# Seguridad Digital para periodistas

Año
2018

Autora
Obeid, María Carolina

# Seguridad Digital para Periodistas

María Carolina Obeid.
Enero 2016/2017.

Universidad Nacional de Córdoba
Facultad de Ciencias de la Comunicación

## Resumen

Los aspectos de seguridad digital que involucran la labor periodística son increíblemente amplios y complejos. El propósito de este trabajo consiste en indagar los cuidados que deben tener los comunicadores que realizan sus labores en entornos informáticos a fin de minimizar la vulnerabilidad y los riesgos de sus equipos digitales. El informe se centra exclusivamente en los elementos de seguridad para resguardar la privacidad e inviolabilidad de la información en computadoras personales, teléfonos móviles e información en la nube.

# Introducción

La tarea de minimizar los riesgos y la vulnerabilidad que implica trabajar en entornos informáticos es cada vez más relevante para quienes realizan la labor periodística. En este ámbito, los aspectos de seguridad digital son increíblemente amplios y complejos. El propósito de este trabajo es indagar el estado actual de la Tecnología de la Información y Comunicación exclusivamente en los elementos de seguridad relacionados con computadoras personales, teléfonos móviles e información en la nube para resguardar la privacidad e inviolabilidad de la información de los periodistas.

El mundo digital provee a los comunicadores las herramientas de trabajo, la interrelación en redes sociales, la información periodística de las fuentes y personal con el riesgo de quedar expuestos a quienes por algún motivo pretendieran acceder a sus datos. Debido a esto, el periodista debe poseer el conocimiento y las habilidades necesarias para enfrentar el desafío de resguardo.

Existe una gran cantidad de precauciones a adoptar y tecnologías informáticas a aplicar, de manera que, sin pretender alcanzar el conocimiento de un experto en seguridad informática, un comunicador puede incrementar notablemente la seguridad digital con respecto a usuarios comunes.

Al estar la actividad del periodista actual, íntimamente ligada al mundo digital, se realizan constantes intercambios de datos por infinidad de medios. Toda la información con la que contamos está realmente al alcance de quien desee accederla, independientemente del lugar en el mundo en que se encuentre. Es como si estuviéramos trabajando en la misma habitación con todos los servicios de seguridad del mundo, con todos los periodistas del mundo, con todos los hackers del mundo, solo que sin verlos.

Debemos entender por qué la seguridad de la información digital de la que disponemos es tan vulnerable y, en consecuencia, necesitamos hacer todo lo posible para resguardarla. En este sentido, es importante implementar medidas de seguridad con un nivel de profundidad relacionada al riesgo del trabajo periodístico desempeñado. El riesgo que corre un periodista deportivo es diferente que el de un investigador de tráfico de personas. Este trabajo no se enfoca hacia los periodistas expuestos a altos niveles de inseguridad sino al grupo mayoritario de quienes necesitan, en su labor profesional cotidiana, tomar medidas de protección.

¿Cuáles son los peligros a los que los periodistas están expuestos al manejarse en entornos digitales? ¿Se puede hacer algo al respecto? ¿Qué métodos y herramientas se pueden emplear? ¿Cuáles son los límites que los periodistas deberían conocer? ¿Qué se puede hacer más allá de esos límites? ¿Cuál es la tendencia en cuanto a la necesidad de resguardar la información? Estos interrogantes guiaron la búsqueda realizada mediante la exploración de documentos -publicaciones científicas, notas periodísticas, bibliografía específica, producidas en América Latina- que dan cuenta y analizan hechos de inseguridad informática, en un rango temporal que abarca los años 2016 y 2017.

## Escenario vulnerable

De qué hablamos cuando hacemos referencia a la "vulnerabilidad de sistemas informáticos"? Los antecedentes que se enumeran a continuación permiten anticipar que no existe la fórmula para garantizar la seguridad absoluta de la información aun en entornos con altos presupuestos. Hemos seleccionado casos paradigmáticos develados por el Informe de WikiLeaks (organización internacional sin fines de lucro que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes). Aunque es posible minimizar la

inseguridad de nuestra información, para tomar conciencia de lo que esto significa describiremos sólo algunos puntos del informe para tener una idea de lo que estamos hablando: En el artículo ¿**Qué descubrió Wikileaks en informes de la CIA?**[1] se describe un caso paradigmático de uso de malware (un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información) para hackear (ingresar a un sistema de cómputos sin permiso) televisores inteligentes. El ataque a Samsung se atribuyó a softwares maliciosos y herramientas de hackeo desarrollados por el Grupo de Ingeniería de Desarrollo (EDG) de la Agencia norteamericana CIA que pudo obtener información de conversaciones dentro de cualquier hogar o sala de reuniones. A continuación, una breve descripción de algunos de los puntos del extenso estudio:

- La CIA, con ayuda del Reino Unido, introdujo en los televisores inteligentes Samsung serie 7, un malware (software malicioso) llamado WeepingAngel que posibilitaba hackearlos grabando audio desde el micrófono del equipo para luego enviarlo a los servidores de la CIA, incluso aunque el televisor estuviera apagado.
- De forma similar, la CIA logró un desarrollo tecnológico suficiente en sus malwares como para introducirlos en teléfonos celulares inteligentes e interceptar el contenido de las cámaras, audios e información tipeada antes del proceso de cifrado de Telegram, WhatsApp, Signal, Clockman, Confide y Wiebo
- Otro tipo de malware desarrollado por la CIA permitiría ocultarse en zonas protegidas de los discos, USB, CD, DVD y archivos de imágenes con el objetivo de que se activaran para extraer información de todo tipo en los equipos utilizados.
- Desarrollaron herramientas de software que permitirían tomar el control de servidores y equipos con sistemas operativos Mac OS X, Linux y Windows tales como Cutthroat y Swindle.

- Aparecieron versiones muy avanzadas de software del tipo Zero Year, que bajo la apariencia de ser inofensivo tiene el poder de ejecutarse remotamente y ser de muy difícil detección.
- La CIA logró hackear los sistemas Android y iPhone y espiar a funcionarios, ejecutivos y otros en Estados Unidos.
- Otro hecho revelado que demuestra hasta dónde llega el descontrol a nivel de seguridad digital es que no hay control del software empleado para espionaje ya que puede ser copiado por cualquier persona y utilizado según sus intereses o copiado por cualquiera que logre hacerse de una copia.
- Muchas agencias de inteligencia en Estados Unidos han sido objeto de importantes filtraciones de seguridad en los últimos años.

Estos son solo algunos puntos como para que nos hagamos una idea de lo insegura que está nuestra información. Hay muchísimos temas más que exceden la finalidad de este trabajo, como hackeo de routers por parte de países como Rusia y Estados Unidos, comercialización de nuestros datos por parte de Facebook y otros, solo para mencionar algunos.

El propósito de estos ejemplos es simplemente el de dejar claro que cualquier sistema informático es vulnerable, inclusive los altamente protegidos.

## Recomendaciones: El cuidado empieza por casa

Los antecedentes mencionados ilustran la imposibilidad técnica de conseguir seguridad absoluta, pero es importante conocer medidas que pueden maximizar -o minimizar- la inseguridad de los datos. Cada medida de protección que tomamos disminuye, en alguna medida, los riesgos. Una aceptable inmunidad en la información pocas veces trata sobre cómo

defendernos de ciberataques y de hackers. Se refiere, más bien, a cómo comprender los motivos y las capacidades de los eventuales atacantes y cómo desarrollar "hábitos constantes" sobre la base de dichas evaluaciones.

No es conveniente que los comunicadores hagan públicas sus fuentes de información. Hay datos que podrían parecer inofensivos en determinado contexto y representar un peligro en otros. Algunos son evidentes y probablemente no sería bueno perderlos o divulgarlos, como por ejemplo archivos de computadora y móviles o interrupciones temporales del servicio de telecomunicaciones o webs. Otros datos son más intangibles. Probablemente no sería conveniente que se divulgara nuestra ubicación actual, el historial de ubicaciones, la lista de personas con las cuales nos comunicamos, los sitios de Internet que visitamos, etc.

Es recomendable realizar una lista de todos los servicios que utilizamos normalmente para evaluar las implicancias de interrupciones del servicio que nos impediría trabajar, comunicarnos, acceder a nuestros datos, a internet, a nuestro correo electrónico, usar el móvil, la mensajería, etc. Por ejemplo, no es lo mismo trabajar on-line en un documento colgado en la nube que hacerlo en un archivo local ya que en el primer caso si se corta el acceso a internet no podemos seguir trabajando.

La seguridad informática tiene algunas debilidades específicas. Por ejemplo, es muy difícil saber cuándo alguien ha revisado nuestros datos. Si alguien hace una copia del disco duro de la computadora, es posible que nunca lo sepamos.

