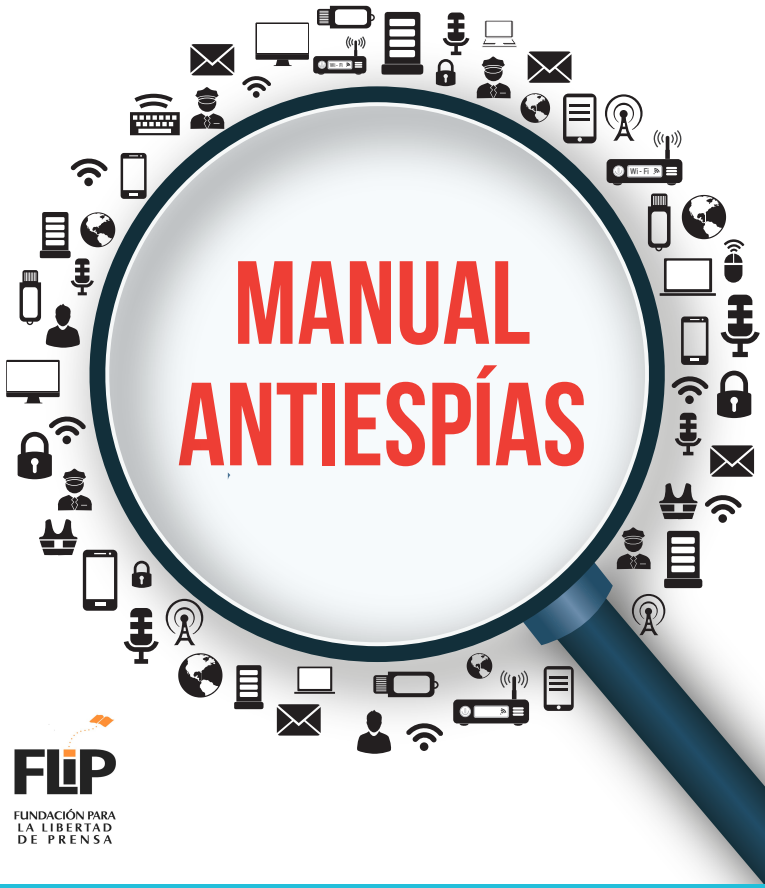



FLIP
FUNDACIÓN PARA LA LIBERTAD DE PRENSA

# HERRAMIENTAS PARA LA PROTECCIÓN DIGITAL DE PERIODISTAS


MANUAL ANTIESPÍAS
HERRAMIENTAS PARA LA PROTECCIÓN
DIGITAL DE PERIODISTAS

**MANUAL ANTIESPÍAS**
Herramientas para la protección digital de periodistas

**Investigación:** Amalia M. Toledo y Pilar Sáenz, con la colaboración de Fernando Castro. Fundación Karisma

**Redacción:** Amalia M. Toledo

**Asistente de redacción:** Daniel Suárez Pérez

**Coordinación y edición:** Jonathan Bock Ruiz
Emmanuel Vargas Penagos

**Diseño y diagramación:** Maranta producción y diseño

"Este material ha sido financiado parcial o íntegramente por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura **(UNESCO)**; la Agencia Sueca de Cooperación Internacional para el Desarrollo **(Asdi)**, **Forum Syd** y **Reporteros sin Fronteras Suecia**. Las opiniones en él vertidas no son compartidas necesariamente por las anteriores organizaciones. La responsabilidad sobre el contenido recae exclusivamente en el autor del material".

UNESCO
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
Oficina en Quito
Representación para Bolivia, Colombia, Ecuador y Venezuela

UNESCO
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
PIDC Programa Internacional para el Desarrollo de la Comunicación

FORUMSYD

REPORTEROS SIN FRONTERAS
POR LA LIBERTAD DE PRENSA

FLIP
FUNDACIÓN PARA LA LIBERTAD DE PRENSA

Con la colaboración de:
Fundación Karisma
www.karisma.org.co

# INTRODUCCIÓN

La seguridad digital de la información no es otra que la defensa de los datos, aquellos que se han obtenido a través de notas periodísticas, de información confidencial que aportan los contactos, de los archivos audiovisuales e incluso de la agenda de trabajo, y que se encuentran almacenados en dispositivos digitales. Significa proteger la información que es valiosa y que, de perderla, podría significar la pérdida de una oportunidad de contar una historia o el peligro de poner en riesgo la vida de un contacto y de los periodistas.

A nivel global, el volumen y sofisticación de los ataques digitales contra los periodistas muestra alarmantes patrones de crecimiento. En Colombia, la tendencia también es visible. Entre 2013 y 2014 se identificó un importante y acelerado aumento de ataques en espacios digitales o generados desde ellos.

Durante el 2014, operativos realizados por la Fiscalía General de la Nación revelaron que los comunicadores han sido vigilados en virtud de su actividad. Estas acciones han sido reiteradas e incluyen interceptaciones ilegales, así como la elaboración y distribución de bases de datos con información sobre ellos.

Se calcula que más de un centenar de periodistas fueron vulnerados, la mayoría cubrían el proceso de paz entre el Gobierno colombiano y la guerrilla de las FARC.

Algunos de los casos registrados son altamente preocupantes. La evaluación sobre estos ataques ha dejado al descubierto el escaso conocimiento que tienen los periodistas sobre la seguridad digital. En una era donde el trabajo periodístico está estrechamente vinculado al uso y acceso de tecnologías digitales, incluida Internet, no se puede ignorar la urgente necesidad de entender cuáles son las amenazas digitales y de aprender a proteger la información.

Al identificar esta necesidad y siguiendo las recomendaciones del Plan de Acción para la seguridad de los perio



distas de las Naciones Unidas (ONU), la Fundación para la Libertad de Prensa (FLIP), con la colaboración de la Fundación Karisma, publica este manual que tiene como objetivo mejorar el conocimiento y conciencia sobre la seguridad digital de la información y las comunicaciones.

Además, este documento es un insumo para despertar el interés suficiente para tomar acciones y aprender más sobre seguridad digital. Sin embargo, dado al carácter evolutivo de las tecnologías y los ataques, no se encontrarán soluciones absolutas y únicas; las recomendaciones y herramientas tecnológicas tienen un tiempo esperado de caducidad relativamente corto, por lo que se aconseja su continua revisión. Existen organizaciones internacionales, como Electronic Frontier Foundation (EFF) **(https://www.eff.org/)**, Tactical Tech **(https://www.tacticaltech.org/)** o Privacy International **(https://privacyinternational.org),** dedicadas a monitorear los desarrollos tecnológicos y riesgos digitales para ofrecer defensas o soluciones adecuadas.

El manual contiene recuadros, con seis recomendaciones, que son los principios básicos para protegerse en el mundo digital. Estos puntos tienen como objetivo motivar la reflexión sobre la seguridad digital y la implementación de estrategias de protección, que en espacios digitales requieren de la modificación de hábitos de uso. Sólo los periodistas pueden establecer dónde están sus vulnerabilidades, qué amenazas pueden enfrentar y las probabilidades de que ocurran. Así llegarán a un punto

de equilibro que les permitirá realizar su trabajo de manera eficiente y segura de ataques digitales. Al considerar las soluciones, deben actuar con honestidad acerca de sus capacidades y no imponerse estrategias o medidas de seguridad imposibles para ellos mismos. Los principios, que están marcados con el ícono de una memoria USB, son para guardarlos y llevarlos siempre consigo.

Cada periodista sabe qué es más importante para su seguridad digital y decide tomar medidas para protegerse. Este manual puede servir de inspiración para mejorar la seguridad y privacidad de la información que poseen y las comunicaciones que realizan a diario.

Para la elaboración de este manual se realizaron dos grupos focales con comunicadores de distintas regiones del país, donde se discutió con ellos sobre las amenazas o ataques digitales que afronta el periodismo. En estas dos actividades participaron 12 periodistas, 4 mujeres y 8 hombres. Además, se contó con el acompañamiento de expertos de EFF y Privacy International.

# DE QUÉ Y QUIÉN PROTEGERSE

No hay una solución única para estar seguro en línea. La seguridad digital se trata de la comprensión de las amenazas a las que se enfrentan y de cómo contrarrestarlas. Por ello, lo primero que se determina es qué información y de quién se quiere proteger. Las amenazas pueden cambiar dependiendo del lugar, lo que se está haciendo y con quién se trabaja. Por lo tanto, para hallar las mejores soluciones primero hay que realizar una evaluación del tipo riesgo.

**Violaciones a periodistas en entornos digitales:**

**1. Intrusión a domicilios/oficinas o robo a personas**

- Entrar por la fuerza al domicilio o al lugar de trabajo con la intención de robar o acceder a dispositivos digitales y/o información sensible en soportes digitales.
- Estas acciones pueden ser parte de un plan dirigido o una situación de crimen común.

