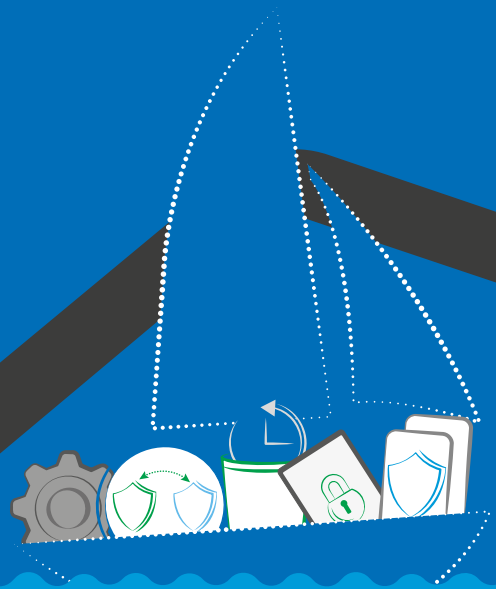
CAJA DE HERRAMIENTAS
TOOLBOX

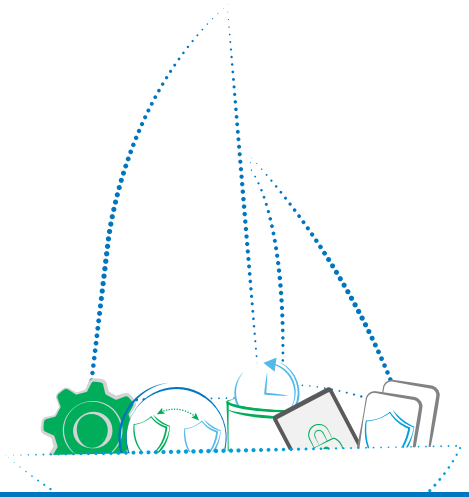
para una actuación más segura en el entorno digital en América Latina:

Herramientas y recursos de seguridad digital para personas defensoras de derechos humanos y periodistas



NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO

CAJA DE HERRAMIENTAS TOOLBOX
para una actuación más segura en el entorno digital en América Latina:
Herramientas y recursos de seguridad digital para personas defensoras de derechos humanos y periodistas



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

ADVERTENCIA

Esta caja de herramientas ha sido elaborada durante 2022 y 2023 por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACNUDH), para ofrecer apoyo a las personas defensoras de derechos humanos y periodistas frente a algunas de las principales amenazas que enfrentan en el ámbito regional. Su contenido ha sido consultado con personas y organizaciones en materia de libertad de expresión y seguridad digital. El desarrollo de esta caja de herramientas ha sido financiado por el Reino de los Países Bajos como parte del proyecto "Global Drive for Media Freedom, Access to Information and the Safety of Journalists". La información contenida en este documento aborda algunas de las amenazas en el entorno digital y las formas de combatirlas que existen 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.*

1 INTRODUCCIÓN y objetivos

Las tecnologías de la información y la comunicación juegan un papel crucial en la forma en la que nos comunicamos, accedemos a la información y la compartimos. En consecuencia, impactan en la labor periodística, la defensa de los derechos humanos y el pleno ejercicio de las libertades de expresión y de opinión. Sin embargo, también se ha incrementado el uso malicioso de esas tecnologías y los riesgos que se afrontan que se afrontan en el entorno digital. Las personas defensoras de derechos humanos y periodistas enfrentan descalificaciones, intentos de acceder a la información confidencial, obstáculos para acceder o difundir información y otras muchas acciones contra su labor. Esta caja de herramientas busca responder a los desafíos actuales más comunes en materia digital, brindando información sobre problemas concretos presentes en América Latina, y presentando algunas acciones y herramientas para enfrentarlos. Recopila una selección de recursos relevantes existentes y brinda información sobre dónde encontrarlos y cómo utilizarlos. Entre otros temas, incluye información práctica sobre medios de comunicación seguros (llamadas, correos y mensajería), transferencia de archivos, protección de contraseñas, uso de redes sociales, protección contra programas maliciosos (*malwares*), uso de VPN y otras herramientas para garantizar la privacidad, incluyendo consejos sobre amenazas y situaciones de inseguridad digital.

La caja de herramientas busca mejorar la ciberseguridad y mitigar riesgos específicos en el entorno digital. La persona lectora encontrará:

RECURSOS: manuales, infográficos y otras fuentes de información sobre seguridad digital.

HERRAMIENTAS: programas, aplicaciones y servicios en línea para navegar en el entorno digital de manera segura. Se ofrece información adicional sobre cómo implementar su uso, por medio de tutoriales en línea.

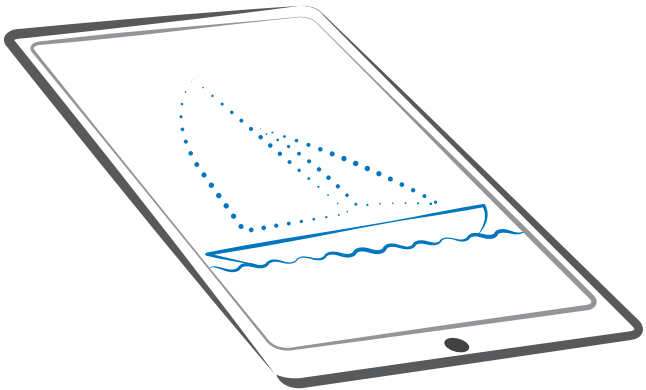
POSIBILIDADES DE FORMACIÓN: priorizando opciones que sean gratuitas y disponibles en línea. En cada sección se presenta una descripción del recurso, herramienta o formación disponible y sus principales usos. Es fundamental saber que, aunque la **eliminación total de riesgos es imposible, cada pequeña medida tomada contribuye a disminuirlos sustancialmente**. Entre más recomendaciones y medidas de seguridad se implementen, mayor será la protección. Es muy importante tomar un tiempo para familiarizarse con los recursos y herramientas, de manera que adoptemos de manera progresiva mejores hábitos y mecanismos de seguridad. Para minimizar la exposición al riesgo, el cambio de comportamiento es tan importante como usar herramientas: de poco sirve tener aplicaciones seguras en la computadora si dejamos nuestras contraseñas escritas en un papel su lado. En el caso de organizaciones, grupos y redes, es imprescindible un compromiso colectivo con el uso de herramientas seguras. Si una sola persona no hace un uso consciente y cuidadoso de las herramientas, puede comprometerse la protección que se buscaba como grupo. Adoptar buenas prácticas y hábitos seguros en nuestro día a día, evitar comportamientos de riesgo e incorporar de herramientas seguras y de fácil uso para actividades como mensajería, llamadas, correo, almacenamiento de información o intercambio de archivos, pueden llevar a una reducción significativa del riesgo.

El cambio de hábitos no sucede radicalmente de un día para otro, sino que normalmente es un proceso de cambio paulatino. Aplicar progresivamente estas medidas y actualizarlas regularmente nos irá protegiendo cada vez más, ayudando a ganar la carrera a quienes ponen en riesgo a las personas defensoras de derechos humanos y periodistas y su labor en el espacio digital.

2

CINCO REGLAS básicas del uso de los dispositivos electrónicos

ESCANEA Y ACCEDE AL CONTENIDO ONLINE



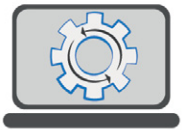
REGLA 1

Todos los dispositivos deben protegerse mediante la configuración de un medio de seguridad o verificación. Estos pueden ser:

a) PIN (clave normalmente numérica de 4 a 6 dígitos).
b) Contraseña segura (clave normalmente alfanumérica de al menos 8 dígitos).
c) Patrones (usualmente es una secuencia de unión de puntos).
d) Huella digital o dactilar (común en los dispositivos móviles).
e) Reconocimiento facial (común en los dispositivos móviles más recientes).

Los más comunes y los más seguros son a) y b): PIN y contraseña segura. Cuanto más largo sea el PIN o la contraseña más seguro será. Además, es importante que no sea asociable con la persona (es fácil probar un PIN de 4 cifras con el año de nacimiento de la persona o de sus seres queridos u otras fechas significativas). El reconocimiento facial o la huella dactilar pueden ser usados para desbloquear un dispositivo por parte de un agresor con suficiente capacidad. Por ejemplo, en caso de detención, un agente puede desbloquear un dispositivo de una persona detenida sólo situándolo frente a la cara de la persona defensora o periodista"

REGLA 2



Los *softwares* y los sistemas operativos deben mantenerse actualizados. La mayoría de las actualizaciones contienen parches de seguridad, que juegan un papel esencial para la seguridad digital y el correcto funcionamiento de las aplicaciones y los dispositivos.

REGLA 3

Usa la **autentificación o verificación en dos o más factores** para todas las aplicaciones que contengan información sensible y confidencial, **particularmente aquellas de mensajería instantánea como WhatsApp, Signal o Telegram, y aquellas de correo electrónico.** La autentificación o verificación de dos pasos es un mecanismo de control que pide dos o más pruebas diferentes para confirmar la identidad de la persona propietaria antes de permitir el acceso a la aplicación, cuenta o información. Normalmente opera mediante un código o clave de único uso, como las aplicaciones Google Authenticator o Microsoft Authenticator, o mediante el envío de notificaciones

de confirmación a otras aplicaciones, como los correos electrónicos o la mensajería. No se recomienda el uso de autenticación de dos pasos con el envío de mensajes SMS, pues estos pueden llegar a ser incerceptados por un atacante con suficiente capacidad. Aunque este mecanismo puede resultar incómodo y tardado, incrementa de manera muy importante la seguridad.

REGLA 4

Borrar datos regularmente de forma segura y permanente la información sensible de los dispositivos y cuentas, especialmente cuando ya no es necesaria, o cuándo podamos encontrarnos en contextos de mayor riesgo. Por ejemplo, eliminar información sensible de fuentes cuya identidad buscamos proteger antes de acudir con el celular a cubrir una manifestación dónde pueda haber detención de periodistas por las fuerzas de seguridad. Las palabras "borrar", "eliminar", "limpiar" o "triturar" tienen diferentes significados cuando hablamos de computación. Borrar datos no necesarios, eliminar los archivos borrados de la papelera o incluso reformatear los dispositivos son medidas de positivas pero insuficientes, pues no eliminan la información de manera permanente; ésta queda oculta y podría ser recuperada por alguna persona. Realizar la limpieza del disco de almacenamiento del dispositivo es un hábito que ayudará a eliminar esa información que queda almacenada. Para limpiar la información de manera segura y permanente, se debe recurrir a programas y aplicaciones creadas para ese fin específico -encontrarás algunas opciones en este documento. **Es importante también borrar periódicamente el contenido de los chats o conversaciones guardadas en aplicaciones de mensajería instantánea como WhatsApp, Signal o Telegram.** Estas aplicaciones te dan la opción de borrar automáticamente las conversaciones de manera periódica, lo que facilita e incrementa ampliamente la seguridad.

REGLA 5

Realizar copias de seguridad. Es muy probable que en algún momento seamos víctimas de la pérdida accidental o intencionada de un dispositivo con información o de la pérdida directa de la información. Establecer con antelación un plan de copias de seguridad (*back-up*), y realizarlo de forma regular ayudará a hacer frente a una situación de pérdida de información. Las copias de seguridad deben realizarse de forma regular, y almacenarse de manera segura.

ABC de los dispositivos electrónicos (computadoras, teléfonos móviles, tabletas, etcétera)

CÓDIGO ABIERTO/CERRADO
Se utiliza para describir si el código fuente de un software está o no abiertamente disponible para cualquier persona que lo quiera usar, copiar, estudiar, modificar y redistribuir sin restricciones.

NUBE
Almacenamiento de datos que se realiza en redes de computadoras. Los datos se alojan en servidores de forma virtual. Los servidores, por lo general, son proporcionados por terceros.

SOFTWARE
Son componentes intangibles que controlan el funcionamiento de los dispositivos informáticos permitiéndoles realizar sus diferentes funciones. También se les llama “programas”.

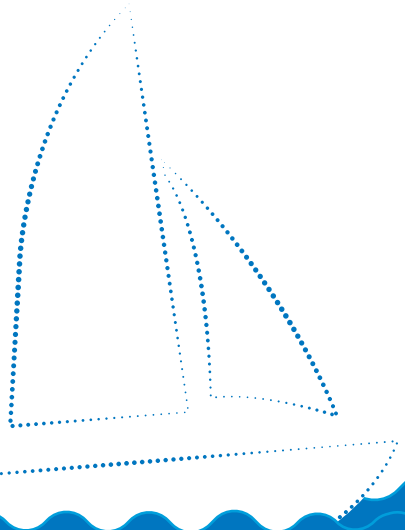
SISTEMA OPERATIVO
Es un programa que gestiona el funcionamiento de un dispositivo. Windows, iOS y Android son ejemplos de sistemas operativos.

APLICACIÓN (APPS)
Tipo de software utilizado en algunos dispositivos para realizar una función determinada. WhatsApp es un ejemplo de aplicación para mensajería.

3

LA NAVEGACIÓN en línea

ESCANEA Y ACCEDE AL CONTENIDO ONLINE



Siempre que nuestros dispositivos están conectados a la internet somos vulnerables ante ataques digitales. Para utilizar la internet y visitar páginas web utilizamos un tipo de software llamado "navegadores", como Google Chrome, Microsoft Edge, Mozilla Firefox o Safari. Existen algunos mecanismos básicos que ayudan a incrementar la seguridad de la navegación y pueden ser rápidamente implementados:

EXTENSIONES O COMPLEMENTOS:

Son softwares que pueden ser instalados directamente en el navegador. Hay varios tipos de extensiones, desde aquellas que bloquean anuncios hasta las que ofrecen protección de datos personales o incluso traducción. Es importante usar complementos que pueden ayudarte a aumentar la seguridad durante la navegación, pero también evitar descargar e instalar complementos de fuentes no confiables que pueden ser una manera de acceder a tu información.

INDICADOR DE PÁGINA WEB SEGURA:

Para saber si estamos accediendo a una página segura, la URL -que es el *link* completo que nos lleva a una determinada dirección en línea- deberá empezar por **HTTPS** y no por HTTP. **La letra "S" significa "seguridad"** y que la página está cifrada y protegida. A la izquierda de algunas URL se puede ver un ícono de candado, que se refiere al certificado digital de la página e indica que se trata de una página segura. (https://www.) El navegador normalmente indica cuando la página no es segura. (Not secure | example.com) Esto no garantiza que estés accediendo al sitio que deseas, por lo que es importante que siempre revises la barra de direcciones.

COMPRUEBA QUE LA DIRECCIÓN DE LA PÁGINA WEB ES CORRECTA:

En ocasiones los atacantes generan páginas con direcciones muy similares a la dirección legítima a la que queremos acceder, como por ejemplo registrar una página como 0hchr.org (con un cero simulando ser una "o") en lugar para intentar simular la dirección web del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Esto puede servir para robar nuestra información. Comprobar que la dirección a la que intentamos acceder se encuentra correctamente escrita nos ayudará a prevenir múltiples problemas.

HISTORIAL Y *CACHÉ*:

Los navegadores guardan el historial de los sitios web que visitaste. Al mismo tiempo, guardan información temporal de todo tipo (por ejemplo, llenado de formularios, personas usuarias e incluso contraseñas), a la que se le llama "*caché*". Borrar tanto el historial como la *caché* de los navegadores incrementa la seguridad y privacidad digital.

MODO INCÓGNITO:

La mayoría de los navegadores incluyen la posibilidad de usarlos en modo "incógnito". Este modo permite que no queden registrados rastros del uso del navegador, como el historial de búsqueda y la *caché*. Sin embargo, es importante destacar que el "modo incógnito" no te protege de la obtención de información por parte de quien tenga control de tu equipo o de la red a la que te conectas.

VIRTUAL PRIVATE NETWORK (VPN):

La VPN es una herramienta que oculta los datos del dispositivo de la persona usuaria y todos los datos enviados o recibidos. Así, el uso de VPN aumenta la seguridad de todo el tráfico de datos en internet y la identidad, ubicación u otra información sobre la persona usuaria.

CIFRADO DIGITAL:

Para asegurar la privacidad de nuestras comunicaciones en línea, se recomienda el uso de **cifrado**. El cifrado es un proceso en el cual se codifican datos, archivos o conversaciones para que no puedan ser leídos si hay personas que intentan interceptarlos. Existen aplicaciones de mensajería bastante seguras, que utilizan el cifrado de extremo a extremo (o sea, de la persona que envía a la persona que recibe) para codificar las comunicaciones y garantizar su privacidad.
Este es el caso de Signal en el servicio de mensajería instantánea o el de Protonmail para correos electrónicos. En el caso del correo electrónico, el cifrado es efectivo cuando tanto la persona que lo envía como la que lo recibe lo utilizan haciendo uso del mismo servicio o programa. Por ejemplo, enviar un correo de una cuenta Protonmail a una cuenta de otro proveedor de correo electrónico no necesariamente garantiza su cifrado. La seguridad de un correo dependerá del sistema menos seguro de los usados en la comunicación.

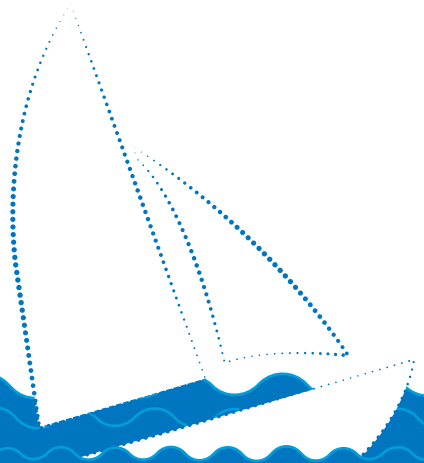
REDES PÚBLICAS:

Los **puntos de conexión públicos,** como las redes wifi que se usan en aeropuertos, hoteles, restaurantes o instituciones públicas **conllevan mayores riesgos** que la conexión a una red privada. Si usas estas redes, puedes aumentar tu seguridad implementando algunas de las medidas anteriores como el uso de VPN o el acceso sólo a páginas https. Además, evita acceder a información sensible, desactiva las funciones para compartir archivos y desactiva de la opción de “Conectar automáticamente” a las redes públicas.

4

QUÉ NO HACER en cuanto a la seguridad digital: hábitos y buenas prácticas

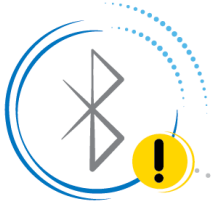
ESCANEA Y ACCEDE AL CONTENIDO ONLINE



HÁBITOS

EVITA utilizar redes de internet / wifis públicos, comunes en restaurantes, hoteles, aeropuertos o instituciones públicas, pues implican mayores riesgos que conectarse a una red privada. Cuando sea inevitable conectarse a redes públicas, **ACTIVA el VPN previamente** y NO sincronices fotos o videos ni abras aplicaciones de bancos o hagas compras en línea.

NO DEJES la conexión inalámbrica o *bluetooth* activada cuando no esté en uso. Actívala solamente cuando vayas a usarla y estés en un entorno seguro.

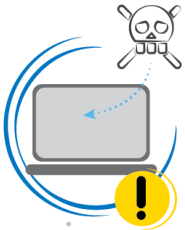


NO DEJES el dispositivo abierto o sin claves al alcance de cualquier persona.

NO PUBLIQUES información privada o confidencial, como números de tarjetas de crédito o contraseñas, en sitios públicos, incluyendo a las redes sociales. **Utiliza la configuración de privacidad en las redes sociales para restringir el acceso a tu información personal**. Puedes crear perfiles de uso público y privado para diferenciar su uso y proteger información sensible.

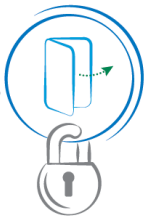
NO HAGAS CLIC en enlaces de origen desconocido o que no sean de confianza. **No respondas a correos electrónicos o mensajes de texto que soliciten datos confidenciales.** En caso de que te sea necesario atender llamadas telefónicas de números desconocidos, mantén una bitácora de llamadas y reporta los números desconocidos en tu red de seguridad.

Y BUENAS PRÁCTICAS



NO INSTALES programas no autorizados por su creador en la computadora. Las aplicaciones maliciosas a menudo se hacen pasar por software legítimos.

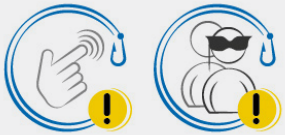
NO MARQUES las opciones “Mantenerme conectado/a” o “Recordarme” en los sitios web, especialmente en las computadoras públicas. No guardes contraseñas en los navegadores web.



SIEMPRE CIERRA la sesión de las cuentas en línea al terminar de utilizarlas. Esto es especialmente importante cuando estás utilizando una computadora pública.

NO MANTENGAS conversaciones sensibles o confidenciales por línea telefónica o por mensajes SMS. **USA siempre aplicaciones con cifrado de extremo a extremo.** Evita compartir información sensible respecto de familiares y seres queridos en redes sociales.

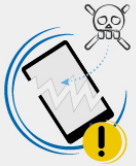
En lo posible, **NO USES** tarjetas de memoria, *pendrives* o *memory flash/sticks* para documentos importantes o en dispositivos desconocidos**. En particular, no uses estos dispositivos cuando han sido regalados y no se encuentran en su empaque de fábrica, fueron encontrados en lugares públicos o son de dudosa procedencia.**



Phishing/vishing

o suplantación de identidad

Es una de las amenazas digitales más comunes. La persona es engañada mediante solicitudes por mensaje o correo electrónico que parecen legítimas, pero no lo son; por ejemplo, un correo diciendo que tienes que actualizar información de tu cuenta bancaria, o un mensaje diciéndote que algo grave pasó y pidiendo que hagas clic en un enlace para saber más.
También pueden pedir o dar permisos en sitios webs o incluso descargar archivos o software que pueden ser maliciosos.
Los atacantes esperan que la víctima les crea y otorgue acceso voluntario a su información o dispositivos. En el vishing se realiza una llamada telefónica que simula proceder de una institución legítima para solicitar información personal, como datos bancarios.



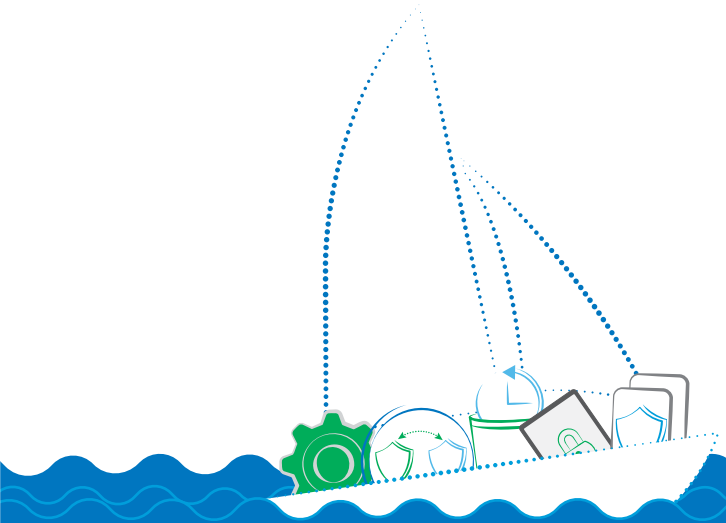
Malware

o software malicioso

Es un software que al ejecutarse realiza acciones maliciosas en el equipo sin el conocimiento ni autorización de la persona propietaria.
Entre las acciones que puede realizar se encuentran el robo de información, el daño a los equipos o archivos, o tomar el control del equipo para realizar ataques informáticos o enviar correo basura.

5 ACCIONES INMEDIATAS ante cuatro amenazas comunes

ESCANEA Y ACCEDE AL CONTENIDO ONLINE



¿QUÉ HACER
si pierdo mi información?

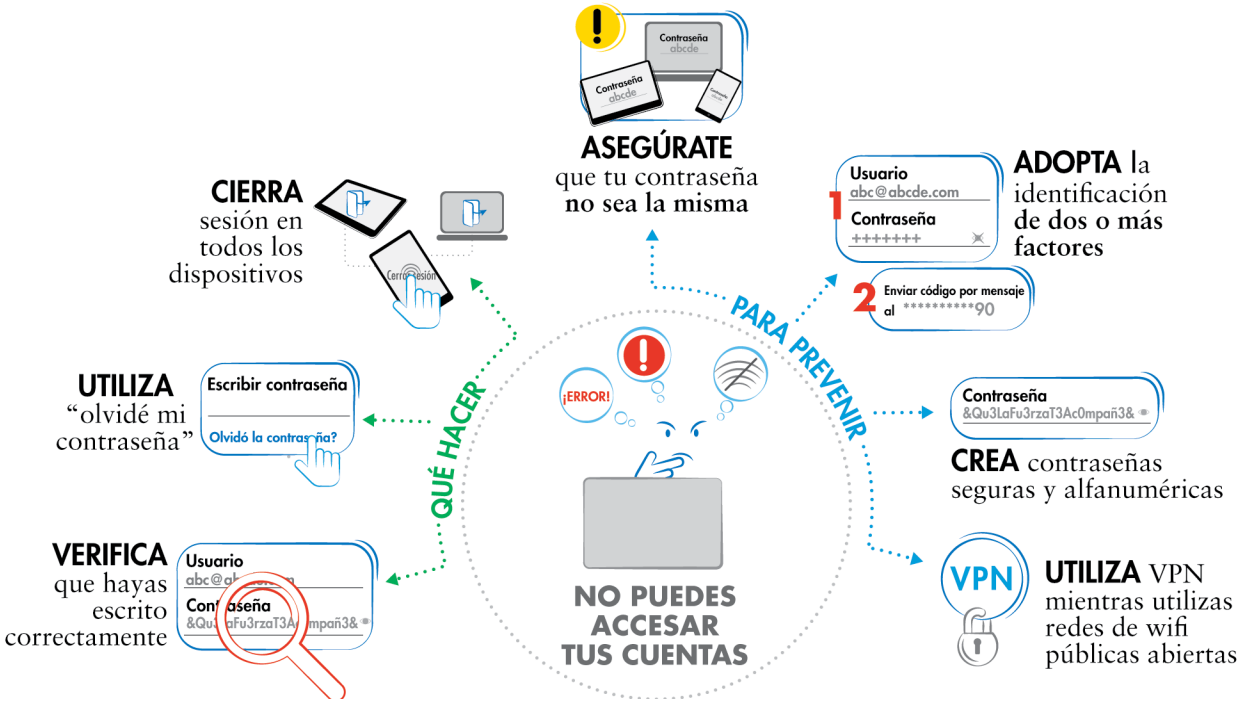
QUÉ HACER:

- **INTENTA** recuperar la información de tu papelera de reciclaje.
- Si recuerdas el nombre del archivo, **PRUEBA** la función "Búsqueda" para intentar localizarlo.
- **REVISA** si has enviado un correo electrónico con el archivo, si lo has compartido con alguien o si en algún momento lo agregaste a una nube.
- Las medidas para pérdida de información son aplicables incluso cuando alguien te obligue a borrarla.
- Puedes **USAR** programas específicos para recuperar archivos borrados en tus equipos.

PARA PREVENIR:

- **REALIZA** copias de seguridad o respaldo en nubes o dispositivos físicos de almacenamiento externo, como tarjetas de memoria, discos o pen drives.
- **PROTEGE** estas copias de seguridad con cifrado.

¿QUÉ HACER
si pierdo el acceso a mis cuentas?



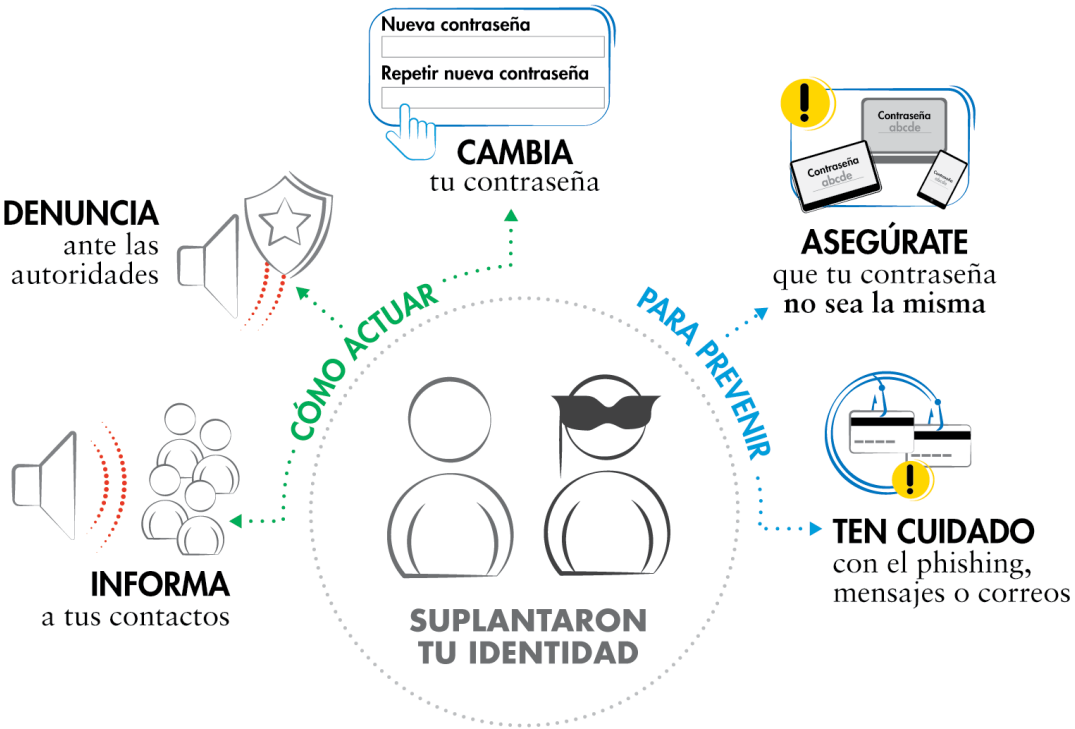
QUÉ HACER:

- **VERIFICA** que has escrito de forma correcta la información de la persona usuaria (user) y la contraseña (password).
- **UTILIZA** el recurso "Olvidé mi contraseña" si tienes acceso al correo electrónico o o número de teléfono asociado a la cuenta.
- Si no tienes acceso a la cuenta de recuperación, **UTILIZA** el recurso "Solicitar ayuda para restaurar tu cuenta". Se trata de un proceso un poco más tardado porque pasa por toda la verificación de identidad.
- Cuando recuperes el acceso, utiliza el recurso "**CERRAR SESIÓN** en todos los dispositivos" para asegurarte de que personas no autorizadas o maliciosas ya no tengan acceso a la cuenta.

PARA PREVENIR:

- **ASEGÚRATE** de que tu contraseña no sea la misma que usas en otros sitios y que no se trate de una contraseña compartida. Evita usar contraseñas que puedan ser fácilmente asociadas a ti (nombre de personas cercanas, fechas de nacimiento, etc.).
- **ADOPTA** la identificación en dos factores.
- **UTILIZA** un administrador de contraseñas para poder crear contraseñas seguras.
- **UTILIZA** VPN para proteger tu navegación, especialmente mientras utilizas redes de wifi públicas abiertas.

¿CÓMO ACTUAR FRENTE
a la suplantación de identidad?



QUÉ HACER:

- **INFORMA** de la suplantación a tus contactos, usando perfiles, correos electrónicos u otros medios.
- **DENUNCIA** la suplantación en la propia plataforma o red social para solicitar que eliminen la cuenta falsa.
- **DENUNCIA** la suplantación a las autoridades.
- Si usas la misma contraseña de la cuenta que fue suplantada en otras plataformas, **CÁMBIALA** inmediatamente.

PARA PREVENIR:

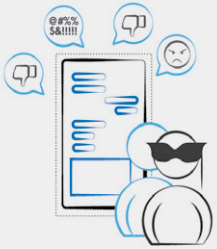
- **ASEGÚRATE** de que tu contraseña no sea la misma que usas en varias cuentas y que tampoco sea una contraseña compartida.
- **TEN CUIDADO** con el phishing, mensajes o correos que te urgen o incitan a acceder a enlaces fraudulentos dónde te piden tu información personal.

¿QUÉ HACER
si soy víctima de troles y acosadores en línea?

QUÉ HACER:

- Toma un tiempo para procesar lo ocurrido. Si posteriormente te sientes cómoda o cómodo, socializa lo que pasó. **BUSCAR APOYO** psicoemocional puede ayudarte a procesar y afrontar lo que sucedió.

  ¡No normalicemos la ciberviolencia!
- **BUSCA** tener un buen análisis de la situación e identificar quiénes podrían ser los perpetradores de los ataques o los intereses detrás de ellos y las distintas maneras en las que acosan en línea, por ejemplo, identificando a otras víctimas del mismo grupo de acosadores.
- **REGISTRA Y DOCUMENTA** los hechos (fecha, hora, tipo de acoso, forma y contenido del mensaje, autor, plataforma utilizada y captura de pantalla) o pídele a alguien de tu confianza que lo haga por ti.
- **BLOQUEA**, silencia y reporta la cuenta acosadora en la propia plataforma.
- De acuerdo con el caso, **DENUNCIA** ante las autoridades pertinentes.
- **NO INTERACTÚES** con los troles, pues actúan para provocar y desgastar.
- Si crees que esto puede ayudar, **BUSCA APOYO** de organizaciones de la sociedad civil, organizaciones profesionales, personas solidarias que puedan emitir comunicados públicos en solidaridad contigo o realizar otras acciones de respaldo.
- En el caso de campañas de desprestigio, **SIGUE** los pasos indicados en la siguiente sección.

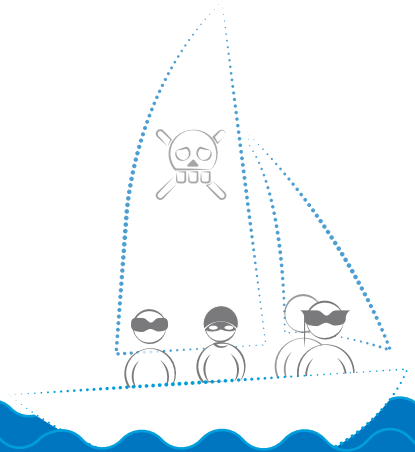


Troles

Son personas que utilizan perfiles falsos con el objetivo de acosar a alguien en una red social, mediante insultos, cuestionamientos y críticas negativas, para generar un perjuicio. Es una forma muy común de ciberviolencia de género.

6

10 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.

1 INTERRUPCIÓN DEL SERVICIO DE INTERNET

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

1) COMPRUEBA que el dispositivo, módem o *router* del servicio funcione. Reinícialo y revisa si la conexión se estabiliza.
2) BORRA la *caché*, el historial y otros datos de los navegadores para acelerar la velocidad de conexión.
3) Cuando existan cortes de energía y/o conexión inestable a Internet, ASEGURA que no se pierda información almacenándola de manera offline (sin usar internet) mediante el uso de Tella o Save hasta que se restablezca el servicio.

TELLA y SAVE son aplicaciones que permiten almacenar, compartir y cifrar de forma segura archivos (incluso audiovisuales) sin temor a la censura, la vigilancia o las represalias. Ambas funcionan en la modalidad offline y retienen la información hasta que se restablezca la conexión a la internet.

HERRAMIENTAS

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

Para comprobar la velocidad de la conexión:

» www.speedtest.net

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

2 BLOQUEO SELECTIVO DE PÁGINAS WEB

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

1) Se puede ACCEDER a una página que está bloqueada si utilizamos el servicio de VPN para que parezca que estás intentando acceder desde otro país. Esto muchas veces burla el bloqueo.
2) INTENTA acceder mediante diferentes proveedores de acceso a Internet.
3) Puedes verificar si efectivamente la página se encuentra bloqueada mediante aplicaciones como OONI Probe.
4) Si es seguro y viable, DENUNCIA el bloqueo ante las instituciones públicas pertinentes y/o reclama a los proveedores del servicio, públicos o privados.

HERRAMIENTAS

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

3 ROBO, PÉRDIDA Y CONFISCACIÓN DE EQUIPO

ANTES

PROTEGE el dispositivo con una contraseña segura

RESPALDA tu información de manera periódica

ENCRIPTA el dispositivo o la unidad

BORRA de manera permanente

PROTÉGETE ante situaciones y contextos de riesgo

DURANTE

SOLICITA al operador que bloquee el dispositivo

BUSCA el dispositivo si tienes la app "Encontrar" activada

CIERRA remotamente las sesiones

BUSCA y **BLOQUEA** remotamente del dispositivo

DESPUÉS

SOMETE a revisión técnica el equipo confiscado o robado

EVALÚA la efectividad de las medidas de prevención adoptadas

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

ANTES

1) PROTEGE el dispositivo mediante una contraseña segura, es decir, que combine letras, números y otros símbolos intercalados (como #, $, @, *, !) y sea de al menos 8 dígitos y si es posible más. Es importante que sea una contraseña que puedas recordar, pero difícil de adivinar para otras personas (por ejemplo, que no se relacione con información personal tuya o con cosas que te gustan y que todo tu entorno sabe). En el caso de los dispositivos móviles, **las contraseñas en formato de frase son más difíciles de hackear que los PIN o contraseñas numéricas y pueden ser fáciles de recordar. Por ejemplo: &Qu3LaFu3rzaT3Ac0mpañ3&.**
2) Realiza una copia de seguridad o RESPALDA tu información de manera periódica. Para eso, es posible usar los medios de almacenamiento en nube que recomendamos aquí, o bien usar de manera segura los más populares. Si su organización o medio cuenta con servicios de respaldo en la nube, úsalos.
3) ENCRIPTA el dispositivo o, al menos, la unidad que contenga los archivos principales. En computadoras Mac puedes usar FileVault, mientras que Windows cuenta con Bitlocker. Para la encriptación del disco duro o de unidades específicas se puede usar VeraCrypt.
4) Es importante mantener como hábito el BORRAR de manera regularmente la información que fue almacenada en nuestros dispositivos electrónicos y limpiarlos periódicamente, sobre todo si queremos evitar que alguien acceda a ella en caso de que se apodere del dispositivo. **Recuerda utilizar 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.
5) **PROTÉGETE ante situaciones y contextos de riesgo**, como protestas, eventos masivos, viajes, visitas a embajadas, tribunales o a organismos del Estado de seguridad elevada, prisiones, otras zonas de alto riesgo (fronteras), etcétera. En estas situaciones, los teléfonos celulares pueden ser objeto de robo o confiscación y las autoridades pueden incluso intentar presionarte para que los desbloquees. Un buen hábito de seguridad antes de acudir a estos lugares es cerrar las sesiones de cuentas abiertas en el celular, borrar el contenido de los navegadores y limpiar las conversaciones almacenadas en aplicaciones de mensajería, así cómo cualquier otro contenido que pueda ser comprometedor para ti, para tus colegas, fuentes, o víctimas con las que trabajas. Esto es particularmente efectivo ante una detención arbitraria.

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

DURANTE

6) En el caso de robo, pérdida y/o confiscación del dispositivo móvil, actúa con rapidez:
   a) CONTACTA al operador para dar de baja la tarjeta SIM y realiza verificación en dos pasos, que es una medida de seguridad adicional al uso de una contraseña.
   b) De contar con el código de identidad internacional de equipo móvil o International Mobile Equipment Identity (IMEI), SOLICITA al operador que bloquee el dispositivo para evitar totalmente su uso.
   c) El código IMEI también puede ser rastreado por algunas operadoras, dependiendo de sus capacidades.
   d) Para los dispositivos Android, ACTIVA la función integrada de Google: "Encontrar mi dispositivo". Luego borra los datos, bloquea la pantalla remotamente y cambia la contraseña.
   e) Para iPhone, puedes BUSCAR el dispositivo si tienes la app "Encontrar" activada. En la página de iCloud se puede marcar el dispositivo como perdido (modo perdido) y borrar remotamente el contenido.
   f) CIERRA remotamente las sesiones o cambia las contraseñas de los servicios que tengas instalados en el móvil.
7) En el caso de robo y/o confiscación del computador portátil, actúa con rapidez:
   a) BUSCA y bloquea remotamente el dispositivo. Tanto Windows como Mac ofrecen la opción accediendo a las cuentas de Microsoft o iCloud.
   b) CIERRA remotamente las sesiones o cambia las contraseñas de los servicios que tengas instalados en la computadora o que cuenten con la opción de rellenov automático en el navegador. La opción más segura sería cambiar todas las contraseñas, lo que automáticamente cierra todas las sesiones.

DESPUÉS

8) Ante la devolución por parte de una institución pública en la que no confiamos, de equipos que fueron confiscados o robados, **SOMÉTELO A REVISIÓN** técnica por un profesional de confianza antes de volver a utilizarlo.
9) EVALÚA la efectividad de las medidas de prevención adoptadas y piensa en cómo mejorar el plan de seguridad.

HERRAMIENTAS

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 iOS, 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)

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.

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#

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

ANTES

1) Para prevenir el robo de cuentas y accesos no autorizados:
   a) USA contraseñas seguras. b) UTILIZA un **gestor de contraseñas** (estilo Bitwarden o Keepass)
   c) ADOPTA la autenticación en dos pasos.
   d) NO GUARDES contraseñas en los navegadores web, ya que aumenta el riesgo de robo total de las contraseñas.
   e) 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.
2) Mantén el hábito de LIMPIAR los dispositivos y borrar regularmente información que no sea necesaria y que no quieras que caiga en manos ajenas.
3) Para no ser víctima de phishing es importante seguir los consejos dados en las secciones anteriores y **NO COMPARTIR información sensible; examinar atentamente los mensajes, correos y links a los que se accede;** revisar que las páginas web tengan los signos de seguridad correspondientes; activar la verificación de factor múltiple; usar software antimalware y siempre dudar de cualquier comunicación que prometa premios, saldos a favor o regalos o que nos presione para actuar urgentemente proporcionando información personal.

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

DURANTE

4) Ante la duda, deja registro a través de fotos, capturas de pantalla y almacenamiento de páginas de internet. Cuando no sea posible, toma nota de su contenido.

DESPUÉS

5) En caso de haber sido víctima de hackeo, phishing o robo de cuentas, denuncia ante los proveedores de servicios, 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.

6) Si a consecuencia de un ataque perdiste información almacenada en tus equipos, puedes usar software específico para buscar los archivos que hayan podido ser borrados.

HERRAMIENTAS

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/

Recuperación de información perdida o eliminada del dispositivo:

- Recuva: https://www.recuva.site/es/

Herramientas de borrado y limpieza:
Ver sección sobre "Robo, pérdida y confiscación de equipo".

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

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

IMPLEMENTA las medidas de robo, pérdida y confiscación de equipo

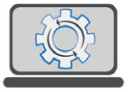
- **PROTEGE** el dispositivo con una contraseña segura
- **RESPALDA** tu información de manera periódica
- **ENCRIPTA** el dispositivo o la unidad
- **BORRA** de manera permanente
- **PROTÉGETE** ante situaciones y contextos de riesgo
- **SOLICITA** al operador que bloquee el dispositivo
- **BUSCA** el dispositivo si tienes la app "Encontrar" activada
- **CIERRA** remotamente las sesiones
- **BUSCA** y **BLOQUEA** remotamente del dispositivo
- **SOMETE A REVISIÓN** técnica el equipo confiscado o robado
- **EVALÚA** la efectividad de las medidas de prevención adoptadas

5 SOSPECHA INFECCIÓN DE TUS EQUIPOS

ANTES

UTILIZA un antivirus

NO DESCARGUES ni abras archivos de fuentes desconocidas o sospechosas.



MANTÉN ACTUALIZADO el sistema operativo

REALIZA copias de seguridad seguras

NO USES software de dudosa procedencia

DESCONFÍA si pide permisos que resultan excesivos

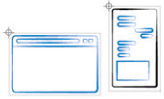
DURANTE Y DESPUÉS

DESCONECTA tu dispositivo de redes de wifi y bluetooth

INSTALA y ejecuta un antivirus

REINICIA el ordenador

BORRA los datos de navegación y archivos



REGISTRA a través de fotos, capturas de pantalla y almacenamiento

SOMETE a revisión técnica el equipos confiscado o robado

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

ANTES

1) IMPLEMENTA las medidas para protegerte ante situaciones y contextos de riesgo, como protestas, viajes, visitas a tribunales u organismos del Estado de seguridad elevada, prisiones, zonas de alto riesgo (fronteras), Etc. mencionadas en la sección de "Robo, pérdida y confiscación de equipo".
2) UTILIZA un antivirus en tus equipos y mantenlo actualizado.
3) NO DESCARGUES ni abras archivos de fuentes desconocidas o sospechosas.
4) MANTÉN actualizado el sistema operativo y el resto del software en tus equipos.
5) REALIZA copias de seguridad seguras de tu información de forma regular.
6) NO USES software de dudosa procedencia, pues puede haber sido modificado para infectar tu equipo.
7) En el caso de las aplicaciones para celular, DESCONFÍA si pide permisos que resultan excesivos para las funciones que debe realizar.

DURANTE Y DESPUÉS

8) DESCONECTA tu dispositivo de redes de wifi, bluetooth, etcétera, hasta que la situación esté resuelta.
9) EJECUTA tu antivirus. Si no tienes, instala uno.
10) REINICIA el ordenador.
11) BORRA los datos de navegación y archivos temporales y cambia todas las contraseñas.
12) REALIZA todas las actualizaciones pertinentes en el dispositivo (sistema operativo, softwares, aplicaciones).
13) Ante la duda, DEJA REGISTRO a través de fotos, capturas de pantalla y almacenamiento de páginas de internet. Cuando no sea posible, toma nota de su contenido.
14) Ante la devolución de equipos confiscados, SOMÉTELOS a revisión técnica antes de volver a usarlos.
15) CONSULTA con personas u organizaciones profesionales que puedan evaluar lo sucedido.

HERRAMIENTAS

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

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

ANTES

1) Cuando generes links para reuniones en línea, configúralos para que pidan contraseña para entrar. Comparte el enlace y la contraseña por canales seguros, como aplicaciones de mensajería o correo cifradas.
2) Siempre AVERIGUA la lista de participantes de las reuniones en línea y pide que la gente no identificada lo haga.
3) ELIGE siempre aplicaciones seguras y cifradas para tu comunicación. 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.
4) Para evitar el rastreo, UTILIZA VPN vsiempre que sea posible.

DURANTE

5) Si hay personas sospechosas presentes en una reunión en línea, DESCONÉCTALAS de la reunión. Tratar de precisar nombre, toma una imagen de la pantalla y obtén cualquier otro dato que permita su futura identificación.

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

6) 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. Es importante EVITAR descargar archivos o programas de fuentes desconocidas o sospechosas e incluso hacer clic en enlaces sospechosos. Algunos de estos programas pueden hacer que tu equipo tenga un comportamiento extraño. Si tienes dudas busca el apoyo de una persona u organización experta en seguridad que pueda revisar el equipo.

7) En caso de ser posible, DOCUMENTA pruebas o rastros de la posible intercepción de la comunicación mediante capturas de pantalla, fotos o cualquier otro medio.

8) **INCREMENTA medidas de seguridad cuando utilices redes abiertas o públicas de wifi**. Siempre comprueba la seguridad de los sitios navegados (asegurándote de 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

9) Si sospechas que tus comunicaciones han sido comprometidas, avisa a las personas que puedan verse afectadas.

10) Busca asesoría de personas y organizaciones expertas en seguridad.

HERRAMIENTAS

Mensajería telefónica cifrada:

» Signal: https://signal.org/

» Ver cómo usar WhatsApp de forma más segura. https://faq.whatsapp.com/361005896189245/?locale=es_LA

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

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

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.

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

7 SEÑALAMIENTOS ONLINE, DIFAMACIÓN, CAMPAÑA DE DESPRESTIGIO, ACOSO Y/O AMENAZA

ANTES

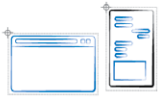
SEA CONSCIENTE
la información que compartes en redes sociales

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

REVISA
la configuración de privacidad

DURANTE

CONTRARRESTA
las acciones mediante respuestas y mensajes positivos



DOCUMENTA
los ataques a través de fotos, capturas de pantalla

DESPUÉS

DENUNCIA
en las propias plataformas

DENUNCIA
el hecho como violencia cibernética u otro tipo penal disponible

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

ANTES

1) Las campañas de acoso en línea pueden usar información o imágenes que tú u otras personas han publicado. SEA CONSCIENTE de la informacion que compartes en redes sociales, especialmente de forma pública. No publiques información de terceras personas sin su consentimiento. Por ejemplo, publicar fotos de reuniones, conferencias o asambleas puede suponer un riesgo para las personas presentes.
2) Es importante FAMILIARIZARTE con las medidas de seguridad en el uso de redes sociales.
3) Revisa la configuración de privacidad de las redes sociales y aplicaciones que utilizas.

DURANTE

5) La respuesta a este tipo de ataques dependerá del análisis de riesgo de cada persona y del contexto. Intenta responder a las acusaciones o señalamientos directamente puede ser desgastante y es parte de la estrategia de muchos atacantes; evitar implicarte en discusiones con los atacantes. En muchos casos, contrarrestar las acciones mediante respuestas y mensajes positivos puede ser un buen abordaje.
6) Documenta los ataques a través de fotos, capturas de pantalla y almacenamiento de páginas de internet.

DESPUÉS

7) Denuncia en las propias plataformas y otras instancias apropiadas.
8) En caso de que la legislación local lo permita, denuncia el hecho como violencia cibernética u otro tipo penal disponible.

HERRAMIENTAS

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

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

8 CIBERABUSO, EXTORSIÓN SEXUAL, DIFUSIÓN NO CONSENTIDA DE IMÁGENES ÍNTIMAS Y OTRAS FORMAS DE CIBERVIOLENCIA

ANTES

NO DES CLIC
en enlaces poco confiables

EVALÚA
no compartir datos

UTILIZA
autenticación de dos o más factores

FAMILIARÍZATE
con las normas comunitarias de las plataformas

DURANTE

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

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

USA
aplicaciones seguras, con cifrado

OCULTA
características

ELIGE
que sean vistas una única vez

TOMA
medidas para protegerte

No es necesario compartir contenido íntimo para ser víctima de su difusión, la manipulación de imágenes, cada día es más accesible.

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

DESPUÉS

DENUNCIA
el incumplimiento de las normas comunitarias

PIDE AYUDA
y asesórate

RECURRE
a entidades estatales especializadas de atención a la víctima

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

Es importante tener en cuenta todas las medidas preventivas y reacciones relativas a los "Señalamientos online, difamación, campaña de desprestigio, acoso y/o amenaza". Sin embargo, la particularidad de esta amenaza, su alta probabilidad de riesgo, su contenido misógino y el impacto también agravado contra personas defensoras de derechos humanos y periodistas no binarias, amerita la mención de formas adicionales de enfrentarla.

ANTES

1) NO DES CLIC en enlaces que te parezcan poco confiables y sospecha de propuestas tentadoras, dado que pueden ser un ardid para robar tus datos, imágenes y/o identidad digital.
2) Muchos perfiles falsos suelen verse vacíos, tiene poca actividad en las redes, poca historia, pocas imágenes personales y pocas amigas/seguidores. EVALÚA no compartir datos, imágenes o cualquier otro contenido con estos perfiles.
3) Siempre UTILIZA autenticación de dos o más factores en tus dispositivos o cuentas.
4) **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.

DURANTE

5) Existen múltiples actividades de intercambio virtual de información personal que pueden facilitar que la información privada sea filtrada por la persona receptora o interceptada. Esta pérdida del control de nuestra información 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. En algunos casos puede ser idóneo actuar, reaccionar y contrarrestar, mientras que otras veces es más efectivo no responder, bloquear y denunciar.
6) 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**. Sin embargo, es importante RECONOCER sus riesgos y reforzar las medidas de seguridad. Algunas medidas de seguridad pueden ser:
   a. OCULTAR características que puedan identificarte, como tu rostro, marcas o un tatuaje; o bien, puedes pixelar esa parte de la imagen.
   b. CONFIGURA tus aplicaciones de mensajería para que eliminen la imagen o video en el tiempo que determines. También puede elegir que sean vistas una única vez y se auto eliminen.

c. Prefiere aplicaciones seguras, con cifrado, eliminación automática de mensajes y que no permitan tomar capturas de pantallas.

7) No es necesario compartir contenido íntimo para ser víctima de la difusión de imágenes que nos puedan presentar en situaciones de contenido o connotación sexual. La manipulación de imágenes, cada día más accesible gracias a algunas herramientas de inteligencia artificia,l que facilita la manipulación de la información.

8) **PRESERVAR la evidencia digital en el momento de los hechos es una buena forma de mantener la posibilidad de tomar medidas ante las plataformas en las que se produce el acoso, o de carácter legal**. Sin embargo, la evidencia digital es muy volátil. Es importante no borrar ningún contenido (conversaciones, imágenes y videos) que haya sido intercambiado con el presunto victimario, al menos hasta poder guardar la información. Es importante entender que en diferentes países los requisitos para que un elemento digital pueda ser considerado evidencia válida en un proceso penal puede variar. No existe una guía general, pero algunas ideas que pueden ser útiles sobre cómo actuar para poder realizar una denuncia por la posible comisión de un delito son las siguientes:

   a. TOMA CAPTURAS de pantalla y almacénalas en otro dispositivo o medio.
   b. NO DENUNCIES EL PERFIL desde el que se realiza el acoso o amenaza hasta que hayas realizado la denuncia formal a las autoridades, ya que al bloquearla se puede perder información necesaria para una investigación.
   c. No te hagas pasar por otra persona para obtener más información.
   d. EVITA responder a las amenazas o campañas de hostigamiento. Esto puede alentar aún más a los atacantes y puede llegar a ofrecer información sobre ti.

DESPUÉS

9) Denuncia ante las aplicaciones y plataformas 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.

10) Pedir ayuda y asesorarse es siempre importante, tanto en lo legal como en lo emocional. 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.

11) Si eres víctima de violencia cibernética de género o sexual, mediante el uso de imágenes, videos, o información personal no consentida, es posible recurrir a entidades estatales especializadas de atención a la víctima, denuncia e investigación criminal. Estas entidades pueden realizar acciones para contrarrestar los efectos de la agresión.

HERRAMIENTAS

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.

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

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

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

1) Un riesgo común en los casos de allanamiento de oficinas o casas de personas defensoras de derechos humanos y periodistas es la pérdida de información. Es importante prevenir este tipo de consecuencia con aspectos como la GENERACIÓN de copias de seguridad.
2) Otro riesgo es el acceso a la información por parte de los responsables del allanamiento. Para ello, cifrar la información y contar con contraseñas robustas ayudará. También será de utilidad el borrado regular de aquella información que ya no se necesita.

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

DURANTE

3) No permitas el acceso a personas extrañas al lugar, salvo la existencia y muestra de orden judicial que justifique el procedimiento. Procura asistencia legal y comunícate con tus familiares.
4) En caso de que el ingreso sea forzado mantén la calma en todo momento y no te resistas, pregunta los motivos del allanamiento.
5) Presta atención de las personas que ingresen al lugar, incluyendo nombres, rangos, su vocabulario y vestimenta, y posibles testigos.
6) Toma nota de todo lo que las personas funcionarias hagan en el lugar y pide el acta del procedimiento para verificar que su contenido sea veraz.
7) Ten en cuenta que estos procedimientos pueden darse en cualquier momento, incluso 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

8) En un allanamiento, es posible que los dispositivos electrónicos no solamente sean confiscados, sino que sean intervenidos en el lugar sin tu conocimiento. En ese caso, es necesario implementar las medidas de prevención y mitigación correspondientes a un hackeo y robo de cuentas, e incluso sospechar la posible infección de cuentas o dispositivos mediante malware.
9) 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. Por ello, ante un allanamiento es necesario hacer uso de las copias de seguridad restaurando la información al momento anterior al allanamiento y comprobar minuciosamente la información que no cuenta con respaldo para evitar cualquier tipo de alteración.
10) Es importante someter los dispositivos a revisión técnica por parte de un profesional si sospechas de intervenciones indebidas.

HERRAMIENTAS

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".

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

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

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

1) IMPLEMENTAR las medidas de prevención ya mencionadas para los casos de confiscación, pérdida o robo, hackeo y sospecha de intercepción de comunicación.
2) Además de las medidas técnicas y las buenas prácticas en el uso de tecnologías, en contextos de riesgo debemos adoptar otro tipo de medidas preventivas. Una buena práctica es ESTABLECER un plan de comunicación con llamadas, mensajes o contactos de seguridad periódicos cuando acudas a contextos de riesgo de detención o desaparición.

CÓMO MINIMIZAR LA PROBABILIDAD Y/O EL IMPACTO DE LA SITUACIÓN

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.

3) La persona detenida o desaparecida no podrá realizar esas acciones directamente. Por ello, es importante que dentro del protocolo de seguridad DESIGNEN roles a personas que se encuentren en resguardo o libertad, otorgándoles 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

4) Algunas acciones inmediatas del protocolo de seguridad a implementar por terceros pueden ser CAMBIAR las contraseñas o bloquear el acceso a las cuentas de la persona detenida y de la organización a la que pertenece, 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.

5) Los mecanismos de GEOLOCALIZACIÓN de dispositivos que brindan los sistemas operativos o aplicaciones específicas pueden ser de ayuda para intentar determinar la ubicación de la persona desaparecida.

DESPUÉS

6) Una vez que la persona recupere la libertad, se deben tomar las medidas de seguridad digital señaladas en las secciones de confiscación, pérdida o robo, hackeo y sospecha de intercepción de comvunicación sobre todos los dispositivos y cuentas pertinentes.

HERRAMIENTAS

Mensajería cifrada, llamadas y video llamadas cifradas:

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

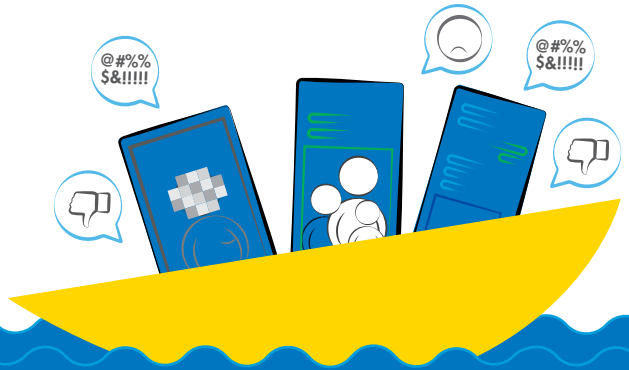
Gestores de contraseñas, autenticación de dos factores o para averiguar si tu correo o teléfono han sufrido una violación:

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

Herramientas de cifrado, geolocalización y borrado seguro de información:

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

ESCANEA Y ACCEDE AL CONTENIDO ONLINE



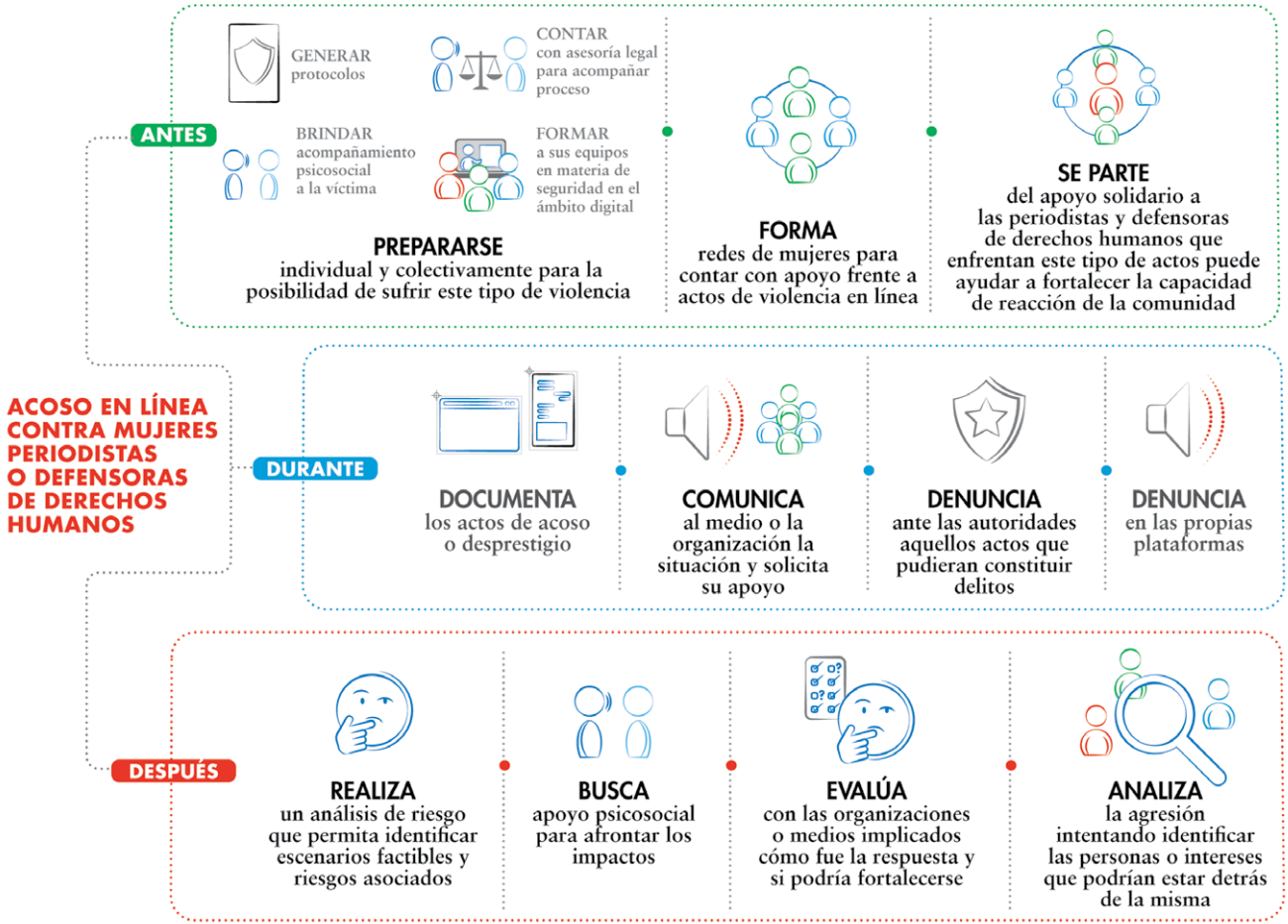
7

Acoso en línea contra mujeres defensoras de derechos humanos y periodistas

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

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.

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 PERIODISTAS O DEFENSORAS DE DERECHOS HUMANOS
ANTES
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
PREPARARSE individual y colectivamente para la posibilidad de sufrir este tipo de violencia
FORMA redes de mujeres para contar con apoyo frente a actos de violencia en línea
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
DURANTE
DOCUMENTA los actos de acoso o desprestigio
COMUNICA al medio o la organización la situación y solicita su apoyo
DENUNCIA ante las autoridades aquellos actos que pudieran constituir delitos
DENUNCIA en las propias plataformas
DESPUÉS
REALIZA un análisis de riesgo que permita identificar escenarios factibles y riesgos asociados
BUSCA apoyo psicosocial para afrontar los impactos
EVALÚA con las organizaciones o medios implicados cómo fue la respuesta y si podría fortalecerse
ANALIZA la agresión intentando identificar las personas o intereses que podrían estar detrás de la misma

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.

ANTES

1. PREPARARSE individual y colectivamente para la posibilidad de sufrir este tipo de violencia. Adoptar 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, como generar protocolos, contar con asesoría legal para acompañar proceso de denuncia, contar con capacidad para brindar acompañamiento psicosocial a la víctima, formar a sus equipos en materia de seguridad en el ámbito digital.
2. FORMAR redes de mujeres periodistas, o trabajar con organizaciones sindicales, profesionales o de libertad de expresión o de defensa de los derechos humanos para contar con redes de apoyo que puedan ayudar frente a actos de violencia en línea.
3. 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. Ser 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 frente a estas agresiones.

DURANTE

4. Documentar los actos de acoso o desprestigio, y transmitir el resultado de esa documentación a organizaciones nacionales e internacionales.
5. COMUNICAR al medio o la organización la situación y solicita su apoyo.
6. DENUNCIAR ante las autoridades aquellos actos que pudieran constituir delitos, como las amenazas. Es importante insistir que se tomen en cuenta los elementos discriminatorios por motivos de género. Solicitar que se lleven a cabo las acciones de investigación que permitan incorporar legalmente la información a los expedientes correspondientes con perspectiva de género.
7. DENUNCIAR ante las plataformas, indicando que se tratan de actos de violencia de género.

DESPUÉS

8. 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. REALIZAR un análisis de riesgo que permita identificar escenarios factibles y riesgos asociados. Valorar solicitar medidas de protección a las autoridades o adoptar estrategias de protección también en el ámbito físico
9. BUSCAR apoyo psicosocial para afrontar los impactos de este tipo de campañas.
10. EVALUAR con las organizaciones o medios implicados cómo fue la respuesta y si podría fortalecerse.
11. ANALIZAR la agresión, intentando identificar las personas o intereses que podrían estar detrás de la misma.

HERRAMIENTAS

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

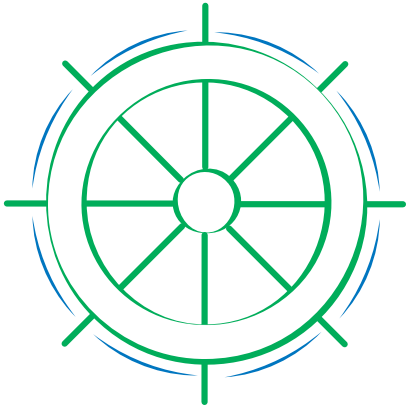
Manual para el borrado de información:
» https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual/es#Introducci.C3.B3n

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

8

Aprende a usar algunas **herramientas para aumentar tu seguridad**



ESCANEA Y ACCEDE AL CONTENIDO ONLINE

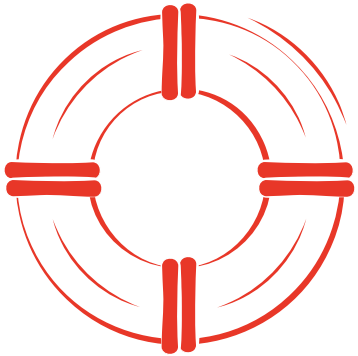
El cambio de comportamiento digital y el uso de herramientas seguras, con todo un universo de opciones, no es una tarea sencilla. Sin embargo, **recomendamos el uso de 7 herramientas** que mejoran sustancialmente la seguridad digital. Para facilitar el aprendizaje y la implementación, puede recurrir a tutoriales.

HERRAMIENTA	TUTORIALES
JITSI 	Tutorial con imágenes, disponible en español: https://www.frontlinedefenders.org/es/resource-publication/infographic-jitsi-meet Tutorial en video, disponible en inglés: https://www.youtube.com/watch?v=e-31LT0zQK4 Tutorial en video, disponible en español: https://www.youtube.com/watch?v=fRSO3_rm4-I
SIGNAL 	Tutorial escrito, disponible en español: https://support.signal.org/hc/es/categories/5592576449306-Primeros-pasos Tutorial en video, disponible en español: https://youtu.be/UtE9kWybZ_0?t=110
BITWARDEN 	Tutorial escrito, disponible en inglés: https://bitwarden.com/learning/getting-started-as-an-individual-user/ Tutorial en video, disponible en inglés: https://bitwarden.com/learning/getting-started-password-manager/

HERRAMIENTA	TUTORIALES
PCLOUD	Tutoriales y guías de uso, disponibles en inglés: https://www.youtube.com/@pCloud/videos Respuestas a preguntas frecuentes, disponibles en español: https://www.pcloud.com/es/help.html
PROTON VPN	Tutorial en video, disponible en español: https://www.youtube.com/watch?v=adDVaRFxFH8 Guía de uso y preguntas comunes, disponibles en inglés: https://protonvpn.com/support/protonvpn-setup-guide/ Tutorial escrito, disponible en inglés: https://protonvpn.com/support/protonvpn-windows-vpn-application/
PROTON MAIL	Tutorial escrito, disponible en español: https://ciberpatrulla.com/protonmail/ Tutorial en video, disponible en inglés: https://youtu.be/bO4QIXv7Ysc?t=175
TELLA	Tutorial desarrollado por organizaciones asociadas a Tella (Horizontal), disponible en inglés: https://huridocs.org/2022/07/the-new-tella-app-lets-uwazi-users-document-violations-safely-and-while-offline/

9

Recursos para la seguridad en el entorno digital



ESCANEA Y ACCEDE AL CONTENIDO ONLINE

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Security in a Box[1]	Es una herramienta básica creada por Front Line Defenders y Tactical Technology Collective que ofrece tácticas diversas para la seguridad digital. El manual está dividido en 5 secciones: 1) contraseñas; 2) comunicaciones; 3) teléfono y computadoras; 4) conexión a internet y 5) archivos. Cada una tiene 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.	Security in a Box provee información sobre cómo proteger contraseñas; cómo asegurar conexión a internet y comunicación seguras, y cómo proteger información y datos diversos, en particular en cuanto al almacenamiento, destrucción y recuperación. Presenta consejos concretos sobre cómo proteger dispositivos contra *malware* y *phishing*.
Protege.La[2]	Protege.la es un espacio abierto para compartir recursos sobre seguridad y privacidad digital de SocialTIC.org	Al ser un portal de colaboración abierta cuenta con múltiples herramientas, tutoriales y guías rápidas para abordar situaciones comunes de inseguridad digital.

[1] https://securityinabox.org/es/
[2] https://protege.la/

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Surveillance Self-Defense[3]	Es un recurso avanzado creado por Electronic Frontier Foundation para proteger la privacidad en línea y apoyar en la protección contra la vigilancia. Está compuesto de tres guías principales: una Guía Básica con conceptos clave y orientación general sobre seguridad digital; una Guía de Herramientas con explicación paso a paso de cómo instalar y usar herramientas seguras para aparatos móviles y computadoras, y una Guía de Aprendizaje Adicional sobre temas diversos. El manual utiliza recursos audiovisuales sobre varios temas y tiene una sesión específica sobre cómo llevar a cabo un modelo de amenazas digitales y análisis de riesgos.	La guía ofrece conceptos básicos para descubrir cómo funciona la vigilancia en línea y para eludir la censura de la red, además de orientación específica sobre diversos temas en materia de seguridad digital, en particular sobre el uso de VPN y de autenticación de dos factores. También brinda instrucciones para la encriptación de dispositivos, eliminación de datos de forma segura y formas de evitar ataques de *phishing* y *malware*. Ofrece consejos concretos sobre resguardo de información durante protestas. En cuanto a la instalación y el uso de herramientas, presenta instrucciones sobre una variedad de recursos, como Signal, Tor, PGP/GPG y KeePassXC.

[3] https://ssd.eff.org/es

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Committee to Protect Journalists[4]	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 no se encuentran traducidas al español y solamente están disponibles en inglés.	Algunas de las notas de seguridad más relevantes abordan 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.
Kit de Primeros Auxilios Digitales (*Digital First Aid Kit* - DFAK)[5]	Se trata de una guía publicada por varias ONG que trabajan con periodistas y medios de comunicación, incluidas Free Press Unlimited, Freedom House, Global Voices e Internews. El recurso busca apoyar de manera rápida y práctica a personas defensoras de derechos humanos, periodistas y activistas a protegerse mejor a sí mismos y a las comunidades a las que apoyan contra los tipos más comunes de emergencias digitales.	Todos los contenidos se organizan con base en el problema enfrentado: pérdida de dispositivos, datos y acceso a cuentas; dispositivos y cuentas que actúan de manera sospechosa; sitios web que no funcionan; suplantación de identidad en línea; privación de libertad y acoso digital. Para cada situación la página propone un cuestionario que ayuda a evaluar la situación enfrentada.

[4] https://cpj.org/reports/2012/04/technology-security/

[5] https://digitalfirstaid.org/es/

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Front Line Defenders – Guía sobre herramientas seguras para conferencias y chats grupales[6]	La guía surge en el contexto de la crisis sanitaria de la COVID-19, ante un incremento del trabajo remoto y de las amenazas digitales a la labor de personas defensoras de derechos humanos y periodistas. Tiene por objetivo promover comunicaciones más seguras en el entorno digital.	La guía ofrece criterios para seleccionar herramientas o plataformas más seguras, información específica relacionada con cada herramienta o servicio enumerado y recomendaciones sobre videollamadas, 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.
Derechos Digitales – Infografías[7]	La página presenta 22 infografías y boletines imprimibles sobre variados tópicos de seguridad digital que pueden ser utilizados de forma diversa – para circular información, como herramientas educativas en talleres, etcétera.	Entre los recursos más relevantes se encuentran infografías sobre softwares seguros para hacer llamadas; el uso de Tor; estrategias para asegurar el anonimato en línea y la privacidad del celular.
Proyecto Conexión Segura[8]	Conexión Segura es una iniciativa que busca promover el entendimiento y uso de prácticas y herramientas básicas de seguridad digital y evasión de censura en internet entre los ciudadanos, activistas y sociedad civil en general.	Consta de una serie de videos tutoriales cortos que utilizan un lenguaje sencillo, así como videos de preguntas y respuestas que buscan aclarar las dudas más comunes sobre seguridad digital.

[6] https://www.frontlinedefenders.org/es/resource-publication/guide-secure-group-chat-and-conferencing-tools

[7] https://www.derechosdigitales.org/tipo_publicacion/infografias/

[8] https://conexionsegura.org/about.html

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Open Global Rights: Para fortalecer la seguridad digital de los defensores de derechos humanos, el comportamiento es importante[9]	Este artículo académico destaca la importancia de mejorar el comportamiento práctico en materia de seguridad digital de personas defensoras de derechos humanos y periodistas actuando en entornos hostiles.	El recurso ofrece una reflexión crítica sobre la forma en que las herramientas técnicas pueden tener un alcance limitado cuando no son practicadas de manera consciente o frente a situaciones de real amenaza a la integridad física y a la vida de periodistas y personas defensoras de derechos humanos.
¿WiFi gratis? Tips de seguridad digital para navegar de forma segura[10]	Conectarse a redes de wifi abiertas y públicas expone a los equipos y facilita el robo de información. Este artículo académico busca presentar consejos sobre cómo acceder a conexiones de wifi públicas de manera más segura.	Presenta 5 tips concretos con enlaces para recursos adicionales.
Artículo 19[11]	Los materiales en esta página recuperan información de ARTICLE 19 Oficina para México y Centroamérica, así como de periodistas, instituciones académicas y de otras organizaciones de la sociedad civil.	Es un portal de herramientas sobre seguridad física, seguridad digital, normatividad, 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.

[9] https://www.openglobalrights.org/to-strengthen-digital-security-for-human-rights-defenders-behavior-matters/?lang=Spanish
[10] https://socialtic.org/blog/wifi-gratis-tips-de-seguridad-digital-para-navegar-de-forma-segura/
[11] https://seguridadintegral.articulo19.org/

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Manual de seguridad digital: kit de herramientas para una internet feminista[12]	"Manual de seguridad digital: kit de herramientas para una internet feminista" es una investigación de Larissa Saud [trayectos.org] realizada para ArsGames en el marco de Gamestar(t), arte, tecnología y videojuegos, programa que se desarrolló en Málaga entre 2017 y 2018.	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.
Guía práctica para mujeres periodistas sobre cómo responder al acoso en línea[13]	Publicación de UNESCO, TrustLaw, Thomson Reuters Foundation e International Women's Media Foundation con consejos de como actuar según el momento en que nos encontremos en función de la temporalidad del proceso penal.	Guía rápida que busca ofrecer recomendaciones concretas y rápidas en función del riesgo.
Red International de Periodistas – Digital Security DO's and DON'Ts for journalists[14]	Se trata de un artículo académico que presenta consejos concretos sobre qué hacer y qué no hacer en el entorno digital como periodista.	Entre los consejos concretos trata del uso de la autenticación en dos pasos, del cifrado y del VPN – para este último, el artículo incluye un video muy didáctico.

[12] https://arsgames.net/manual-de-seguridad-digital-kit-de-herramientas-para-una-internet-feminista/

[13] https://unesdoc.unesco.org/ark:/48223/pf0000379908_spa

[14] https://ijnet.org/es/node/7865

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Fondo Acción Urgente[15]	Fondo feminista regional para América Latina y el Caribe hispanohablante, que contribuye a la sostenibilidad y el fortalecimiento de las activistas y sus movimientos, con apoyos ágiles ante situaciones de riesgo y oportunidad.	En el sitio encontrarás el trabajo que realiza este fondo. Entre otras cosas, brinda Apoyos de Respuesta Rápida que constan de una financiación flexible y de corto plazo. Creados por los Fondos de Acción Urgente, buscan apoyar de manera oportuna y estratégica acciones que respondan a situaciones de riesgo que atentan contra la seguridad de las activistas y defensoras, de sus colectivos u organizaciones o bien permitan un avance en favor de los derechos de la diversidad de mujeres o eviten su retroceso.
Journalist's toolbox[16]	La caja de herramientas recopila varios recursos, en particular aquellos recomendados por Reporteros Sin Fronteras. Asimismo, ofrece miles de cursos y herramientas digitales – algunos gratuitos, otros de pago – para el ejercicio de la labor periodística. Cuenta con una sección dedicada a la privacidad y fuentes de información, con consejos sobre resguardo de la información y seguridad digital.	Los recursos contenidos en la caja de herramientas son muy diversos. Algunos traen consejos sobre formas de proteger la información digital, de compartir archivos y de trabajar en línea de forma anónima. También presenta aplicaciones seguras para remoción de metadatos de archivos, encriptación o cifrado y VPN, entre otros.

[15] https://www.fondoaccionurgente.org.co/

[16] https://www.journaliststoolbox.org/2023/05/25/security-tools/

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Watch your hack[17]	Se trata de un manual que explica cómo protegerse de los piratas informáticos o *hackers*.	El manual explica qué son los *hackers* y cómo actúan, además de dar consejos concretos para evitar hackeos a través de varias tácticas, como la navegación en sitios seguros, la realización de respaldos regulares, reconocimiento de ataques de phishing y cuidados en cuanto a archivos adjuntos a correos y el uso de wifi público. También trata sobre la utilización segura de tarjetas de memoria y otros dispositivos inteligentes.
Online Protection and Digital Security: User guide for human rights defenders[18]	Esta guía ha sido desarrollada por la Red Iraquí de Medios Sociales (INSM), con el apoyo de la Oficina de Derechos Humanos, Misión de Asistencia de las Naciones Unidas en Irak (UNAMI), para proporcionar a las personas defensoras de los derechos humanos herramientas prácticas para protegerse de los piratas informáticos y otros atacantes. Las directrices forman parte del proyecto "Derechos digitales y seguridad digital", que ha sido implementado desde 2021 por el INSM con el apoyo de la UNAMI.	Ofrece a las personas usuarias, en particular a las defensoras de los derechos humanos, información práctica para mitigar los riesgos en línea, proteger su privacidad y sus datos y preservar sus derechos y libertades en el entorno digital.

[17] https://watchyourhack.com/

[18] https://iraq.un.org/en/205333-online-protection-and-digital-security-hro-report

RECURSO	DESCRIPCIÓN	PRINCIPALES USOS
Digital security tips series for human rights defenders in South-East Asia[19]	Es una guía sobre qué hacer y qué no hacer respecto de la seguridad digital. Fue realizada por la sede Regional del Sudeste Asiático de la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos.	Si bien ha sido confeccionada para un entorno regional, contiene recomendaciones que son implementables en el contexto latinoamericano.
How to set up a secure phone: A how-to guide for whistleblowers, journalists and privacy advocates[20]	Este artículo académico contiene consejos concretos para incrementar la seguridad de teléfonos celulares. Las recomendaciones abarcan no sólo aspectos técnicos de hardware y software, sino también cambios de comportamiento necesarios para una utilización segura del dispositivo.	El artículo presenta información relevante sobre cambios de configuraciones en el iPhone que aumentan la seguridad del dispositivo. Además de ello, trae una lista de aplicaciones seguras compatibles con iOS y una explicación de cómo utilizarlas.
The Safe Sisters Guide[21]	Este folleto fue elaborado para ayudar a las mujeres, principalmente en el contexto africano, a conocer los problemas que pueden encontrar en internet (como fotos filtradas o robadas, virus y estafas) y formas de tomar decisiones informadas cada día para protegerse y hacer de internet un espacio seguro para ellas, sus familias y todas las mujeres.	Este corto recurso ilustra situaciones muy comunes de seguridad digital a las que se ven expuestas las mujeres y da consejos concretos para evitarlas y contrarrestarlas.

[19] https://bangkok.ohchr.org/civic-space/
[20] https://thetechtutor.medium.com/how-to-set-up-a-secure-phone-c8f3ad090871
[21] https://safesisters.org/resources/

10

Formaciones para entender la seguridad en el entorno digital

ESCANEA Y ACCEDE AL CONTENIDO ONLINE

FORMACIONES	DESCRIPCIÓN	PRINCIPALES USOS
Totem[22] (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.	Algunos de sus cursos destacados tratan sobre: mujeres periodistas y seguridad; cobertura segura en terreno; seguridad en las manifestaciones; navegación segura y anónima; aplicaciones de mensajería seguras; y cómo eludir la censura en internet, entre otros temas.
Google News Initiative – formaciones en seguridad digital[23] (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.	Ofrece cinco cursos, además de un cuestionario final para evaluación de aprendizaje: » Protect Shield: Defiéndete de la censura digital » Protección ante ataques DDoS » Verificación de dos pasos » Password Alert: Protégete de robos de contraseña » Protección Avanzada
IFEX-ALC Campaña: Seguridad Digital para Periodistas[24] (formaciones disponibles en español)	Esta página contiene videos para la promoción estratégica de herramientas y prácticas de seguridad digital para periodistas.	La plataforma contiene desde videos genéricos sobre cómo mejorar la seguridad en línea hasta contenidos más específicos como la protección de contraseñas, la seguridad móvil y la protección a fuentes de información.

[22] https://totem-project.org/es/

[23] https://newsinitiative.withgoogle.com/es-es/resources/trainings/safety-and-security/

[24] https://ifex.org/es/ifex-alc-digital-security-for-journalists-campaign/

FORMACIONES	DESCRIPCIÓN	PRINCIPALES USOS
Cyberwar, Surveillance and Security[25] (formación disponible en inglés)	Se trata de un curso ofrecido en la modalidad MOOC (Curso en línea abierto y masivo). Se puede tomar en modalidad verificada con certificado, de manera pagada, o de manera completamente gratuita en modalidad de auditoría.	El curso trata sobre los propósitos y el impacto de las tecnologías de vigilancia en red global y sobre la naturaleza y consecuencias del ciberactivismo y la ciberguerra. También analiza las respuestas a la complejidad de los problemas relacionados con la vigilancia y la seguridad en línea.
Cybersecurity Basics[26] (formación disponible en inglés)	Este curso brinda información básica sobre los conceptos esenciales de la ciberseguridad. Explora la seguridad de la información desde su historia hasta una descripción de las varias amenazas. Presenta también recomendaciones de herramientas concretas para prevenir ataques digitales. Se puede tomar el curso en modalidad verificada con certificado, de manera pagada, o de manera completamente gratuita en modalidad de auditoría.	El curso está dividido en 4 módulos: 1) Historia de la Ciberseguridad; 2) una breve descripción de los tipos de actores y sus motivos; 3) una descripción general de los conceptos clave de seguridad y 4) una descripción general de las herramientas de seguridad clave.

[25] https://www.edx.org/es/course/cyberwar-surveillance-and-security

[26] https://www.edx.org/es/course/cybersecurity-basics?index=spanish_product&queryID=a42b60f38f41e3a0c6ceb3e31d6a29e1&position=15&device=app

FORMACIONES	DESCRIPCIÓN	PRINCIPALES USOS
Freedom of the Press Foundation[27] (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.	En la sección sobre comunicación segura hay recursos escritos y audio-visuales sobre el uso de herramientas como ProtonMail, el cifrado de correos y Signal.
The Chilling: A global study of online violence against women journalists[28] (disponible en inglés)	Estudio mundial realizado en colaboración entre el International Center for Journalists (ICFJ) y la UNESCO. Recopila el resultado de tres años de investigación sobre la violencia de género en línea contra mujeres periodistas en 15 países.	El informe contiene casos de estudio a nivel mundial y elabora 35 descubrimientos claves para entender la violencia de género en el entorno digital.
Security Education Companion[29] (disponible en inglés)	SEC es un recurso para las personas que enseñan seguridad digital a sus amigos y vecinos. Si deseas ayudar a tu comunidad pero no sabes por dónde empezar, estos artículos, planes de lecciones y materiales didácticos son para ti.	Contiene secciones didácticas sobre muchas de las herramientas que ya hemos abordado.

[27] https://freedom.press/training/
[28] https://www.icfj.org/sites/default/files/2022-11/ICFJ_UNESCO_The%20Chilling_2022_1.pdf
[29] https://www.securityeducationcompanion.org/

ESCANEA Y
ACCEDE AL
CONTENIDO
ONLINE

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

CAJA DE HERRAMIENTAS TOOLBOX
para una actuación más segura en el entorno digital en América Latina:
Herramientas y recursos de seguridad digital para personas defensoras de derechos humanos y periodistas

Esta edición se terminó de imprimir
en abril de 2024 en Panamá.
Tiraje de 100 ejemplares.

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

NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO