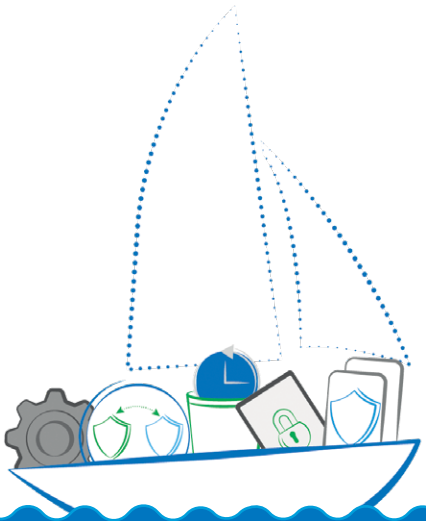
KIT DE EMERGENCIA
para la seguridad en el entorno digital

Herramientas, recursos y formaciones utiles en seguridad digital para la sociedad civil ante situaciones concretas en América Latina

NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO

KIT DE EMERGENCIA
para la seguridad digital
Herramientas, recursos y formaciones para la sociedad civil en América Latina



NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO

NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO

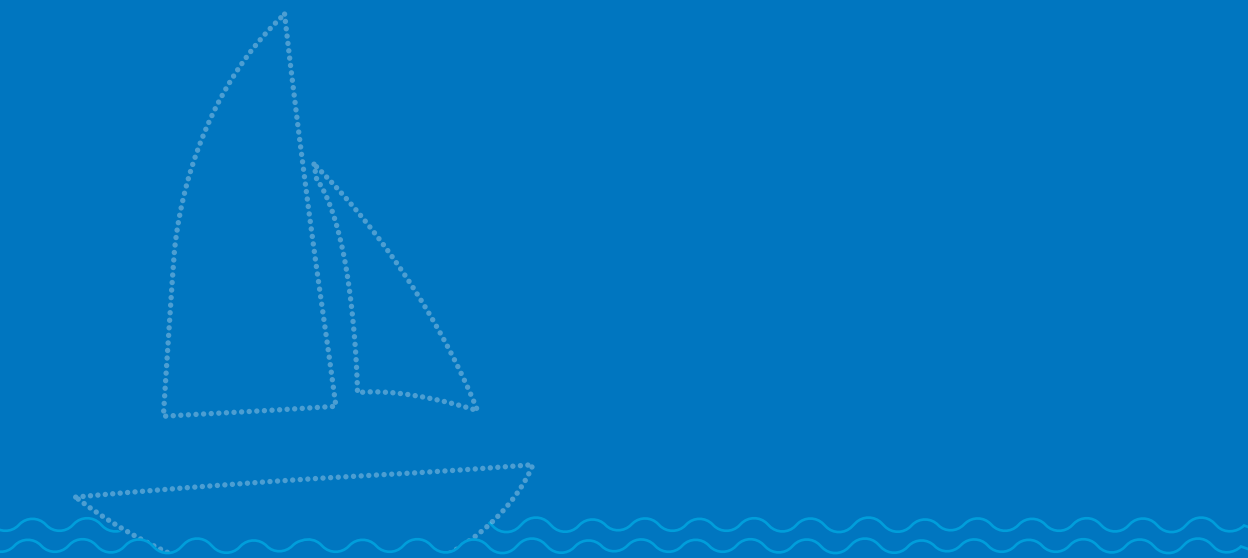
1a Edición, abril 2024.

Esta obra ha sido desarrollada por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos para hacer frente a algunas de las necesidades de seguridad en el ámbito digital de periodistas y medios de comunicación en diversos países de las Américas en el marco del proyecto "Global Drive for Media Freedom, Access to Information and the Safety of Journalists", apoyado por el Reino de los Países Bajos.

Las referencias a entidades, herramientas y sitios web externos son indicativas y no debe considerarse un respaldo de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos a dichas entidades y sitios web ni a los servicios que prestan.

Alejandro Dumas 165, Col. Polanco, Miguel Hidalgo,
CP 11560, Ciudad de México, México.
hchr.org.mx

ÍNDICE



INTRODUCCIÓN Y ADVERTENCIA

Este kit de emergencia se desprende de la "Caja de herramientas (toolbox) para una actuación más segura en el entorno digital en América Latina: recopilación de herramientas, recursos y formaciones útiles en seguridad digital para periodistas y personas defensoras de derechos humanos". Es una versión resumida con recomendaciones concretas frente a las principales amenazas digitales a las que se enfrentan diferentes personas, actores e integrantes de la sociedad civil en la región, incluyendo un enfoque diferenciado de género. Las recomendaciones contenidas en este recurso no requieren ser adoptadas en su integridad para ser efectivas. Su implementación dependerá de las condiciones, capacidades, dimensiones de género y entornos de seguridad de cada persona u organización. Cada avance contribuye sustancialmente a disminuir el riesgo. El kit de emergencia no desarrolla nuevos materiales, sino que recopila recursos hasta ahora existentes y brinda información sobre dónde encontrarlos y cómo utilizarlos,

La eliminación total de riesgos es IMPOSIBLE.

...

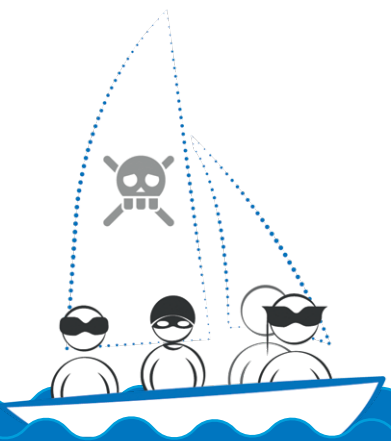
La seguridad es un camino. Tómate un tiempo para familiarizarte con los recursos y herramientas y adopta de manera progresiva mejores hábitos y mecanismos de seguridad.

haciendo énfasis en situaciones de riesgo concretas en América Latina.

La información contenida en este documento aborda algunas de las amenazas y formas de neutralizarlas disponibles al momento de su elaboración. Sin embargo, tanto las amenazas como las herramientas para contrarrestarlas cambian rápidamente, *por lo que esta guía no puede garantizar su eficacia a lo largo del tiempo y tampoco agota los recursos y problemas actuales en el entorno digital.*

Las referencias a entidades, herramientas y sitios web externos son indicativas y no deben considerarse un respaldo de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH) a dichas entidades y sitios web ni a los servicios que prestan. Dichas referencias se facilitan sin garantía de ningún tipo, ya sea expresa o implícita, incluidas, a título enunciativo y no limitativo, las garantías de comerciabilidad, idoneidad para un fin determinado y no infracción. La OACNUDH no será responsable en ningún caso de las pérdidas, daños, responsabilidades o gastos en que se incurra o que se pudieran sufrir como resultado del uso de los mismos. Su utilización corre por cuenta y riesgo de la persona usuaria. Los sitios web externos no están bajo el control de la OACNUDH, y la OACNUDH no es responsable de su contenido ni de ningún enlace contenido en estos sitios.