Este tipo de agresiones puede constituir los delitos de violación de habitación ajena, violación de habitación ajena por servidor público, violación en lugar de trabajo, acceso abusivo a un sistema informático, hurto, hurto agravado y hurto calificado de los artículos 189, 190, 191, 269A, 239, 240 y 241 del Código Penal, respectivamente.

**2. Incautación ilegal de equipos**

- Confiscar ilícitamente dispositivos con la intención de obtener información sensible guardada en los mismos.



-Si existe una orden judicial para incautar equipos, esta debe autorizar la recuperación de información, de lo contrario, se está ante una confiscación ilícita.

Este tipo de agresiones puede constituir los delitos de interceptación de datos informáticos y abuso de autoridad por acto arbitrario e injusto de los artículos 269C y 416 del Código Penal, respectivamente.

**3. Destrucción de dispositivos y/o información (fotos, datos de entrevista, etc.)**

- Destruir el hardware de un dispositivo con la intención de deshacerse de información incómoda para uno o varios agresores.
- Que un tercero borre fotografías, videos u otra información.

Este tipo de agresiones puede constituir los delitos de sabotaje y daño en bien ajeno de los artículos 199 y 265 del Código Penal, respectivamente.

**4. Interceptación y vigilancia ilegal a las comunicaciones**

- Intervenir y monitorear comunicaciones telefónicas o en línea sin orden judicial y con la intención de conocer la información, movimientos, fuentes, etc.
- Una práctica actual es analizar los ***metadatos*** o los datos que describen otros datos. Por ejemplo, las fichas

bibliográficas de las bibliotecas contienen metadatos y en las redes sociales pueden ser los campos que se diligencian para crear perfiles.

Este tipo de agresiones puede constituir los delitos de violación ilícita de comunicaciones, interceptación de datos informáticos y uso de software malicioso, de los artículos 192, 269C y 269E del Código Penal, respectivamente.

**5. Intimidación o ciberacoso**

• Usar medios digitales para acechar a los periodistas por información incómoda de un agresor potencial.

• Puede ocurrir de diversas formas:
**a)** vigilancia de las comunicaciones con el objetivo de ocasionar temor en las comunicaciones entre colegas, fuentes principales para una investigación, etc;
**b)** uso de información electrónica y de medios digitales (ej. redes sociales, correo electrónico, sección de comentarios en páginas web, etc.) para asediar a periodistas y causar temor, ya sea por su vida, su integridad física o la de otros;
**c)** mecanismos de extorsión utilizando información o medios digitales para coaccionar a periodistas y evitar que publiquen determinada información, entre otros.

Este tipo de agresiones puede constituir los delitos de violación ilícita de comunicaciones, interceptación de datos



informáticos, extorsión, extorsión agravada y amenazas, de los artículos 192, 269C, 244, 245 y 347 del Código Penal, respectivamente.

**6. Robo de credenciales**

• Sustraer información confidencial o de credenciales, como nombre de usuario o contraseñas, y usarla para hacerse pasar por la persona dueña de la información, ya sea para intimidar o para obtener información sensible de esa persona.

Este tipo de agresiones puede constituir los delitos de falsedad personal y violación de datos personales de los artículos 269F y 296 del Código Penal, respectivamente.

**PARA NO OLVIDAR**

**Reconocer el entorno digital**

• No se trata de convertirse en expertos de la seguridad digital, sino de reconocer los riesgos digitales y enfocar esfuerzos en prevenir y mitigar la ocurrencia de estos.

**Paso a paso**

• Es mejor establecer prioridades y metas. Convertir en una rutina la estrategia de seguridad digital.
• Empezar el plan con la creación de contraseñas seguras y distintas para todas las cuentas online.

**7. Falsificación de cuentas (redes sociales, cuentas de correo)**

• Falsear cuentas digitales de, por ejemplo, redes sociales o correo electrónico con la intención de atacar la reputación de los periodistas u ocasionar un daño en su nombre.

Este tipo de agresiones puede constituir el delito de falsedad personal del artículo 296 del Código Penal.

**8. Ciberataque de páginas webs/correos**

• Atacar una página web o correo electrónico y comprometer la seguridad del sitio para obtener información de datos de acceso o información sensible (ej. nombres de usuario, contraseñas) o para dejar fuera de servicio servidores a los que va dirigido el ataque. Esto último también es conocido como *ataque DDoS* o *ataque distribuido de denegación de servicio*.

Este tipo de agresiones puede constituir los delitos de sabotaje, obstaculización ilegítima de sistema informático o red de telecomunicación por acto arbitrario e injusto, interceptación de datos informáticos y violación de datos personales de los artículos 199, 269B, 269C y 269F del Código Penal, respectivamente.



**9. Invasión de la vida privada**

• Usar la información personal (ej. ubicación, fotos, contactos, etc.) disponible en los perfiles de redes sociales para coaccionar a una persona o sus contactos.

Además de los delitos mencionados antes en casos en los que se obtiene la información de forma fraudulenta, este tipo de agresiones puede constituir los delitos de constreñimiento ilegal, constreñimiento ilegal agravado, constreñimiento para delinquir, constreñimiento para delinquir agravado y amenazas de los artículos 182, 183, 184, 185 y 347 del Código Penal, respectivamente.

**10. Espionaje industrial**

• Obtener ilícitamente datos o información confidencial que está trabajando un medio por parte de un tercero, con la intención de adelantarse a su competidor.

Este tipo de agresiones puede constituir los delitos de violación ilícita de comunicaciones, interceptación de datos informáticos y uso de software malicioso, de los artículos 192, 269C y 269E del Código Penal, respectivamente.

**11. Instalación de programas maliciosos**

• Enviar virus o programas maliciosos que infectan un dispositivo permitiendo el robo de información sensible, la transmisión de datos a distancia, la captura de la

información de los usuarios en sus dispositivos, la activación del micrófono y/o cámara web de un dispositivo, etc.

Este tipo de agresiones puede constituir el delito de uso de software malicioso del artículo 269E del Código Penal.

**12. Ataque enmascarado (phishing emails)**

- Usar correos electrónicos que aparentan ser auténticos y provenir de fuentes confiables, para enviar un software malicioso disfrazado como archivo adjunto o enlace a sitio web.
- Al abrir el archivo o el enlace se instala el software malicioso con capacidad para copiar en secreto contraseñas y otra información sensible, acceder a credenciales de entrada, etc.

Este tipo de agresiones puede constituir el delito de suplantación de sitios web para capturar datos personales del artículo 269G del Código Penal, respectivamente.