Los sistemas tecnológicos son complejos y están conformados por muchos elementos diferentes que están en constante cambio. Ni siquiera los técnicos más preparados y meticulosos pueden conocer acabadamente el funcionamiento de cada programa en sus computadoras, y mucho menos cómo interactúan con otros programas de software presentes

en la red y dónde se pueden aprovechar esas interacciones. La seguridad informática es mucho más difícil de comprender de manera intuitiva.

La mejor actitud en pos de minimizar la inseguridad de nuestra información es recurrir a la simplicidad con un pequeño número de herramientas, técnicas y hábitos. Los sistemas complejos son difíciles de comprender en su totalidad. Debemos siempre tener en cuenta que en la web todo evoluciona y cambia a un ritmo vertiginoso y lo que hoy es medianamente seguro puede dejar de serlo en el futuro.

Una vez que entendemos y verificamos los puntos anteriores, y luego de conocer el abanico de herramientas, técnicas y hábitos de los que disponemos, podremos elaborar un plan de acción con diferentes grados de periodicidad a fin de brindar seguridad a nuestra información.

## Cuidar las herramientas

A continuación, se describen las características, las recomendaciones y los riesgos que implica el uso de determinadas herramientas informáticas como los dispositivos móviles, Internet, correo electrónico y dispositivos de almacenamiento, entre otros.

## Dispositivos móviles

Las intercepciones telefónicas son una de las maneras más comunes de vigilar a los periodistas. Siempre que hace una llamada, la empresa de telefonía tiene la capacidad de ver a quién llama y de escuchar la llamada. Los mensajes de texto son incluso más fáciles de interceptar porque son breves y fáciles de almacenar lo cual hace innecesario contar con costosos equipos de grabación. Es posible reducir en alguna medida esta amenaza al utilizar herramientas como Signail y RedPhone para encriptar las llamadas. TextSecure para cifrar los

mensajes de texto. Estas solamente ocultan el contenido de las conversaciones, no los participantes, el horario, las ubicaciones, etc.

Los teléfonos y las tarjetas SIM tienen números de serie únicos y ambos son informados a la empresa de telefonía siempre que el aparato esté encendido. Simplemente colocando la tarjeta SIM en otro teléfono o manteniendo el mismo dispositivo y cambiando la tarjeta no ocultará mucho a una empresa de telefonía, ya que les basta con comparar los dos números de serie.

El teléfono móvil constantemente se conecta con las antenas de celulares que están a su alrededor lo que deja un rastro de las torres a las que se ha acercado proporcionándole a la empresa de telefonía una buena constancia de los lugares donde hemos estado. Retirar la batería del teléfono evita esto, pero hay que ser conscientes del rastro que pueden dejar varias personas que se la quitan apenas horas antes de encontrarse para una reunión. Puede que sea más sensato quitar la pila antes de salir o dejar el dispositivo.

Además de que los teléfonos móviles pueden utilizarse como dispositivos de rastreo, se pueden emplear como terminales de escucha a distancia. Apagar un teléfono no garantiza que no pueda usarse para escucha. Para la mayoría de los dispositivos, “apagado” es en realidad apenas una modalidad de muy poca potencia. La única manera de asegurar que un teléfono no se está utilizando para escuchar a distancia es quitar la batería, al menos en la mayoría de los casos.

## Conexiones a Internet

Al usar una conexión inalámbrica en un lugar público, otras personas conectadas a la misma red podrían espiar dónde navegamos, correos electrónicos, mensajes instantáneos, etc. Si estamos en un hotel o en un bar, por ejemplo, esa institución también tiene la posibilidad

de observar este tipo de información. Si utilizamos una conexión a Internet privada y nuestra  conexión inalámbrica fuera segura (lo más probable es que no lo sea), solamente el proveedor de servicio de Internet sabría lo que hacemos en Internet.

**Conexiones a Internet VPN**

Es posible ocultar esta información de los curiosos y los proveedores de servicio de Internet empleando una **red privada virtual (Virtual Private Network o VPN)**.

Una VPN es un software que encripta y envía todos los datos que entran y salen de nuestra computadora por Internet a través de un servidor especialmente dispuesto a tal fin, que se encuentra en otra parte de Internet y que se llama servidor VPN. Cuando se configura de modo correcto, la red VPN garantiza que todas las comunicaciones estén seguras contra interferencias. Es como si toda la información que enviamos y recibimos desde nuestra computadora viajara por los medios de comunicación intervinientes en esa comunicación encerradas en un tubo inviolable. A este conducto, en realidad, lo posibilita la encriptación. Hay varias compañías que ofrecen el servicio de VPN, tanto pagos como de uso libre.

Desde el resto de Internet pareciera que estuviéramos accediendo a la web y a otros servicios de la Red desde el servidor VPN, no desde nuestra ubicación real. Esto significa que podemos ocultar nuestra ubicación actual y pasar inadvertidos por los sistemas de censura locales.

Los VPN no cifran todos los tramos del recorrido de nuestros datos en línea. La encriptación se efectúa entre nuestra computadora y el servidor VPN. Los tramos de comunicación comprendidos entre este y el destino de la comunicación se realizan sin codificación. Si quisiéramos ocultarnos de organismos locales debiéramos contratar un servidor VPN que se encuentre fuera de su jurisdicción.

**Conexiones a Internet (Tor)**

Otra alternativa para asegurar las comunicaciones vía Internet es el servicio seguro por anonimato llamado Tor, ya que protege el tráfico de sus usuarios encriptando y mezclando los datos a través de varios servidores antes de que finalmente salgan a la Internet. La manera más fácil de utilizar Tor es con el navegador Tor para Windows. También existe Tails, que es un sistema operativo en vivo (almacenado en un medio extraíble, tradicionalmente un CD, DVD, pendrive u otro, que puede ejecutarse directamente en una computadora) y que envía todo el tráfico por medio de Tor.

**Conexiones a Internet (https)**

Otra forma de comunicación segura por medio de navegadores de Internet es cuando el sitio web al que accedemos protege la comunicación por medio del protocolo HTTPS. Si la dirección del sitio web comienza con “https://” y no con “http://” y si hay un ícono de candado al lado, entonces la conexión está encriptada. En este caso, un espía podrá saber qué sitio estamos visitando pero no cuál página de ese sitio ni la información que se transfiera. Esto es particularmente importante para cualquier sitio al que ingresamos por medio de contraseña. ¡Y ni hablar de home banking! De esto se desprende que nunca hay que utilizar servicios de correo electrónico web que no cumplan con esta condición.

Existen complementos para navegadores o add-on que ayudan con esto. Un ejemplo es HTTPs-everywhere, que contribuye a garantizar una conexión segura donde quiera que sea posible, solo que algunos sitios y servicios no lo permiten.

**Correo electrónico y mensajería**

Además de una VPN o HTTPS en el que se codifica todo lo que entra y sale del navegador, existen también encriptaciones dedicadas solo para algún servicio en particular, ya sea correo, mensajería, accesos remotos, etc. Si solo precisamos seguridad para uno de estos servicios en particular, podemos optar por algún producto de software de este tipo.

Los referentes obligados de la encriptación para correo electrónico son GNU PrivacyGuard (GPG), que es un programa gratuito y de código abierto, y bPretty Good Privacy (PGP), de la empresa Symantec. Ambos tienen una pronunciada curva de aprendizaje y son difíciles de usar. Tanto los emisores y receptores de los mensajes deben usar el mismo software. El contenido permanece protegido con un elevado nivel de seguridad pero no ocultan la identidad de los interlocutores. Muchos programas de correo electrónico como Outlook, Thunderbird y Apple Mail tienen complementos o plugins que brindan soporte a GPG/PGP.

Cuando un servicio de correo electrónico encriptado transfiere mensajes entre emisor y receptor del mismo servicio, los mensajes viajan con un buen nivel de seguridad. También ocurre que cuando un servicio de correo electrónico envía un mensaje a otro servicio, se abre una oportunidad para que el contenido sea interceptado. Algunos servicios utilizan el cifrado cuando envían un mensaje hacia afuera; otros, no.

Aunque la encriptación de servidor a servidor puede proteger los mensajes en tránsito por Internet, los atacantes pueden intentar obtener un archivo de mensajes previos instalando software en la computadora de origen y en la computadora de los destinatarios. Por eso es tan importante proteger el ordenador y las contraseñas de todo servicio de correo.

Las herramientas de mensajería instantánea como Google Hangout, Skype, Facebook Messenger, Kik, Viber y otros similares pueden ser tan vulnerables a la intercepción como el correo electrónico. Muchos programas de chat utilizan la encriptación para asegurar que solamente los participantes y el proveedor del servicio puedan leer mensajes o ver quién se

está comunicando. Algunos servicios, como CryptoCat, utilizan un método incluso más seguro en el que solamente los participantes de un chat pueden leer mensajes, pero esto es menos común. Algunos proveedores están dispuestos a entregar los registros de los chats cuando se los piden; otros no.

**Cuidar la información**

Los smartphones, las tabletas y las computadoras laptop pueden guardar grandes cantidades de datos y permiten el acceso a muchas herramientas valiosas. Por otro lado, si las computadoras o los teléfonos son robados o destruidos, corremos el riesgo de perder una gran cantidad de información importante. Es primordial proteger la información de dos maneras: asegurando que no se pueda destruir y cerciorando que no se pueda robar. Existe una gran cantidad de herramientas que permiten perseguir este propósito.

Siempre es importante encriptar la computadora. Esto es, codificar con algoritmos la información para que nadie pueda descifrarla. Los programas BitLocker de Windows, FileVoult de MacOS o TrueCrypy permiten proteger toda la computadora, lo que es mucho más seguro que simplemente resguardar cada archivo individual. Los dispositivos Android e iOS también tienen funciones de encriptación que se pueden activar en las opciones de configuración. También es imprescindible que utilizaremos contraseñas fuertes para la encriptación, ya que lo único que mantiene segura a la información es la frase de contraseña.

Asimismo, es recomendable que bloqueemos la pantalla de los dispositivos digitales usando un PIN (Personal Identification Number) en lugar de deslizar los dedos en un patrón. Es conveniente apagar o poner en modo de hibernación (en lugar de poner en modo de suspensión) la laptop al descansar o cuando puedan registrarla, como por ejemplo al cruzar

una frontera, puesto que ello obligará a un agresor a enfrentarse a la encriptación, que es muy difícil de atacar.

También es posible copiar información importante en un dispositivo USB encriptado, ya que es más fácil de ocultar que una laptop o teléfono inteligente.

No hay que usar nunca computadoras de acceso público para cuestiones importantes en cibercafés ni hoteles; tampoco conectarles dispositivos USB y menos aún ingresar contraseñas.

No hay nada más difícil, por no decir imposible, que garantizar la seguridad de un smartphone, fundamentalmente por el simple hecho de que cada aplicación instalada posee acceso a mucha o toda la información del celular, y lo peor de todo es que somos nosotros mismos quienes lo permitimos, en la mayoría de los casos explícitamente. De hecho, la mayoría de las aplicaciones dicen ser "gratuitas", y como sabemos, lo gratis no existe y el precio lo pagamos con nuestra privacidad entregando a los propietarios de las aplicaciones "toda la información" disponible en nuestros móviles: contactos, mensajes, conversaciones, fotos, videos, links visitados, claves introducidas, teclas apretadas, archivos de todo tipo, etc. Todo esto para que los propietarios de las aplicaciones vendan esa información a anunciantes a cambio de dinero.

Esta exposición abusiva de nuestra privacidad la permitimos incluso si bajamos las aplicaciones de las webstore, que de hecho nos garantizan cierta "seguridad". Si descargamos aplicaciones de otros sitios, la exposición puede ser absoluta ya que les resulta incluso más fácil hacerse del control absoluto del teléfono, incluyendo cámara y micrófono.

Los malware son aplicaciones tanto para smartphone como para PC que, valiéndose de las vulnerabilidades del software del dispositivo (que debido a su complejidad son innumerables), entran al sistema y acceden a diferentes niveles. Los más sofisticados pueden tomar el control

absoluto del equipo, más inclusive que los propios usuarios, y para peor, estos no se enteran hasta que es demasiado tarde, o quizás nunca.

Los malwares pueden ingresar al sistema a través de archivos adjuntos que viajan en mensajes de correo electrónico falsos pero convincentes e inclusive en sitios de Internet que se ven como cualquier otro, en enlaces asociados a imágenes, etc. No debemos hacer clic en enlaces que recibimos por correo electrónico aunque provengan de colegas sin considerar la posibilidad de que el correo pudiera ser una copia a medida que usa detalles personales que un atacante extrajo en línea.

Es absolutamente necesario utilizar software antivirus y mantenerlo actualizado; éste podrá detectar todos los ataques de los cuales son víctima nuestros dispositivos, excepto los más sofisticados.

Existen muchas posibilidades a la hora de guardar nuestra información privada o laboral: en el disco de la PC, de la notebook, en la memoria de la tablet o smartphone, en memorias USB, discos externos, CD, DVD, Blueray Disks, et. Y también en almacenamientos externos como servidores de la compañía, servidores de almacenamiento privados, servidores de correo y, sobre todo, muy usado por estos tiempos, servidores en la nube.