Situaciones de inseguridad digital comunes en América Latina



Existen herramientas específicas que son útiles para contrarrestar las amenazas y disminuir los riesgos ante cada situación de inseguridad digital. Estas recomendaciones no deben verse de manera aislada para cada caso, pues funcionan mejor si se utilizan en conjunto.

INTERRUPCIÓN
del servicio de internet

COMPRUEBA
que el módem o router del servicio funcione

« REINICIA y REVISA si la conexión se estabiliza.

BORRA
la caché, el historial y otros datos

« Esta acción acelerará la velocidad de conexión.

ASEGURA
que no se pierda información almacenándola de manera offline

« Cuando existan cortes de energía y/o conexión inestable a Internet, almacena de manera offline mediante el uso de Tella o Save hasta que se restablezca el servicio.

Son aplicaciones que permiten almacenar, compartir y cifrar de forma segura archivos sin temor a la censura, la vigilancia o las represalias.

Para comprobar la velocidad de la conexión:
» www.speedtest.net

Herramientas de documentación:
» Tella (sólo disponible para Android): https://tella-app.org/
» Save (disponible para iOS y Android): https://open-archive.org/save
» OnionShare (para Windows, MacOS y Linux): https://onionshare.org/

Accede a los tutoriales para borrar historial, *caché* y otros datos temporales en las páginas web de los siguientes navegadores:
» Google Chrome
» Microsoft Edge/explorer
» Mozilla
» Safari

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

BLOQUEO SELECTIVO
de páginas web

ACCEDE utilizando el servicio de VPN

« Esto muchas veces burla el bloqueo.

INTENTA acceder mediante diferentes navegadores de internet

« Puedes VERIFICAR si efectivamente la página se encuentra bloqueada mediante aplicaciones como OONI Probe.

DENUNCIA el bloqueo

« Si es seguro y viable, denuncia ante las instituciones públicas pertinentes y/o reclama a los proveedores del servicio, públicos o privados.

Aplicaciones de VPNs y similares:

» Proton VPN: https://protonvpn.com/
» Psiphon: https://psiphon.ca/
» RiseUp VPN: https://riseup.net/pt/vpn
» TunnelBear: https://www.tunnelbear.com/
» Lantern (alternativa al VPN): https://getlantern.org

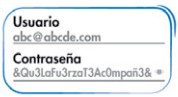
Herramienta para el chequeo de bloqueo en web:

» OONI Probe: https://ooni.org/install/

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

ROBO, PÉRDIDA
y confiscación de equipo

ANTES



PROTEGE el dispositivo con una contraseña segura

« COMBINA letras, números sea de al menos 8 dígitos.
« En el caso de los dispositivos móviles, las contraseñas en formato de **frase son más difíciles de hackear que los PIN o contraseñas numéricas.**

RESPALDA tu información de manera periódica

« USA los medios de almacenamiento en nube que recomendamos aquí, o bien usar de manera segura los más populares.

ENCRIPTA el dispositivo o la unidad

« En Mac es importante tener FileVault.
« Windows cuenta con Bitlocker.
« Para la encriptación del disco duro o de unidades específicas se puede usar VeraCrypt.

BORRA de manera permanente

« UTILIZA las aplicaciones señaladas y recomendaciones de uso, ya que el mero borrado, eliminado, vaciado de papelera o formateo de los equipos no elimina completamente la información.

PROTÉGETE ante situaciones y contextos de riesgo

Un buen hábito de seguridad antes de exponerse a estas situaciones es:
« CERRAR las sesiones de cuentas abiertas en el celular.
« BORRAR el contenido de los navegadores.
« LIMPIAR las conversaciones almacenadas en aplicaciones de mensajería.

Herramientas de cifrado:
» FileVault (disponible para macOS): https://support.apple.com/es-mx/guide/mac-help/mh11785/mac
» Veracrypt (Windows y macOS) - posibilita cifrar archivos y carpetas específicas: https://www.veracrypt.fr/en/Home.html
» Bitlocker (disponible para Windows): https://www.youtube.com/watch?v=5sXEzoengV0

Descubre cómo encontrar mi laptop / borrar contenido en las páginas web de los siguientes navegadores:
» Windows
» macOS

Herramientas de borrado y limpieza:
» Ver “liberar su espacio" en computador Windows Microsoft, en su página web de soporte.
» Ver “liberar espacio" en computador Mac iO, en su página web de soporte.
» CCleaner: https://www.ccleaner.com/es-es
» BleachBit: https://www.bleachbit.org/
» Andro Shredder (disponible solo para Android en Google Play)

HERRAMIENTAS

DURANTE

SOLICITA al operador que bloquee el dispositivo

« CONTACTA al operador para dar de baja la tarjeta SIM y realiza verificación en dos pasos.
« También puede ser rastreado por algunas operadoras.

BUSCA el dispositivo si tienes la app "Encontrar" activada

« **Android,** ACTIVA la función integrada de Google: "Encontrar mi dispositivo". Borra los datos, bloquea la pantalla y cambia la contraseña.
« **iPhone,** BUSCA el dispositivo si tienes la app "Encontrar" activada. En iCloud se puede marcar el dispositivo como perdido y borrar remotamente el contenido.

CIERRA remotamente las sesiones

« CAMBIA las contraseñas de los servicios que tengas instalados en el móvil.

BUSCA y **BLOQUEA** remotamente del dispositivo

« ACTÚA con rapidez.
« Tanto Windows como Mac ofrecen la opción accediendo a las cuentas de Microsoft o iCloud.
« CIERRA remotamente las sesiones o cambia las contraseñas de los servicios. **La opción más segura sería cambiar todas las contraseñas, lo que automáticamente cierra todas las sesiones.**

DESPUÉS

SOMETE a revisión técnica el equipo confiscado o robado

« Que la revisión técnica sea por un profesional de confianza antes de volver a utilizarlo.

EVALUA la efectividad de las medidas de prevención adoptadas

« PIENSA en cómo mejorar el plan de seguridad.

Herramientas de geolocalización:

» Encontrar mi dispositivo Android (Google Play).
» Encontrar mi iPhone (Apple Store).
» Rastrear o bloquear el dispositivo móvil a través de IMEI: https://www.imei.info/es/about/
Cada dispositivo electrónico cuenta con un código IMEI de 15 dígitos y es distinto al número de serie, el cual debes registrar y almacenar para su uso posterior. Así se puede localizar:
» En una etiqueta blanca debajo de la batería de tu dispositivo.
» Ir al menú de Ajustes del teléfono. Dentro del apartado "Acerca del teléfono", "Información del teléfono" o "Sistema > Información del teléfono" encontraremos un apartado donde nos mostrará el IMEI.
» En varios países, marcando desde el teléfono *#06#

Almacenamiento de datos en nube:

» pCloud (recomendada): https://www.pcloud.com/es/
» Ver cómo usar Dropbox de manera segura, en su página web de soporte.
» Ver cómo usar Google Drive de manera segura, en su página web de soporte.

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

HACKEO,
suplantación de identidad, robo de cuentas e información

ANTES

USA contraseñas seguras y no repitas las contraseñas

UTILIZA un gestor de contraseñas

ADOPTA la autenticación en dos pasos

« NO REPITAS las contraseñas; en lo posible, utiliza una distinta por cada dispositivo o aplicación.

Las contraseñas en formato de frases, incluso con idiomas combinados y utilizando números o símbolos (cómo #, $, @, *, !) intercalados pueden ser mecanismos seguros y confiables por su fácil memorización y la dificultad para que alguien más la deduzca.

NO GUARDES contraseñas en los navegadores web

BORRA regularmente información

« MANTÉN el hábito de limpiar los dispositivos.

NO COMPARTAS información sensible y **EXAMINA** los mensajes, correos y links

« Para no ser víctima de phishing es importante SEGUIR los consejos dados en las secciones anteriores; REVISA que las páginas web tengan los signos de seguridad correspondientes; ACTIVA la verificación de factor múltiple; USA software antimalware y siempre DUDA de cualquier comunicación que prometa premios, saldos a favor o regalos o que nos presione para actuar urgentemente proporcionando información personal.

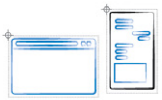
Gestores de contraseñas:
- » Bitwarden (en nube) https://bitwarden.com/
- » Keepass (fuera de la nube): https://keepass.info/
- » Ver cómo usar el gestor de contraseñas de Google de forma segura, en su página web de soporte.
- » Ver cómo usar el gestor de contraseñas de Apple iOS de manera segura, en su página web de soporte.

Autenticación de dos factores, disponibles en Apple Store y Google Play:
- » Google Authenticator
- » Microsoft Authenticator

Para averiguar si el correo electrónico o teléfono ha sufrido alguna violación de datos:
- » https://haveibeenpwned.com/

HERRAMIENTAS

DURANTE



REGISTRA a través de fotos, capturas de pantalla y almacenamiento

« TOMA NOTA de su contenido.

DESPUÉS

DENUNCIA ante los proveedores de servicios

« En caso de haber sido víctima de hackeo, phishing o robo de cuentas, INFORMA a tus redes de contactos y, dependiendo del contenido de la información, DENUNCIA ante instituciones públicas que aborden el asunto -si es posible y seguro.

USA software específico para buscar los archivos que hayan podido ser borrados

« REALIZA esta acción si a consecuencia de un ataque perdiste información almacenada en tus equipos

Extensiones útiles para la prevención durante la navegación en línea:

» Privacy Badger, provee un modo similar a la navegación en incognito: https://privacybadger.org/

» Ghostery, bloquea anuncios y mensajes no deseados en el navegador: https://www.ghostery.com/

» HTTPS Everywhere, provee un cifrado al ingresar a sitios no autenticados - htpps - para mayor seguridad: https://www.eff.org/https-everywhere

Herramientas de borrado y limpieza:

» Ver sección sobre "Robo, pérdida y confiscación de equipo".

Recuperación de información perdida o eliminada del dispositivo:

» Recuva: https://www.recuva.site/es/

Descubre lo consejos de Google y Microsoft para evitar la suplantación de identidad en sus páginas web de soporte.

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

SOSPECHA
de infección de tus equipos

ANTES

IMPLEMENTA
las medidas de robo, pérdida y confiscación de equipo

PROTEGE
el dispositivo con una contraseña segura

PROTÉGETE
ante situaciones y contextos de riesgo

BUSCA y **BLOQUEA**
remotamente del dispositivo

RESPALDA
tu información de manera periódica

SOLICITA
al operador que bloquee el dispositivo

SOMETE A REVISIÓN
técnica el equipo confiscado o robado

ENCRIPTA
el dispositivo o la unidad

BUSCA el dispositivo
si tienes la app "Encontrar" activada

EVALÚA
la efectividad de las medidas de prevención adoptadas

BORRA
de manera permanente

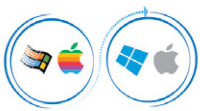
CIERRA
remotamente las sesiones

UTILIZA
un antivirus

« MANTENLO actualizado.

NO DESCARGUES
ni abras archivos de fuentes desconocidas o sospechosas.

REALIZA
copias de seguridad de manera regular y confiable



MANTÉN ACTUALIZADO
el sistema operativo

« REALIZA todas las actualizaciones pertinentes en el dispositivo (sistema operativo, softwares, aplicaciones).

NO USES
software de dudosa procedencia

« Puede haber sido modificado para infectar tu equipo.

DESCONFÍA
si pide permisos que resultan excesivos

« Las entidades bancarias y otros servicios no deberían pedirte datos completos por mail o mensaje de texto

DURANTE Y DESPUÉS

DESCONECTA
tu dispositivo
de redes de wifi
y bluetooth

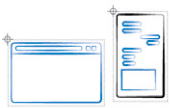
« TOMA ESTA MEDIDA hasta que la situación esté resuelta.

INSTALA
y ejecuta
un antivirus

REINICIA
el ordenador

BORRA
los datos de
navegación
y archivos

« CAMBIA todas las contraseñas.



REGISTRA
a través de fotos,
capturas de pantalla
y almacenamiento

SOMETE
a revisión técnica
el equipo confiscado
o robado

CONSULTA
con personas
u organizaciones
profesionales que
puedan evaluar
lo sucedido.

« Ver sección “A quién acudir”.

Antivirus gratuitos (y de opción paga):
» Malwarebytes: www.malwarebytes.com
» Avira: www.avira.com/es

Herramientas de borrado y limpieza:
» Ver sección sobre “Robo, pérdida y confiscación de equipo”.

ESCANEA Y
ACCEDE AL
CONTENIDO
ONLINE

HERRAMIENTAS

SOSPECHA
que la comunicación ha sido o puede ser interceptada

La intercepción de las comunicaciones puede ser en la mayoría de los casos imperceptibles, y pueden tomar la forma de ruidos extraños, recalentamiento de dispositivos o fallas poco usuales en los mismos. Evita utilizar las líneas telefónicas. La utilización de mecanismos de comunicación por datos o internet con encriptación de extremo a extremo, incluso en tus llamadas, pueden ser opciones más seguras.

ANTES

COMPARTE el enlace y la contraseña por canales seguros

« Cuando generes links para reuniones en línea, CONFIGÚRALOS para que pidan contraseña para entrar.

AVERIGUA la lista de participantes de las reuniones en línea

« PIDE que la gente no identificada lo haga.

UTILIZA VPN siempre que sea posible

ELIGE aplicaciones seguras y cifradas

« Una intercepción puede no ser visible, por ello EVITA usar la línea telefónica o mensajes SMS. En cualquier caso, averigua la forma de utilizar tus aplicaciones de mensajería o llamada de forma más segura.

Mensajería telefónica cifrada:

» Signal: https://signal.org/

» Ver cómo usar WhatsApp de forma más segura. https://faq.whatsapp.com/360105896189245/?locale=es_LA

» Ver cómo usar Telegram de forma más segura. https://telegram.org/faq/es%23seguridad

DURANTE

DESCONECTA
si hay personas sospechosas

« TRATA de precisar nombre, toma una imagen de la pantalla y obtén cualquier otro dato que permita su futura identificación.

EVITA
descargar archivos o programas de fuentes desconocidas

« Las comunicaciones pueden ser comprometidas por software malicioso instalado en tus equipos que recopile y envíe información. Este tipo de programas pueden ser muy difíciles de detectar.

« Si tienes dudas BUSCA el apoyo de una persona u organización experta en seguridad que pueda revisar el equipo.

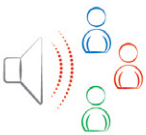
DOCUMENTA
pruebas de la posible intercepción

« DOCUMENTA mediante capturas de pantalla, fotos o cualquier otro medio.

INCREMENTA
medidas de seguridad cuando utilices redes abiertas o públicas de wifi

« Siempre COMPRUEBA la seguridad de los sitios navegados (asegúrate que la dirección inicie por HTTPS) y la encriptación de las comunicaciones. Las redes abiertas pueden instalarse maliciosamente para interceptar las conexiones y acceder de manera no consentida a los dispositivos y a la información.

DESPUÉS



AVISA
a las personas que puedan verse afectadas

« TOMA ESTAS MEDIDAS si sospechas que tus comunicaciones han sido comprometidas.

BUSCA
asesoría de personas y organizaciones expertas en seguridad

« Ver sección “A quién acudir”.

Llamadas y videollamadas cifradas:

» Jitsi: https://meet.jit.si/

» Ver cómo usar Zoom de manera segura, en su página web de soporte.

» Ver cómo usar Google Meet de manera segura, en su página web de soporte.

» Ver cómo usar Microsoft Teams de manera segura, en su página web de soporte.

Correo electrónico cifrado:

» Protonmail: https://proton.me/

» Ver cómo usar GMAIL de manera segura, en su página web de soporte.

» RiseUp Mail: https://riseup.net/es/vpn

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

SEÑALAMIENTOS
online, difamación, campaña de desprestigio, acoso y/o amenaza

En un mundo caracterizado por una conectividad sin precedentes y la transformación del espacio digital, el internet y las tecnologías de la información se han convertido en una piedra fundamental para realizar la labor periodística y promover, defender y ejercer los derechos humanos, pero también se convirtieron en un espacio para coartarlos y vulnerarlos. Particularmente las redes sociales se prestan como espacios de oportunidades y riesgos, por lo que requiere de precauciones y acciones de mitigación.

ANTES

SEA CONSCIENTE la información que compartes en redes sociales

« Las campañas de acoso en línea pueden usar información o imágenes que tú u otras personas han publicado. **NO PUBLIQUES información de terceras personas sin su consentimiento.**

FAMILIARÍZATE con las medidas de seguridad en el uso de redes sociales

REVISA la configuración de privacidad

« También la configuración de las aplicaciones que utilizas.

Extensiones útiles:
» Para capturar la pantalla: FireShot
https://chromewebstore.google.com/detail/take-webpage-screenshots/mcbpblocgmgfnpjjppndjkmgjaogfceg?hl=pt-PT&gl=US

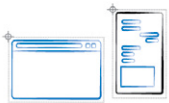
Para guardar y almacenar la página:
» Internet Archive (principal recomendada): https://archive.org/
» Zotero: https://www.zotero.org/download/connectors

HERRAMIENTAS

DURANTE

CONTRARRESTA
las acciones mediante respuestas y mensajes positivos

« La respuesta a este tipo de ataques dependerá del análisis de riesgo de cada persona y del contexto. Intentar responder a las acusaciones o señalamientos directamente puede ser desgastante y es parte de la estrategia de muchos atacantes; EVITA implicarte en discusiones con los atacantes.



DOCUMENTA
los ataques a través de fotos, capturas de pantalla

« Cualquier medio de verificación puede ser útil para demostrar lo ocurrido.

DESPUÉS

DENUNCIA
en las propias plataformas

« Las redes sociales y otros servicios suelen tener la obligación de contar con mecanismos para abordar estos casos.

DENUNCIA
el hecho como violencia cibernética u otro tipo penal disponible

« Las fiscalías y otros mecanismos nacionales pueden tener unidades especializadas para estas investigaciones.
« Ver sección “A quién acudir”

Cómo usar redes sociales de manera segura:
» Video de ACNUR: https://www.youtube.com/watch?v=axOSuT5CNl8

Cómo reaccionar ante la agresión o violencia cibernética:
» Portal Infoactivismo: https://infoactivismo.org/combatir-la-discriminacion-y-el-odio-en-linea/

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

CIBERABUSO,
extorsión sexual, difusión no consentida de imágenes íntimas y otras formas de ciberviolencia

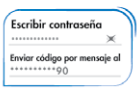
ANTES

NO DES CLIC en enlaces poco confiables

« SOSPECHA de propuestas tentadoras, dado que pueden ser un ardid para robar tus datos, imágenes y/o identidad digital.