**¿En qué casos se pueden interceptar las comunicaciones de una persona?**

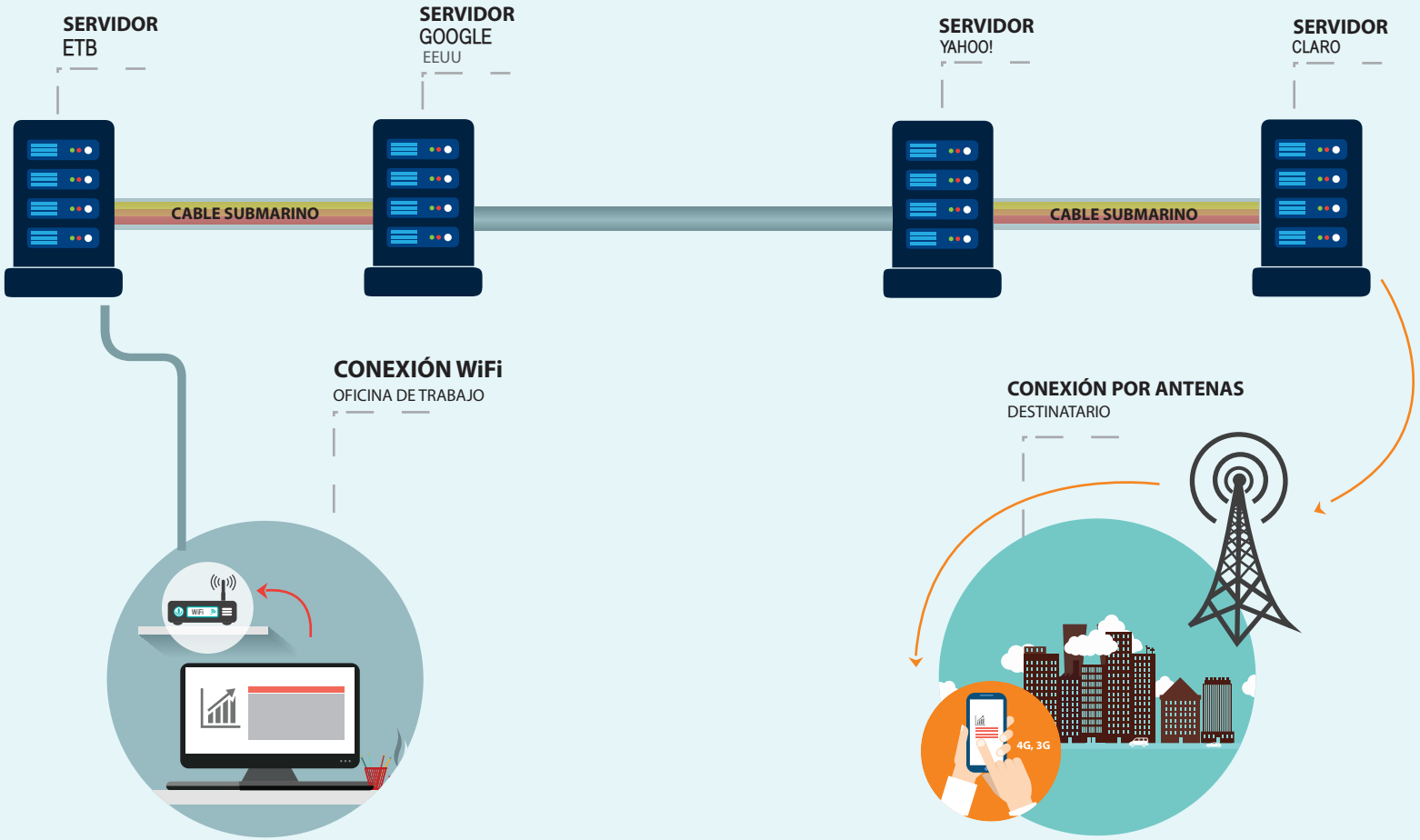
Según el artículo 235 del Código de Procedimiento Penal o ley 906 de 2006, cuando se trate de una investigación penal, el Fiscal puede ordenar la interceptación de comunicaciones telefónicas y similares "con el único objeto de buscar elementos materiales probatorios y evidencia física" y, según el artículo 236 de la misma ley, la aprehensión de computadores, servidores, equipos o medios de almacenamiento cuando haya motivos para considerar que la persona ha estado "transmitiendo información útil para la investigación". Posteriormente, 24 horas después de la orden, el Fiscal deberá acudir ante un juez de control de garantías para que revise la legalidad de las actuaciones.



**Según la Ley de Inteligencia y Contrainteligencia o 1621 de 2013,** el monitoreo del espectro electromagnético, espacio donde circulan diferentes tipos de mensajes como, las llamadas de celular, puede realizarse por parte de autoridades de inteligencia sin necesidad de orden judicial.

# ASÍ VIAJAN LOS DATOS POR LA RED

Este gráfico muestra cómo el computador y el teléfono inteligente se conectan a Internet



**¿Por qué es importante conocer el recorrido de los datos por la red?**

Conocer el recorrido que hacen los datos ayuda a entender mejor cómo se hacen los ataques digitalmente y, al mismo tiempo, cómo actúan las herramientas que hacen frente a las amenazas.

Desde un computador conectado a Internet a través de una conexión inalámbrica en la oficina se envía un correo a una persona que recibe el mensaje en su celular con plan de datos mientras está en la calle.

El computador tiene un programa instalado que permite escribir el mensaje (ej. aplicación de Gmail). Cuando se le dice enviar realmente no llega de inmediato al destinatario, sino que pasa a través de múltiples equipos que hacen parte de la infraestructura de Internet. Es similar al funcionamiento del correo análogo que cuenta con oficinas de correo, centros de distribución, el cartero y, finalmente, el buzón del destinatario. Entonces, al enviar el mensaje, este sale de su equipo y llega al router, que se encarga de definir la ruta que va a seguir. De ahí, el mensaje pasa por una serie de cables hasta que llega al servidor del **ISP**, como ETB. Esta empresa, a su vez, mira cuál servicio utiliza el remitente y envía el mensaje al servidor de esa empresa. En este caso, si la cuenta es de Gmail, significa que el mensaje deberá viajar por cables submarinos hasta un servidor de Google que se encuentra en Estados Unidos. Cuando Google recibe el mensaje



mira a quién va dirigido y lo envía al servidor correspondiente, por ejemplo, a Yahoo!. Ellos también miran para quién va dirigido el mensaje. Para entregarlo, este deberá viajar de vuelta desde Estados Unidos hasta el país usando otro cable submarino que conecta al ISP del destinatario, por ejemplo, Claro. De ahí, esta empresa envía el mensaje por su red de antenas de telefonía celular hasta que, finalmente, llega al teléfono celular del destinatario. Es sorprendente que un proceso tan complejo, que involucra a tantos intermediarios, suceda en cuestión de segundos.

Una vez que se tiene la idea del proceso y los múltiples pasos, es más sencillo analizar cuáles son los posibles riesgos para que el mensaje no llegue o sea interceptado.


Cualquier equipo es susceptible de recibir ataques. Primero, es importante recordar que ningún programa es perfecto. Siempre existen errores, se llaman bugs, que pueden ser aprovechados por terceros para ingresar a los dispositivos y acceder a la información guardada en ellos. Además, existen programas maliciosos como virus, malware o spyware que pueden estar instalados tanto en los teléfonos celulares, como en los computadores e incluso en los servidores. Estos programas pueden dañar o borrar la información que está almacenada en ellos. También pueden enviar archivos, datos del usuario y contraseñas a terceros que buscan aprovechar esta información.


También existen dispositivos especializados que son capaces de guardar todo lo que es escrito en el teclado. Estos dispositivos son conocidos como keyloggers. Algunos parecen pequeñas memorias USB que pueden estar conectadas al puerto USB del dispositivo comprometido de forma casi imperceptible para los usuarios. Otros son programas que corren sin que exista evidencia de que están almacenando la información. En algún momento el atacante recoge la memoria USB o descarga el archivo donde está la información. De esta forma, nombres de usuario, contraseñas y otra información sensible puede llegar a manos desconocidas.


Los *routers*, que conectan los equipos a Internet, también pueden sufrir ataques. En casi todos los casos estos equipos tienen puertas traseras, entradas remotas que facilitan la administración y actualización de estos equipos por parte de los proveedores. Sin embargo, estas puertas traseras también pueden ser aprovechadas por terceros para monitorear el tráfico que pasa por el *router*. Esta información permite conocer qué páginas se visitan, con quiénes nos comunicamos y con qué frecuencia.




Los servidores de los ISP, como todos los demás equipos, son vulnerables. Quizás es más problemático el hecho de que estos proveedores almacenan durante años la información de conexiones de sus usuarios. El análisis de datos permite crear perfiles muy precisos de sus usuarios sobre hábitos, gustos e intereses. Bien utilizados sirven para recibir publicidad específica, pero mal utilizados facilitan la identificación de conductas y también ponen en riesgo la privacidad y seguridad de los usuarios.


Los cables que transportan toda la información entre los grandes servidores y los dispositivos pueden ser atacados. Existen sondas, dispositivos que permiten clonar todo el tráfico que pasa por estos cables sin que nadie se dé cuenta. Como sucede con la información almacenada en los ISP, esta gran cantidad de datos puede ser utilizada para crear perfiles y/o hacer seguimientos de las comunicaciones entre varias personas, vulnerando la privacidad y seguridad de las mismas. Cualquiera con los recursos técnicos puede instalar una sonda, aunque para esto se requiere de una infraestructura importante para hacerlo. Sin embargo, este método es utilizado, principalmente, por gobiernos para hacer vigilancia masiva de sus ciudadanos con o sin la participación de los ISP.

## DEFINICIONES:

**ISP:** *Internet Service Provider* o Proveedor de servicios de Internet es la empresa que brinda servicios relacionados con Internet, como la conexión a la red, el servicio de correo, etc.

**Bugs:** Es un error en el software que desencadena un resultado indeseado en el funcionamiento de los programas. Estos permiten la fácil entrada de terceros a la información.

**Virus:** Es un malware que afecta el funcionamiento del dispositivo, sin el permiso o el conocimiento del usuario.

**Malware:** Software malicioso, en español, trabaja de muchas maneras pero su carácter es siempre criminal, pues buscan hacer daños, obtener información de manera ilícita, espiar comunicaciones, acceder a credenciales de entrada, etc.

**Spyware:** Software espía, en español, es una clase de software malicioso, como los virus, que puede rastrear todo lo que se hace desde un dispositivo o en Internet, y enviar esa información a alguien que no debe tener acceso a ella.

