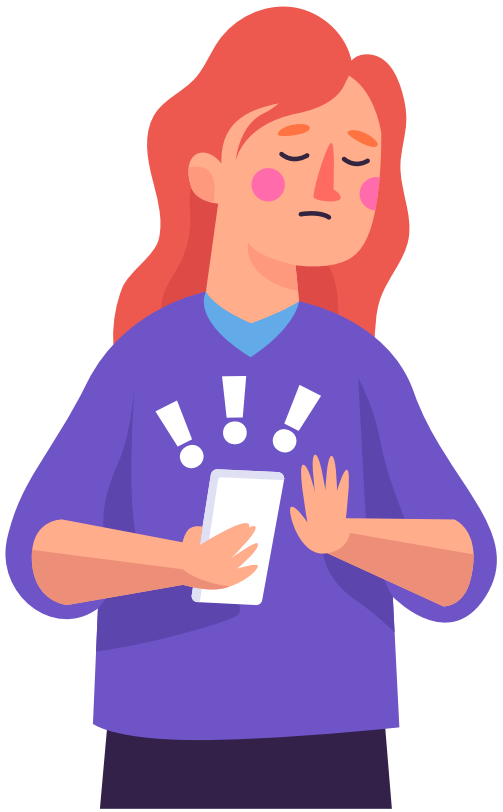
Stalking

Comúnmente esta práctica es una conducta obsesiva, acosadora e insistente en averiguar información de una persona, a través de redes sociales (Twitter, Facebook, Instagram, TikTok, entre otras).[4]

[2] UNICEF. (2020). *Ciberacoso: Qué es y cómo detenerlo.* [online] Disponible en: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo [Consultado 16 Jun. 2022].

[3] RAE https://dle.rae.es/trolear (Consultado 20 junio 2022).

[4] Concepto. (2013). *'Stalkear' - Concepto, conductas de stalker y qué es un crush*. [online] Disponible en: https://concepto.de/stalkear/ [Consultado 16 Jun. 2022].



Grooming

Es cuando un adulto mediante engaños y mentiras se gana la confianza y establece algún tipo de amistad con un menor de edad a través de internet, ya sea vía redes sociales, aplicaciones de mensajería instantánea, correo electrónico, entre otros, con el fin de obtener imágenes o videos con connotación o actividad sexual.

Shaming

Es un tipo de acoso en línea, el cual busca avergonzar y humillar a una persona en redes sociales (Twitter, Facebook, Instagram, TikTok, entre otras).

Doxing

Otro tipo de acoso en línea, consiste en revelar información confidencial de una persona sin su consentimiento, por ejemplo: nombre real, dirección, teléfono, datos financieros.[5] Esta práctica es utilizada para acosar, amenazar o vengarse.[6]

Sexting

Es una práctica, principalmente entre jóvenes, que consiste en el intercambio de mensajes de contenido sexual o erótico, especialmente fotos o videos[7]; también puede derivar en violencia digital si el contenido de los mensajes se difunde sin consentimiento.

---

5 Kaspersky (2021). *Doxing: definición y explicación*. [online] latam.kaspersky.com. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-doxing [Consultado 16 Jun. 2022].

6 Latto, N. (2021). *¿Qué es el doxing y cómo puede evitarlo?* [online] ¿Qué es el doxing y cómo puede evitarlo? Disponible en: https://www.avast.com/es-es/c-what-is-doxxing [Consultado 16 Jun. 2022].

7 GCFGLOBAL. (2013). *Seguridad en internet: ¿Qué es el sexting?* [online] Disponible en: https://edu.gcfglobal.org/es/seguridad-en-internet/que-es-el-sexting/1/ [Consultado 16 Jun. 2022].

La violencia digital

contra las mujeres en México

Para el Instituto Nacional de Estadística y Geografía (INEGI) el ciberacoso se define como un acto intencionado que, de forma individual o grupal, tiene como fin dañar o molestar a una persona mediante el uso de tecnologías de información y comunicación, específicamente el internet.[8]

Asimismo, considera que el ciberacoso puede constituirse en una forma de victimización delictiva que puede derivar en daños morales, psicológicos y económicos e incluso en la intención de las víctimas de terminar con su vida.

A partir de estas consideraciones, el Módulo sobre Ciberacoso (MOCIBA) 2021 otorga información estadística para conocer la prevalencia del ciberacoso entre la población de 12 y más años de edad que es usuaria de internet; la caracterización de aquella que vivió alguna situación de ciberacoso en los últimos 12 meses; así como la identidad y sexo de la persona acosadora y las consecuencias para la víctima.

En este documento se retoma la información proveniente del módulo debido a que permite tener una aproximación al comportamiento de la violencia digital contra las mujeres en el país.

8 INEGI (2022-07-13) *Modulo sobre Ciberacoso 2021*. Comunicado de Prensa. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/mociba/MOCIBA2021.pdf

En México, el 77.9 por ciento del total de la población de 12 años y más utiliza internet, de las cuales 42.3 millones son mujeres.

