5

Ciudades Seguras

Protegidas en Internet

Guía de cuidados digitales para organizaciones sociales de mujeres

ONU MUJERES

Ciudades Seguras

Protegidas en Internet

Guía de cuidados digitales para organizaciones sociales de mujeres

Protegidas en Internet- Guía de cuidados digitales para organizaciones sociales de mujeres

ONU Mujeres. 2025

ONU Mujeres Ecuador.
Ana Elena Badilla G.
Representante

ONU Mujeres Ecuador
Vía Nayón s/n y Av. Simón Bolívar
Complejo EkoPark, Torre 4, piso 2.
onumujeres.ecuador@unwomen.org

Coordinación de la publicación
Ma. Alejandra Guerrón M. – Analista de Programa en eliminación de violencia contra las mujeres.

Taller de Comunicación Mujer
Monica Diego
Directora Ejecutiva

Diseño y diagramación:
Joseler

Ilustraciones Ciudades Seguras/ONU Mujeres-Manthra Comunicación 2023

Quito – Ecuador

ONU Mujeres es la entidad de las Naciones Unidas para la Igualdad de Género y el Empoderamiento de las Mujeres.

La iniciativa “Ciudades Seguras y Espacios Públicos Seguros” descansa en nuestro programa mundial “Ciudades Seguras Libres de Violencia contra las Mujeres” que fuera lanzado en noviembre de 2010 con destacadas organizaciones de mujeres, organismos de Naciones Unidas y más de 70 aliados del ámbito mundial y local. Se ejecuta desde 2011 con sus programas inaugurales de Quito, Ecuador; El Cairo, Egipto; Nueva Delhi, India; Port Moresby, Papua Nueva Guinea; y Kigali, Rwanda, en la actualidad se extiende a más de 20 ciudades en el mundo.

La iniciativa mundial de ONU Mujeres Ciudades Seguras y Espacios Públicos Seguros continúa generando múltiples resultados innovadores a través de las alianzas establecidas con alcaldías, gobiernos nacionales, grupos de mujeres y otros aliados comunitarios.

Ciudades Seguras en Ecuador ha contado con el financiamiento de la Agencia Española para la Cooperación Internacional para el Desarrollo, AECI y del Gobierno de Korea, así como el apoyo y participación de autoridades y funcionarias/os municipales, organizaciones de la sociedad civil y mujeres y hombres que han hecho posibles los avances alcanzados durante estos años.

¿Qué contiene esta guía?

¿Qué es esta guía?

Protegidas en Internet. Guía de cuidados digitales para organizaciones sociales de mujeres es una herramienta elaborada en el marco del Programa Ciudades Seguras y Espacios Públicos Seguros de ONU Mujeres, para fortalecer la protección digital de las organizaciones de la sociedad civil en Ecuador.

Internet y las tecnologías digitales son herramientas que ofrecen diferentes posibilidades para el desarrollo del trabajo de las organizaciones de mujeres. Esta guía busca que las mujeres aumenten sus conocimientos sobre los cuidados digitales, con el fin de prevenir riesgos en el uso de las tecnologías, y se aproximen a acciones generales de respuesta a situaciones de violencia de género en el ámbito digital.

Este recurso se realiza como resultado de las recomendaciones obtenidas del **Estudio exploratorio complementario sobre la violencia facilitada por la tecnología contra las mujeres y las niñas (VFTCMN) en las ciudades de Quito, Cuenca y Guayaquil** en 2023, donde se identificaron necesidades de formación en seguridad digital y protección integral por parte de mujeres defensoras de derechos humanos, activistas y otras que acompañan a víctimas de violencia de género.

Además, durante dicho estudio las organizaciones sociales de mujeres reportaron riesgos y agresiones digitales específicas hacia sus integrantes que evidenciaron la relevancia de adoptar acciones frente a este tipo de violencia, en especial en grupos poblacionales que se encuentran en condiciones de vulnerabilidad.

A lo mencionado, se suma el aumento de la inseguridad y violencia en Ecuador en los últimos años, donde los esfuerzos para contribuir al diseño e implementación de acciones de protección integral de las mujeres de las organizaciones sociales se torna sumamente urgente, en particular en el ámbito digital donde aún las medidas llevadas a cabo son incipientes.

Esta guía se dirige a agrupaciones, asociaciones, colectivas y organizaciones sociales de mujeres que realizan diferentes actividades como la defensa de los derechos humanos y la promoción de los derechos culturales, laborales, económicos y sociales de las mujeres, en toda su diversidad.

El presente material se elaboró en 2024 con la participación de organizaciones sociales de mujeres de las ciudades de Cuenca, Guayaquil y Quito a través de grupos focales donde se identificaron necesidades y recomendaciones para elaborar los contenidos que fueron validados posteriormente en talleres de formación en cuidados digitales en cada ciudad.

Glosario

Aplicación (App): programa informático que se usa en teléfonos inteligentes, tabletas y otros dispositivos móviles para llevar a cabo diferentes tareas o acceder a plataformas educativas, profesionales o de ocio.

Brecha digital: hace referencia a la desigualdad que existe entre personas, hogares, y zonas geográficas de diferentes condiciones sociales en cuanto a sus oportunidades de acceso a las Tecnologías de la Información y Comunicación (TIC).

Cifrado o encriptado de información: es un proceso para garantizar la seguridad y privacidad de la información que viaja por internet y consiste en convertir datos en un código ilegible para que la información solo pueda ser leída por quienes tiene la clave que descifra el código.

Cifrado de extremo a extremo (E2EE End-to-End Encryption): es un tipo de cifrado o encriptado de información que se suele usar en las comunicaciones de apps de mensajería instantánea y correos electrónicos. Consiste en que los datos son convertidos a código durante todo el viaje o recorrido de un mensaje de tal forma que solo puede ser leído por el emisor y receptor.

Cookies: archivos de texto que un sitio web envía al navegador de la persona usuaria. Suelen usarse para recordar accesos y hábitos de navegación. Las cookies hacen que las páginas web puedan identificar los dispositivos (celular o computadora) y que al volver a visitarlas recuerden qué se ha hecho dentro de ellas. Correo o teléfono de recuperación: dirección de correo electrónico o número telefónico que permite restablecer una contraseña y recuperar el acceso a cuentas de redes sociales, correos electrónicos, entre otras.

Datos biométricos: datos personales sobre las características físicas o conductuales únicas que se utilizan para identificar personas. Se refiere a las huellas dactilares, reconocimiento facial, escaneo de iris, entre otras.

Datos personales: cualquier información relacionada con una persona que permita que esta sea identificada, por ejemplo: nombre, edad, dirección, cédula, entre otros.

Datos sensibles: se refiere a categorías especiales de datos personales que afectan al ámbito más íntimo de una persona, y cuyo mal uso puede causar discriminación o un riesgo grave. Por ejemplo: etnia, identidad de género, orientación sexual, estado de salud, datos biométricos, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, pasado judicial, condición de discapacidad, estatus migratorio, entre otras.

Geolocalización: ubicación geográfica de un objeto en tiempo real.

Hardware: partes físicas de una computadora o dispositivo como el procesador, la memoria, el teclado o el disco duro.

HTTPS *(Protocolo Seguro de Transferencia de Hipertexto o Hypertext Transfer Protocol Secure)*: es un protocolo que garantiza la transferencia segura de datos cifrados entre un navegador y un sitio web y que evita que los datos sean interceptados por terceros durante la navegación. Al visitar un sitio web es muy importante fijarnos que aparezca https:// y no http:// o que en el navegador se visualice un candado junto al sitio web que se está visitando.

Huella digital: rastro que las personas dejan en Internet a través de sus comunicaciones y conexiones y que contiene la información que se sube o baja de Internet a través de redes sociales, páginas web, apps de mensajería, entre otros.

Inteligencia artificial (IA): hace referencia a la creación de computadoras y máquinas que pueden generar procesos automatizados y veloces a través de su programación y entrenamiento con el manejo de grandes volúmenes de datos.

IP *(Protocolo de Internet o Internet Protocol)*: es el conjunto de reglas que establecen la forma en que los datos son enviados a través de Internet. A su vez, cada dispositivo posee una dirección IP única que le permite ser identificado.

Metadatos o metadata: hace referencia a los “datos de los datos”. Es la información de un dato, pero no es el dato en sí mismo. Por ejemplo, los metadatos de un archivo, documento o fotografía pueden contener la IP del dispositivo con el que fueron creados, el lugar donde se hizo, la fecha, entre otros.

Malware o programa malicioso: tipo de software o programa que pretende infiltrarse y/o dañar un sistema de información sin el consentimiento de la persona usuaria. Por ejemplo: un virus informático.

Nube de almacenamiento: es un servicio que permite guardar y gestionar información en internet. Esta información es alojada en un servidor que suele ser administrado por entidades externas a la persona usuaria.

Phishing: técnica maliciosa utilizada para obtener información como datos de tarjetas de crédito, nombres de usuario y contraseñas, entre otros. Una estrategia común es que los atacantes se hacen pasar por una entidad de confianza para que las víctimas confíen en ellos y revelen sus datos confidenciales con el fin de realizar un robo financiero, de identidad, u obtener acceso a sus cuentas.

Redes Sociales *(RRSS)*: servicios o plataformas de comunicación a través de Internet donde las usuarias pueden crear perfiles o comunidades en línea y comunicarse mediante mensajes, así como compartir información, imágenes o videos, de forma inmediata.

Servidor: es una computadora conectada a Internet que proporciona servicios a otras computadoras conectadas a la misma red. Estos servicios suelen ser: almacenar páginas web, correos electrónicos y nubes, entre otros.

SMS (Short Messages Services o Servicio de mensajes cortos): servicio de telefonía móvil que permite enviar y recibir mensajes entre teléfonos.

Software: conjunto de programas, instrucciones y reglas informáticas que permiten a los dispositivos electrónicos realizar determinadas tareas. Por ejemplo, sistemas operativos, aplicaciones, navegadores web, juegos o programas.

Software de código abierto: se refiere a un tipo software o programa con código fuente que cualquier persona con los conocimientos necesarios puede examinar, utilizar, modificar y mejorar. El código fuente es la parte del software que las y los programadores informáticos manipulan para cambiar el funcionamiento de un programa o aplicación o agregarle otras características.

Software Libre: es un tipo de software o programa que se basa en cuatro libertades: libertad de usar, estudiar, distribuir y mejorar el software. Esto permite su desarrollo continuo, y libre distribución para generar copias o modificaciones. Por tanto, mayor autonomía tecnológica. Este tipo de software se asocia a iniciativas por el derecho de acceso a cultura libre en internet.

Software Espía o spyware: tipo de programa maligno que infecta un dispositivo y extrae de forma oculta y sin consentimiento datos de navegación, información personal, ubicación del dispositivo, registro de llamadas o mensajes, entre otros datos.

Tecnologías de la Información y Comunicación (TIC): conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos y formatos (texto, imagen, sonido, entre otros).

Ticketing: herramienta o sistema utilizado para la gestión, seguimiento y documentación de casos, solicitudes o incidentes en una entidad u organización.

Troll o trol: persona o perfil de redes sociales cuya identidad se suele desconocer y que publica de forma sistemática mensajes en línea con la intención de molestar, alterar y provocar una respuesta emocional por parte de las personas usuarias.

Virus: es un tipo de malware o programa malicioso que tiene la característica de auto propagación, es decir, es capaz de copiarse de un archivo o un ordenador a otro sin el consentimiento de la persona usuaria.

Verificación en dos pasos o autenticación en dos pasos: es una medida de doble protección que consiste en añadir un paso adicional a la contraseña para confirmar que quien accede a una cuenta es la persona usuaria. Suele consistir en el envío de un código de seguridad mediante SMS o correo electrónico; o un aviso al dispositivo registrado en la configuración.

VPN *(Red Privada Virtual o Virtual Private Network)*: herramienta digital que redirige el tráfico de navegación en internet a través de una especie de túnel seguro, que oculta la dirección IP y encripta los datos, protegiendo y ocultando la privacidad de las personas usuarias.

Wi-Fi *(Fidelidad inalámbrica o Wireless Fidelity)*: red de dispositivos inalámbricos, es decir que no requieren de cables, interconectados entre sí y generalmente también conectados a la Internet.

1. ¿Qué es la violencia facilitada por la tecnología contra las mujeres y las niñas?

La violencia facilitada por la tecnología contra las mujeres y las niñas (VFTCMN) es “cualquier acto cometido, asistido, agravado o amplificado por el uso de tecnologías de la información y la comunicación u otras herramientas digitales que resulte o pueda resultar en daños físicos, sexuales, psicológicos, sociales, políticos o económicos u otras violaciones de los derechos y libertades” (ONU Mujeres y OMS, 2022).

Es decir, se refiere a las agresiones que se dan en internet o mediante el uso de redes sociales, correos electrónicos, páginas web, apps, chats de mensajería instantánea, programas informáticos y otras herramientas digitales.

También se denomina **violencia de género facilitada por la tecnología**. Este tipo de violencia tiene graves repercusiones en la vida de las mujeres y la población LGBTIQ+, tanto en salud integral como en el ejercicio de sus derechos humanos

Este tipo de violencia se interrelaciona con otras formas de violencia fuera de línea y en otros contextos como la violencia intrafamiliar, la violencia política, la violencia comunitaria o la violencia simbólica.

Formas de violencia de género facilitada por la tecnología

A continuación, se definen algunas formas de violencia de género facilitada por la tecnología que pueden afectar a integrantes de colectivas, asociaciones, agrupaciones y otras organizaciones sociales de mujeres.

- **Violencia y acoso sexual facilitado por la tecnología:** múltiples actos de carácter sexual que utilizan las TIC para aterrorizar e intimidar mediante amenazas físicas, psicológicas y emocionales, comentarios sexuales, misóginos, transfóbicos, homofóbicos y sexistas no deseados en línea, ya sea públicamente o a través de mensajes directos y privados.

Algunas manifestaciones específicas de violencia y acoso sexual facilitado por la tecnología son:

– **Acoso sexual en línea o ciberacoso sexual:** toda forma de conducta de naturaleza sexual no deseada que tiene por objetivo o consecuencia atentar contra la dignidad de la persona y en particular crear un entorno intimidatorio, hostil, degradante, humillante u ofensivo.

Ejemplos:
- Solicitar citas o prácticas sexuales por medios digitales sin consentimiento.
- Comentarios sexuales o íntimos no solicitados sobre la apariencia, la ropa o partes del cuerpo en redes sociales y chats.
- Insultar o utilizar calumnias con connotación sexual o de género.
- Amenazas de violencia sexual.
- Comentarios despectivos sobre la orientación sexual, identidad o expresión de género.

– **Abuso basado en contenido sexual o íntimo:** elaboración, difusión, manipulación y/o almacenamiento de fotografías, vídeos, textos o audios íntimos o sexuales sin consentimiento.

Ejemplos:
- La difusión de imágenes íntimas o la amenaza de hacerlo, en páginas web, redes sociales, chats de mensajería, entre otros.
- La creación de imágenes sexuales falsas con Inteligencia Artificial.
- La transmisión de agresiones sexuales en línea.
- Grabar vídeos o realizar fotografías íntimos o sexuales sin autorización.
- Utilizar contenido sexual en campañas de desprestigio contra mujeres lideresas, activistas, defensoras de derechos humanos o con perfiles públicos.

– **Contacto para fines sexuales con niñas, niños y adolescentes:** se refiere al contacto de adultos con personas menores de 18 años a través de engaños o para ganarse su confianza a fin de generar situaciones de explotación sexual, entre otras. También se denomina grooming en inglés.

– **Explotación sexual de niñas, niños y adolescentes facilitada por la tecnología:** situaciones de violencia sexual cometidas contra niñas, niños y adolescentes mediante las tecnologías digitales.

– **Extorsión sexual:** situaciones en las que, mediante el uso de la violencia, las amenazas o la intimidación se busca obtener favores sexuales de la víctima o coaccionarla para que realice actos sexuales o con el fin de incitar u obligar a alguien a exhibir su cuerpo desnudo o semidesnudo o en actitudes sexuales.

- **Acceso no consentido a cuentas, dispositivos o sistemas informáticos:** es el acceso no autorizado a redes sociales, correos electrónicos y dispositivos electrónicos con el fin de tomar el control y manipular información o datos personales. Incluye la instalación de software espía, el robo de contraseñas, archivos, fotografías y vídeos o la manipulación de un servidor o página web.

- **Acoso en línea o ciberacoso:** diferentes conductas (diferentes a las de naturaleza sexual) que tienen por objeto el uso de las TIC para abusar, humillar, atacar, amenazar, degradar, intimidar, asustar, ofender y/o insultar a una persona creando un ambiente ofensivo y hostil. Se ejerce en diferentes espacios digitales como las redes sociales, chats de mensajería, páginas web, blogs, correos electrónicos o juegos en línea e incluye comentarios humillantes y amenazas generadas por perfiles reales o trolls, chantajes, extorsión, difamación, vigilancia de la ubicación física y de las publicaciones en línea, entre otros.

- **Desinformación basada en género:** tiene que ver con la utilización de narrativas falsas o engañosas basadas en el género y el sexo, a menudo con cierto grado de coordinación, destinadas a disuadir a las mujeres de participar en la esfera pública, generarle daños, discriminación o situaciones de violencia. Se caracteriza por la falsedad, la intención maligna y la coordinación. El discurso de odio y la desinformación de género pueden estar relacionadas. Incluye: noticias falsas sobre víctimas de violencia, defensoras de derechos humanos, activistas, lideresas comunitarias y otras mujeres con perfiles públicos; información engañosa sobre acciones de defensa de los derechos humanos como el acceso a la interrupción libre del embarazo, el matrimonio igualitario, la educación sexual integral, entre otras.

- **Discurso de odio basado en género:** son aquellos contenidos publicados y compartidos (de forma pública o privada) a través de las TIC que incitan, promueven o justifican el odio motivado por el género y otros factores identitarios (discapacidad, orientación sexual, etnia, religión, nacionalidad, entre otros).

- **Difamación:** la acción de generar información falsa sobre una o varias personas con el fin de dañar su reputación.

- **Difusión de información personal o privada:** revelar datos personales como la dirección, nombre y apellidos, documentos de identidad o ubicación con el fin de dañar. Puede incluir la comunicación de mensajes que incitan a generar agresiones. Se conoce como doxing/doxxing en inglés.

- **Suplantación de identidad:** creación de una identidad falsa a partir del uso de la imagen y datos de una persona sin consentimiento mediante el uso de las TIC, con el fin de amenazarla, intimidarla o dañar su reputación. Incluye la duplicación de perfiles en redes sociales, la creación de cuentas falsas de usuarios en páginas pornográficas u otros sitios web: la duplicación de líneas de atención de servicios de las organizaciones de mujeres con fines maliciosos, entre otras.

- **Violencia algorítmica:** reproducción de estereotipos discriminatorios en el diseño y programación de algoritmos. Incluye la publicidad que promueve prejuicios sobre la belleza, el género y la etnia, la censura de contenido según palabras sobre la promoción de derechos de las mujeres, la población LGBTIQ+, la educación sexual integral, entre otras.

RECUERDA

*La **Ley Orgánica Integral para Prevenir y Erradicar la Violencia contra las Mujeres de 2018**, reconoce el ámbito mediático y cibernético como un espacio donde se ejerce la violencia contra las mujeres. Esta ley establece los derechos de las mujeres sobrevivientes de violencia facilitada por la tecnología para acceder a la justicia, a obtener medidas de protección y reparación con el fin garantizar su seguridad y la no repetición de los hechos y a que se generen políticas de prevención de este tipo de violencia.*

*Consulta la ley aquí: **https://www.lexis.com.ec/biblioteca/ley-prevenir-erradicar-violencia-contra-mujeres***

*Además, el **Código Orgánico Integral Penal** reconoce diferentes delitos relacionados con la violencia facilitada por la tecnología como la violación a la intimidad, el ciberacoso sexual, la extorsión sexual, el contacto con niñas, niños y adolescentes para fines sexual, el acceso no consentido a un sistema informático o la suplantación de identidad (**revisa más delitos en el Anexo 1**)*

*Consulta la ley aquí: **https://www.lexis.com.ec/biblioteca/coip***

AVISO: Este listado no es exhaustivo y puede variar debido a los cambios en las dinámicas de violencia en el ámbito digital. Además, pueden existir diferentes formas de llamar a las manifestaciones de VGFT en los distintos países de la región latinoamericana y otros territorios.

2. ¿Qué son los cuidados digitales?

Los cuidados digitales son medidas y hábitos que permiten estar protegidas en el uso de Internet y de las tecnologías digitales.

Pueden ser medidas tecnológicas, estrategias creativas, acuerdos con otras personas y hábitos de autocuidado que buscan proteger los datos personales, la información sensible, la privacidad de las personas, su integridad, su salud, así como sus relaciones y actividades en línea y fuera de línea. (Taller de Comunicación Mujer, 2024)

Ejemplos de cuidados digitales:
usar comunicaciones seguras; sistemas de cifrado de la información personal y colectiva; actualizar los dispositivos; utilizar navegación segura; aplicar dinámicas de desconexión de las redes sociales, entre otras.

El enfoque de cuidados digitales excede el concepto de seguridad digital desarrollada y dirigida exclusivamente a empresas y Estados. Se centra en las necesidades de las personas que usan internet y las tecnologías digitales desde la experiencia de las mujeres, las personas LGBTIQ+, las niñas, niños y adolescentes, los pueblos y comunidades indígenas, afros, entre otros.

Conocer y practicar cuidados digitales forma parte de los derechos digitales de las mujeres y de todas las personas. Además, permite garantizar el ejercicio de otros derechos digitales como el derecho a la intimidad, la privacidad, la integridad, la protección de los datos personales y la libertad de expresión.

Enfoque de protección integral

Los cuidados digitales se deben abordar desde un enfoque protección integral que permita abarcar las diferentes aristas que pueden afectar a las mujeres integrantes de las organizaciones sociales de manera interrelacionada.

De esta manera, es importante abordar la protección desde tres aspectos: el físico, el psicosocial y el digital. Estos componentes dependen de cada persona y organización, por lo que es fundamental realizar un análisis particular.

Algunas preguntas de partida pueden ser:

- **Protección física:** ¿qué medidas podemos tomar para hacer más seguro nuestro entorno físico? ¿cómo podemos habitar y transitar de manera segura?

- **Protección psicosocial:** ¿qué redes de apoyo podemos fortalecer? ¿qué prácticas de salud integral atendiendo a la dimensión emocional podemos sumar?

- **Protección digital:** ¿qué herramientas y cuidados digitales debemos conocer e implementar?

"Los cuidados digitales son una forma de abordar la seguridad digital a partir de la perspectiva del cuidado cotidiano. Una vez que lo online y offline son indisociables, y que las tecnologías digitales hacen parte de nuestro día a día, lo que afecta nuestros datos también impacta nuestros cuerpos. Así, desde la perspectiva de los cuidados digitales, cuidar de nuestros datos también es cuidar de nuestro cuerpo, y ese cuidado necesita ser hecho diariamente, como un hábito, una cultura, una política." (Amelia e Foz, Marialab (2022)

3. ¿Por qué es importante protegernos? Riesgos digitales para las organizaciones de mujeres

¿Cómo funciona Internet?

Internet significa red de redes, en inglés interconnected networks. Es decir, es una serie de computadoras que se conectan entre sí, que gestionan y almacenan información.

Al usar internet dejamos una huella digital con información que puede ser almacenada en diferentes servidores o computadoras.

HUELLA DIGITAL

Es el rastro que las personas dejan en Internet a través de sus comunicaciones y conexiones. Incluye toda la información que se sube y baja mediante redes sociales, páginas web, apps de mensajería, búsquedas en navegadores, y/o datos que se comparten en servidores de Internet (por ejemplo, la ubicación).

Estas computadoras pueden pertenecer a empresas privadas o instituciones públicas donde las políticas sobre el tratamiento de los datos y su almacenamiento no son siempre claras o de conocimiento público. Algunas empresas incluso pueden guardar y vender información sobre las personas usuarias con fines lucrativos o no contar con la suficiente seguridad para proteger la información adecuadamente.

Por ello, es necesario adoptar medidas que aseguren mayor privacidad y la protección de la información personal y de nuestras organizaciones, además de generar acuerdos con terceros sobre el manejo de nuestros datos.

El funcionamiento de Internet nos plantea algunas preguntas:

- ¿Qué datos sabe Internet sobre las integrantes de la organización?
- ¿Qué información es pública? ¿puede esta información ponernos en riesgo?
- ¿Cuán confiables son los lugares donde guardamos nuestra información? ¿Quiénes podrían tener acceso?
- ¿Tomamos suficientes medidas de manera personal y colectiva para proteger nuestros datos?

Conoce más...

Sobre qué es internet y cómo funciona:
https://developer.mozilla.org/es/docs/Learn/Common_questions/Web_mechanics/How_does_the_Internet_work

Riesgos digitales de las organizaciones sociales de mujeres

Las organizaciones de mujeres enfrentan diferentes riesgos digitales según el trabajo que realizan y la identidad y contextos de las personas que las integran. A continuación, se recogen algunos de los riesgos digitales comunes.

- **Múltiples actores que pueden generar agresiones en línea y fuera de línea:** Estado, crimen organizado, grupos anti derechos, empresas transnacionales y locales, agresores de víctimas de violencia que acompaña la institución, personas que realizan estafas en línea, entre otros.
- **La violencia facilitada por la tecnología es recurrente hacia las organizaciones sociales y personas con perfiles públicos** como activistas, políticas, periodistas, comunicadoras, lideresas barriales, estudiantiles y de territorio, entre otras. En concreto, el robo de información y dispositivos; los discursos de odio; la difusión de contenido sexual e íntimo; la difamación; el ataque a servidores y páginas webs de las organizaciones; entre otras.
- **Falta de políticas de protección integral**, incluida la seguridad digital, hacia defensoras de derechos humanos, activistas y organizaciones sociales.
- **Falta de infraestructura y recurso**s que permitan fortalecer las medidas de protección digital de las organizaciones: formación continua en cuidados digitales; sitios web con servidores propios; programas y apps que no dependan de empresas privadas con políticas de tratamiento de datos no accesibles; brecha digital entre las diferentes integrantes, entre otros.
- **Actividades que implican la creación y difusión de contenidos en línea.**
- **Obstáculos para acceder a la justicia e impunidad** en casos de delitos relacionados a violencia facilitada por la tecnología.
- **Contextos de inseguridad, discriminación y violencia estructural por diferentes causas** (género, etnia, edad, nacionalidad etc.) aumentan la posibilidad de vivir violencias en el ámbito digital.

Análisis de riesgo

En una organización social, será fundamental analizar los riesgos de la institución y aquellos que pueden darse de manera particular hacia cada integrante, tanto por las actividades al interior de la organización como por su contexto y características específicas.

Nivel individual
(sobre cada integrante de la organización)

¿Qué riesgos identificas considerando estos aspectos?

- **Sobre tu identidad y las condiciones sociales:** edad, etnia, identidad y expresión de género, orientación sexual, situación migratoria, condición de discapacidad, situación socioeconómica, personas bajo su cuidado, entre otros. Estas condiciones pueden generar mayor vulnerabilidad hacia las integrantes en contexto de discriminación y desigualdad social.
- **Territorio:** factores que pueden existir asociados al lugar de residencia, el hogar el vecindario, el lugar de trabajo, los espacios de estudios y los medios de transporte. Por ejemplo: residir en un sector inseguro; no contar con medios de transporte seguros, vivir en espacios donde la violencia de género es recurrente, entre otros.
- **Actores que pueden generar amenazas o implicar vulnerabilidades:** el gobierno, los grupos anti derechos, el crimen organizado, las plataformas de redes sociales y los proveedores de Internet, la familia, las amistades, compañeras de trabajo y/o de la organización, entre otros.
- **Actividades:** el tipo de trabajo que se realiza; si se es activista y si se tiene un perfil público o roles que implican intereses hacia otros actores; si se estudia o se realizan actividades extracurriculares, si se crea contenido de Internet, entre otras.

Por ejemplo:

- el gobierno puede ser un actor recurrente en generar amenazas de vigilancia hacia las integrantes de organizaciones sociales y acceder sin consentimiento a su información;

- las plataformas de redes sociales pueden exponer a riesgos los perfiles de las integrantes si no cuentan con políticas eficaces de protección frente a amenazas y violencias digitales;

- las personas del entorno cercano de las integrantes pueden ser objeto de ataques digitales con el fin de buscar información.

Nivel colectivo
(sobre las organizaciones)

¿Qué riesgos identifican teniendo en cuenta los siguientes aspectos?

• **Sobre la identidad de la organización:** qué tipo de organización es, con qué grupos poblacionales trabaja o acompaña, cuál es su alcance, entre otras.

• **Actores que pueden generar amenazas o implicar vulnerabilidades:** el gobierno, los grupos anti derechos, el crimen organizado, las plataformas de redes sociales y los proveedores de Internet, empresas transnacionales o privadas, personas cercanas a integrantes de las organizaciones o de las personas con las que trabajan o acompañan, entre otros.

• **Territorio:** lugar de las instalaciones de la organización, si la infraestructura solo es digital al no haber oficina física, espacios donde se generan encuentros, talleres, jornadas y otras actividades con diferentes grupos poblacionales u otras organizaciones, medios de transporte, entre otras.

• **Actividades:** si crea y genera contenido en internet y campañas comunicacionales, si realiza incidencia política, acompañamiento a víctimas de violencia, patrocinio legal, entre otras.

Recomendaciones para realizar un análisis de riesgo

• Generar el análisis tanto a nivel individual como colectivo. Es importante que cada integrante de la organización pueda compartir alertas que haya identificado en el análisis de riesgos individuales para que se puedan tomar las medidas necesarias de forma colectiva.

• De ser necesario, solicitar apoyo a organizaciones de confianza y especializadas en violencia facilitada por la tecnología o seguridad digital, con el fin de identificar nudos críticos.

• Hacer el análisis de riesgo de manera periódica y cada vez que haya una alerta o incidente de seguridad para revisar el contexto y actualizar posibles medidas de protección.

Conoce más...

Sobre cómo hacer un análisis de riesgo aquí: **https://hiperderecho.org/wp-content/uploads/2020/11/Kit-de-cibercuidado-para-activistas-.pdf**

Tips para detectar incidentes de seguridad y alertas de violencia facilitada por la tecnología

Algunas señales de alerta que puede estar relacionadas con violencia en línea o conllevar agresiones digitales, y que, en caso de ser detectadas, deben ser tomadas en cuenta son:

• Si otras personas constantemente saben dónde están, lo que hacen, o con quién hablan, aunque no se lo hayan dicho.

• Si otras personas han tenido acceso a sus dispositivos sin consentimiento o si han accedido con autorización, pero se sospecha que han revisado las redes sociales, correos electrónicos o descargado archivos desconocidos o extraños.

• Si otras personas utilizan su información para conseguir algo a cambio a través del chantajes o manipulaciones.

• Si les solicitan datos personales sin motivo aparente o sin darles información suficiente sobre para qué será usada.

• Si reciben llamadas y mensajes recurrentes de perfiles falsos o desconocidos.

• Si les presionan a entregar contraseñas, información o contenidos digitales.

• Si perciben que sus publicaciones tienen menor alcance de lo normal sin una razón aparente.

• Si empieza a filtrarse información que solo conocía un número reducido de personas.

• Si sus dispositivos empiezan a fallar o a tener comportamientos extraños.

• Si se reciben enlaces, archivos o correos extraños, desconocidos, con alertas, o que no sea posible verificar suprocedencia y se han abierto, podrían contener un virus o software espía.

4. Prevenir riesgos y agresiones en línea: cuidados digitales para estar más seguras

Los cuidados digitales son fundamentales, tanto para prevenir situaciones de violencia de género facilitada por la tecnología, como, para dar respuesta a las agresiones virtuales.

En esta sección, se recogen cuidados digitales que pueden ser aplicados por cualquier persona y organización.

Abordamos los cuidados digitales desde dos dimensiones:

Parte 1. Cuidados digitales de las integrantes de la organización	Parte 2. Cuidados digitales de las organizaciones
Medidas de seguridad digital que cada participante puede adoptar de manera cotidiana. Se refiere a las acciones que las integrantes aplican para proteger sus cuentas personales y sus dispositivos como celulares y computadores.	Recomendaciones para abordar la seguridad digital colectiva de la organización. Se refiere a los protocolos internos de comunicaciones seguras y almacenamiento de información de la información interna; al uso seguro de herramientas de trabajo que se utilizan para gestionar la información y comunicarse, entre otros cuidados.

Parte 1 - Cuidados digitales de las integrantes de la organización

Parte importante de los cuidados digitales de las organizaciones sociales de mujeres son los hábitos de seguridad digital que cada integrante tiene en sus dispositivos y cuentas.

Así, los cuidados digitales personales son un componente fundamental de la seguridad colectiva de las organizaciones de mujeres. Uno de los riesgos frecuentes es que actores externos intenten obtener información de una organización a través de los dispositivos y cuentas personales de sus integrantes.

Por ello, es necesario empezar por abordar cuidados digitales que podamos aplicar en nuestro uso cotidiano de Internet y las tecnologías digitales.

Practica el consentimiento digital

Para abordar los cuidados digitales, es importante preguntarnos si aplicamos activamente el consentimiento en el ámbito digital.

El consentimiento digital son las acciones que generamos con otras personas para sentirnos seguras y cuidadas en el uso de Internet y las tecnologías. Es una práctica libre y voluntaria que se basa en acuerdos, respeto, límites, deseos, confianza, seguridad, y otros hábitos de cuidado entre personas que se relacionan (Taller de Comunicación Mujer, 2024).

Características del consentimiento digital
(Taller de Comunicación Mujer, 2024)

- **Libre y voluntario:** sin manipulaciones, intimidaciones o violencia.
- **Específico:** es concreto y claro.
- **Explícito:** es evidente, aunque puede ser verbal y no verbal.
- **Cotidiano:** va más allá de las prácticas sexuales, es una práctica habitual.
- **Revocable:** debe ser revisado a lo largo del tiempo.
- **Es una explicación en sí misma:** no es necesario justificarlo.

Hábitos de consentimiento digital

• ¿Preguntas a tus compañeras de tu organización si puedes compartir su contacto antes de enviárselo a otras personas?

• Si vas a hacer una publicación en redes sociales, ¿consultas antes si puedes difundir imágenes o vídeos en Internet con las personas que aparecen en el contenido o si las puedes etiquetar?

Usa contraseñas seguras en todas tus cuentas y dispositivos

Así evitarás accesos no consentidos a tus correos electrónicos, redes sociales, celular, computadora, Tablet, laptop, redes sociales y apps.

Los accesos no consentidos pueden llevar a otras agresiones digitales como la suplantación de tu identidad, el robo de archivos, fotos y vídeos, la difusión de contenido íntimo/sexual, de tus datos personales y de información sensible de la organización, entre otras situaciones.

¿Qué es una contraseña segura?

- Tiene al menos doce caracteres con letras mayúsculas y letras minúsculas, números y caracteres especiales (¡%&$#.@/_*?).
- No contiene datos personales como nombres de familiares, fechas de nacimiento o nombres de mascotas.
- Es única y privada, no se repite en tus diferentes cuentas y dispositivos; ni se difunde a otras personas.
- Se cambia de manera periódica, al menos una vez al año. Si vives una situación de riesgo, con mayor frecuencia: cada tres meses.

Evita el uso de:

- **Pin – Es una clave demasiado corta y, por tanto, fácil de identificar.**
- **Patrón – Deja huellas en tu pantalla y puede replicarse con facilidad.**
- **Huella dactilar o reconocimiento facial – Si estás en una situación de violencia, inconsciente o en estado de vulnerabilidad, podrían forzarte a entrar a tu celular a través de tus datos biométricos. ***

***Ten en cuenta que los datos biométricos son datos personales que permiten identificarte. Es importante cuestionarte en qué dispositivos se registran y a qué empresas se facilitan, especialmente si realizas actividades de riesgo como defensora de derechos humanos, debido a los peligros que puede implicar un mal uso de estos datos por parte de terceros.**

Pasos para crear una contraseña segura

- Elige una frase fácil de recordar o la letra de una canción con al menos 12 caracteres: como la flor con tanto amor
- Junta las palabras: comolaflorcontantoamor
- Incluye mayúsculas: comolaflorContantoAmor
- Sustituye vocales por números: c0mol4florContantoAmor
- Sustituye otras letras por símbolos, y/o suma símbolos a la frase: c0mol4flor&ContantoAmor%
- ¡Perfecto! Ya tienes un ejemplo de contraseña segura: c0mol4flor&ContantoAmor%

RECUERDA: También puedes generar contraseñas de manera automática y aleatoria con un gestor de contraseñas o cuando las aplicaciones y programas te den la opción.

¿Dónde puedes guardar tus contraseñas?

- En un **gestor de contraseñas** de confianza.

Un gestor de contraseñas es un programa capaz de generar un archivo o base de datos encriptado con toda la información necesaria para acceder a tus diferentes cuentas. Es un registro de: nombres de usuaria, contraseñas y enlaces de inicio de sesión organizados y protegidos por una contraseña maestra que siempre deberás recordar para tener acceso al archivo.

Los gestores de contraseñas además pueden generar claves seguras para tus cuentas de manera automática y aleatoria.

Un indicador de confiabilidad a la hora de elegir un gestor de contraseñas es que la base de datos se almacene donde tú decidas (por ejemplo, en tu computadora) y no en los servidores o nubes de una empresa o de terceros.

Esto implica que serás la única persona responsable de guardar tu información y que, en caso de pérdida del archivo o de la contraseña maestra, no tendrás acceso. Pero ¡no te preocupes! Al ser un archivo encriptado es posible almacenar varias copias en diferentes lugares (en tu nube, en una memoria USB o un disco externo). Recuerda que cada vez que aumentes nuevas contraseñas en tu gestor, deberás actualizar de forma manual todas las copias que hayas hecho del archivo.

- Si no puedes usar un gestor de contraseñas, escríbelas en lugares ocultos de tu casa, o que no suelas transportar con frecuencia, como un cuaderno o una carpeta secreta o cifrada de la computadora con un nombre no identificable.
- ¡Evita anotar tus claves en tu celular! Por si lo pierdes o te roban.

¡Super consejo!

Activa la verificación en dos pasos en tus cuentas de correos electrónicos, redes sociales y apps de mensajería. También puedes encontrar esta opción como “autenticación de dos pasos”, “autentificación de dos factores” o de doble factor.

Opción de gestor de contraseñas

- **KeePassXC** es gratuito y sirve para celular (Android y iOS) y computadora.
  - Descarga para escritorio: https://keepassxc.org/
  - Para celular, búscalo en la opción de tienda, App Store o Play Store.
  - Guías para instalación y uso de KeePassXC: https://ciberpatrulla.com/keepassxc/ https://ssd.eff.org/es/module/c%C3%B3mo-usar-keepassxc#como-funciona-keepassxc

La **verificación en dos pasos** es una doble protección que consiste en añadir un paso más a la contraseña para confirmar que quien accede a tus cuentas seas tú misma. Suele consistir en el envío de un código de seguridad mediante SMS, correo electrónico o WhatsApp; un aviso al dispositivo que hayas registrado en la configuración o la validación de un código mediante una app de autentificación.

La verificación de dos pasos puede usar códigos de recuperación en caso de pérdida del acceso, recuerda guardarlos siempre un lugar seguro como tu gestor de contraseñas.

¿Cómo activar la verificación de dos pasos?

App/plataforma	Entra en...
Instagram y Facebook	Centro de cuentas<Contraseña y seguridad<Autentificación de dos pasos
Signal y WhatsApp	Ajustes<Cuenta<Verificación en dos pasos
Cuenta de Google	Seguridad<Cómo inicias sesión en tu Google<verificación en dos pasos

Estas indicaciones pueden variar a lo largo del tiempo según la aplicación. Para otros servicios, busca la opción en Ajustes o Configuración y en Cuentas, Seguridad o Privacidad.

Utiliza comunicaciones seguras

Apps de mensajería

Algunos componentes que hacen confiable una app de mensajería son:

- Cifrado de extremo a extremo en los mensajes.
- Recopilación mínima de datos de las personas usuarias.
- Múltiples opciones para ocultar y/o eliminar información como mensajes, archivos, imágenes, vídeos, datos de las personas usuarias.
- Transparencia en sus políticas de tratamiento de datos y funcionamiento del servicio.

La recopilación mínima de datos y la transparencia son especialmente relevantes para mujeres integrantes de organizaciones sociales, ya que la filtración de su información personal, de sus compañeras y personas cercanas o de su organización puede ponerlas en riesgo.

Opción de mensajería segura

- **Signal:** es una app de software libre de descarga gratuita en versión para celular y escritorio que se financia con donaciones de usuarias/os. Es decir, no tiene fines de lucro a través de la recolección de datos para publicidad o investigación.

Signal no almacena metadatos de las comunicaciones ni la lista de contactos. Además, al ser una app de código abierto garantiza mayor transparencia, ya que puede auditarse por terceras personas para verificar sus políticas de funcionamiento.

Descarga para escritorio y celular: https://signal.org/es/download/ o búscala en la opción de tienda, Play Store o App Store de tu celular.

Existen varias diferencias entre Signal y WhatsApp. WhatsApp, propiedad de Meta, recopila más datos de las personas usuarias y, al ser de código cerrado, no es posible comprobar sus políticas de funcionamiento. Esto implica que no se conoce con claridad el uso que podrían hacer de los datos a los que tienen acceso.

Correos electrónicos

A la hora de elegir una plataforma de correos es crucial verificar que el contenido de las comunicaciones esté cifrado. Además, algunos proveedores de correo como Gmail, Outlook y Yahoo! pueden tener mayor acceso a tus datos y usarlos con fines lucrativos de publicidad, entre otros. De esta manera, la información de integrantes de organizaciones sociales puede ser vulnerable si se usan estos servicios.

Opciones de correo seguro

- **Mail de Riseup** (https://riseup.net/es): requiere de un código provisto por una usuaria que cumpla de los requisitos necesarios como mecanismo adicional de seguridad.

- **Mail de Autistici** (https://www.autistici.org/): permite crear una cuenta tras llenar un formulario donde se explicite la necesidad de tener una cuenta de correo segura.

Estas opciones se diseñaron pensando en las necesidades de activistas y defensoras de derechos humanos, por lo que aportan mayor seguridad. Ambas son de uso gratuito y se sostienen a partir de las donaciones de quienes utilizan sus servicios y de otras organizaciones.

- **Protonmail** (https://proton.me/es-es/mail): usa cifrado de extremo a extremo. Si bien se diferencia de las dos anteriores en que pertenece a una empresa privada, tiene configuraciones de seguridad avanzada.

Toma en cuenta que cuando nos comunicamos por correo entre distintas plataformas, es complejo garantizar la protección de los datos.

Por ejemplo, si alguien envía un correo con su cuenta de Riseup a su compañera que también usa Riseup, resulta seguro que la comunicación está cifrada. Sin embargo, si alguien envía el mismo correo desde su cuenta de Riseup a una persona que tiene una cuenta de correo sin cifrado de extremo a extremo, la información podría verse vulnerada.

Por esta razón, para algunas comunicaciones, las apps de mensajería pueden ser más seguras, ya que garantizan la comunicación a través de un mismo proveedor.

RECUERDA: si usas WhatsApp u otras apps que recopilen datos de las personas usuarias, evita compartir información sensible como datos personales o información confidencial tuya y de personas de tu entorno u organización. Activa todas las opciones de seguridad disponibles: verificación en dos pasos, mensajes temporales, visualización única de archivos y fotos, ocultar tu estado y foto de perfil a números desconocidos, usa un seudónimo en tu nombre de usuario y todas aquellas que te permitan mayor privacidad. Revisa las configuraciones de WhatsApp con frecuencia, ya que pueden cambiar con el tiempo e introducir medidas de seguridad adicionales.

Plataformas de videoconferencia

Algunos criterios para elegir una plataforma de videoconferencia se refieren a que las comunicaciones estén cifradas, que cuenten con políticas de privacidad claras, o se guarden grabaciones en servidores desconocidos, y se alojen en servidores seguros (por ejemplo: de la organización o de otras organizaciones sociales de confianza).

Opciones de plataformas de videoconferencia segura

- **Jitsi Meet** (https://jitsi.es/): es una plataforma gratuita, no requiere descargar ninguna app y funciona directamente desde cualquier navegador. La capacidad de participantes depende del servidor, generalmente suele ser 75. En caso de mayor necesidad de asistentes, se puede usar la opción adicional de retransmisión en vivo a través de YouTube.

Para usarla, se debe asignar un nombre a la reunión y compartir el enlace generado con el resto de asistentes.
– Guía de uso aquí: https://jitsi.es/ayuda/

Para mayor seguridad, coloca una contraseña de ingreso y teclea un nombre aleatorio de la sala de reunión, ya que, si se usa uno común como "Reunión lunes", podría coincidir que otras personas generen un enlace con el mismo nombre, permitiendo a desconocidos ingresar por error o con la intención de causar daño.

Además, también puedes usar Jitsi a través de servidores seguros en los siguientes enlaces (la capacidad de participantes puede variar):

– https://chimamanda.vedetas.org/
– https://meet.mayfirst.org
– https://meet.greenhost.net
– https://vc.autistici.org

- **Big Blue Button** (https://bigbluebutton.org/): es una alternativa que requiere la instalación en un servidor propio o contratado. Infórmate con organizaciones de confianza que provean este tipo de servicios en Ecuador o que ya hayan usado esta plataforma.

- **Llamadas y videollamadas grupales por Signal:** las apps de mensajería segura, como Signal, te permiten hacer videollamadas hasta con cincuenta personas e incluso tiene la opción de compartir pantalla desde una computadora. Ten en cuenta que la capacidad de asistentes a una llamada grupal puede verse afectada por factores como la cobertura, entre otros.

Consulta más información aquí: https://support.signal.org/hc/es/articles/360052977792-Llamadas-y-videollamadas-grupales

Llamadas y SMS

Las llamadas tradicionales de telefonía celular o convencional y los SMS no suVelen utilizar sistemas de cifrado de extremo a extremo que permitan proteger el contenido de las conversaciones frente a posibles vulneraciones como escuchas no consentidas. Por tanto, pueden resultar riesgosas.

Se recomienda el uso de llamadas telefónicas por Internet a través de apps de mensajería segura como Signal y evitar el envío de SMS.

Revisa con frecuencia las opciones de seguridad y privacidad de tus comunicaciones

Aunque depende de cada proveedor de correo, aplicación u otros servicios, usualmente estas opciones se encuentran en la sección de Ajustes o Configuraciones > Privacidad y Seguridad. Algunas medidas que puedes aplicar son:

Apps de mensajería	• Activa el cifrado de extremo a extremo si no viene configurado por defecto. • Evita hacer una copia de seguridad de tus chats si la nube donde se guardarán no cuenta con cifrado (actualmente, Google Drive no cuenta con cifrado). • Desactiva las notificaciones donde pueda leerse el texto de los mensajes con la pantalla bloqueada. • Coloca la opción de restringir capturas de pantalla. • Oculta tu número de celular si te lo permite. • Activa la verificación en dos pasos.
Correos electrónicos	• Desactiva los permisos de ubicación. • Revisa que el correo de recuperación esté actualizado y sea tuyo. • Comprueba que en los inicios de sesión solo aparezcan tus dispositivos. Si encuentras otros, haz captura de pantalla para guardar la evidencia del evento inseguro y elimínalos. • No abras enlaces extraños o desconocidos o que pidan ingresar tu nombre de usuario y contraseña desde el correo el electrónico ya que podría tratarse de un ataque de *phishing*.
Plataformas de videoconferencia	• Genera un código de acceso a las salas para mayor seguridad. • Revisa que la configuración no permita que puedan ingresar personas a una sala sin tu autorización. • Puedes usar la opción de silenciar micrófonos para evitar interrupciones o comentarios inapropiados en reuniones donde haya personas desconocidas.

Usa navegación segura

Navegar en internet con mayor privacidad y anonimato reduce la huella digital y previene que se filtren los datos personales o información sensible.

• Revisa que los sitios web donde navegas usen HTTPS y aparezca un candado en la barra de direcciones del navegador. La “s” significa “seguro”, y que las comunicaciones están encriptadas.

http://en.wikipedia.org/ ¡Alerta, sitio web inseguro!	https://en.wikipedia.org/ ¡Sitio web seguro! ¡Puedes entrar!

• Ten en cuenta las alertas que indican que un sitio web puede ser inseguro: si el navegador te advierte que se trata de un lugar “no seguro” o un símbolo de candado con un triángulo amarillo o una barra roja; cuando en el enlace de la página web hay caracteres especiales o letras que no se corresponden a la identidad del sitio (verifica siempre el nombre verdadero del sitio web); o si contiene excesiva publicidad, ya que algunos anuncios podrían contener malware si accedes a ellos.

Recuerda: algunas técnicas de phishing clonan las direcciones del sitio web para acceder a tus datos. Suele ser frecuente en páginas donde debes colocar tu nombre de usuario y contraseña como la página de tu banco. Asegúrate siempre que el nombre de las páginas web se corresponde a la oficial del sitio.

https://www.pichinchas.com/ ¡Alerta, sitio web inseguro!	https://www.pichincha.com/ ¡Sitio web seguro! ¡Puedes entrar!

• Elimina tu historial de navegación con frecuencia para reducir tu huella digital.

• Evita conectarte a redes de Wi-Fi públicas de parques, instituciones, aeropuertos, entre otros espacios. Estas pueden ser objeto de ataques para obtener información. Si las usas, activa un VPN; comprueba que las direcciones de las páginas web no sean falsas en el sitio oficial y que usan HTTPS.

• Asegúrate de revisar las configuraciones de las cookies de los sitios webs que visitas. Algunas cookies pueden registrar datos de ubicación, ventanas abiertas, y otros datos por lo que se recomienda usar las esenciales para la navegación y rechazar el resto.

• Realiza búsquedas en Internet con tus datos personales (nombre, número de teléfono, cédula, domicilio, imágenes) y observa los resultados. Si aparece información sobre ti, o consideras que hay datos sensibles circulando, solicita la baja del contenido al sitio web a través de la información de contacto que este facilite.

Si encuentras tus datos personales a través de Google, además puedes solicitar que no aparezcan en su motor de búsqueda. Ten en cuenta que esto no hará que se retiren de las páginas donde están almacenados, sino que no se mostrarán cuando se busquen a través de Google. Consulta cómo hacerlo aquí:https://support.google.com/websearch/troubleshooter/3111061?hl=es

• Usa una VPN para proteger la dirección de tu IP y así evitarás que se identifique. Una opción es la VPN de Riseup: https://riseup.net/es/vpn.

• Si usas extensiones de internet, investiga sobre el proveedor y sus políticas de tratamiento de la información para evitar que se recopilen tus datos.

• Utiliza navegadores y buscadores que garanticen mayor privacidad y seguridad.

Diferencia entre navegador y buscador

Navegador: es un programa que permite visualizar páginas web de manera sencilla. Actúa como un intermediario entre las personas que usan Internet y la red, interpretando el lenguaje informático de una forma gráfica y amigable.

– Ejemplos de navegadores: Google Chrome, Mozilla Firefox, Internet Explorer, Opera, Safari, Tor, Brave.

Buscador: es un programa que permite buscar información en Internet a través de palabras clave. También se le conoce como “motor de búsqueda”. Para que un buscador funcione, se necesita tener un navegador instalado.

– Ejemplos de buscadores: Google, DuckDuckGo, Yahoo! y Bing.

Opciones de navegadores seguros

• **Navegador Tor:** pertenece al Proyecto Tor que busca brindar diferentes servicios seguros desde la configuración de su diseño para enfrentar la censura y vigilancia en Internet.
– Descarga: https://www.torproject.org/es/download/
– Instrucciones de uso: https://tb-manual.torproject.org/es/running-tor-browser/

• **Brave:** es un navegador que garantiza mayor privacidad y bloquea anuncios.
– Descarga: https://brave.com/es/download/
– Tutorial de instalación: https://www.youtube.com/watch?v=E1Wg_-H0Reg

Opciones de buscadores seguros:

• **DuckDuckGo:** es un motor de búsqueda que garantiza mayor privacidad al no recopilar datos de las personas usuarias y evitar el rastreo en Internet. Conoce más aquí: https://www.xataka.com/basics/duckduckgo-que-principales-diferencias-google
– Descarga: https://duckduckgo.com/&search
– Guía para configurarlo: https://elsoftwarelibre.com/configurar-duckduckgo-en-espanol-alternativa-a-google/

Sobre fake news o noticias falsas

Es común que se divulgue información falsa en Internet, con el fin de desinformar, incitar a la violencia fuera y dentro de línea o desalentar acciones de promoción de los derechos humanos.

Algunas pautas para identificar la información falsa:

- Si la fuente de la noticia está incompleta, no aparece o no es clara es recomendable contrastar la noticia con varias fuentes diferentes.
- Si en los videos o audios que recibimos por chats aparece una pestaña donde se lee “reenviado muchas veces” es posible que se trate de noticias falsas.
- Si en los videos o audios recibidos no se menciona el lugar y fecha en que ocurren los eventos, puede que esa información se haya sacado de contexto para promover noticias falsas.
- Las fotos de noticias que no van acompañadas con el enlace del artículo completo pueden haber sido alteradas para difundir información falsa.
- Los títulos sensacionalistas que no están acompañados de las fuentes de donde se ha obtenido la información pueden tratarse de información tergiversada.

Algunos tips para detectar perfiles falsos

- El usuario no tiene foto de perfil, es una caricatura, o utiliza fotos sospechosas o extrañas.
- No tiene publicaciones ni muchos seguidores o son escasos.
- La apertura de su cuenta es reciente.
- Realiza comentarios con discurso de odio, incoherentes o inadecuados en tus publicaciones o por mensajes privados.
- Te envía enlaces extraños o con contenido malicioso.

¿Qué puedes hacer para verificar un perfil?

- Pregunta a tus amistades en común en las redes sociales si conocen el perfil y si es real y confiable.
- Si se trata de una institución o empresa de servicios, busca fuentes dentro y fuera de línea que confirmen que se trata de una entidad real.
- Haz preguntas al perfil para indagar sobre su identidad, actividades, o los servicios que ofrece. Si detectas alguna respuesta incoherente, extraña o fuera de contexto, sigue tu intuición y para la conversación.

Revisa la privacidad y seguridad en tus redes sociales con frecuencia

- Ten tu perfil en modo privado si no necesitas un perfil público por las actividades que realizas.
- Evita colocar tu nombre completo en perfiles privados. Puedes usar un seudónimo o nombres creativos.
- Evita difundir información personal tuya y de otras personas (domicilio, ubicación, cuenta bancaria, celular, nombres de familiares y compañeras/os de trabajo, entre otras). Además, revisa si tienes fotos y vídeos antiguos con datos personales y si es así, elimínalos.
- Desactiva los permisos de ubicación y no compartas historias en tiempo real donde se pueda identificar el lugar en el que estás tú o tus compañeras.
- Evita agregar entre tus contactos a personas desconocidas. Si tienes dudas sobre un perfil, pregunta a tus amigas/os en común si se trata de un contacto real y conocido.
- Actualiza con regularidad el correo y teléfono de recuperación de tus cuentas.
- Revisa con frecuencia tus inicios de sesión para asegurarte que solo tú entras a tus cuentas desde tus dispositivos.
- Controla quién puede etiquetarte y ver tu información. Activa las opciones más restringidas (solo tú o tus amigos/seguidores) y si te sientes en riesgo, valora desactivar el etiquetado de terceros temporalmente.

Sobre cuentas públicas

Si tienes un perfil público debido a las actividades laborales o las de tu organización, revisa estos consejos:

- Evita compartir información personal o privada como el domicilio, cuenta bancaria, datos e imágenes de familiares o de tu entorno cercano.
- Puedes tener una cuenta privada adicional para generar interacciones con perfiles conocidos o cercanos.
- Si necesitas exponer tu contacto en la red social, revisa la posibilidad de tener un número adicional diferente a tu teléfono personal.
- Oculta tu lista de amigos o seguidores a otros contactos. Limita comentarios con palabras ofensivas o bloquea la posibilidad de que otras cuentas comenten en tus publicaciones.
- Acuerda encuentros presenciales o entrega de productos en lugares seguros diferentes a tu domicilio y genera un plan de seguridad con otras compañeras, amistades o familiares. Por ejemplo, el envío de tu ubicación durante el encuentro y las medidas de acción en caso de que te encuentres en una situación de riesgo.
- Bloquea y/o elimina posibles perfiles falsos.

¡Recuerda siempre ten una contraseña segura y diferente en todas tus cuentas!

Protege tu celular y otros dispositivos

Así podrás asegurar un buen funcionamiento y prevenir accesos no consentidos, salvaguardar tu información y la que te envían otras personas.

Recuerda que si otras personas han accedido a tu celular con tu permiso también podría ser un riesgo. En caso de que esto ocurra, es importante revisar si han podido acceder a tu contenido o han instalado programas desconocidos que podrían vulnerar tu información.

Consejos para proteger tu información

Si tienes un perfil público debido a las actividades laborales o las de tu organización, revisa estos consejos:

- Oculta nombres y apellidos completos de tus familiares, amistades, compañeras de la organización y trabajo en tus listas de contactos. En su lugar, usa seudónimos, siglas, apodos desconocidos, u otros recursos creativos que recuerdes con facilidad.
- Reduce la cantidad de información que almacenas en tu celular para prevenir que pierdas datos en caso de robo, pérdida, avería o accesos no consentidos.
- Evita guardar información sensible y privada de otras personas como datos de víctimas de violencia, defensoras de derechos humanos, activistas, entre otras.
- Guarda tu información sensible (fotos/vídeos íntimos, datos personales o archivos confidenciales) en lugares seguros. Ejemplos: en carpetas con contraseña o cifradas.

Cómo cifrar tu contenido

Cifrar o encriptar tu contenido y dispositivos es una forma de prevenir que otras personas puedan acceder a ellos.

Veracrypt: es un programa gratuito que sirve para cifrar carpetas, archivos, discos duros, unidades USB, entre otros.

–Descarga**:**
https://www.veracrypt.fr/en/Downloads.html

– Tutorial:
https://www.redeszone.net/tutoriales/seguridad/veracrypt-cifra-archivos-gratis/

Cryptomator: es una app gratuita para cifrar archivos en una nube de almacenamiento.

–Tutorial:
https://protege.la/guias-contenido/basicos-seguridad-digital/

– Descarga:
https://cryptomator.softonic.com/

AVISO: si es la primera vez que vas a cifrar una carpeta, archivo o dispositivo, previamente haz una copia temporal de seguridad de tu información. Una vez realizado el cifrado, comprueba si tienes acceso al contenido y, si es así, elimina esta copia de seguridad.

- Respalda toda la información (archivos, imágenes, vídeos, documentos, entre otros) de tu celular de manera periódica en lugares seguros y después elimínala. Ten en cuenta que acumular demasiada información en tus dispositivos puede exponerte a mayores riesgos en caso de pérdida, robo o accesos no consentidos.

Genera copias de tu contenido en dispositivos que no suelas transportar o en carpetas o discos duros cifrados que guardes en lugares seguros.

- Desactiva los permisos de las aplicaciones que no sean necesarios para su funcionamiento. Presta especial atención a los permisos de acceso a tu micrófono, cámara, ubicación y listado de contactos. Por ejemplo: el buscador de Google no necesita acceder a tu cámara, micrófono y contactos para funcionar. Por lo tanto, no es necesario que estos permisos estén activados.

- Elige que los permisos de ubicación, cámara y micrófono solo se activen mientras esté en uso la app.

- Puedes usar pegatinas para tapar la cámara de tu celular y computadora cuando no la utilices.

- Si tienes familiares menores de 18 años, evita el uso de apps de control parental inseguras. Revisa su política de datos y el acceso a los permisos de cámara, vídeo o audio ya que podrían utilizarse para acceder a tu información.

Recuerda siempre conversar con las niñas, niños y adolescentes sobre los riesgos de internet e informarles sobre su uso seguro y cuidados digitales, antes de instalar apps de vigilancia y control que pueden usarse nocivamente por terceros.

Consejos para cuidar la salud de tu celular y otros dispositivos

- Resetea todos tus dispositivos al menos una vez al año. Busca en Ajustes o Configuraciones, la opción de reestablecer, resetear, o volver a configuraciones de fábrica.

Recuerda que al resetear tus dispositivos toda tu información es eliminada. Realiza un respaldo de los datos previamente en lugares seguros como nubes o discos duros cifrados.

- Evita utilizar nubes de almacenamiento donde no existan garantías claras acerca del manejo de tu información personal y no estén cifradas. Si dudas sobre la transparencia de este tipo de herramientas, cifra las carpetas que subas en ellas para prevenir accesos no consentidos.

- Realiza las actualizaciones del sistema operativo y aplicaciones de manera periódica para un buen funcionamiento.

- Elimina de tu celular, laptop, computadora o Tablet las aplicaciones y programas que no uses o que sean desconocidos.

- Usa un servicio técnico de confianza y entrega tus dispositivos sin información, especialmente, sin datos personales, datos de tu organización, e imágenes o vídeos íntimos o sexuales. Además, elimina el historial de navegación antes de entregarlos.

- Ten siempre un antivirus actualizado en todos tus dispositivos, incluido tu celular. Los virus pueden dañarlo o robar información, incluidos datos de cuentas bancarias o información organizacional. Los virus pueden llegar a través de enlaces, archivos, descarga de programas, correos electrónicos maliciosos, discos externos y USB infectados.

Conoce más...

Revisa *El Estado del Stalkerware en 2023*, un estudio que revela cómo existen programas de vigilancia que se hacen pasar por programas de control parental y aplicaciones antirrobo y afectan recurrentemente a mujeres:
https://media.kasperskydaily.com/wp-content/uploads/sites/88/2024/03/21175229/The-State-of-Stalkerware-in-2023-def.pdf

Opciones de antivirus

– **Avira:**
cuenta con versión gratuita y de pago con mayores opciones. Consulta aquí: https://www.avira.com/es

– **AVG:**
https://www.avg.com/es-es/homepage#mac

Existen diferentes opciones de antivirus. A la hora de elegir uno, consulta en internet opiniones de usuarias/os antes de instalarlos y verifica quiénes son sus propietarios para comprobar si son de confianza.

¿Qué hacer en caso de pérdida o robo?

- Contacta lo antes posible con tu operadora de telefonía para avisar de la pérdida o robo y solicita que bloqueen tu número de teléfono.

- Cambia todas las contraseñas de tus cuentas de redes sociales y correos electrónicos.

- Realiza un duplicado de tu SIM cuanto antes, para recuperar tu número e intenta iniciar WhatsApp y otras apps de mensajería instantánea en otro celular para garantizar que solo tú estés accediendo.

- Cierra las sesiones de inicio de tus cuentas donde aparezca el celular robado o perdido.

- Avisa a tu red de personas cercanas y compañeras de la organización para que tomen las medidas necesarias. Por ejemplo: retirar tu número temporalmente de los chats grupales o revisar si tus perfiles de redes sociales están generando interacciones sin tu consentimiento.

Seguridad digital en manifestaciones y otros eventos

Con frecuencia, las mujeres integrantes de organizaciones sociales participan en eventos públicos y privados que pueden comprometer su seguridad, tales como manifestaciones y plantones por la defensa de sus derechos; acciones sociales en el espacio público; y otros eventos donde puede haber riesgos asociados a la intervención de grupos anti derechos, la policía y otros actores que buscan obtener información de sus actividades o dañarlas.

De esta manera, es crucial tener en cuenta algunas acciones de prevención antes, durante y después de la participación en estos eventos.

Antes del evento	Durante el evento	Después del evento
Asiste en grupo y reporta a personas de confianza horarios y rutas del evento.	Anota números de contacto en una parte de tu cuerpo distinta al celular.	Guarda tu información y resetea tu celular si has experimentado alguna situación de riesgo.
Lleva tu celular con saldo y batería llena.	Usa la cámara sin desbloquear tu celular.	No compartas videos o fotografías donde salgan otras activistas o borra su identidad.
Usa Signal para comunicarte.	Comparte tu ubicación solo en situaciones de riesgo o con apps seguras.	Elimina la información del evento que no sea necesaria.
Genera un plan de seguridad con tus compañeras que incluya contactos a los que acudir en casos de emergencia o detenciones y los puntos de encuentro antes, después del evento, y en situaciones de riesgo.	Si te piden tu celular, recuerda que no puede ser revisado sin una orden judicial. Si eres detenida, pide realizar una llamada desde los teléfonos del lugar al que te lleven, no uses tu celular delante de terceras personas.	Usa Signal para comunicar información sensible sobre el evento.

Opción segura para compartir tu ubicación

En círculo: es una app de software libre que no depende de los chats de mensajería instantánea, como WhatsApp, para ser usada. Permite crear un grupo de personas que pueden comunicarse entre sí, compartir su ubicación y alertar en casos de emergencia.

Consulta más aquí: https://encirculo.org/es/

Autocuidado digital

El autocuidado en Internet y las tecnologías se refiere a las prácticas que contribuyen a cuidar tu salud mental e integral y tus relaciones en línea. Sigue estos consejos:

- Desconéctate de redes sociales y chats de mensajería por periodos concretos o establece horarios de uso específicos. Este tipo de apps suelen contar con opciones para regular su uso como activar el modo silencioso, desactivar notificaciones, entre otras.

- Genera acuerdos con tu entorno sobre los tiempos y formas en los que quieres interactuar. Practica el hábito de comunicar tus periodos de desconexión y descanso y pide que no los interrumpan.

- Activa el modo oscuro o modo lectura para cuidar tus ojos.

- Selecciona el tipo de contenido que revisas. Prioriza el contenido que te genere bienestar, disfrute y aquel que te permita conocer más información sobre los temas que te interesan.

- Restringe o desactiva las opciones de publicidad para evitar contenido que no desees.

- Realiza actividades creativas fuera de línea.

Las prácticas de autocuidado digital se complementan con los cuidados fuera de línea

Consulta esta guía, elaborada por defensoras de derechos humanos y activistas en México y Centroamérica, donde encontrarás varias técnicas que buscan cuidar la salud integral a partir de acciones creativas que no involucran dispositivos o proponen hábitos de descanso, ocio y gestión emocional: https://im-defensoras.testing.sutty.nl/public/00odzb99m8yc9agsn0ssb6q8uwtv/Compendio-de-herramientas-de-autocuidado-definitiva.pdf

Parte 2 - Cuidados digitales de las organizaciones

A la hora de abordar los cuidados digitales a nivel organizacional, es importante partir de algunas preguntas clave:

- ¿Tenemos un instrumento o protocolo de seguridad de la organización que incluya los cuidados digitales?
- Si no tenemos una herramienta escrita: ¿existen acuerdos sobre las comunicaciones, el manejo de la información interna, el uso de dispositivos, programas y herramientas de trabajo?
- ¿Los acuerdos son de conocimiento de todas las personas integrantes de la organización?
- ¿Revisamos estos acuerdos de manera periódica?
- ¿Los cuidados digitales que usamos están adaptados a nuestro contexto, necesidades y trabajo que realizamos?

Plan de cuidados digitales

Una opción para incluir la seguridad digital en la cultura de protección integral de una organización es diseñar un Plan de Cuidados Digitales que contenga las acciones de seguridad digital y protección holística que se implementarán. Este tipo de instrumento puede contemplar:

- **Análisis de riesgos y amenazas** de la organización tanto dentro como fuera de línea. Para ello, revisa los componentes presentados en el capítulo 3 de esta Guía: en el apartado «Riesgos digitales de las organizaciones sociales de mujeres».

- **Análisis de posibilidades, fortalezas, necesidades, alianzas** de la organización que permitirán calcular el nivel de riesgo incluyendo la capacidad de respuesta de la organización. Para ello, será importante incluir en el análisis de riesgo un mecanismo de evaluación y nivelación de riesgo: semaforización, indicadores cuantitativos, categorías cualitativas (riesgo alto, medio, bajo), entre otras que cada organización considere más adecuadas según su funcionamiento.

- **Protocolo de cuidados digitales** que recoja las estrategias de seguridad y cuidados digitales en base a los riesgos y amenazas identificados en el marco de las posibilidades y fortalezas de la organización, además de las acciones en caso de incidentes de seguridad y violencia de género facilitada por la tecnología. El protocolo puede ser un instrumento adicional que se incorpore en el plan general.

- **Acciones de evaluación periódica** de las estrategias de seguridad y cuidados digitales de la organización.

- **Configuración de un equipo responsable** de la implementación de los cuidados digitales acordados. La labor de este equipo es tener una mirada global de los cuidados digitales de la organización, identificar necesidades, generar recomendaciones, hacer seguimiento e impulsar acciones con el conjunto de participantes de la organización. Es fundamental que todas se involucren en el proceso.

Protocolo de Cuidados Digitales

Adicionalmente, un Protocolo permite recoger las acciones y acuerdos específicos de seguridad digital de la organización generados en base a los riesgos identificados, además de las acciones de respuesta frente a amenazas digitales que incluyen situaciones de violencia de género facilitada por la tecnología.

Propuesta de componentes de un Protocolo de cuidados digitales

- Presentación, alcance y objetivos del Protocolo.
- Definiciones (conceptos sobre TIC y violencia facilitada por la tecnología).
- Enfoque de Protección integral.

- Cuidados digitales.
- Contraseñas seguras en dispositivos y cuentas.
- Canales de comunicación segura dentro de la organización y con personas externas.
- Uso seguro de las herramientas digitales de la organización (nubes, bases de datos, apps de encuestas y formularios, entre otros instrumentos)
- Acuerdos sobre el manejo y respaldo de la información interna (en oficina, teletrabajo, en nubes, desplazamientos, entre otros ámbitos)
- Cuidados físicos y digitales durante desplazamientos o encuentros con otros actores.
- Cuidados de los dispositivos (celulares, computadoras, discos duro, USB, otros).
- Manejo seguro de redes sociales y sitios web de la organización en caso de tenerlas.
- Autocuidado y cuidado colectivo.
- Cuidados digitales personales de las integrantes.
- Procedimiento en caso de entrada y salida de integrantes (entrega de dispositivo; apertura o eliminación de accesos a herramientas de trabajo, modificación de contraseñas de cuentas de la organización, entre otras).

- Ruta o plan de acción con las medidas de respuesta en casos de violencia de género facilitada por la tecnología.

Cuidados digitales específicos

La protección digital de las organizaciones de mujeres incluye todos los aspectos que se han revisado en la *Parte 1 - Cuidados digitales de las integrantes de la organización* recogidos de esta Guía, además de otros elementos específicos. A continuación, se recogen valoraciones y sugerencias adicionales.

Contraseñas seguras en dispositivos y cuentas de la organización

- Se recomienda guardar las contraseñas de cuentas, dispositivos y herramientas internas de la organización en un gestor de contraseñas seguro, como KeePassXC, administrado por las personas responsables que designe la organización.

- Las contraseñas de redes sociales y páginas web deben ser administradas por un número reducido de personas, y al menos dos, para garantizar la recuperación del acceso en caso de pérdida por alguna de las administradoras.

- Fijar un periodo de cambio de las contraseñas de la organización. Al menos una vez al año de manera general; cada 3 meses si se viven ataques digitales de manera recurrente; y de manera inmediata si existen situaciones de accesos no consentidos, robo y difusión de información, estafas o incidentes como la apertura de enlaces y correos maliciosos o extraños. Es necesario establecer al interior del equipo quién será la persona responsable de este cambio y la actualización del gestor de contraseñas donde se almacenan.

Comunicaciones seguras dentro de la organización y con personas externas

- Evitar el uso de números telefónicos personales. Algunas alternativas son:

– Celulares con doble chip donde se pueda utilizar el número personal y otro de la organización.

– Usar apps que permiten crear un perfil de trabajo en el celular. Así se podrá separar el número personal del número de contacto laboral, así como las cuentas personales de las de trabajo. Para esta opción, no se necesita un chip adicional. Este perfil permitirá desactivar las notificaciones de trabajo durante los días y horas de descanso.

Opciones para crear un perfil de trabajo en el celular

- En algunos dispositivos Android esta opción viene por defecto bajo el nombre de: **Dual app, Clone app o Perfil de trabajo.**

Importante: no siempre este tipo de opciones permite clonar todas las apps sino aquellas más frecuentes como WhatsApp.

- **Shelter:** es una opción disponible para Android que permite crear un perfil de trabajo y duplicar cualquier app incluida Signal.

– Descarga: https://shelter.uptodown.com/android

– Guía de uso: https://www.xatakandroid.com/aplicaciones-android/como-crear-perfil-privado-donde-aislar-a-aplicaciones-tus-datos-personales

- Para la comunicación interna de la organización, se recomienda el uso de Signal, ya que permite mayores garantías de confidencialidad de los datos.

Si se utiliza WhatsApp, es importante no compartir información sensible por esta vía como datos personales, contraseñas, ubicaciones y otros datos sobre viajes y desplazamientos; información sobre personas que acompaña la organización; acciones y movimientos de la organización que puedan ser de interés de grupos anti derechos, instituciones estatales u otros actores.

Si en alguna situación, solo se puede contar con el uso de WhatsApp, se sugiere enviar la información con las opciones de vista única y eliminación de mensajes activadas:

- Evitar usar el nombre y apellidos completos para registrar los contactos telefónicos de las compañeras de la organización. Así, en los chats grupales internos o externos, no podrán ser identificadas si alguien accede sin consentimiento o por error a este tipo de comunicaciones.

- Acordar qué tipo de información puede ser compartida por los diferentes canales de comunicación de la organización (chats, correos electrónicos, redes sociales, entre otras), y qué datos no pueden ser difundidos por estas vías.

- En casos de alto riesgo o donde se sospeche que las comunicaciones pueden estar intervenidas, una opción es compartir la información a través de códigos internos como juegos de palabras, o facilitarla en persona y en espacios seguros.

- Para la realización de reuniones o eventos en línea mediante plataformas de videoconferencia donde asistan personas desconocidas, se puede evitar el uso del nombre completo y apellidos al identificarse.

Manejo de la información interna

Uso de herramientas digitales seguras

Uoa de los cuidados digitales clave al interior de la organización es la elección de herramientas digitales para el trabajo que sean más seguras. Algunas recomendaciones son:

- Nubes de almacenamiento diseñadas por organizaciones de confianza y alojadas en servidores propios.

Opciones de nubes de almacenamiento seguras

- **Cryptpad:** es una opción de almacenamiento de archivos y edición de documentos colaborativos cifrada. Te permite dos modalidades de manera gratuita: usuaria "invitada" donde podrás generar documentos compartidos y guardarlos por un periodo máximo de 90 días; y usuaria "registrada" donde podrás subir archivos hasta 1 GB de capacidad sin que se eliminen. Para registrarse, no solicita datos personales. Recuerda guardar tu nombre y contraseña en un gestor de contraseñas seguro ya que si los pierdes no tendrás acceso.

Además, cuenta con una versión "premium" con costos reducidos que permite una capacidad almacenamiento entre 5 a 50 GB dependiendo del plan escogido.

- Consulta aquí: https://cryptpad.fr/features.html / https://cryptpad.fr/index.html

- **ProtonDrive:** cuenta con una opción gratuita de almacenamiento cifrado hasta de 5GB y diferentes versiones de pago.

- Consulta aquí: https://proton.me/es-es/drive/pricing / https://proton.me/es-es/drive

- **MaadiX:** es un servicio de almacenamiento y mantenimiento que permite disponer de varios servicios en línea en un servidor propio, lo que aporta mayor privacidad y seguridad al no recopilar datos con fines lucrativos.

- Consulta más aquí: https://maadix.net/es/como-funciona/. MaadiX usa Nextloud como opción de nube de almacenamiento. Planes: https://maadix.net/es/servers/ (actualmente no cuenta con una versión gratuita).

- **Nextcloud:** es una nube de almacenamiento de código abierto. Se recomienda su uso en servidores propios o de organizaciones de confianza, es decir, que no estén gestionados por empresas desconocidas o que recopilen datos de las personas usuarias con fines lucrativos.
- Consulta más aquí: https://nextcloud.com/es/

IMPORTANTE: el uso de nubes de entidades con fines de lucro sin cifrado puede hacer que los datos personales o de la organización estén en riesgo. En caso de utilizar este tipo de nubes, es necesario tomar medidas de seguridad adicionales:

– No guardar información sensible.

– Restringir los permisos de uso de documentos colaborativos y evitar difundir enlaces abiertos de los contenidos.

– Subir el contenido a la nube en carpetas cifradas usando programas de encriptado como Cryptomator.

Consulta aquí: https://protege.la/guias-contenido/guia-cryptomator/.

Recuerda: Google Drive no ofrece cifrado y puede recopilar datos. Si se usa, ¡aplica las medidas de seguridad adicionales!

- **Notas colaborativas cifradas**. Una opción es el Pad de Riseup: https://pad.riseup.net/.

- **Formularios y encuesta**s. LimeSurvey ofrece mayores protecciones al permitir el ocultamiento de la IP. Consulta aquí: https://www.limesurvey.org/es

- **Transferencia de archivos**. RiseupShare (https://share.riseup.net/) es una opción cifrada para compartir archivos hasta 1 Gb de capacidad. Otra herramienta es OnionShare: no tiene límite de envío y se puede usar en cuando se tiene instalado el Navegador Tor. Consulta aquí: https://docs.onionshare.org/2.3.1/es/features.html

- **Bases de datos o sistemas de ticketing**. Se recomienda su uso en servidores administrados por organizaciones de confianza para asegurar la protección de la documentación de casos e información interna. Consulta con organizaciones aliadas sobre opciones seguras.

IMPORTANTE: Para otras herramientas de trabajo que puedan almacenar datos de la organización, se recomienda buscar en Internet versiones de software libre y código abierto que hayan sido generadas sin fines de lucro y por entidades de confianza.

Otra estrategia para la seguridad de la información de la organización es determinar el procedimiento de almacenamiento, respaldo y eliminación de los datos. Algunas medidas de seguridad pueden ser:

- Acordar los periodos y métodos para guardar la información interna, y qué integrantes de la organización serán responsables de realizar los respaldos.

- Establecer los lugares donde se respalda la información de la organización (discos duros cifrados, nubes cifradas o con archivos encriptados) y cuál será el protocolo de su mantenimiento y cuidado.

- Acordar las políticas de manejo de la información en desplazamientos: viajes, talleres en espacios diferentes al lugar de trabajo, encuentros o reuniones con otros actores, entre otros. Por ejemplo: si se ha generado información escrita durante un taller mediante papelotes, mapas u otros recursos; digitalizarla lo antes posible y eliminar el formato original.

- Adoptar una política de eliminación de la información según las necesidades y contextos de la organización, incluyendo los periodos de borrado de la información y el tipo de datos que se deben conservar.

Cuidado de celulares y dispositivos

- Si la organización cuenta con recursos, se puede valorar la adopción de antivirus con licencias de pago y mayores elementos de protección, además de utilizar dispositivos específicos de la organización para evitar el empleo de celulares y computadoras personales.

- Acordar los períodos de actualización del sistema operativo y herramientas de las computadoras, laptop y celulares de la oficina, y quiénes serán las personas responsables de hacer este tipo de seguimiento al menos una vez al año.

- Contar con un servicio técnico de confianza y presentar los dispositivos siempre sin información, incluido el borrado del historial de navegación.

Manejo seguro de redes sociales y sitios web de la organización

- **Prevenir accesos no consentidos**
- Actualizar la contraseña al menos cada 6 meses y de forma inmediata si sale una de las integrantes de la organización o hay un incidente de seguridad.
- Activar la verificación en dos pasos con un correo seguro (no usar los celulares personales de las integrantes).

- **Seguridad de las integrantes**
- Evitar etiquetar o seguir a los perfiles privados de las integrantes.
- Asegurarse de tener el consentimiento de todas las integrantes antes de publicar una foto o video en el que aparecen.
- Establecer acuerdos claros que tomen en cuenta los riesgos y amenazas específicos de cada una.

- **Frente a ataques digitales**
- Valorar la necesidad de crear una cuenta adicional de respaldo para la organización en caso de que problemas de seguridad resulten en el cierre de las cuentas.
- Designar una persona o equipo encargado de la seguridad de las redes sociales que se encargue de registrar incidentes y poner en práctica los hábitos de cuidado.

5. ¿Qué hacer en casos de violencia de género facilitada por la tecnología?

Cada situación de violencia de género facilitada por la tecnología es particular y puede necesitar medidas específicas, sin embargo, se pueden tener en cuenta pasos generales necesarios en la mayoría de los casos.

Además, es importante tener en cuenta que las organizaciones de mujeres pueden enfrentar diferentes casos:

- Ataques específicos dirigidos a su infraestructura digital y física: redes sociales y páginas web de la organización, bases de datos, celulares, computadoras del lugar de trabajo, entre otras.

- Agresiones digitales hacia una o varias de sus integrantes por sus actividades dentro de la organización.

- Situaciones de violencia de género fuera y dentro de línea hacia sus integrantes en otros contextos como el intrafamiliar, educativo o comunitario, donde necesiten acompañamiento de la institución durante el proceso de respuesta.

De esta manera, las acciones de respuesta que se recogen a continuación están formuladas considerando el rol de la organización y del conjunto de integrantes de la organización.

Acompañar de manera integral

Cuando se dan situaciones de violencia de género facilitada por la tecnología es necesario diseñar un proceso de acompañamiento dirigido a las personas que están enfrentando las agresiones para asegurar su integridad, cuidado y seguridad.

Procurar que las personas no se sientan solas y garantizar que la organización tomará medidas de acción y respuesta frente a la violencia es clave para fomentar un entorno de confianza y libre de impunidad al interior de la organización.

Además, este tipo de violencia también puede necesitar de diferentes respuestas como el acompañamiento psicológico especializado, legal o tecnológico.

Consejos para acompañar

- Formar un grupo de acompañamiento al interior de la organización que sea responsable de coordinar las acciones de cuidado necesarias.
- Escuchar de manera activa, con empatía y sin juicios de valor, la experiencia de la persona o personas afectadas e indagar sobre sus necesidades.
- Validar las historias de violencia de género facilitada por la tecnología sin minimizarlas.
- Generar espacios de apoyo dentro de la organización para abordar las afectaciones y diseñar colectivamente estrategias de acción.
- Facilitar información sobre los servicios de atención especializada (asesoría y patrocinio legal, acompañamiento psicológico, salud integral) y el proceso de denuncia de acuerdo con las necesidades de la compañera agredida.
- Generar medidas para sostener a las compañeras que se encargan de activar los protocolos de seguridad y las acciones de respuesta, para garantizar su seguridad y su salud emocional y física al interior de la organización.

Recuerda. Todas las situaciones violencia de género facilitada por la tecnología son graves y conllevan impactos. Incluso un comentario aislado en redes sociales puede generar ansiedad, sensación de persecución o detonar otras afectaciones previas. Por tanto, es clave evitar reducir la importancia de este tipo de violencia y validar las necesidades de las personas que la experimentan.

Documentar, guardar la evidencia y analizar los riesgos

Cuando las agresiones digitales ocurren, es fundamental generar un registro de la situación y preservar la evidencia. Además, identificar qué riesgos adicionales implica la agresión que ha ocurrido será clave para asegurar el cuidado de la persona o personas afectadas y diseñar medidas de seguridad y cuidado. De esta manera, se recomienda:

- Realizar un **registro de los incidentes** de seguridad digital que hayan ocurrido para organizar la información disponible. Esto puede ser útil en caso de reportes en plataformas de servicios de Internet y denuncias en el sistema de justicia. Además, permite identificar patrones, dinámicas de violencia y posibles elementos clave para detectar a responsables de las agresiones.

Adicionalmente, en caso de identificar a agresores recurrentes, una estrategia resulta generar una base de datos con los datos disponible.

Una buena práctica es designar una o varias personas responsables de la organización encargadas de registrar esta información en fichas u otras herramientas que permitan su sistematización. También, se puede usar un chat grupal u otro canal seguro donde remitir las situaciones de violencia digital que sea de conocimiento del conjunto de integrantes de la organización.

Ficha o bitácora de incidentes

Es una herramienta para registrar los eventos inseguros. Un incidente puede ser cualquier situación de violencia facilitada por la tecnología u otros eventos extraños, inusuales o riesgosos dentro y fuera de línea que puedan tener o no relación directa con un ataque digital. Por ejemplo: abrir un enlace desconocido y no saber si se trata de un virus; sentirse perseguida en el espacio físico; recibir llamadas extrañas al domicilio, entre otros.

¿Qué puede contener?

- Fecha
- Lugar o medio donde se ha producido el incidente/agresión (espacio virtual o físico)
- Descripción del incidente/agresión
- Responsable del incidente/agresión
- Evidencia sobre el incidente (enlaces, capturas y otras)
- Otros eventos relacionados
- Observaciones
- Riesgos que implica
- Medidas realizadas

- **Guardar las evidencias** de la agresión o situación de riesgo que se hayan experimentado de manera adecuada y segura.

Pasos para guardar evidencias

- Copiar y guardar los enlaces de las publicaciones donde esté contenida la agresión si hubiera.
- Descargar y guardar archivos, vídeos o imágenes recibidos sobre las agresiones, a menos que exista sospecha de que pueden ser maliciosos o contener virus.
- Tomar capturas de pantalla y copiar y guardar los enlaces de los perfiles agresores o que han enviado algún tipo de información.
- Tomar capturas de pantalla del contenido del ataque o incidente donde aparezca el nombre del perfil del agresor y de las personas afectadas.
- Guardar la evidencia en un lugar seguro, como un disco duro o computadora que no se suela transportar o que esté cifrada para mayor seguridad (no almacenar la evidencia en el celular por si se pierde o se produce un robo).

• **Analizar los riesgos** que pueden conllevar las agresiones o incidentes de seguridad ocurridos contribuye a identificar las medidas de respuesta adecuadas.

Preguntas útiles para analizar los riesgos frente a un incidente de seguridad

- ¿A qué tipo de información se ha podido tener acceso?
- ¿Qué riesgos implica para la persona y el conjunto de integrantes de la organización?
- ¿Qué riesgos implica para las personas que acompaña la organización o con las que trabaja en red?
- ¿Quiénes son los agresores y qué capacidades de seguir generando la agresión tienen?
- ¿Qué cuidados digitales y físicos pueden aplicar de manera personal las integrantes de la organización, y qué medidas se necesitan abordar de manera colectiva?
- ¿Se necesitan generar acciones de protección coordinadas con otras organizaciones o instituciones?

Documentar este tipo de información, ayudará a generar un análisis de riesgo e identificar las acciones de seguridad necesarias. de información.

Medidas de protección digital e integral

Frente a una situación de violencia de género facilitada por la tecnología es esencial priorizar las acciones de seguridad y cuidados de las personas involucradas a fin de mitigar los impactos de las agresiones y prevenir que sigan ocurriendo.

Según el caso, estas acciones pueden resultar en que las personas afectadas necesiten suspender temporalmente actividades en la organización, limitar el uso de las redes sociales y otros servicios de Internet temporalmente, o tener espacios específicos de acompañamiento psicológico o emocional, tanto dentro como fuera de la organización.

Además, será importante que las integrantes de la organización, con el fin de estar sostenidas durante el proceso en otros espacios, pidan apoyo a su red de personas cercanas y de confianza que puedan ayudarles en posibles acciones colectivas de respuesta como recabar evidencias y generar múltiples reportes de perfiles agresores en redes sociales.

Reforzar los cuidados digitales

Al momento de experimentar una situación de violencia en línea, será necesario revisar la seguridad digital de cuentas y dispositivos de la persona o la organización afectada.

Para ello, se recomienda algunas **acciones prioritarias**.

- Cambiar las contraseñas de las cuentas y dispositivos afectados de manera inmediata.
- Aumentar la seguridad en redes sociales y correos electrónicos de la organización y de las integrantes. Para ello, consulta los cuidados digitales expuestos en esta guía.
- Garantizar mayor protección en las comunicaciones reforzando el uso de aplicaciones con mayor seguridad como Signal.
- Si se sospecha que los dispositivos han sido vulnerados, se pueden realizar escaneos de virus con antivirus y el restablecimiento de los valores de fábrica.
- En casos donde se haya accedido a cuentas y dispositivos o se haya suplantado la identidad de las integrantes es importante que las integrantes lo notifiquen lo antes posible para retirar su perfil de chats grupales, documentos colaborativos y cualquier herramienta organizacional donde la persona tuviera acceso, a fin de prevenir robo de información. Esta medida sirve también en casos de pérdida o robo de dispositivos.
- De ser necesario, acudir a organizaciones especializadas en protección digital (**consulta el Anexo** 2).

Reportar/denunciar las agresiones

¿Cómo reportar agresiones en internet?

La denuncia de las agresiones en internet es necesaria para mitigarlas y que las plataformas de servicios tomen responsabilidad en estos casos, garantizando el respeto de sus normas de uso. Además, ayudará a generar nuevas medidas de prevención y respuesta de manera constante.

AVISO: ten en cuenta que, si se inicia un proceso judicial, las evidencias de las agresiones en Internet pueden ser útiles. Antes de reportarlas o solicitar el retiro de contenidos de la red, consulta con una abogada.

• **En redes sociales,** sigue las instrucciones de reporte según la plataforma específica. Se puede denunciar comentarios ofensivos, suplantación de identidad, difusión de contenido íntimo o sexual, entre otras situaciones. Cada plataforma tiene diferentes opciones de denuncia, por lo que es necesario consultar los Centros de Ayuda para más información y buscar las opciones que se adapten a las agresiones experimentadas. Para mayor efectividad, se pueden generar múltiples reportes con el fin de alertar a la plataforma de que se trata de una situación grave y recurrente.

A continuación, se recogen enlaces de reporte según diferentes redes sociales.

Instagram	https://help.instagram.com/165828726894770/?helpref=hc_fnav&locale=es_LA
Facebook	https://www.facebook.com/help/263149623790594
TikTok	https://support.tiktok.com/es/safety-hc/report-a-problem
X	https://help.x.com/es/safety-and-security/report-abusive-behavior#:~:text=Ve%20al%20perfil%20de%20la,del%20asunto%20que%20quieres%20denunciar.
Threads	https://www.facebook.com/help/instagram/6602413966453273

Estos enlaces pueden cambiar según las políticas de los proveedores por lo que, si no dan acceso, introduce en un buscador lo siguiente: "¿Cómo puedo denunciar/reportar (descripción de la agresión) en (nombre de la red social)?" Ejemplo: ¿cómo puedo denunciar una suplantación de identidad en Instagram?

• **En páginas webs,** revisa si cuentan con una sección de reportes de incidencias, quejas, acoso, abusos o agresiones y sigue los pasos. Suelen ofrecer un correo electrónico de asistencia técnica donde remitir los hechos.

Abuso basado en contenido íntimo o sexual

Si se ha producido la difusión no consentida de imágenes y/o vídeos íntimos o sexuales, o la amenaza de ellos y se cuenta con los archivos, **crea el caso en StopNCII** (*Stop Non-Consensual Intimate Image Abuse*). Sigue los pasos aquí: https://stopncii.org/?lang=es-mx.

StopNCII es una plataforma que genera un hash o huella digital única de las imágenes y videos. Todas las copias duplicadas de una imagen o video tienen exactamente el mismo marcador específico o hash, y esto permite que las empresas adscritas a StopNCII (Facebook, Instagram, TikTok, Bumble, Reddit, OnlyFans, Pornhub, Threads, Snap Inc. y Niantic) puedan ayudar a detectar y eliminar las imágenes o videos que coincidan con ese *hash*.

También se puede usar esta plataforma para prevenir que otros contenidos sean difundidos. Si tienes imágenes que sospechas que podrían ser compartidas, inclúyelas.
Si la persona de la que se han difundido las imágenes tiene menos de 18 años, usa esta opción: https://takeitdown.ncmec.org/es/

Denuncia en el sistema de justicia u otras instituciones

Para denunciar, acude a la Fiscalía y Unidades Judiciales, en particular, a las especializadas en la atención a mujeres y violencia de género.

Consulta aquí:
Fiscalía: https://www.fiscalia.gob.ec/directorio-fiscalias/
Unidades Judiciales: https://www.funcionjudicial.gob.ec/pdf/unidades-judiciales-violencia-mujer-miembros-nucleo-familiar.pdf

En aquellos lugares donde no existan estas instancias se puede asistir a las Tenencias Políticas locales.

Para obtener medidas de protección, consulta en las Juntas Cantonales de Protección de Derechos. Puntos de atención aquí: http://aplicaciones.consejodiscapacidades.gob.ec/siind/uploads/asesoramiento_legal/78_DIRECTORIO%20DE%20JUNTAS%20CANTONALES%20DE%20PROTECCION%20DE%20DERECHOS.pdf /

Dependiendo del caso, se puede valorar otras acciones administrativas o constitucionales. Es importante que la organización ofrezca su apoyo en aquellos casos donde las integrantes no deseen acudir a la vía penal y prefieran buscar estrategias alternativas de denuncia en instituciones públicas y privadas como universidades, centros culturales, entidades de salud, entre otras. En estos casos, revisa si cuentan con protocolos de actuación frente a la violencia de género y los pasos a seguir.

Buscar apoyo de organizaciones aliadas

Según el caso y las acciones de respuesta que se prevean, se deberá considerar:

- Generar acciones colectivas y articuladas con otras organizaciones sociales como campañas de sensibilización, educativas o de formación en cuidados digitales.
- Solicitar acompañamiento de organizaciones especializadas en protección digital.
- Buscar otro tipo de acompañamiento o servicios en organizaciones o instituciones como asesoría y patrocinio legal, acompañamiento psicológico, entre otras.

Revisa el Anexo 2.

Recuerda: a la hora de poner una denuncia por un delito relacionado con violencia digital, no se necesitan requisitos adicionales ni pruebas digitales. Sin embargo, se recomienda preservar la evidencia digital al momento en el que se producen las agresiones.

Recursos: amplía tus saberes

Tema	Enlaces y materiales de interés
Internet	• ¿Cómo viaja la información por Internet de manera segura? https://youngfeministfund.org/wp-content/uploads/2020/11/frida-PreguntaClave-ESP.pdf
Cuidados digitales y seguridad digital	• Protege.La - Rutas de aprendizaje de seguridad digital: https://protege.la/
	• OACNUDH: Caja de herramientas para la seguridad en el entorno digital. Herramientas y recursos de seguridad digital para personas defensoras de derechos humanos y periodistas https://seguridad-digital.oacnudh.org/
	• Lista de aplicaciones de software libre: https://critical-switch.org/posts/software-libre/
	• Herramientas y tácticas para la seguridad digital - Security in-a-box: https://securityinabox.org/es/
	• Arsgames. Manual de seguridad digital: kit de herramientas para una internet feminista: https://arsgames.net/manual-de-seguridad-digital-kit-de-herramientas-para-una-internet-feminista/
	• Front Line Defenders. Guía sobre herramientas seguras para conferencias y chats grupales https://www.frontlinedefenders.org/es/resource-publication/guide-secure-group-chat-and-conferencing-tools
Violencia de género facilitad por la tecnología	• Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas, desde la perspectiva de los derechos humanos: https://acoso.online/site2022/wp-content/uploads/2018/10/G1818461.pdf
	• Taller de Comunicación Mujer. Diagnóstico Violencia de Género Digital en Ecuador https://navegandolibres.org/que-es-violencia-de-genero-digital-primer-diagnostico-sobre-violencia-de-genero-en-internet-de-ecuador/
	• ONU Mujeres; Taller de Comunicación Mujer: Estudio exploratorio sobre la Violencia Facilitada por la Tecnología contra las Mujeres y las Niñas (VFTCMN) en Quito, Cuenca y Guayaquil https://navegandolibres.org/wp-content/uploads/2024/01/VFTCMN-ONUM-TCM.pdf
Niñas, niños y adolescentes	• Plan Internacional: ¿Libres para estar en línea? Las experiencias de niñas y mujeres jóvenes con el acoso en línea: https://plan.org.ec/la-violencia-en-linea-esta-silenciando-las-voces-de-las-ninas/
	• Podcast Hijas de Internet sobre experiencias de NNA, Internet y tecnologías: https://podimo.com/dk/shows/hijas-de-internet
	• Internet libre y segura. Un juego para el ejercicio de los derechos digitales de niñas, niños y adolescentes y por una Internet libre de violencia de género: https://navegandolibres.org/internet-libre-y-segura/
Consentimiento digital	• https://navegandolibres.org/consentimiento-2/
Guías de acompañamiento en casos de violencia facilitada por la tecnología	• Taller de Comunicación Mujer: Acompañadas y enredadas. Guía para acompañarnos en casos de violencia de género digital: https://navegandolibres.org/wp-content/uploads/2024/10/Acompanadas-y-enRedadas-Interactivo.pdf
	• Taller de Comunicación Mujer: Guía para acompañar adolescentes en casos de violencia de género digital: https://navegandolibres.org/wp-content/uploads/2024/10/Acompanadas-y-en-Redadas-Interactivo.pdf
	• Cultivando Género: Guía de resistencia digital entre amigas: https://cultivandogeneroac.wixsite.com/misitio/nonavegassola
	• Fembloc. Guía Desconecta de tu expareja: https://desconectadetuex.net/?cerrar
	• Digital Defenders Partnership: Crear resiliencia. Manual de acompañamiento para la protección digital https://manual.digitaldefenders.org/es/
Sexteo/sexting seguro	• Tips para un sexting seguro: http://www.libresenlinea.mx/autodefensa/guias-dereaccion-rapida/tips-para-un-sexting-seguro/
	• Consejos para sextear más seguros: https://hiperderecho.org/sexting/
Organizaciones que acompañan en casos de violencia de género facilitada por la tecnología en América Latina	• Taller de Comunicación Mujer – Navegando Libres: https://navegandolibres.org/linea-de-acompanamiento-feminista/
	• Acoso.online - Recursos para Latinoamérica: https://acoso.online/
	• Vita Activa - Centro América y México: https://vita-activa.org/tag/linea-de-ayuda/
	• Luchadoras – México: https://luchadoras.mx/
	• MariaLab – Brasil: https://www.marialab.org/

Referencias bibliográficas

- Asamblea Nacional del Ecuador (2018) *Ley Orgánica para Prevenir y Erradicar la Violencia contra las Mujeres*. Registro Oficial Suplemento 175.
- (2014) *Código Orgánico Integral Penal*. Registro Oficial Suplemento 180.

- Akahata (s/f): *Manual de autocuidados digitales feministas* https://akahataorg/wp-content/uploads/2024/01/Akahata-Manual-Final-Digital.pdf

- Amelia e Foz, Marialab (2022): *Cuidados digitales y filantropía. Hallazgos y recomendaciones básicas* https://www.marialab.org/wp-content/uploads/2022/11/Cuidados-digitales-y-filantropia.pdf

- Front Line Defenders (2021): *Guía sobre herramientas seguras para conferencias y chats grupales* https://www.frontlinedefenders.org/es/resource-publication/guide-secure-group-chat-and-conferencing-tools

- Hiperderecho (2020): *Kit de cibercuidado para activistas*, https://hiperderecho.org/wp-content/uploads/2020/11/Kit-de-cibercuidado-para-activistas-.pdf

- IM Defensoras (2020): *Compendio de herramientas de autocuidado y sanación* https://im-defensoras.testing.sutty.nl/public/00odzb99m8yc9agsn0ssb6q8uwtv/Compendio-de-herramientas-de-autocuidado-definitiva.pdf

- Kaspersky (2024): *El Estado del Stalkerware en 2023*. https://media.kasperskydaily.com/wp-content/uploads/sites/88/2024/03/21175229/The-State-of-Stalkerware-in-2023-def.pdf

- La Libre (2021): *Defensa digital para organizaciones sociales* https://lalibre.net/wp-content/uploads/2022/09/Guia-de-proteccion-digital.pdf

- Oficina del Alto Comisionado de Derechos Humanos de Naciones Unidas (s/f): *Caja de herramientas para la seguridad en el entorno digital. Herramientas y recursos de seguridad digital para personas defensoras de derechos humanos y periodistas* https://seguridad-digital.oacnudh.org/

- ONU Mujeres y Organización Mundial de la Salud [OMS] (2023). *Technology-facilitated violence against women: Taking stock of evidence and data collection*. https://www.unwomen.org/sites/default/files/2023-04/Brief-The-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women-en.pdf

- Organización de los Estados Americanos (s/f): *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta* / [Preparado por la Secretaría General de la Organización de los Estados Americanos]. v.; cm. (OAS. Documentos oficiales; OEA/Ser.D/XXV.25) https://www.oas.org/es/sms/cicte/docs/Manual-practico-de-seguridad-digital-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

- Protege.la (2019): *6 hábitos básicos para tu seguridad digital*: https://protege.la/guias-contenido/basicos-seguridad-digital/

- Taller de Comunicación Mujer (2024): *Acompañadas y enredadas. Guía para acompañarnos en casos de violencia de género digital* (https://navegandolibres.org/wp-content/uploads/2024/10/Acompanadas-y-enRedadas-Interactivo.pdf)

ANEXOS

Anexo 1. Listado de delitos relacionados con la violencia de género facilitada por la tecnología

Diferentes delitos del Código Orgánico Integral Penal pueden cometerse por medios electrónicos o mediante el uso de las tecnologías digitales. Este es un listado de los principales delitos vinculados a la violencia de género en el ámbito digital. Consulte aquí el contenido completo de los tipos penales: https://www.lexis.com.ec/biblioteca/coip#BBB6B784DABAA6383F8AD79D693B518BF0248D18_7A1112624156D03A3E02DE281E5B5E4E29165349

Delito	Descripción
Art. 103 Pornografía con utilización de niñas, niños y adolescentes	La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años. Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.
Art. 104 Comercialización de pornografía con utilización de niñas, niños o adolescentes	La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años.
Art. 154.2 Hostigamiento	La persona natural o jurídica que, por sí misma o por terceros o a través de cualquier medio tecnológico o digital, moleste, perturbe o angustie de forma insistente o reiterada a otra, será sancionada con una pena privativa de la libertad de seis meses a un año, siempre que el sujeto activo de la infracción busque cercanía con la víctima para poder causarle daño a su integridad física o sexual. Cuando la víctima sea menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena privativa de libertad de uno a tres años.
Art. 166 Acoso sexual	La persona que solicite algún acto de naturaleza sexual, para sí o para un tercero, prevaliéndose de situación de autoridad laboral, docente, religiosa o similar, sea tutora o tutor, curadora o curador, ministros de culto, profesional de la educación o de la salud, personal responsable en la atención y cuidado del paciente o que mantenga vínculo familiar o cualquier otra forma que implique subordinación de la víctima, con la amenaza de causar a la víctima o a un tercero un mal relacionado con las legítimas expectativas que pueda tener en el ámbito de dicha relación de subordinación, será sancionada con pena privativa de libertad de uno a cinco años. Se considerará ciberacoso sexual cuando la conducta descrita en el inciso anterior se realice utilizando cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales, y será sancionado con una pena privativa de libertad de uno a cinco años.
Art. 168 Distribución de material pornográfico	Distribución de material pornográfico a niñas, niños y adolescentes.- La persona que difunda, venda o entregue a niñas, niños o adolescentes, material pornográfico, será sancionada con pena privativa de libertad de uno a tres años.
Art. 172. 1 Extorsión sexual	La persona que, mediante el uso de violencia, amenazas o chantaje induzca, incite u obligue a otra a exhibir su cuerpo desnudo, semidesnudo, o en actitudes sexuales, con el propósito de obtener un provecho personal o para un tercero, ya sea de carácter sexual o de cualquier otro tipo, será sancionada con pena privativa de libertad de tres a cinco años.

Delito	Descripción
Art. 173 Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años. Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años. La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.
Art. 174 Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años.
Art. 177 Actos de odio	La persona que cometa actos de violencia física o psicológica de odio, contra una o más personas en razón de su nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición migratoria, discapacidad, estado de salud o portar VIH, será sancionada con pena privativa de libertad de uno a tres años. Si los actos de violencia provocan heridas a la persona, se sancionará con las penas privativas de libertad previstas para el delito de lesiones agravadas en un tercio. Si los actos de violencia producen la muerte de una persona, será sancionada con pena privativa de libertad de veintidós a veintiséis años.
Art. 178 Violación a la intimidad	La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.
Art. 179 Revelación de secreto o información personal de terceros	La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación cause daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año. No habrá delito en aquellos casos en que el secreto divulgado verse sobre asuntos de interés público. Será sancionada con pena privativa de libertad de uno a tres años quien revele o divulgue a terceros contenido digital, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad.
Art. 212 Suplantación de identidad	La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.
Art. 229 Revelación ilegal de base de datos	La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Delito	Descripción
Art. 230 Interceptación ilegal de datos.	Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales. 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder. 3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior. 4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.
Art. 231 Transferencia electrónica de activo patrimonial	La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.
Art. 232.- Ataque a la integridad de sistemas informáticos.-	La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.
Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años. 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.
Art. 234.1.- Falsificación informática:	1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años. 2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena.

Anexo 2. Servicios de atención a víctimas de violencia de género

Pichincha-Quito		
Organización	**Servicios**	**Contacto**
Fundación Casa de Refugio Matilde	Servicio de albergue para mujeres con sus hijos e hijas víctimas de violencia intrafamiliar y de género. Atención externa en orientación legal y psicológica.	https://fundacionmatilde.org/ 099 66 96 723 / 09 8 779 66 88
Red de Primeros Auxilios legales Juntas Nos Cuidamos - Surkuna	Acompañamiento en denuncias de violencia de género y solicitud de medidas de protección	https://surkuna.org/ 099 555 17 89
Centro Ecuatoriano para la Promoción y Acción de la Mujer - CEPAM	Atención y acompañamiento de casos de violencia intrafamiliar. Patrocinio de casos penales sobre delitos sexuales	https://www.cepam.org.ec/
Akuanuna	Atención psicológica y legal / Asistencia en trabajo social	somos@akuanuna.org
Fundación Idea Dignidad	Investigación, educación, protección e incidencia.	https://www.ideadignidad.org/
Salvas	Línea de apoyo 24 horas para sobrevivientes de violencia sexual	099 354 90 07
Diálogo Diverso	Promoción de derechos de la población LGBTIQ+, de las mujeres y otros grupos en situación de vulnerabilidad	https://dialogodiverso.org/didi/
Fundación Alas de Colibrí	Promoción de derechos y protección de sobrevivientes de trata, VBG, infancia, personas en movilidad humana	https://fundacionalasdecolibri.org/
Fundación Equidad	Servicios e información para población LGBTIQ+. Albergue comunitario para personas LGBTIQ+	https://www.fequidadecuador.org/
La Libre	Servicios de Infraestructura en Tecnología de la Información para defensoras/es de los DDHH y de la naturaleza	https://lalibre.net/
Taller de Comunicación Mujer - Navegando Libres	Línea de acompañamiento en casos de violencia de género digital dirigida a mujeres, niñas, niños y adolescentes y población LGBTIQ+. Capacitación sobre protección y seguridad digital.	https://tcmujer.org/ y https://www.navegandolibres.org
	Azuay-Cuenca	
Fundación María Amor	Atención especializada a mujeres víctimas y sobrevivientes de violencia, sus hijos e hijas.	(072) 283-4139 / 095 893 4487
Centro de apoyo a la Mujer y a la familia 'Las Marías'	Centro de atención integral a víctimas de violencia	0979186468
Casa de la Mujer	Servicios de atención integral del Municipio de Cuenca	07 4134900 Ext. 2345
Las Hijas de Pandora	Incidencia social en casos de violencia de género	hijasdepandora1@gmail.com

Guayas-Guayaquil		
Organización	**Servicios**	**Contacto**
Centro Ecuatoriano para la Promoción y Acción de la Mujer - CEPAM	Atención integral, atención legal, clínica jurídica feminista	https://cepamgye.org/ (593-4) 2447347 / 2446945 / 2447649
CDH	Asesoría y seguimiento de casos de violaciones a los DDHH. Orientación legal nacional, regional y universal	https://www.cdh.org.ec/
Fundación Estudios y Apoyo para la Mujer y la Familia Ecuatoriana María Guare	Defensa de los DDHH de la mujer y la familia, atención legal, social y psicológica.	https://www.fundacionmariaguare.com/ / (593-4) 2447347 / 2446945 / 2447649
Fundación Mujer y Mujer	Asistencia humanitaria a personas en movilidad humana, y acompañamiento entre pares, colectivas LGBTIQ+ y organizaciones.	https://mujerymujer.org.ec/
Ecuador dice no más	Grupos anónimos de autoayuda para sobrevivientes de abuso sexual.	https://ecuadordicenomas.com/
Colectivo Vigilia	Vigilancia social de actos de violencia sexual contra las niñas.	
Fundación Resurgir	Asistencia a personas en situación de VG en Ecuador. Atención psicológica, legal y social.	
Casa de acogida transitoria Trans - Dejando Huella	Casa de acogida transitoria para personas trans ex privadas de libertad	odalysbustamat@gmail.com

Consulta más servicios de atención en:

- Consejo de Protección de Derechos de Cuenca y RIAP - VIF. Catálogo de servicios y centros de atención especializada en violencia basada en género: https://www.cuenca.gob.ec/system/files/Catalogo-de-Servicios-y-Centros-de-Atencion-especializada-en-violencia-basada-en-genero.pdf

- Consejo de Protección de Derechos del D.M. Quito. Ruta de Protección de Derechos de Mujeres víctimas de violencias en el Distrito Metropolitano de Quito: https://protecciondederechosquito.gob.ec/wp-content/uploads/2023/08/FIN_RUTA_MUJERES_VIC_VIOLENCIA_5.pdf

- Quito, Guayaquil, Cuenca y otras ciudades: Ruta de atención para Mujeres Víctimas de Violencia https://guayaquil.consulado.gov.co/sites/default/files/ruta_consulado_guayaquil.pdf

- Puntos de atención de la Defensoría Pública (patrocinio legal gratuito): https://www.defensoria.gob.ec/?page_id=22777

Ciudades Seguras

Protegidas en Internet

Guía de cuidados digitales para organizaciones sociales de mujeres