**Keylogger:** Programa que captura todo lo que se teclea, como usuarios y contraseñas. Los datos son enviados remotamente o se almacenan en el mismo dispositivo afectado, hasta que un tercero acceda a él.

**Puertas "traseras":** Dispositivos físicos que permiten un acceso remoto y que quedan abiertos para su administración y acceso. Pueden ser utilizados de manera ilegal.

**Análisis de datos:** Realizaciones de perfiles de usuarios basados en la información recopilada de sus actividades en Internet.

**Sonda:** Dispositivo que interfiere en las conexiones y clona el tráfico o la información bit a bit, o pedazo a pedazo.


# LA SEGURIDAD DIGITAL EN PRÁCTICA:
# HERRAMIENTAS ÚTILES

**Las necesidades de cada periodista dependen de su nivel de uso de la tecnología en el trabajo, de los temas que trate y de los factores de riesgo en los que esté inmerso. Las siguientes son algunas recomendaciones que pueden servir para la protección digital dependiendo de cada caso:**

**1. Contraseñas seguras**

**a. Frase de acceso**

- Las contraseñas seguras también son llamadas **frases de acceso** (passphrase): una frase solo conocida por quien la crea, con muchos caracteres, difícil de adivinar, pero fácil de recordar y escribir correctamente.

- Para crear esta contraseña se puede utilizar la cita de una canción, un verso de un poema favorito o cualquier frase fácil de recordar y que no sea muy evidente.

- Añadir letras mayúsculas y minúsculas, números y símbolos para hacerla aún más segura.

- Crear contraseñas seguras para cada cuenta.

- Cambiar las contraseñas con bastante regularidad. Lo recomendable es cada 3 meses.

**b. Administrador de contraseñas**

- Ayuda a gestionar una multitud de contraseñas, una para cada cuenta.

- Este tipo de software permite generar contraseñas únicas y almacenarlas de forma segura con una sola frase de acceso, que servirá como clave maestra para acceder a todas las demás contraseñas.

- Estar seguro de recordar siempre la clave maestra, de lo contrario, se pierde el acceso a las otras contraseñas. Ante un ataque digital, todas las contraseñas también quedarían comprometidas.

- La ventaja es que solo se debe crear y recordar una única contraseña segura. El resto de las contraseñas pueden ser automáticamente generadas por el software y almacenadas de forma segura en un archivo cifrado.

- Las contraseñas que genera el administrador suelen ser altamente seguras por lo intrincadas y largas que son (ej. kU%>Dl1#'v6X&wBXG;).

- Otra ventaja de un administrador de contraseñas es que permite sincronizar el archivo de contraseñas en todos los dispositivos digitales que se utilicen. Algunos administradores incluso ofrecen almacenar las contraseñas en 'la nube', permitiendo acceder a ellas desde cualquier dispositivo.

- Tener siempre una copia de respaldo del archivo donde se almacenan las contraseñas. Así, en caso de pérdida del dispositivo, se puede recuperar la información contenida en el administrador.

- Esta copia de respaldo se debe guardar en una memoria USB, disco duro, portátil o en cualquier dispositivo externo. Se debe mantener en un lugar seguro.



Algunos administradores de contraseñas son:

**KeePass (http://keepass.info/):** Es seguro y de uso fácil, disponible para Windows, Linux, Mac OS, iPhone, BlackBerry, Android, PocketPC, etc. Para instalar este software, puede consultar en este enlace la guía de instalación de KeePass en español (https://securityinabox.org/es/keepass_principal).

**1Password (https://agilebits.com/onepassword):** Es compatible con plataformas Mac OS, Android, Windows, iPhone y iPad.

**LastPass (https://lastpass.com/es/):** Es compatible con plataformas Mac OS, Android y Windows.

**c. Preguntas de seguridad**

- Existen sitios web que usan las preguntas de seguridad para recuperar una contraseña que se haya olvidado (ej. ¿Dónde estudiaste? ¿Cuál es el nombre de tu primera mascota?).

- Responder de manera honesta puede que no sea la mejor idea, pues muchas de las respuestas a estas preguntas son hechos públicos que otros pueden encontrar haciendo una búsqueda en Internet. Se recomienda usar una respuesta ficticia.

- Las respuestas también se pueden guardar en el administrador de contraseñas.

- No usar las mismas respuestas a las preguntas de seguridad en distintos sitios web.

**d. Autenticación de cuentas**

- Los operadores de servicio de cuentas de correo, como Gmail de Google, ofrecen una identificación de dos pasos.

- Esta autenticación está conectada a un dispositivo físico como un celular o un token de seguridad en el que se recibe un código especial que permite acceder al servicio.

- Si alguien tiene acceso a la contraseña no podrá entrar a la cuenta a menos que también tenga acceso físico al segundo dispositivo (celular o token).

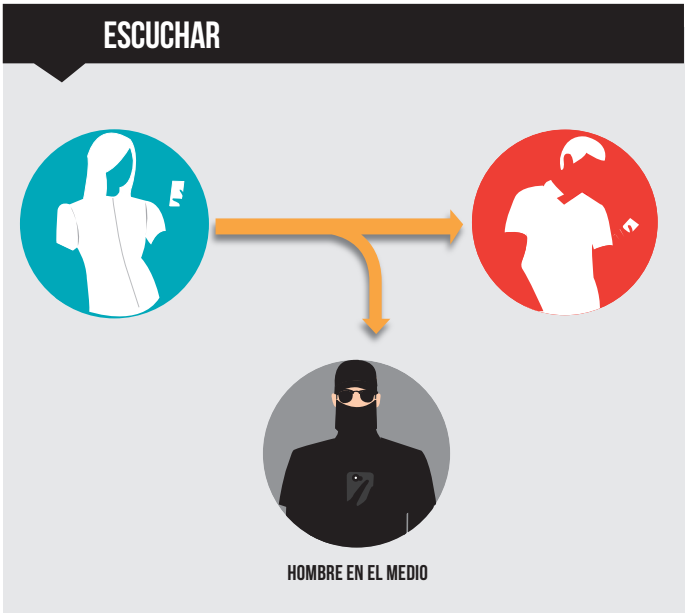
**Intervención de comunicaciones**

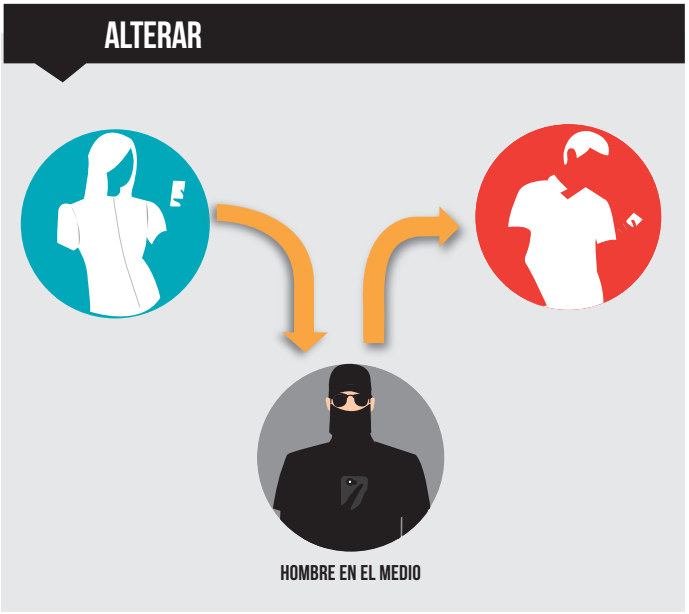
Aunque cualquier comunicación puede ser intervenida, particularmente, con el uso de dispositivos digitales, la posibilidad de que terceros comprometan la comunicación de los usuarios se ha incrementado. La amenaza más común es la conocida como el ataque del **hombre en el medio**, que comprende las acciones que puede desarrollar alguien que intervenga el canal de comunicación. Este agresor puede, por ejemplo, escuchar, alterar, interrumpir o incluso suplantar la identidad de quienes se comunican. La paranoia lleva a pensar que todos están chuzados, pero la verdad es que cualquier intervención



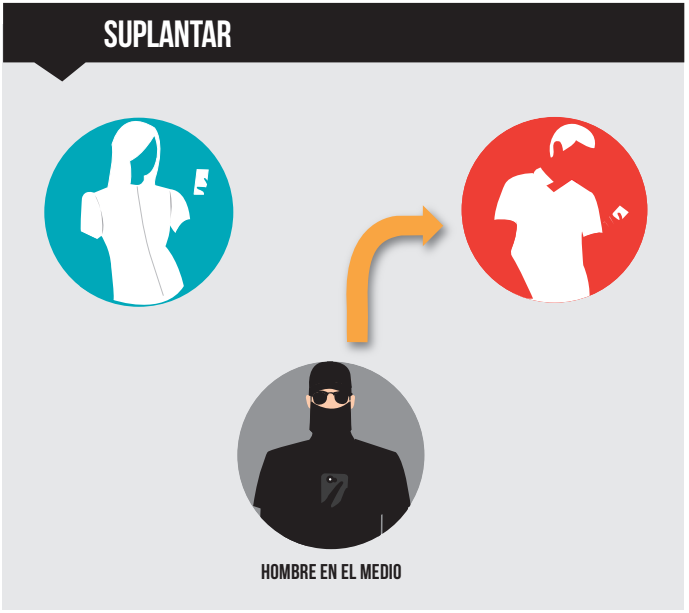
en las comunicaciones requiere esfuerzo y una infraestructura especializada que no es fácilmente utilizable por cualquiera.

Para reducir los riesgos de la intervención de las comunicaciones existen diversas alternativas, desde configurar correctamente los equipos y las cuentas de los usuarios, hasta utilizar extensivamente el **cifrado** de comunicaciones. En este último caso, aun cuando se presenta la intervención, el hombre en el medio quedará con un código ilegible que le impedirá leer o escuchar el mensaje.








**2. Comunicación segura con terceros**

Los teléfonos inteligentes mal utilizados son una fuente permanente de emisión de datos personales porque permiten conocer la ubicación de una persona minuto a minuto, dejan rastros de sus actividades y tienen mayores vulnerabilidades.

Estos dispositivos son más difíciles de configurar y proteger adecuadamente que otros aparatos, pues están diseñados para aprovechar la conectividad y, por

lo general, están configurados de forma automática para acceder al correo, a las redes sociales y a otros servicios sin mayor seguridad. Esto facilita las posibilidades de que las comunicaciones sean espiadas, por lo que un mayor grupo de tipos de agresores pueden interceptar y entrar a las comunicaciones telefónicas y en línea.

**a. Seguridad del equipo y configuraciones predeterminadas**

- El punto de partida para la seguridad en un dispositivo móvil es tener claridad para configurarlo. Se puede dedicar un tiempo a navegar y entender los ajustes del dispositivo y las aplicaciones instaladas en el celular (ej. chats, redes sociales, mapas, etc.).

- Restringir la capacidad del teléfono o de las aplicaciones para registrar información de ubicación apagando esta funcionalidad. Un registro de los lugares permitiría a los agresores hacer conexiones entre los sitios donde ha estado el periodista y las personas con las que se ha relacionado. En otros casos, quizá se deba considerar no llevar el celular al lugar de reunión.

- Crear un código de bloqueo o número de identificación personal (PIN). Es importante mantener en secreto ese código. Si el dispositivo móvil tiene un código preestablecido de fábrica, es mejor cambiarlo.

- Hacer copias de respaldo de la información contenida



en el teléfono o en el computador regularmente.

- Guardar la copia de respaldo de manera segura (Ver el punto 7 "Archivos seguros"). En caso de que se pierda el teléfono, tener ese respaldo permitirá conocer qué información sensible contiene y así, tomar las medidas pertinentes.

Para mayor información sobre este tema, se puede consultar la guía de la Electronic Frontier Foundation sobre Problemas con los teléfonos móviles (https://ssd.eff.org/es/module/el-problema-con-los-tel%C3%A9fonos-m%C3%B3viles). Según el tipo de equipo que se use, se recomienda revisar el capítulo de Configuración básica de seguridad para dispositivos Android de la guía Security in-a-box (https://ssd.eff.org/es/module/el-problema-con-los-tel%C3%A9fonos-m%C3%B3viles) y Cómo cifrar Tu iPhone en la guía de la Electronic Frontier Foundation (https://ssd.eff.org/es/module/como-cifrar-tu-iphone).

**b. Llamadas seguras**

Se podría decir que lo más seguro para comunicarse con una fuente es hacerlo personalmente, pero a veces es imposible hacerlo de esta forma, por lo que los periodistas realizan el contacto telefónicamente. Una de las opciones más efectivas para llamar a las fuentes o hacer

las averiguaciones por teléfono es utilizar una herramienta digital que cifre la comunicación de punta a punta.

- El **cifrado de comunicaciones de punta a punta** es el proceso por el cual un mensaje es convertido en un código ilegible, mientras es transmitido por redes de telecomunicaciones.

- Con esta herramienta el proveedor de servicios de telecomunicaciones o cualquier tipo de amenaza no puede conocer fácilmente el contenido de las comunicaciones.

- Si bien el contenido queda protegido, este cifrado no evita que se conozca el número telefónico de quien llama y quien recibe la llamada.

Las herramientas que se listan a continuación requieren de conexión a Internet para poder ser utilizadas y que la persona con quien se quiere establecer comunicación también tengan instalada la misma herramienta. Estos son algunos programas de **comunicación de voz sobre Protocolo de Internet** -también conocido como VoIP o Voz sobre IP- entre dos dispositivos que corren con una misma aplicación.

**RedPhone**
(https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone): Desarrollada por el proyecto Open-Whisper System (https://whispersystems.org/), permite



realizar comunicaciónes seguras de una manera muy sencilla. Está disponible para plataformas Android.

**Signal**
(https://itunes.apple.com/app/id874139669): Ofrece las mismas características de RedPhone, pero para plataformas iOS.

**Jitsi**
(https://jitsi.org/): Se usa para conversaciones por voz cifradas desde que la llamada sale del computador hasta que llega al computador de la persona a la que se envía el mensaje. En esta guía (en inglés) (https:// securityinabox.org/jitsi) se explican sus características y cómo instalarla.

**Hancel**
(http://hanselapp.com/index.html): También incluye una herramienta de comunicación de voz por Internet disponible para plataformas Android.

Todas estas aplicaciones son una alternativa a las llamadas de voz por Skype, pues ofrecen características de seguridad más fiables. La transición se puede ir haciendo paulatinamente. Para conocer más sobre los problemas de seguridad relacionados con Skype, consulte la información que Security in-a-box ha desarrollado al respecto (https://securityinabox.org/es/chapter_7_3).

**c. Mensajes de texto seguros**

La interceptación de llamadas telefónicas es costosa, requiere de muchos recursos humanos y tecnológicos, además de acceso a los sistemas de telecomunicación. Los mensajes de texto o MSM, en cambio, son especialmente fáciles de interceptar, pues quien esté haciendo la interceptación no necesita tener una persona que escucha y transcribe las llamadas.

- Ante la gran vulnerabilidad de este tipo de comunicación, se debe evitar enviar mensajes de texto. Si es muy necesario, se puede acordar un sistema de códigos entre los colegas durante situaciones críticas.

- Según el artículo 4 del Decreto 1704 de 2012, en Colombia los proveedores de servicios de telecomunicaciones y de Internet están obligados a retener los datos de las comunicaciones por 5 años que, por supuesto, deben quedar a disposición de las autoridades judiciales y de inteligencia.

- Se recomienda eliminar de inmediato los mensajes recibidos y enviados para evitar que alguien lea los mensajes cuando se roba el dispositivo.

Para los teléfonos inteligentes también existen herramientas que hacen posible enviar mensajes de texto cifrados de punta a punta. Tienen las mismas indicaciones, ventajas y desventajas que el cifrado por voz que se



listaron en el punto anterior. Algunas de estas herramientas son:

**TextSecure**
(https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms): Es una aplicación que permite enviar y recibir SMS de forma segura en los teléfonos Android. Funciona tanto para mensajes cifrados como no cifrados, por lo que se puede utilizar por defecto como una aplicación SMS. Esta guía contiene más información sobre su uso (https://securityinabox.org/es/node/3003).

**Telegram**
(https://telegram.org/): Es un servicio de mensajería por Internet que permite enviar mensajes, fotos, vídeos y archivos a los contactos que tienen instalada la aplicación. Está basado en la nube y sirve para sistemas operativos OS X, Windows y Linux, y para dispositivos móviles iPhone, iPad, Android y Windows.

**Hancel**
(http://hanselapp.com/index.html): También incluye una herramienta de mensajes de textos seguros para teléfonos Android.

Whatsapp no fue diseñada para compartir información confidencial y/o sensible. Su vulnerabilidad o fallas en la privacidad y seguridad de las comunicaciones ha sido ampliamente demostrada[1]. En noviembre de 2014, se conoció que la última actualización de Whatsapp incluía un fuerte cifrado punta a punta (https://whispersystems.org/blog/whatsapp/) de todas las comunicaciones realizadas con esta herramienta, lo que cambia radicalmente la situación anterior. La característica inicialmente está disponible para teléfonos Android, aunque se espera que paulatinamente sea implementada en otros sistemas operativos. En este sentido, es recomendable utilizar herramientas más seguras como las que se presentaron anteriormente.

### 3. Mensajería instantánea segura

Los servicios de mensajería instantánea normalmente no son seguros (ej. Google Talk, Facebook Messenger, mensajes de texto por Skype, etc.). Por suerte, existen herramientas de software que pueden ayudar a asegurar la privacidad de las sesiones de chat. Al igual que con las

[1] Véase Araujo, S. (2013, 11 de noviembre). Dos españoles hackean Whatsapp y demuestran la inseguridad del servicio, Hipertextual, en http://hipertextual.com/2013/11/seguridad-whatsapp-hack; Arcos, E. (2013, 10 de octubre). Cualquier apuede leer tus conversaciones de Whatsapp, Hipertextual, en http://hipertextual.com/2013/10/leer-conversaciones-whatsapp; Gualtieri, T. (2014, 19 de noviembre).



llamadas y los mensajes de textos seguros, las herramientas presentadas a continuación harán un cifrado de punta a punta de las comunicaciones. Las advertencias del punto anterior aplican también para este caso.

**Pidgin**
(https://www.pidgin.im/): Permite iniciar sesión en múltiples redes de chat simultáneamente, por lo que no es necesario cambiar el nombre de la cuenta o crear de nuevo la lista de contactos. Para poder tener conversaciones privadas cifradas, se necesita instalar y activar el complemento **Fuera de Registro** (Off-the-Record o OTR). La herramienta está disponible para plataformas Windows y Linux. Esta guía muestra los pasos de instalación (https:// securityinabox.org/es/chapter_7_3).

**Adium**
(https://adium.im/): Ofrece las mismas características que Pidgin, pero para plataformas OS X.

**Gibberbot**
Es una aplicación segura para chatear en teléfonos Android y iPhone. Para conocer sobre sus características y los pasos para instalarlo en teléfonos Android, consulte esta guía (https://securityinabox.org/es/gibberbot_principal). En 2014, Gibberbot cambió su nombre a **ChatSecure** (https://chatsecure.org).

**PARA NO OLVIDAR**

**Dificultar la entrada del intruso**

• Uno de los fines principales de la seguridad digital es dificultar el acceso externo a la información que se considera valiosa. Para esto, se deben escoger las medidas y estrategias de seguridad digital pensando en cuáles serán los obstáculos más efectivos y útiles ante un potencial ataque de las amenazas e individuos que se identificaron.

**¿Qué información se debe proteger?**

• Los periodistas manejan y producen mucha información. Quizás no todo lo que se tiene amerita protección.
• Establecer qué información es más importante y las consecuencias propias para personas cercanas o fuentes, si alguien consigue acceder; esto permitirá optimizar los esfuerzos de protección.

**4. Evitar la censura y navegación segura en Internet**

En ocasiones, el control sobre el acceso y el uso de la red tiene objetivos legítimos, como el bloqueo de la pornografía infantil. En muchas otras circunstancias este control se realiza para evitar que se conozca algún tipo de información que perjudica los intereses de algunos actores con poder. Es así como, frecuentemente ocurren casos de



censura digital al filtrar y bloquear contenidos, aplicaciones o servicios en línea. Esto, a su vez, puede llevar a que grupos privados o gubernamentales usen técnicas de control de actividades en línea de personas consideradas como indeseables, incómodos o peligrosas.

Diversidad de grupos han creado herramientas y técnicas para eludir la censura en Internet. Estos son conocidos como **métodos de elusión**, en donde se da la orden al navegador web para que tome un desvío a través de un computador intermediario o **proxy**. Las ventajas de este dispositivo son:

**1)** Se encuentra en otro lugar donde no existe censura en internet
**2)** No tiene bloqueado el contenido
**3)** Sabe cómo buscar y enviar contenidos a quien se envía el mensaje

**a. Protocolo seguro de transferencia de hipertexto o HTTPS**

Para navegar de manera segura hay que verificar siempre la dirección web en la parte superior del navegador. Si empieza en http:// -en lugar de https://- (sin la "s") significa que las navegaciones son inseguras. **HTTPS** impide a otros leer el tráfico en el sitio web que se está visitando y de ahí su ventaja.

**HTTPS Everywhere**
(https://www.eff.org/https-everywhere): Es un complemento que se instala en los navegadores Firefox, Chrome y Opera. En esta guía (en inglés) (http://en.flossmanuals.net/bypassing-censorship/ch018_https-everywhere/) aparece una explicación y los pasos de instalación.

**b. Navegación anónima**

Según el nivel de riesgo se puede considerar el uso de herramientas que permitan **navegar anónimamente.** Es decir, la ubicación real o dirección IP estará oculta porque el tráfico de datos pasa por diversos nodos cifrados.

**Navegador Tor**
(https://www.torproject.org/): Las actividades en línea quedan ocultas porque los datos viajan a través de varias redes de servidores distribuidos (ej. computadores, servidores). Esto hace que la conexión sea más lenta. Con este sistema no se muestra la dirección IP, sino la dirección del último servidor por el que transitaron los datos.

Las comunicaciones son potencialmente visibles desde que salen del último servidor Tor hasta que llegan a la persona que recibe el mensaje. Es recomendable usar una herramienta de comunicación segura que complemente las funcionalidades de Tor. Este software está disponible para plataformas Linux, Windows y OSX. En esta guía desarrollada por la *Electronic Frontier Foundation* se detalla el uso para Windows,



(https://ssd.eff.org/es/module/como-usar-tor-en-windows/).

**Orbot**
(https://guardianproject.info/apps/orbot/): Es una herramienta que ofrece navegación anónima para teléfonos Android.

**DuckDuckGo**
(https://duckduckgo.com/): Es un navegador web que, a diferencia de Google, Bing o Yahoo!, no registra el historial de búsqueda.

Existen muchas otras medidas de elusión que presentan un nivel más avanzado de conocimiento y de complejidad técnica. Algunas aparecen en la guía de la *Electronic Frontier Foundation* sobre **Cómo evadir la censura en Internet** (https://ssd.eff.org/es/playlist/%C2%BFperiodista-en-acci%C3%B3n#c%C3%B3mo-evadir-la-censura-en-l%C3%ADnea) y en el capítulo Mantenerse en el anonimato y evadir la censura en Internet (https://securityinabox.org/es/chapter-8) de la guía Security in-a-box.

**5. Privacidad y seguridad en redes sociales**

En algunas regiones de Colombia las redes sociales como Twitter y Facebook se han convertido en espacio de denuncia y de acceso a información de interés noticioso, en parte

como resultado de la ausencia de medios de comunicación. Pero, cuando el periodista utiliza estas redes sin precaución, está poniendo a disposición de otras personas -conocidas y desconocidas- información personal y/o sensible de la que pueden hacer un mal uso.

Para evitarlo, se recomienda:

- Ponderar la posibilidad de crear cuentas separadas o perfiles distintos para las actividades personales de las profesionales.

- Al crear un perfil oficial vinculado con las actividades laborales, hay que evitar mezclar actividades que puedan revelar información personal sensible, estableciendo unas reglas personales sobre qué tipo de interacciones e información se va a mostrar en cada perfil. Es importante ser consciente de los problemas de privacidad y seguridad vinculados con las redes sociales. La información disponible en ellas puede revelar datos sobre el usuario o sobre personas cercanas (ej. familiares, fuentes, contactos, etc.).

- La guía de *Security in-a-box* ofrece unos consejos generales sobre el uso de redes sociales (https://securityinabox.org/es/chapter_9_1).

- Muchos de los consejos ofrecidos en puntos anteriores son igualmente válidos para la gestión de los perfiles y cuentas en redes sociales: contraseña segura, acceso



usando HTTPS, revisión y cambio de los ajustes predeterminados y las configuraciones de privacidad y ubicación, etc.

- Las políticas de privacidad de las redes sociales cambian continuamente. Vale la pena hacer un esfuerzo por actualizarse y entender los cambios de estas políticas.

- Los sitios de redes sociales son propiedad de empresas privadas que hacen negocio con los datos que sus usuarios le ceden y confían.

- El capítulo sobre configuraciones de privacidad y seguridad (https://securityinabox.org/es/social_networking _tools) de la guía de *Security in-a-box* ofrece una orientación paso a paso para Facebook y Twitter, como también indicaciones generales para usar YouTube y Flickr.

**6. Protección contra software malicioso o espía**

Primero, hay que asegurarse que los dispositivos no estén vulnerables a ataques de piratas informáticos o a la intrusión de un *malware* (software malicioso), sea un virus o *spyware* (software espía). Ver Glosario para más información.

Además, hay que tener en cuenta las siguientes recomendaciones:

- Evitar abrir archivos o enlaces enviados por correo electrónico de remitentes desconocidos.

- Revisar el contenido de un archivo adjunto sospechoso con un software antivirus y usar el sentido común: los archivos que dicen contener las últimas imágenes de algún famoso o incluso las fotos de supuestas infidelidades de personas cercanas o los anuncios de algún premio son trampas para descargar software malicioso o para conocer los datos personales.

- Si para acceder al contenido pide que se registren o ingresen los datos de usuario y contraseña en algún servicio o en una red social, se debe revisar cuidadosamente que no se trate de un sitio falso.

- Instalar y utilizar software antivirus y actualizarlo con frecuencia. Estos tendrán la capacidad de detectar casi todo software malicioso, salvo que se esté ante un ataque dirigido y altamente sofisticado.

- Acudir a expertos informáticos para limpiar los dispositivos de cualquier software malicioso. Es necesario crear copias de respaldo antes de iniciar este proceso y asegurarse que la copia no albergue también el *malware*.

Algunos programas de software antivirus que se recomiendan son los siguientes:



**avast!**
(http://www.avast.com/en-za/index): Es un antivirus gratuito para Windows, OSX y para dispositivos móviles Android, iPhone y iPad. Consulte esta guía de uso (https://securityinabox.org/es/avast_principal) para conocer más sobre sus características y cómo funciona.

**Spybot**
(http://www.safer-networking.org/): Ofrece actualizaciones gratuitas y permite inmunizar el navegador de Internet de futuras infecciones producidas por software malicioso conocido. Está disponible para plataformas Windows. Sus características y su funcionalidad están en esta guía de instalación (https://securityinabox.org/es/spybot_principal).

**Comodo Firewall**
(https://securityinabox.org/es/comodo_principal):
Es un programa cortafuego *(firewall)* que funciona como un sistema de alerta temprana para ayudarle a reconocer cuando la seguridad del computador está amenazada. Está disponible para plataformas Windows. En esta guía de uso puede encontrar más información (https://securityinabox.org/es/comodo_principal).

## 7. Contactos, información y archivos seguros, y eliminación segura de archivos

### a. Contenidos seguros

Toda la información que manejan y generan los periodistas se encuentra almacenada en computadores, dispositivos móviles, discos duros externos, etc. Cualquier herramienta no los blinda de amenazas completamente, lo mejor es tomar medidas de seguridad que dificulten el acceso.

El bloqueo de los dispositivos a través de claves de acceso, contraseñas o PIN no es una medida suficiente, porque la información sigue guardada en una forma de fácil acceso. Para subsanar esa deficiencia, lo más recomendable es volver una práctica habitual el **cifrado de información** de los datos que se consideren sensibles.

- Hacer uso de las opciones de cifrado de disco completo que ofrecen la mayoría de los dispositivos.

- En teléfonos Android, se puede hacer en la configuración de "Seguridad" y seguir los pasos que indique el dispositivo.

- En iPhone y iPad, buscar la configuración de *"Data Protection"* o "Protección de Datos", en la sección de ajuste; el cifrado de la información en el dispositivo se activará una vez se cree una clave.

- En Windows, esto se conoce como *"BitLocker"*, mientras que en Mac es *"FileVault"*.

- Para plataformas Linux, el cifrado de disco completo



usualmente se ofrece cuando se instala el sistema por primera vez.

- El cifrado de los archivos será tan bueno como la contraseña que se va a crear (Ver "Contraseñas seguras").

También existen herramientas que ayudan a guardar la información en volúmenes cifrados. Por ejemplo, se pueden guardar todas las grabaciones de las entrevistas, en lugar de mantenerlas almacenadas en la grabadora digital. Algunas herramientas que se recomiendan son las siguientes:

**AxCrypt**
(http://www.axantum.com/AxCrypt/): Es un pequeño programa que permite cifrar archivos o carpetas utilizando un algoritmo de cifrado fuerte. Más información en la guía de la página oficial de AxCrypt (en inglés) (http://www.axantum.com/AxCrypt/HowToUse.html).

**DiskCryptor**
(https://diskcryptor.net/wiki/Main_Page): Es una solución para el sistema operativo Windows que es de cifrado abierto y ofrece el cifrado de todas las particiones de disco, incluyendo la partición del sistema. Más información en la guía de DiskCryptor (en inglés) (http://www.maketecheasier.com/diskcryptor-encrypt-partitions-in-windows/).

**b. Eliminación segura de archivos**

Al borrar un archivo de cualquiera de los dispositivos, incluso antes de vaciar la papelera de reciclaje del computador, los contenidos del archivo se mantienen en el disco duro y pueden ser recuperados por cualquiera que sepa cómo hacerlo. La solución es utilizar los programas de borrado de información. Estos programas hacen una **limpieza de datos**, es decir, no eliminan el archivo, sino que escriben encima del archivo datos aleatorios.

**Eraser**
(http://eraser.heidi.ie/): Elimina permanentemente datos sensibles y puede limpiar cualquier dato recuperable. La aplicación está disponible para plataformas Windows. Esta guía contiene características y funcionalidades (https://securityinabox.org/es/eraser_principal).

**CCleaner**
(http://www.piriform.com/ccleaner): Hace posible la fácil eliminación o depuración del historial de navegación, cookies y otros archivos temporales creados durante la sesión de trabajo, y la liberación de espacio en el disco. La herramienta está disponible para Windows, Mac y Android. En esta guía aparecen las características y la se explica cómo funciona (https://securityinabox.org/es/ccleaner_principal).



**PARA NO OLVIDAR**

**La solución puede ser desconectarse**

Si bien la tecnología ha facilitado muchos aspectos de la vida y del trabajo periodístico, ante una amenaza digital no siempre la solución está ligada a estos mecanismos. Aquí dos ejemplos:

- Si existe el riesgo potencial de que las comunicaciones sean interceptadas y una fuente quiere entregar información valiosa, la mejor estrategia podría ser reunirse personalmente.
- Ante el peligro de que estén rastreando la ubicación de alguien, es mejor reunirse sin llevar el teléfono celular o apagarlo antes de salir a la reunión.

**Conocer cómo funcionan las redes de comunicación ayuda a prevenir riesgos**

- El conocimiento sobre el funcionamiento de las redes de comunicación telefónica y en línea permite identificar algunas vulnerabilidades y, por tanto, prevenir riesgos.
- No se trata de convertirse en un ingeniero en telecomunicaciones o en informática, sino de ser conscientes de cómo transitan las comunicaciones y la información en estas redes.

## 8. Correo electrónico cifrado

El correo electrónico, desde el diseño, es una herramienta insegura. La mayoría de la información del correo electrónico que viaja por la red va sin cifrar. Esto a pesar de que desde hace unos años los principales proveedores de correo como Gmail, Yahoo! y Outlook (Hotmail/MSN) empezaron a cifrar las conexiones entre los servidores de correo (usando SSL).

El problema principal con el correo es que, aunque la conexión punto a punto vaya cifrada, el mensaje no lo está. Herramientas como PGP (http://www.pgpi.org/) o OpenPGP (http://www.openpgp.org/) se basan en utilizar firmas digitales cifradas para transmitir de manera segura un mensaje.

- Estas herramientas solicitan la creación de las llaves privadas y públicas.

- Las **llaves privadas** sirven para "firmar" los correos, lo que le permite a quien recibe el mensaje verificar la identidad del autor y descifrar el mensaje si está cifrado.

- Con las **llaves públicas** el destinatario puede verificar la identidad y confirmar que el remitente es confiable.

Para hacer lo anterior, es necesario instalar en el computador el siguiente software:



**Thunderbird**
(https://www.mozilla.org/es-ES/thunderbird/), con el plugin Enigmail (https://www.enigmail.net/home/index. php), un programa que permite conectarse a cualquier servidor de correo. Ayuda a gestionar el correo directamente en el computador y utilizarlo para enviar correos inseguros. Mozilla ofrece esta guía sobre cómo instalar y usar esta herramienta (https://support.mozilla.org/es/kb/firma-digital-y-cifrado-de-mensajes).

**OpenMailBox**
Es una plataforma en línea que busca enfrentar el reto de cifrar correo electrónico masivamente, ofreciendo el cifrado seguro por omisión. Es una herramienta que salió hace unos meses y vale la pena explorarla.

## 9. Todo en uno

Existe un sistema operativo que contiene casi todas las herramientas de seguridad mencionadas para preservar la privacidad y el anonimato: navegación anónima, cifrado de archivos, correos electrónicos y mensajes instantáneos, uso de la red Tor para el tránsito de los datos y cero rastro en el computador que se esté utilizando. Esta herramienta "todo en uno" se conoce como Tails (https://tails.boum.org/) y está basada en Linux. El sistema está diseñado para darle inicio desde un CD o memoria USB, independiente del sistema operativo original del computador.

**Crear un entorno seguro**

Afuera del mundo digital también hay riesgos. Tener en cuenta estas recomendaciones básicas puede ayudar a proteger aún más la información:

- Evitar usar el mismo café Internet o red de WiFi del sitio distinto a la oficina

- Si se está preparando una publicación muy sensible, se aconseja escribirla en un computador que esté en un sitio seguro y que nunca tenga conexión a Internet. Si se quiere almacenar información allí, se debe verificar la seguridad de las memorias USB en las que se pasarán los datos.

- Ingresar al correo electrónico o redes sociales desde el computador propio. Si se hace desde un dispositivo prestado, es necesario cerrar la sesión, usar la navegación privada y no olvidar los demás consejos entregados anteriormente.

- Apagar siempre el computador cuando se abandone el escritorio por largo tiempo.

- Existen candados o guayas de seguridad para computadores. Se pueden usar en dispositivos que se dejen de utilizar por lapsos largos de tiempo.

- Guardar los dispositivos que contengan las copias de



seguridad en una zona segura. Se debe evitar transportarlos de un lugar a otro.

- Evaluar el nivel de seguridad de la oficina. Se debe valorar quiénes tienen acceso a ella y a los equipos.

- Establecer un entorno seguro creando con los compañeros de trabajo protocolos de seguridad.

También es importante recordar que el Estado colombiano tiene planes de atención y prevención frente a los delitos informáticos. A continuación se explican las funciones de la Policía y la Unidad Nacional de Protección:

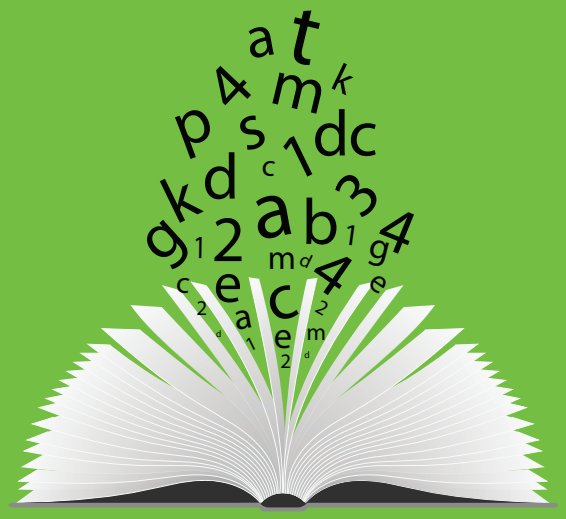
**Policía Nacional**

Estableció la creación de la Unidad de Delitos Informáticos, dedicada a perseguir este tipo de actividades criminales. En su página web tipifican los tipos de delitos que son punibles y también, enlistan varias recomendaciones para mitigar los riesgos, algunas de ellas son útiles para los periodistas. Para mayor información, consultar la página de la unidad:

http://www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Seguridad_Ciudadana/Planes_de_Seguridad/Recomendaciones_de_seguridad/delitos_informaticos

**Unidad Nacional de Protección**

Todos los periodistas gozan de protección por parte del Estado, donde la UNP es la entidad encargada de su correcto funcionamiento. La UNP tramita todas las amenazas, tanto las que son dirigidas a través de medios digitales o por medios físicos, siempre y cuando el periodista entable una denuncia ante las autoridades competentes. Hay que señalar que la UNP no investiga los hechos delictivos.



# GLOSARIO

**Ataque enmascarado (phishing emails):** Usar correos electrónicos que aparentan ser auténticos y provenir de fuentes confiables, para enviar un software malicioso disfrazado como archivo adjunto o enlace a sitio web.

**Malware:** Software malicioso, en español, trabaja de muchas maneras, pero su carácter es siempre criminal, pues busca hacer daños, obtener información de manera ilícita, espiar comunicaciones, acceder a credenciales de entrada, etc. Su uso, además, es muy diverso; gobiernos, grupos criminales o individuos pueden hacer uso de todo tipo de software malicioso. También son variados los medios que se utilizan para infectar un dispositivo no protegido, ya sea a través de un correo electrónico, un archivo adjunto, un enlace a una página web u otros.

**Metadatos:** Datos que describen otros datos. Un ejemplo de metadato en el mundo análogo son las típicas fichas bibliográficas que se encuentran en las bibliotecas, en donde se especifican autores, títulos, casas editoriales y lugares para buscar los libros. Es decir, los metadatos que ayudan a ubicar datos. En las comunicaciones telefónicas y en línea los metadatos son toda aquella información que identifica quiénes se comunican, desde dónde y en qué momento. Hoy en día, los metadatos revelan más sobre los hábitos, movimientos y relaciones de las personas, que del contenido mismo de las comunicaciones, incluso si estas se mantienen privadas.

**PGP:** Pretty Good Privacy (PGP) o privacidad bastante buena es un programa que protege la información distribuida a través de Internet mediante el uso de criptografía de clave pública. También facilita la autenticación de documentos gracias a firmas digitales. Para más información, consulte el siguiente enlace: https://es.wikipedia.org/wiki/Pretty_Good_Privacy.



**Proxy:** Servidor que sirve de intermediario en las peticiones de recursos e información que realiza un cliente a otro servidor.

**Servidor:** Punto de intersección o conexión (nodo) que está conectado a una red y provee servicios a otros nodos denominados clientes.

**Spyware:** Software espía, en español, es una clase de software malicioso, como los virus, que puede rastrear todo lo que se hace desde un dispositivo o en Internet, y enviar esa información a alguien que no debe tener acceso a ella. Estos programas pueden registrar las palabras que se escriben, los movimientos del ratón, las páginas que se visitan y los programas que se ejecutan, entre muchas otras cosas. De esta manera, la información confidencial o sensible que se tengan, las actividades y los contactos quedan comprometidos y desprotegidos.

**SSL:** Secure Sockets Layer (SSL) o la capa de conexión segura es un protocolo criptográfico que proporciona comunicaciones seguras por una red. Para más información, consulte el siguiente enlace: https://es.wikipedia.org/wiki/transport_Layer_Security.

# OTRAS LECTURAS SOBRE SEGURIDAD DIGITAL

**1.** Artículo 19 (2013). Guía de Seguridad digital y de la información para periodistas. Disponible en Internet:
**http://coberturaderiesgo.articulo19.org/wp-content/uploads/2013/07/guia_seguridad_digital.pdf**

**2.** Committee for Journalist Protection (2012). Seguridad de la información. Manual de Seguridad para Periodistas. Disponible en Internet:
**https://www.cpj.org/es/2012/04/seguridad-de-la-informacin.php**

**3.** Electronic Frontier Foundation (Octubre 2014). Autoprotección digital contra la vigilancia. Consejos, herramientas y guías para tener comunicaciones más seguras. Disponible en Internet:
**https://ssd.eff.org/es**

**4.** European Digital Rights (2012). ¿Cómo funciona internet? The EDRi Papers. Edición 3. Disponible en Internet:
**https://edri.org/files/paper03_20120725_02_esp.pdf**

**5.** Digital Defenders Partnership (2014). Digital First Aid Kit. Disponible en Internet:
**https://digitaldefenders.org/digitalfirstaid/#DFAk/**



**6.** DW Akademia (Noviembre 2013). What's your threat? Working out your security needs. Disponible en Internet:
**http://akademie.dw.de/digitalsafety/whats-your-threat-working-out-your-security-needs/**

**7.** ICFJ & Freedom House (Octubre 2013). Manual de seguridad digital y móvil para periodistas y blogueros. Disponible en Internet:
**http://www.icfj.org/sites/default/files/Manual%20de%20seguridad%20web.pdf**

**8.** Internews (2012). Speak up, speak out: A toolkit for reporting on human rights issues. Disponible en Internet:
**https://www.internews.org/sites/default/files/resources/Internews_SpeakUpSpeakOut_Full.pdf**

**9.** Peña Ochoa, P. (2013). ¿Cómo funciona Internet? Nodos críticos desde una perspectiva de los derechos. Guía para periodistas. Santiago de Chile: ONG Derechos Digitales. Disponible en Internet:
**https://www.derechosdigitales.org/wp-content/uploads/Como-funciona-internet-ebook.pdf**

**10.** Tactical Tech (s.f.). Security in-a-box. Disponible en Internet:
**https://securityinabox.org/es/howtobooklet**

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

**Oficina en Quito**
Representación para Bolivia, Colombia, Ecuador y Venezuela

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

PIDC Programa Internacional para el Desarrollo de la Comunicación

FORUMSYD

REPORTEROS SIN FRONTERAS
POR LA LIBERTAD DE PRENSA


Con la colaboración de:


www.karisma.org.co