El 21 por ciento de la población de 12 años y más que utilizó internet en 2021 fue víctima de ciberacoso, lo cual equivale a 17.7 millones de personas de 12 años y más usuarias de internet a través de cualquier dispositivo.

Aunque hombres y mujeres pueden ser víctimas de ciberacoso, son estas las más vulnerables a este hecho victimizante. El INEGI registró que, en 2021 del total de mujeres usuarias de internet, el 22.8 por ciento fue víctima de alguna forma de ciberacoso, lo que corresponde a un total de 9.6 millones de mujeres mayores de 12 años, a diferencia de los hombres que experimentaron violencia (8 millones).

El mayor porcentaje de mujeres que sufrieron ciberacoso, el 60 por ciento, se encuentra en el grupo de edad de 12 a 29 años.

La importancia de prevenir

la violencia digital contra las mujeres

La violencia digital contra las mujeres representa un obstáculo para el ejercicio del derecho a la información y al acceso seguro a las telecomunicaciones, por tanto, prevenirla nos permite avanzar hacia un ejercicio igualitario entre mujeres y hombres que además contribuye al goce y disfrute de otros derechos humanos, por ejemplo: la recreación, la educación, la libertad, la seguridad y el derecho de todas las personas a una vida libre de violencia.

Para prevenir la violencia digital contra las mujeres es necesario realizar acciones que provoquen cambios y reflexiones en torno a las ideas que tenemos sobre cómo ser mujer u hombre en nuestra sociedad, eliminando viejas creencias sobre los roles y estereotipos de género y construyendo nuevas formas de relacionarnos, evitando que mujeres, niñas y adolescentes sean víctimas de alguna forma de violencia.

Objetivo del Código de ética

para la prevención de la violencia digital contra las mujeres

El código de ética es una herramienta para promover el uso y consumo responsable, informado, sostenible, seguro y saludable del internet, telefonía celular y otros servicios de telecomunicaciones.

Su propósito es difundir entre las personas usuarias de servicios telecomunicaciones, información sobre aquellas conductas y acciones que son —o pueden llegar a ser— manifestaciones de violencia digital contra las mujeres, a fin de promover su prevención o eliminación.

Acciones, prácticas y conductas que constituyen violencia digital y mediática

Compartir contenido sexual sin consentimiento

La creación, difusión, distribución o intercambio digital de fotografías, videos o audio clips de naturaleza sexual o íntima, sin el consentimiento de una mujer, es violencia digital y puede constituir un delito.

Realizar proposiciones sexuales sin consentimiento

La clave es el consentimiento, por lo cual formular proposiciones sexuales indeseadas y reiteradas, enviar fotos sexuales no solicitadas o monitorear y vigilar constantemente la actividad de una mujer, constituyen actos de ciberacoso y ciberhostigamiento.

Uso indebido de datos personales

En el uso de redes sociales se han normalizado comportamientos en torno al mito del amor romántico, pero que de fondo significan cibercontrol y ciberacoso contra las mujeres. Por ejemplo: exigir contraseñas y claves personales de teléfonos celulares y cuentas de redes sociales, interferir y monitorear la comunicación digital con otras personas, intentar controlar las interacciones en redes sociales, censurando fotos o publicaciones, revisar contactos o conversaciones y exigir mostrar de forma constante la geolocalización de la pareja.

Obtención de información personal

Los hackeos de cuentas y dispositivos para obtener, manipular y/o publicar información personal y utilizarla para intimidar, acosar, hostigar o abusar sexualmente a una mujer son ataques cibernéticos orientados a generar violencia contra las mujeres.

Suplantación y robo de identidad

Consiste en la creación de perfiles o cuentas falsas en redes sociales o la usurpación de cuentas de correo o números de teléfono para contactar a amistades, familiares, colegas o conocidos de las víctimas con el propósito de obtener información sobre ellas, o incluso con el fin de realizar bromas. Esta práctica constituye un delito y debe ser denunciada.

Acosar o espiar por internet *(stalkear)*

Investigar la actividad de otra persona a través de internet puede parecer un acto inofensivo; sin embargo, a medida que se adentra en la búsqueda de información se puede llegar a generar un patrón de conductas amenazantes que vulneren la sensación de seguridad de la persona que está siendo vigilada.

Es necesario respetar la privacidad de las personas, no compilar su información o entablar comunicación constante con ella sin su consentimiento. Es importante evitar enviar de manera reiterada solicitudes de amistad en redes sociales, llamar, enviar correos o mensajes de texto o voz.

Llamadas y mensajes ofensivos

Las llamadas o mensajes ofensivos, con discursos de odio o con el propósito de acosar, hostigar, amenazar, insultar o molestar son prácticas que vulneran la integridad (física, psicológica y moral) y la dignidad e intimidad de la persona y su bienestar personal.

Insinuaciones o propuestas sexuales

Las insinuaciones o propuestas sexuales no deseadas u ofensivas, realizadas mediante redes sociales o medios digitales constituyen actos de acoso sexual, y son un tipo de violencia sexual.

Troleo o campaña de desprestigio

El troleo, o campaña de desprestigio, son actividades que consisten en publicar comentarios ofensivos para generar polémicas y provocaciones, causando reacciones emocionales en otras personas en perjuicio de alguien.

Al troleo de género se suma la publicación de mensajes, imágenes o videos, así como la creación de *Hashtags* con el propósito de perjudicar a mujeres, niñas y adolescentes e incitar violencia en su contra.

Manipulación o extorsión bajo amenaza de difundir información íntima o privada

Amenazar o chantajear con difundir información íntima o privada en medios digitales es una forma de manipular o extorsionar a una persona para forzarla a actuar de cierta manera bajo amenazas, intimidación o agresiones.

Críticas y discriminación

La violencia de género en línea afecta de manera diferenciada según las diversas experiencias e identidades de las mujeres, es decir, la violencia digital se manifiesta junto a otras formas de discriminación por motivos de origen étnico, orientación sexual, identidad de género, clase social, participación política, nacionalidad, situación migratoria, entre otros.

Acciones de prevención

No reproducir contenido discriminador

Si identificas memes, comentarios, opiniones u otras formas de información que reproduzcan discursos de odio evita reproducirlos o difundirlos o celebrarlos. Repórtalos en la plataforma donde suceda.

Es importante verificar los perfiles de los que se reciben invitaciones o solicitudes. Antes de aceptar la solicitud de alguien analiza los siguientes elementos: nombre de usuario, fotografía del perfil, contactos y actividad de la cuenta.

Los perfiles falsos pueden contener letras o números aleatorios o nombres que llamen tu atención, suelen no tener fotos personales;

así como pocos contactos o del mismo género; además de tener pocos comentarios o baja actividad. Tómate el tiempo de analizar las cuentas o perfiles, desconfía de lo que parezca sospechoso.

No almacenar contenidos sexuales

Aunque exista consentimiento para intercambiar fotos, videos, audios o datos de naturaleza sexual o íntima (incluso en presencia de otras personas), este consentimiento no implica un permiso para almacenarlos. Si recibes este tipo de información es importante borrarla o destruirla.

Siempre debe de haber consentimiento

No se deben estigmatizar prácticas como el *sexting* porque todas y todos tenemos derecho a usar la tecnología para expresar nuestra sexualidad, la clave es el consentimiento. Sin embargo, al hacerlo es muy importante considerar que existen riesgos y por consiguiente es necesario considerar medidas de seguridad en la comunicación digital.

No proporcionar datos personales

No compartir contraseñas ni difundir información privada a través de redes sociales. Procura que tus redes sociales sean privadas, crea filtros de seguridad desde los ajustes de privacidad.

Reportar el robo de información personal

Si tienes información de páginas de internet o personas que hackean cuentas y dispositivos para obtener, manipular y/o publicar información personal y utilizarla para intimidar, acosar u hostigar, es importante denunciar ante la Policía Cibernética al número 089.

Si estás viviendo una situación así, apóyate de alguien de confianza –familiares, amigas o amigos–, evita cualquier contacto con los extorsionadores, busca ayuda legal y denuncia.

No reproducir, ni compartir contenido sexual

Si por alguna razón llegas a recibir imágenes, videos, audios o encuentras en redes sociales hashtags con contenido sexual, no los reproduzcas ni los compartas; romper la cadena de transmisión de la información puede contribuir a evitar que una persona sea revictimizada. Bloquea este tipo de mensajes o repórtalos con el proveedor del servicio.

Reporte

Todas las mujeres, niñas y adolescentes que han sido víctimas de violencia digital tienen el derecho a interponer una denuncia y a ser atendidas por las autoridades, es muy importante señalar que ninguna mujer que ha vivido violencia digital ha inducido o provocado los actos que la han agredido.

Tanto las mujeres, niñas y adolescentes que han sufrido violencia, como el resto de personas que tenemos conocimiento de este tipo de actos podemos informarlo a las autoridades llamando al 911 o al 089, así como acudiendo a cualquier centro de atención de la violencia contra las mujeres.

La denuncia es anónima.

Reflexiones finales

- No revictimizar al atribuir a las víctimas la responsabilidad de protegerse, en vez de recalcar la conducta ilícita de los agresores.
- Evitar normalizar y minimizar la violencia digital.
- Adoptar medidas de ciberseguridad como antivirus, anti-malware, redes virtuales privadas (VPN), entre otras.
- Bloquear (a la persona, cuenta o página) que está realizando actos de violencia digital.
- Cambiar o cancelar número telefónico, cuenta o contraseña.
- Eliminar la publicación, el mensaje o video.
- Denunciar ante el ministerio público, policía o el proveedor del servicio
- No ser parte de conductas de ciberacoso o violencia digital.
- En el siglo XXI es indispensable que como consumidoras y consumidores de servicios de telecomunicaciones, hagamos uso y consumo responsable, informado, seguro, sostenible y saludable de la tecnología.

GOBIERNO DE MÉXICO | ECONOMÍA SECRETARÍA DE ECONOMÍA | INMUJERES INSTITUTO NACIONAL DE LAS MUJERES | PROFECO PROCURADURÍA FEDERAL DEL CONSUMIDOR