EVALÚA no compartir datos

« Muchos perfiles falsos suelen verse vacíos, tiene poca actividad en las redes, poca historia, pocas imágenes personales y pocas amigas/seguidores.



UTILIZA autenticación de dos o más factores

« Esta es una de las medidas más efectivas en la seguridad digital.

FAMILIARÍZATE con las normas comunitarias de las plataformas

« El acoso, la suplantación de identidad digital y la difusión no consentida de imágenes, así como otras prácticas aquí planteadas, violan las normas comunitarias de las principales plataformas, como META (Facebook e Instagram), Twitter, Tik Tok y/o Kwai.

Herramientas de borrado y limpieza:

» Ver sección sobre "Robo, pérdida y confiscación de equipo".

Autenticación de dos factores:

» Ver sección sobre "Hackeo, suplantación de identidad, robo de cuentas y/o información".

Utilización de herramientas de comunicación e intercambio de información y contenido más seguras:

» Ver sección sobre "Sospecha que la comunicación ha sido o puede ser interceptada".

» **Advertencia:** Signal es una de las aplicaciones de mensajería más recomendadas por sus altos niveles de seguridad, sin embargo, no alerta ni bloquea la captura de pantalla por parte de las personas receptoras.

Hay aplicaciones de mensajería que tienen configuraciones que impiden que otra persona realice una captura de pantalla de los mensajes intercambiados, o te avisa si la persona interlocutora intenta capturar la pantalla. Estas funciones aumentan la seguridad, pero no previenen totalmente un mal uso de nuestra información, pues no protegen frente a otras formas de registrar las conversaciones o intercambios.

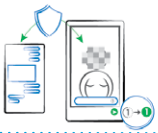
DURANTE

ANALIZA
si es idóneo actuar y contrarrestar o no responder, bloquear y denuncia

« Existen múltiples actividades de intercambio virtual de información personal que pueden facilitar la pérdida
« del control de nuestra información y puede ser usada para el hackeo, suplantación de identidad, robo de cuentas e información, señalamientos online, difamación, campaña de desprestigio, acoso y/o amenaza, entre otras.

RECONOCER
los riesgos y refuerza las medidas de seguridad ante la ciberviolencia

« En ocasiones la ciberviolencia se relaciona con el uso de información, imágenes o contenido de carácter íntimo o sexual reales o manipuladas. El sexting consensual entre adultos (compartir imágenes de contenido íntimo de manera consensuada) es una forma de expresión sexual que no debe estigmatizarse.



TOMA
medidas para protegerte

« USA aplicaciones seguras, con cifrado.
« OCULTA características.
« ELIGE que sean vistas una única vez.

PRESERVA
la evidencia digital

« TOMA capturas de pantalla y almacénalas.
« NO DENUNCIES el perfil de la persona victimaria para evitar perder información.
« EVITA responder a las amenazas.

No es necesario compartir contenido íntimo para ser víctima de su difusión, la manipulación de imágenes, cada día es más accesible gracias a algunas herramientas de inteligencia artificial.

DESPUÉS

DENUNCIA
el incumplimiento de las normas comunitarias

« También existen canales para el reporte de difusión de contenido íntimo sin consentimiento o de suplantación de identidad ante páginas de diversos tipos.

PIDE AYUDA
y asesórate

« No estás sola. La culpa no es tuya y no debes avergonzarte por ser víctima de este tipo de delitos. Las redes de apoyo son una parte elemental de todo plan de contingencia.

RECURRE
a entidades estatales especializadas de atención a la víctima

« Si eres víctima de violencia cibernética de género o sexual, mediante el uso de imágenes, videos o información personal no consentida, estas entidades pueden realizar acciones para contrarrestar los efectos de la agresión.

Consejos de privacidad para prevenir la ciberviolencia de género durante el uso de algunas redes sociales y herramientas de comunicación en este enlace:
» https://www.semujeres.cdmx.gob.mx/violencia-cibernetica-contra-mujeres/uso-seguro-de-las-redes-sociales

Recursos e historias relevantes sobre la ciberviolencia de género:
» https://www.pantallasamigas.net/

Herramienta desarrollada por Thomson Reuters Foundation y Google para documentar el acoso en línea contra periodistas, específicamente en Twitter/X:
» https://www.trfilter.org/

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

ALLANAMIENTO
a tu domicilio u oficina

En un allanamiento pueden darse múltiples riesgos para la seguridad de la información y los equipos. Estas situaciones requieren de un análisis de riesgo que permita tomar medidas preventivas y en caso de que se concrete el riesgo, medidas de mitigación. Algunas de las medidas útiles para hacer frente a un allanamiento han sido tratadas en otros apartados.

ANTES

REALIZA un análisis de riesgo para tomar las medidas preventivas indicadas

« En un allanamiento pueden darse múltiples riesgos para la seguridad de la información y los equipos. Algunas medidas útiles para hacerle frente han sido tratadas en otros apartados.

GENERA copias de seguridad

« Es importante prevenir. La pérdida de información es un riesgo común en los casos de allanamiento de oficinas o casas de personas defensoras de derechos humanos y periodistas.

CIFRA la información

CUENTA con contraseña robustas

BORRA regularmente

« Otro riesgo es el acceso a la información por parte de los responsables del allanamiento.

Herramientas de cifrado y localización:
» Ver sección sobre "Robo, pérdida y confiscación de equipo".

Gestores de contraseñas:
» Ver sección sobre "Hackeo, suplantación de identidad, robo de cuentas y/o información".

Para averiguar si el correo electrónico o teléfono ha sufrido alguna violación de datos:
» Ver sección sobre "Hackeo, suplantación de identidad, robo de cuentas y/o información".

DURANTE

NO PERMITAS el acceso a personas extrañas al lugar

« Cerciórate de la existencia y muestra de orden judicial que justifique el procedimiento. PROCURA asistencia legal y comunícate con tus familiares.

MANTÉN LA CALMA en todo momento

« En caso de que el ingreso sea forzado, no te resistas, pregunta los motivos del allanamiento.

PRESTA ATENCIÓN de las personas que ingresen al lugar

« Está atento de sus nombres, rangos, su vocabulario y vestimenta, y posibles testigos.

TOMA NOTA de todo

« Observa lo que hagan las personas funcionarias en el lugar y pide el acta del procedimiento para verificar que su contenido sea veraz.