Cada uno de estos medios de almacenamiento posee sus ventajas y vulnerabilidades. No los detallaremos en este artículo, pero sí abordaremos servicios de almacenamiento en la nube ya que son relativamente nuevos y ampliamente utilizados, como Google Drive, DropBox, iCould, OneDrive, etc. Consisten en servidores que se encuentran en algún lugar del mundo a los que se accede para trabajar con archivos en línea casi con la misma facilidad que implica un almacenamiento local y con la ventaja de poder accederlos desde cualquier lugar y con cualquier dispositivo digital. En estos casos, no hay que olvidar que quien se haga de nuestra contraseña podrá acceder a todo lo que tenemos allí sin restricción alguna.

También hay que considerar que las empresas de Internet entregan datos privados ante demandas presentadas por el gobierno si lo exige la ley local o si poseen vinculaciones estrechas con autoridades políticas o económicas.

En cuanto a la información que se hace pública desde las redes sociales, a estos sitios les agrada decirles a todos lo que nosotros le decimos a ellos. Vale la pena intentar, en forma periódica, tratarnos a nosotros mismos como si fuéramos espiados y observar cuánto puede saber de nosotros alguien que se lo propusiera.

Con respecto al almacenamiento de nuestros datos, debemos considerar la posibilidad de que se destruya el medio físico de almacenamiento, perdamos nuestra laptop, nuestro pendrive, etc. En estos casos, si no tenemos copias de nuestra información, las consecuencias pueden ser nefastas. Por ello, es aconsejable realizar copias periódicas de nuestros datos, si es posible en medios locales, aunque también podemos realizar copias de seguridad remotas. En este último caso hay que tomar la precaución en encriptar los archivos.

Podemos realizar esta tarea con Crachplan o SpiderOak, entre otros. Incluso tenemos la posibilidad de configurarlos para que realicen las copias automáticamente sin que siquiera lo notemos.

Una vez que hayamos asimilado todo lo expuesto, seremos conscientes de que cada medida de seguridad que tomamos disminuye riesgos. Una aceptable seguridad en la información pocas veces trata sobre cómo defendernos de ciberataques y de hackers. Se refiere más bien a cómo comprender los motivos y las capacidades de los eventuales atacantes y cómo desarrollar hábitos sobre la base de dichas evaluaciones.

Es necesario tener en claro qué queremos proteger y de qué; pensar en la información que tenemos y los riesgos a los que nos enfrentamos a fin de adoptar recaudos coherentes y

equilibrados. Los riesgos pueden ser básicamente por pérdida, divulgación o interrupciones de servicio. Las herramientas descriptas ayudarán a realizar un trabajo más seguro.

## Bibliografía

**Ifex** (2017) Seguridad digital. Buenas prácticas para periodistas. Recuperado de: https://ifex.org/2017/08/04/digital%20security_best%20practices_sp.pdf

**Lafontaine, D.** (2017) Vocabulario sobre ciberataques que todo periodista debería conocer. Recuperado de: https://ijnet.org/es/blog/vocabulario-sobre-ciberataques-que-todo-periodista-deber%C3%ADa-conocer

**Molano, A.** (2016) La nube es la computadora de alguien más. Recuperado de: https://colombiadigital.net/actualidad/articulos-informativos/item/8742-la-nube-es-la-computadora-de-alguien-mas.html

**Perfil.com** (2017) El caso de Nancy Pazos: cómo actúa un hacker. Recuperado de: http://trends.perfil.com/2017-01-06-3995-el-caso-de-nancy-pazos-como-actua-un-hacker/?utm_campaign=shareaholic

**Ricchiardi, S.** (2017) Recursos y consejos de seguridad digital para periodistas. Recuperado de: https://ijnet.org/es/blog/recursos-y-consejos-de-seguridad-digital-para-periodistas

**Sembramedia.org** (2016) Los ataques cibernéticos están empeorando; ¿estás protegido? Recuperado de: https://www.sembramedia.org/recursos/herramientas-para-periodistas-digitales/seguridad-para-periodistas/

**Warner, J. y Lafontaine, D.** (2017) Los ataques cibernéticos son cada vez peores. ¿Estás protegido? Recuperado de: https://ijnet.org/es/blog/los-ataques-cibern%C3%A9ticos-son-cada-vez-peores-%C2%BFest%C3%A1s-protegido

**WikiLeaks** (2016) CIA Espionage orders for the 2012 French presidential election. Recuperado de: https://wikileaks.org/cia-france-elections-2012/

**WikiLeaks** (2017). Recuperado de: https://web.archive.org/web/20170825003917/https://wikileaks.org/ciav7p1/