TEN EN CUENTA que estos procedimientos pueden darse en cualquier momento

« Incluso pueden proceder en horas de la noche y en medio de tu descanso, por lo que posiblemente no puedas o no te encuentres en condiciones de reaccionar rápidamente ni de la mejor manera.

DESPUÉS

IMPLEMENTA las medidas de prevención y mitigación correspondientes a un hackeo y robo de cuentas

« En un allanamiento, es posible que los dispositivos electrónicos no solamente sean confiscados, sino que sean intervenidos en el lugar sin tu conocimiento.

USA contraseñas seguras

BORRA de manera permanente

NO COMPARTAS información sensible

REGISTRA

DENUNCIA

HAZ uso de las copias de seguridad restaurando la información

« Un riesgo menos visible es la alteración de la información, de manera que si bien no parezca que haya habido una pérdida, pueda darse una modificación del contenido que afecte posteriormente a las actividades a realizar.

SOMETE a revisión técnica el equipos confiscado o robado

« Que la revisión técnica sea por un profesional de confianza antes de volver a utilizarlo.

Antivirus y limpiadores:

» Ver sección sobre "Sospecha que la computadora / cuenta fue infectada".

Herramientas de borrado y limpieza:

» Ver sección sobre "Robo, pérdida y confiscación de equipo".

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

DETENCIÓN
y desaparición

Estas medidas son aplicables a los casos de detención por parte de las autoridades o los contextos de desaparición forzada (cometidas por agentes del Estado o por particulares con su autorización, apoyo o aquiescencia) o desaparición cometida por particulares (como grupos armados, bandas delictivas, o individuos).
Existen países o contextos dónde las detenciones por fuerzas de seguridad o las desapariciones, con independencia de su duración, de personas defensoras de derechos humanos y periodistas son más probables. En estos casos los perpetradores muchas veces tendrán acceso a los equipos y la información de la persona privada de la libertad.

ANTES

IMPLEMENTA las medidas de prevención y mitigación correspondientes a un hackeo y robo de cuentas

USA contraseñas seguras

BORRA de manera permanente

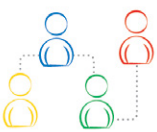
NO COMPARTAS información sensible

REGISTRA

DENUNCIA

ESTABLECE un plan de comunicación con contactos de seguridad

« Este plan puede dar tranquilidad a tu entorno y, al mismo tiempo, alertar sobre una posible detención o desaparición. Es importante que el plan incluya también las acciones que deben realizarse en caso de perder la comunicación o de tener la sospecha de una detención o desaparición.



DESIGNA roles a personas en resguardo o libertad dentro del protocolo de seguridad

« Es importante que se les otorgue la capacidad para restringir o bloquear el acceso a las cuentas y sesiones de la persona en riesgo e implementar las medidas de seguridad digital.

DURANTE

CAMBIA
las contraseñas o bloquear el acceso a las cuentas de la persona detenida y de la organización

« Otras acciones inmediatas del protocolo de seguridad a implementar por terceros pueden ser bloquear teléfonos celulares y otros dispositivos electrónicos de manera remota, sacar a la persona de listas de difusión de correo electrónico y de grupos de aplicaciones de mensajería, como WhatsApp, Signal y otras, y realizar copias de seguridad y borrar contenido de dispositivos y cuentas de manera remota.

UTILIZA
los mecanismos de geolocalización de dispositivos para intentar determinar la ubicación de la persona desaparecida

DESPUÉS

TOMA
las medidas de seguridad digital

« Robo, pérdida y confiscación de equipo.
« Hackeo, suplantación de identidad, robo de cuentas e información.
« Sospecha que la comunicación ha sido o puede ser interceptada.

Mensajería cifrada, llamadas y video llamadas cifradas
» Ver sección sobre "Sospecha que la comunicación ha sido o puede ser interceptada".

Herramientas de cifrado, geolocalización y borrado seguro de información:
» Ver sección sobre "Robo, pérdida y confiscación de equipo".

Gestores de contraseñas, autenticación de dos factores o para averiguar si tu correo o teléfono han sufrido una violación:
» Ver sección sobre "Hackeo, suplantación de identidad, robo de cuentas y/o información".

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

HERRAMIENTAS

ACOSO EN LÍNEA
contra mujeres defensoras de derechos humanos y periodistas

Las mujeres defensoras de derechos humanos y periodistas están especialmente expuestas a sufrir campañas de acoso y desprestigio en línea. La violencia de género en línea puede tomar la forma de amenazas de violación, asesinato o violencia sexual, difusión de mensajes o información falsos, suplantación de identidad, doxing (publicación de información privada), troleo, extorsión sexual, difusión no consentida de imágenes íntimas reales o manipuladas, acusaciones de actuar contra la moral, las leyes o los roles estereotipados de género, campañas de desprestigio, etc. En ocasiones estas amenazas se dirigen también contra el ámbito familiar de las mujeres defensoras y periodistas.

No hay una respuesta tecnológica sencilla a este problema. Algunas de las medidas expuestas en apartados anteriores pueden ayudar a prevenir o mitigar este tipo de violencia, pero no podrán evitarla totalmente, por lo que es importante prepararse para ella. Es especialmente importante entender que afrontar este tipo de violencia no es una cuestión meramente individual de una defensora de derechos humanos o periodista que sea objeto de violencia en línea, sino que es una tarea colectiva en la que medios de comunicación, organizaciones de derechos humanos, redes solidarias, deben asumir una responsabilidad.

Una encuesta de

2020

de UNESCO y el ICFJ mostró que el

73%

de las **MUJERES PERIODISTAS**

entrevistadas fueron

víctimas de acoso en línea.

ACOSO
en línea contra mujeres

ANTES

PREPARARSE
individual y colectivamente para la posibilidad de sufrir este tipo de violencia

« ADOPTA medidas para proteger la información confidencial y las comunicaciones, reducir la exposición propia y de otras personas.

Las organizaciones y medios deben dotarse de herramientas para atender este tipo de situaciones, tales como:

GENERAR protocolos

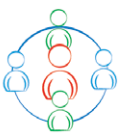
CONTAR con asesoría legal para acompañar proceso

BRINDAR acompañamiento psicosocial a la víctima

FORMAR a sus equipos en materia de seguridad en el ámbito digital

FORMA
redes de mujeres para contar con apoyo frente a actos de violencia en línea

« FORMA redes de mujeres periodistas, o TRABAJA con organizaciones sindicales, profesionales o de libertad de expresión o de defensa de los derechos humanos.



SE PARTE
del apoyo solidario a las periodistas y defensoras de derechos humanos que enfrentan este tipo de actos puede ayudar a fortalecer la capacidad de reacción de la comunidad

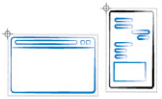
« Muchas veces, antes de llegar a ser víctimas de este tipo de acoso otras colegas de otros medios pueden haber sido víctimas de este tipo de actos.

Curso sobre Acoso en Línea para mujeres
» https://www.iwmf.org/programs/acoso-en-linea/

Guía práctica para mujeres periodistas sobre cómo responder al acoso en línea
» https://unesdoc.unesco.org/ark:/48223/pf0000379908_spa

HERRAMIENTAS

DURANTE



DOCUMENTA
los actos de acoso o desprestigio

« TRANSMITE el resultado de la documentación a organizaciones nacionales e internacionales.

COMUNICA
al medio o la organización la situación y solicita su apoyo

DENUNCIA
en las propias plataformas

« INDICA que se tratan de actos de violencia de género.

DENUNCIA
ante las autoridades aquellos actos que pudieran constituir delitos

« Es importante INSISTIR que se tomen en cuenta los elementos discriminatorios por motivos de género. SOLICITA que se lleven a cabo las acciones de investigación que permitan incorporar legalmente la información a los expedientes correspondientes con perspectiva de género.

DESPUÉS

REALIZA
un análisis de riesgo que permita identificar escenarios factibles y riesgos asociados

« El acoso en línea puede ir seguido de violencia física. La difusión de información como la dirección el lugar de trabajo de una periodista o defensora de derechos humanos (una forma de doxing), puede animar las agresiones o el acoso físico.

« VALORA solicitar medidas de protección a las autoridades o adoptar estrategias de protección también en el ámbito físico

BUSCA
apoyo psicosocial para afrontar los impactos

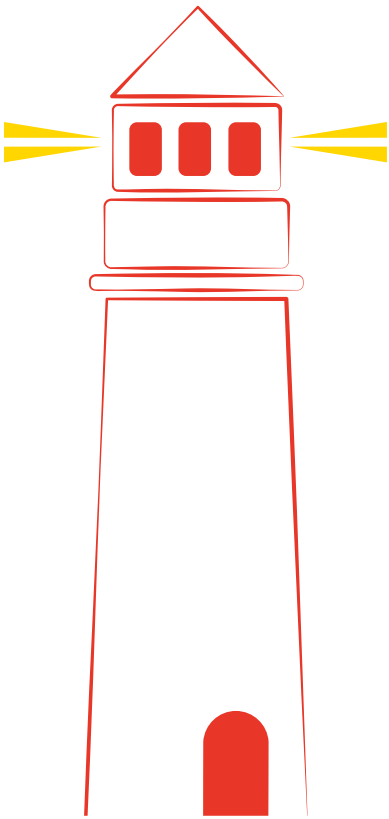
EVALÚA
con las organizaciones o medios implicados cómo fue la respuesta y si podría fortalecerse

Manual para el borrado de información
» https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Introducci.C3.B3n

Portal de la UNESCO sobre seguridad para mujeres periodistas
» https://www.unesco.org/es/safety-journalists/safety-women-journalists

ESCANEA Y ACCEDE
AL CONTENIDO ONLINE

A quién acudir



La OACNUDH cuenta con oficinas de país, presencia y asesorías nacionales en las Américas. Ante una situación de riesgo, recurre a los datos de contacto y ubicación. La Comisión Interamericana de Derechos Humanos (CIDH) también cuenta con mecanismos de atención de consultas y un sistema de petición en línea de medidas cautelares de protección. La OACNUDH y la CIDH forman parte del Mecanismo de Acciones Conjuntas para Contribuir a la Protección de las Personas Defensoras de los Derechos Humanos en las Américas.

Existen múltiples organizaciones de la sociedad civil que trabajan a nivel nacional e internacional en materia de protección de periodistas, medios de comunicación, organizaciones no gubernamentales y personas defensoras de derechos humanos a las que puedes acudir en caso de estar en riesgo. Puedes conocer algunas de ellas en el siguiente enlace. Unas más cuentan con **líneas de apoyo de emergencia** en caso de materialización de un riesgo inminente.

Mecanismos Internacionales de Derechos Humanos

OACNUDH en las Américas
» https://www.ohchr.org/es/about-us/where-we-work

Comisión Interamericana de Derechos Humanos
» https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/atencion/contacto.asp

» https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/portal/default.asp

Líneas internacionales de apoyo en emergencias

Protect Defenders
» https://protectdefenders.eu/

Access Now
» https://www.accessnow.org/help-es/

Front Line Defenders
» https://www.frontlinedefenders.org/en/emergency-contact-human-rights-defenders

Comité para la Protección de Periodistas
» https://cpj.org/emergency-response/how-to-get-help/

Coalición contra la Violencia Online
» https://onlineviolenceresponsehub.org/

A nivel nacional, existen fiscalías o ministerios públicos encargados de investigar agresiones que puedan constituir un delito. En algunos casos, tienen la facultad de establecer o solicitar medidas de protección. Por otra parte, las instituciones nacionales de derechos humanos (Defensorías del Pueblo, Comisiones de Derechos Humanos, Procuradurías de Derechos Humanos o similares) tienen la responsabilidad de proteger y promover los derechos humanos, específicamente ante las acciones u omisiones de las autoridades. Algunos países de la región (Brasil, Colombia, Honduras, México y Perú) cuentan con mecanismos nacionales de protección para personas defensoras de derechos humanos, periodistas y otros actores sociales. Finalmente, algunos países tienen instituciones nacionales de lucha contra la discriminación que pueden resultar relevantes para aquellas agresiones digitales con contenido discriminatorio.

Si bien las instituciones nacionales mencionadas pueden ser mecanismos útiles de protección, es necesario evaluar en cada caso concreto la pertinencia de acercarse a ellas, particularmente si el origen de los ataques proviene de actores estatales o se cometen con la aquiescencia de estos. Es importante analizar el riesgo y asesorarse con colegas, actores de la sociedad civil especializados u organizaciones internacionales para decidir a qué instituciones recurrir.

También cuentas con organizaciones de la sociedad civil a nivel nacional que brindan más información o pueden ayudarte.

Organizaciones de la sociedad civil a nivel nacional que brindan ayuda e información

En Argentina:
» https://adc.org.ar/

En Bolivia:
» https://internetbolivia.org/

En Brasil:
» https://www.marialab.org/
» https://escoladeativismo.org.br/

En Colombia:
» https://web.karisma.org.co/
» https://flip.org.co/

En Costa Rica:
» https://www.acceso.or.cr/

En Chile:
» https://www.derechosdigitales.org/
» https://amarantas.org/

En Ecuador:
» https://navegandolibres.org/
» https://lalibre.net/

En Guatemala:
» https://redrompeelmiedoguatemala.org/
» https://www.protectioninternational.org/locations/guatemala-2/

En Honduras:
» https://clibrehonduras.com/

En México:
» https://socialtic.org/
» https://r3d.mx/

En Paraguay:
» https://www.tedic.org/

En Perú:
» https://hiperderecho.org/

En Uruguay:
» https://idatosabiertos.org/
» https://cainfo.org.uy/sitio/

En Venezuela:
» https://vesinfiltro.com/

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

Recursos y formaciones para entender la seguridad en el entorno digital

FORMACIONES	DESCRIPCIÓN
Security in a Box[1] (recurso disponible en español, excepto la sección de herramientas, que está disponible en únicamente inglés)	Manual bastante completo sobre seguridad digital. Contiene información sobre seguridad en contraseñas, comunicaciones, teléfono, computadoras conexión a internet y archivos. Para cada sección hay una subsección llamada "Herramientas asociadas", que presenta opciones de herramientas seguras, encriptadas y/o de fuente abierta, con orientación específica sobre su instalación y uso. El recurso presenta también consejos concretos sobre cómo proteger dispositivos contra ataques de *malware* y *phishing*.
Front Line Defenders – Guía sobre herramientas seguras para conferencias y chats grupales[2] (recurso disponible en español e inglés)	La guía ofrece criterios para seleccionar herramientas o plataformas más seguras; información específica relacionada con cada herramienta o servicio enumerado; recomendaciones sobre videollamadas y capacitaciones en línea o webinars. Herramientas y servicios mencionados: Signal, Delta Chat, Element, Wire, Jitsi Meet, Bigbluebutton, Whereby, Blue Jeans, Facetime / Imessage, Google Meet, Duo y Whatsapp.
Protege.La[3] (recurso disponible solo en español)	Protege.la es un espacio abierto para compartir recursos sobre seguridad y privacidad digital de SocialTIC.org
Artículo 19[4] (recurso disponible solo en español)	Portal de herramientas sobre seguridad física, seguridad digital, normatividad y derecho a la información, entre otros temas, que podrán ayudar a periodistas y personas defensoras de derechos humanos a reducir los riesgos relacionados con su labor.

1 https://securityinabox.org/es/
2 https://www.frontlinedefenders.org/es/resource-publication/guide-secure-group-chat-and-conferencing-tools
3 https://protege.la/
4 https://seguridadintegral.articulo19.org/

FORMACIONES	DESCRIPCIÓN
Manual de seguridad digital: kit de herramientas para una internet feminista[5] (recurso disponible solo en español)	Este manual tiene como objetivo aportar teoría y práctica para aprender a usar tecnologías de software abierto y no privativas que permitan navegar de forma más segura en ordenadores y telefonía móvil. Introduce en el concepto de "huella digital", que explica los ataques tanto *offline* como *online* a personas por su identidad de género o sexualidad
Committee to Protect Journalists[6] (recurso disponible en español con algunas secciones disponibles exclusivamente en inglés)	El Comité para la Protección de los Periodistas presenta notas orientativas sobre seguridad para periodistas. La mayoría de las notas presentan consejos que van desde medidas de prevención, buscando minimizar el riesgo, hasta medidas de reacción, con el objetivo de reducir el impacto de incidentes. Algunas de las notas de seguridad más relevantes tratan sobre cómo protegerse del acoso en línea y de ataques dirigidos, cómo retirar los datos personales de la internet y cómo proteger fuentes. También señalan cómo asegurar la protección de datos e información de dispositivos frente a una posible privación de libertad y cómo resguardar la salud mental frente al acoso cibernético. El recurso brinda recomendaciones concretas sobre cómo actuar ante un corte de internet.
Totem[7] (formaciones disponibles en español)	Es una plataforma en línea desarrollada en colaboración entre Greenhost y Free Press Unlimited. Ofrece opciones de entrenamiento de seguridad digital para activistas, personas defensoras de derechos humanos y periodistas.

[5] https://arsgames.net/manual-de-seguridad-digital-kit-de-herramientas-para-una-internet-feminista/
[6] https://cpj.org/reports/2012/04/technology-security/
[7] https://totem-project.org/es/

FORMACIONES	DESCRIPCIÓN
Google News Initiative – formaciones en seguridad digital[8] (formaciones disponibles en español)	Se trata de una plataforma de aprendizaje de Google destinada a personas periodistas que ofrece una serie de formaciones sobre seguridad digital y otros temas de interés.
IFEX-ALC Campaña: Seguridad Digital para Periodistas[9] (formaciones disponibles en español)	Esta página contiene videos para la promoción estratégica de herramientas y prácticas de seguridad digital para periodistas.
Freedom of the Press Foundation[10] (formaciones disponibles en inglés)	La plataforma mezcla una serie de guías y cursos sobre temas diversos como la comunicación segura, el acoso en línea y la seguridad de cuentas diversas.
Guía práctica para mujeres periodistas sobre cómo responder al acoso en línea[11]	Esta Guía es un documento corto creado por la UNESCO está destinada a ayudar a las periodistas a afrontar los desafíos de la violencia en línea. Incluye consejos de como preparase para el acoso en línea de manera preventiva, como reaccionar y como mitigar sus efectos. Asimismo, deriva a recursos adicionales a los cuales se puede acceder ante distintas circunstancias.

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

8 https://newsinitiative.withgoogle.com/es-es/resources/trainings/safety-and-security/
9 https://ifex.org/es/ifex-alc-digital-security-for-journalists-campaign/
10 https://freedom.press/training/
11 https://unesdoc.unesco.org/ark:/48223/pf0000379908_spa

ESCANEA Y
ACCEDE AL
CONTENIDO
ONLINE

https://seguridad-digital.oacnudh.org/

KIT DE EMERGENCIA
para la seguridad digital
Herramientas, recursos y formaciones para la sociedad civil en América Latina

Esta edición se terminó de imprimir
en abril de 2024 en México.
Tiraje de 50 ejemplares.

https://seguridad-digital.oacnudh.org/

NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO