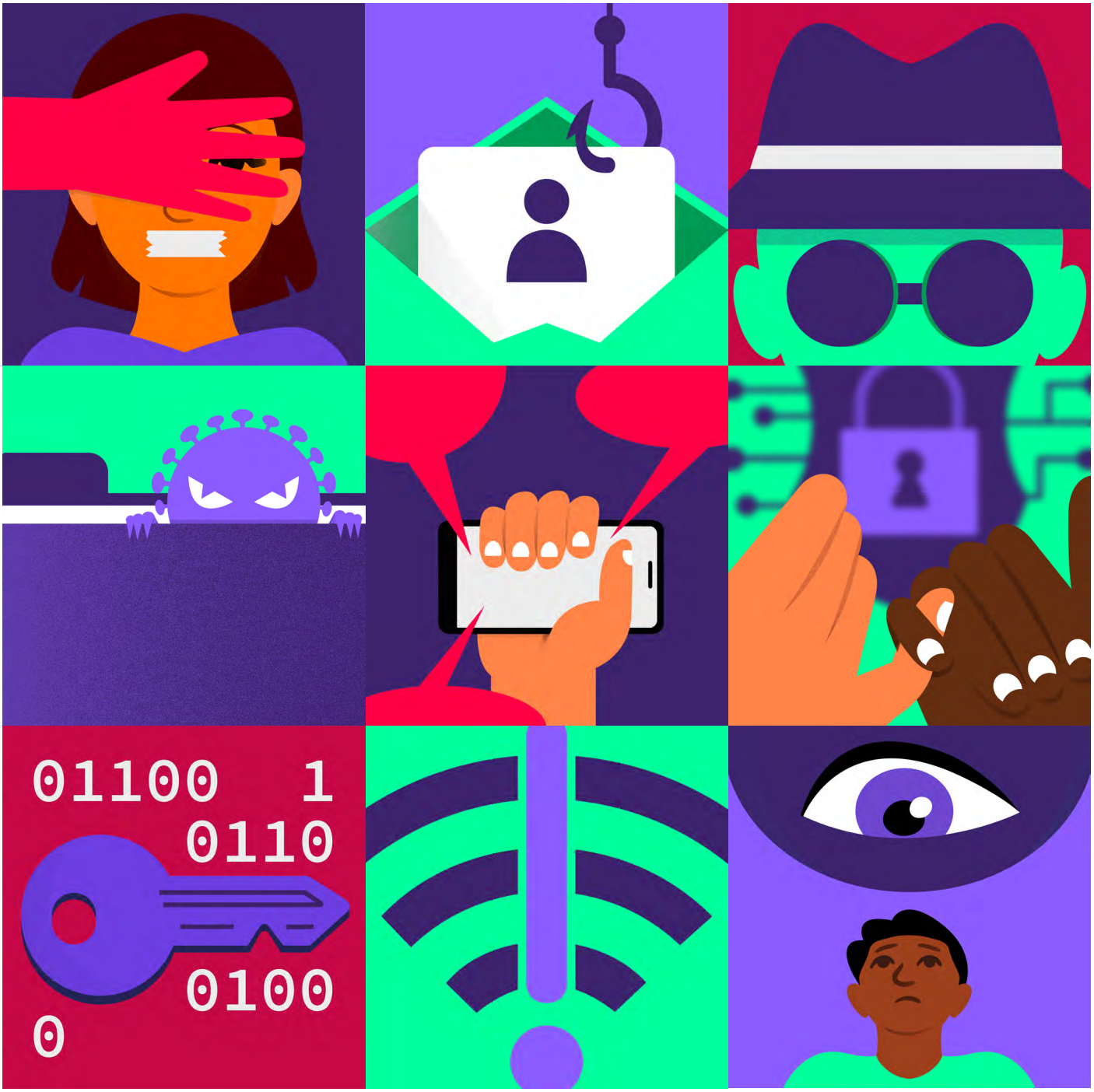
# S.O.S PERIODISTA

## DIRECTRIZ:
## SEGURIDAD DIGITAL PARA COBERTURAS DE ALTO RIESGO EN PARAGUAY




UNA GUÍA PRÁCTICA PARA LA SEGURIDAD DE PERIODISTAS EN PARAGUAY CON ENFOQUE DE GÉNERO E INTERSECCIONALIDAD EN LA LUCHA CONTRA LA VIOLENCIA DIGITAL

Esta directriz fue realizada en el marco del proyecto “Hacia un enfoque feminista de la seguridad de las personas periodistas” con el apoyo del Fondo para la defensa de los medios de UNESCO.

**TEDIC es una organización no gubernamental fundada en el año 2012,**

cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

# Directriz de seguridad digital para coberturas de alto riesgo en Paraguay

Enero 2025

Tecnología & Derechos Humanos TEDIC

unesco

Con el apoyo del Fondo Mundial de la UNESCO para la Defensa de los Medios



**AUTORES**
Maricarmen Sequera • TEDIC
Lupa Alonzo • TEDIC

**COMUNICACIÓN**
Araceli Ramírez

**DISEÑO GRÁFICO**
Ivanna Serratti

**DIAGRAMACIÓN Y ADAPTACIÓN DE DISEÑO**
Horacio Oteiza

**ILUSTRACIÓN**
Manuel Meden

# TABLA DE CONTENIDO

# INTRODUCCIÓN

Los medios libres, independientes y pluralistas juegan un papel fundamental en la defensa de la democracia al informar sobre temas cruciales como la corrupción y el crimen organizado. Para poder cumplir con esta responsabilidad, es esencial que las personas periodistas puedan realizar su labor sin enfrentar amenazas de violencia o intimidación.

**La capacidad de investigar y reportar con libertad es vital para exponer los entramados de corrupción que socavan las instituciones y afectan directamente a la sociedad.**

Sin un entorno seguro para la prensa y medios de comunicación, los esfuerzos por transparentar estas prácticas ilícitas se ven gravemente comprometidos.

A través de su compromiso con la verdad, la ética y el rigor profesional, los y las periodistas investigan y verifican hechos complejos relacionados con el narcotráfico, el lavado de dinero y el crimen organizado. Estos reportes no solo tienen el potencial de revelar la profundidad y el alcance de estas actividades ilegales, sino que también pueden permitir contrastar y verificar las declaraciones de actores involucrados, tanto del sector público como privado. Al exhibir estas redes criminales, el periodismo no solo informa a la ciudadanía, sino que también contribuye a fortalecer el Estado de derecho y promueve la rendición de cuentas en todos los niveles.

Esta directriz tienen como objetivo proporcionar herramientas útiles para que los y las periodistas puedan enfrentar, de manera más segura, contextos de riesgo debido a la presencia de grupos armados o situaciones de violencia. Se plantea que la mejor forma de aproximarse a estos eventos es mediante un análisis cuidadoso del contexto y el establecimiento de relaciones empáticas con la comunidad en la que se trabaja, siempre respetando las particularidades y vulnerabilidades de las víctimas de violencia criminal, a través del diseño y aplicación de un modelo de amenazas.

Las recomendaciones de seguridad digital presentadas en este documento surgen de entrevistas en profundidad realizadas con periodistas de Paraguay que cubren este tipo de eventos. Estas entrevistas permiten responder de manera más adecuada a las amenazas que enfrentan los y las profesionales de la comunicación en contextos de riesgo.

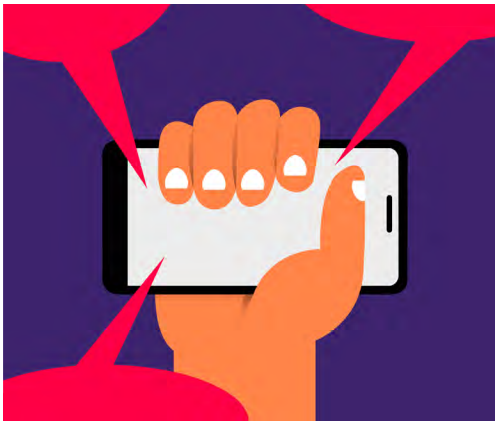
Desde TEDIC se afirma que la seguridad de los y las periodistas, fuentes, organizaciones y medios de comunicación está profundamente interconectada. La protección de la vida de unos asegura la integridad de los demás. Aunque este documento representa un primer esfuerzo para abordar las coberturas periodísticas en contextos de alto riesgo y seguridad digital, su objetivo principal es sentar las bases para que los y las periodistas puedan desarrollar estrategias más seguras y efectivas en el ejercicio de su labor.

# MITOS SOBRE LA SEGURIDAD DIGITAL PARA PERIODISTAS

**MITO**

**"Defendés la privacidad porque tenés algo que ocultar"**

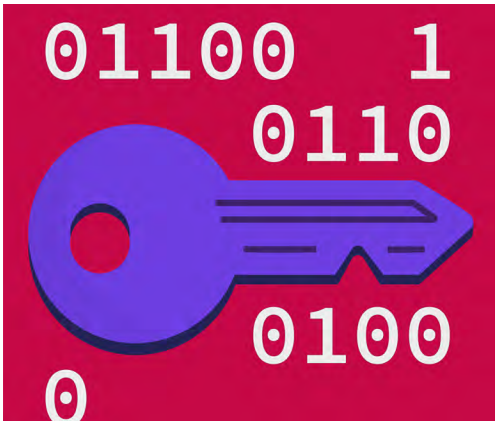
**REALIDAD:** La privacidad no es para quienes "tienen algo que esconder"; es un derecho humano fundamental. Protege nuestra vida privada frente a la injerencia del Estado y otros poderes, y es clave para preservar nuestra identidad e individualidad en relación con los demás.



**MITO**

**"No tengo nada que esconder, ¿por qué debería preocuparme?"**

**REALIDAD:** Incluso la información más básica puede ser utilizada en ataques selectivos, poniendo en riesgo tu seguridad o la de otras personas. La pregunta clave frente a la vigilancia debería ser: "Si no hago nada malo, ¿por qué me están vigilando?"




**MITO**

**"El software de seguridad es suficiente"**

**REALIDAD:** La protección efectiva debe ser integral, abarcando no solo vulnerabilidades digitales, sino también físicas, psicológicas y sociales. Por ejemplo, un periodista que cubre temas de alto riesgo no puede depender únicamente de medidas de seguridad digital; descuidar su salud mental puede provocar consecuencias graves, como estrés crónico o incluso problemas físicos, como la pérdida de cabello. Enfrentar estos riesgos de manera completa y sostenible requiere una mirada holística.

**MITO**

**"Las herramientas gratuitas son suficientes"**

**REALIDAD:** Aunque pueden ser útiles, es fundamental invertir en soluciones de seguridad robustas y confiables que brinden protección frente a riesgos complejos. Más allá de si una herramienta es gratuita o no, lo importante es que sea de código abierto, lo que permite auditorías independientes y reduce el riesgo de vulnerabilidades ocultas o accesos no autorizados.

**MITO**

**"Los teléfonos analógicos son seguros y no pueden ser espiados"**

**REALIDAD:** aunque los teléfonos analógicos no están conectados a Internet y parecen menos vulnerables a los ataques digitales, no son inmunes a la vigilancia. Las llamadas realizadas desde teléfonos analógicos pueden ser interceptadas fácilmente mediante equipos de escucha tradicionales o dispositivos avanzados de vigilancia, como IMSI catcher[1], que capturan señales de celulares cercanos. Además, las comunicaciones no están cifradas, lo que las hace accesibles para actores malintencionados. La protección de las comunicaciones debe incluir tanto tecnología actual como medidas de seguridad apropiadas para cualquier tipo de dispositivo.

1 Es un dispositivo de espionaje telefónico que se utiliza para interceptar el tráfico de teléfonos móviles y rastrear los datos de ubicación de los usuarios de teléfonos móviles.

# PRINCIPIOS GENERALES

## ¿Qué es la privacidad?

La privacidad es un requisito previo para el ejercicio significativo de la libertad de expresión, en particular a través y con el uso de las tecnologías. Sin privacidad, las personas carecen del espacio para pensar y hablar sin intrusiones y para desarrollar su propia voz. En el centro de la protección de este derecho se encuentra el respeto y la protección de la dignidad humana y la capacidad de las personas para vivir libremente y relacionarse entre sí.

En Paraguay este derecho está consagrado en la constitución nacional en su artículo 33:

> *"La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, estará exenta de la autoridad pública. Se garantiza el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas."*

La privacidad no se limita a la ocultación de información, sino que abarca el derecho a decidir cuándo y con qué propósito se comparten ciertos datos. Este concepto implica el control sobre la información personal y la capacidad de gestionar cómo se utiliza, garantizando así que se respete la autonomía y dignidad de todas las personas en un mundo interconectado.

## ¿Qué es la seguridad digital?

La seguridad digital es un enfoque integral que engloba un conjunto de prácticas, herramientas y medidas estratégicas diseñadas para salvaguardar la información y los sistemas tecnológicos frente a incidentes, ataques malintencionados, fallos o uso indebido. Va más allá de simples herramientas tecnológicas: incluye políticas organizacionales, procesos de gestión de riesgos y la educación constante de las personas para mitigar vulnerabilidades. Su objetivo principal es proteger los datos sensibles, garantizar su integridad, confidencialidad y disponibilidad, así como asegurar la continuidad operativa frente a amenazas tanto internas como externas, fomentando una cultura de seguridad proactiva.

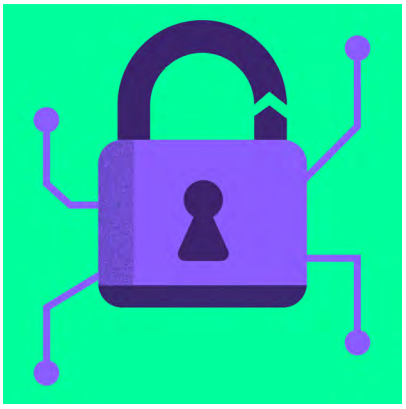
La seguridad digital se fundamenta en la **triada CIA[2]: Confidencialidad, integridad y disponibilidad**, tres pilares esenciales para la protección de cualquier sistema de información. Estos conceptos permiten salvaguardar los datos y garantizar su manejo adecuado:

**a. Confidencialidad:** Se refiere a la protección de la información para que solo los actores autorizados puedan acceder a ella. El objetivo es evitar accesos no autorizados, manteniendo la privacidad de los datos en todo momento, ya sea durante su transmisión o almacenamiento.

**b. Integridad:** Garantiza que la información sea precisa y completa, y que no pueda ser alterada de manera no autorizada o accidental. Mantener la integridad asegura que los datos permanezcan fiables y que cualquier modificación sea rastreable y permitida, protegiendo su validez.

**c. Disponibilidad:** Se enfoca en asegurar que los sistemas, equipos e información estén accesibles para las personas autorizadas siempre que sea necesario. Esto implica evitar interrupciones no planificadas o fallos y asegurar que los recursos estén operativos y protegidos frente a desastres, pérdidas o ataques que comprometan el acceso a la información.

2 Seguridad de la información disponible en: https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Confidencialidad



# AUTOCUIDADO DIGITAL Y SEGURIDAD PERSONAL

El autocuidado digital se refiere a las prácticas que las personas adoptan para proteger su bienestar y seguridad en el entorno digital. Este concepto abarca una variedad de acciones que ayudan a gestionar la exposición a riesgos y a mantener un equilibrio saludable en el uso de la tecnología. Entre estas prácticas se incluyen la configuración de mecanismos de privacidad en redes sociales, el uso de contraseñas seguras y únicas, la activación de la verificación en dos pasos y la educación sobre las amenazas cibernéticas.

El autocuidado siempre se centra en la persona y, aunque presenta ciertas limitaciones, representa un primer paso hacia un enfoque colectivo en la defensa de derechos fundamentales como la privacidad y la libertad de expresión. A través de la práctica del autocuidado, los y las periodistas y otros actores pueden fortalecer su seguridad personal y desarrollar una conciencia crítica sobre las amenazas que enfrentan. Esto, a su vez, sienta las bases para la colaboración en la búsqueda de soluciones colectivas para mitigar los abusos de algunos gobiernos y empresas, que a menudo utilizan la vigilancia y la persecución como herramientas para silenciar a quienes investigan asuntos de interés público. Al unir esfuerzos, es posible construir un entorno más seguro y resistente, donde la comunicación sea verdaderamente segura y los derechos humanos se respeten.

Algunos puntos a tener en cuenta en esta etapa individual:

- **Actualización de programas, tanto en dispositivos móviles como de escritorio.**

  Tanto los programas o aplicaciones como el mismo sistema operativo deben mantenerse actualizados para incorporar las mejoras y corregir las vulnerabilidades de seguridad.

- **Entender cómo funcionan los enlaces de Internet para evitar acceder a enlaces sospechosos o descargar archivos de fuentes no verificadas.**

  Estos pueden llevarnos a páginas fraudulentas o contener malware[3] que podría potencialmente infectar los dispositivos.

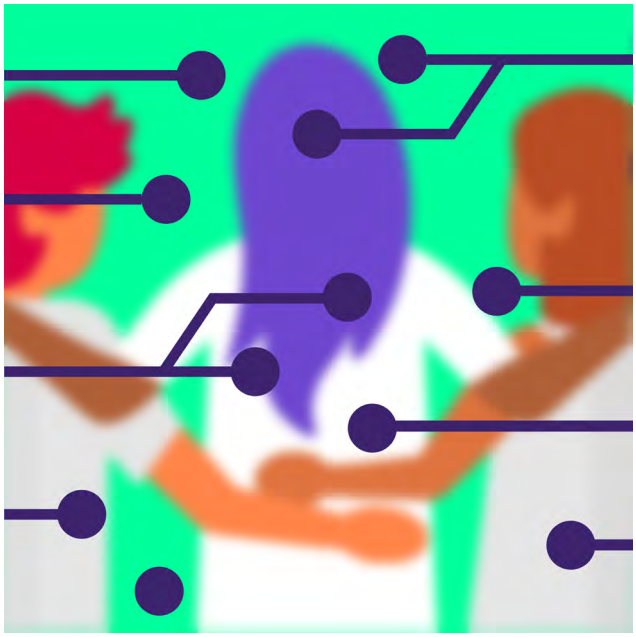
- **Evita conectarte a redes Wi-Fi públicas ya que suelen ser vulnerables a ataques.**

  Es preferible utilizar los propios paquetes de datos móviles. Si se viaja al extranjero, es importante considerar adquirir una tarjeta SIM local para navegar de forma más segura y reducir la exposición de los datos personales. Esto no solo protege la información personal frente a posibles intrusiones en redes abiertas, sino que también limita el acceso del proveedor de servicios de internet (ISP) local (del país de origen) a los hábitos de navegación y uso de datos.

3 Un *malware*, traducido del inglés como programa malicioso, programa maligno, programa malintencionado o código maligno, es cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento de la persona usuaria: https://es.wikipedia.org/wiki/Malware

# CUIDADO COLECTIVO

El enfoque de cuidado colectivo es una forma de enfrentar las opresiones estructurales y violentas que afectan a los y las periodistas. Si bien las herramientas tecnológicas son útiles, no ofrecen una seguridad absoluta ya que pueden en última instancia ser vulneradas cuando existen ataques dirigidos. El verdadero sustento de la protección está en la defensa de derechos. La lucha por la seguridad y la justicia no es una tarea individual, sino colectiva; es mediante la solidaridad y la organización comunitaria que se pueden desafiar las estructuras de poder que buscan silenciar, vigilar o perseguir. Solo a través de una respuesta conjunta podemos hacer frente de manera efectiva a las amenazas a la libertad y a la seguridad.



Algunos puntos a tener en cuenta:

- **Definir colectivamente las herramientas seguras entre tu grupo de amigos, colegas de trabajo y familiares.**

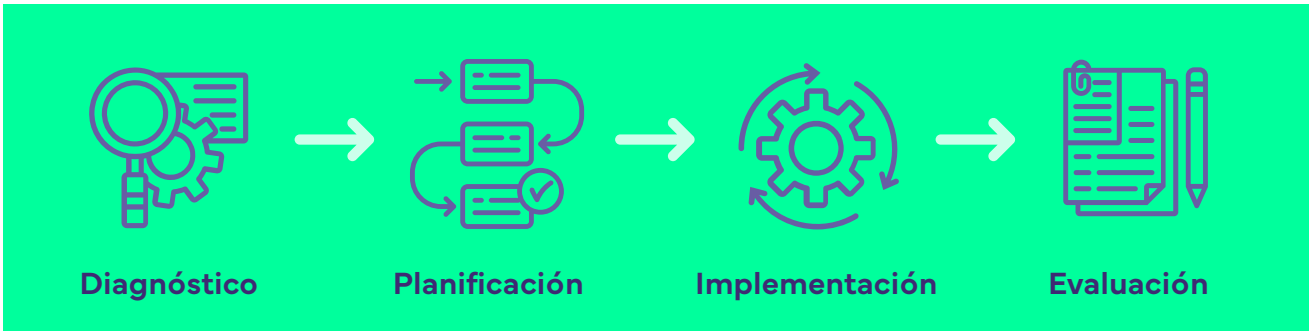
  La protección personal depende también del cuidado que tengan los demás, por lo que es esencial poner este tema en conversación. Por ejemplo, tu familia debe evitar publicar fotos tuyas sin tu consentimiento, especialmente si tu labor periodística cubre temas delicados, ya que esto puede exponerte innecesariamente. Del mismo modo, deben abstenerse de realizar llamadas sin cifrado o de compartir tu ubicación sin precaución. La conciencia sobre la seguridad debe ser constante y compartida.

- **Publicar fotos o imágenes solo después de que las actividades hayan concluido, evitando compartir información en tiempo real.**

  Esto ayuda a minimizar el riesgo de restreo y reduce la posibilidad de sufrir doxing[4], una práctica que puede comprometer gravemente la seguridad de las y los periodistas. Es importante mantener un margen de tiempo en la divulgación de contenido, y proteger tu ubicación y movimientos, preservando así tu integridad y la de quienes te rodean.

4 Describen el acto de revelar intencional y públicamente información personal sobre un individuo u organización, generalmente a través de Internet.

# PROTOCOLO DE SEGURIDAD




El protocolo de seguridad es un plan estructurado que define los mecanismos y procedimientos necesarios para prevenir y enfrentar amenazas a la seguridad de una persona o grupo. Este documento es importante para establecer un marco de acción claro y coherente, que permita a equipos y personas responder de manera efectiva ante situaciones de riesgo.

La seguridad digital implica comprender tres conceptos clave: **amenazas**, **vulnerabilidades** y **riesgos**. Las amenazas son eventos o circunstancias que pueden perjudicar los recursos críticos de una organización o persona, incluyendo desde ataques digitales a desastres naturales. Las **vulnerabilidades** son debilidades en sistemas o procesos que pueden ser explotadas por estas amenazas y su identificación es crucial para reducir riesgos. Por otro lado, los **riesgos** son la combinación de la probabilidad de que una amenaza ocurra y el impacto que tendría sobre los activos en caso de un incidente.

El análisis de los riesgos es un proceso que permite identificar y evaluar los riesgos asociados con amenazas digitales, considerando la identificación de activos valiosos y la evaluación de vulnerabilidades. Este proceso se complementa con el modelado de amenazas, que ayuda a comprender cómo los atacantes pueden comprometer la seguridad.

El ciclo de análisis de riesgos y modelado de amenazas incluye diversas actividades, como identificar activos críticos, evaluar posibles amenazas, así como calcular el impacto y la probabilidad de que ocurran incidentes. Las estrategias para gestionar riesgos pueden incluir la mitigación, transferencia, aceptación y evitación de riesgos, permitiendo monitorizar y revisar continuamente la eficacia de las medidas implementadas. En conjunto, estos elementos permiten crear un entorno más seguro y proteger la información y los sistemas contra posibles incidentes[5].

| AMENAZA | ADVERSARIO | VULNERABILIDADES | CAPACIDADES ACTUALES | CAPACIDADES REQUERIDAS | PROBABILIDAD | IMPACTO | RIESGO |
|---|---|---|---|---|---|---|---|
| Filtración de información sensible | Delicuente común | Mala protección de repositorio institucional | Repositorio con contraseña | Activar 2FA | Media | Alto | 🟢 |
| Filtración de información sensible | Empleado/a | Entorno mafioso | Repositorio con contraseña | Detectar quien filtra, recolectar evidencia y realizar denuncia penal | Media | Alto | 🟢 |
| Robo de celular | Delincuente común | Ciudad insegura | Realizar respaldos | Precaución de no salir tarde o sola de la oficina | Alta | Medio | 🟢 |
| Robo de celular | Delincuente contratado | Entorno mafioso | Realizar respaldos | N/C | Alta | Alto | 🟡 |
| Captura de información en wifi pública | Policía | No uso de cifrado | Utilizar https en la navegación y apps seguras | Tener una política de uso de redes públicas. Usar VPN | Alta | Alto | 🟡 |
| Retención de celular | Policía | Sin cifrado o bloqueo | Bloqueo o apagado de dispositivo | Cifrado completo de dispositivo | Alta | Catastrófico | 🔴 |
| Escucha telefónica (red móvil) | Delincuente contratado | Usar redes inseguras como la red móvil (SMS y llamada tradicional) | Usar Signal o Whatsapp | Análisis forense del dispositivo para descartar infección | Media | Catastrófico | 🟡 |
| Perfilamiento que Google hace a través de G Forms, Docs u otros | Google | Usar corporaciones para depositar información institucional | Usar otros mecanismos si es posible | Tener un mejor sistema de formularios para que la gente no quiera usar Google | Muy alta | Bajo | 🟢 |

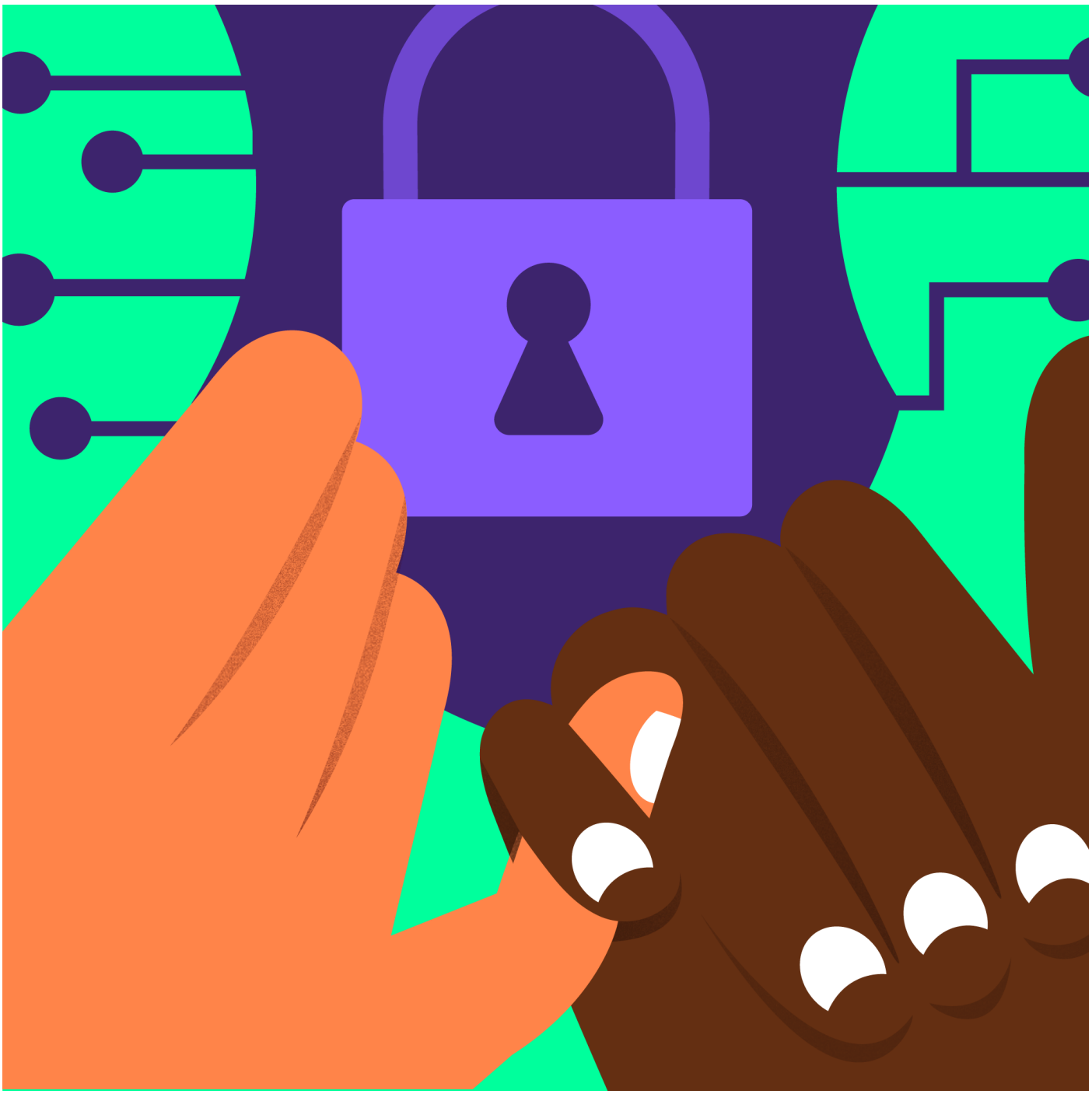
5 Artículo 19. Breve guía para hacer un protocolo de seguridad. https://seguridadintegral.articulo19.org/wp-content/uploads/2020/11/art19_2020_infografia-ProtocoloSeguridad-1.pdf

# PLANIFICACIÓN PARA LA SEGURIDAD

Es esencial que las y los periodistas identifiquen qué activos desean proteger y los riesgos a los que están expuestos. Los activos pueden incluir datos personales, archivos de trabajo y la información de sus fuentes, mientras que los riesgos pueden abarcar la pérdida de datos, divulgación no autorizada y la interrupción de conexiones de red. En este contexto, es fundamental reflexionar sobre qué información es crucial para realizar su trabajo y qué datos podrían poner en peligro a sus fuentes si se divulgan. Por ejemplo, la información de contacto de fuentes en un país hostil puede generar consecuencias graves si se filtra. Además, es importante considerar las herramientas técnicas que utilizan diariamente y cómo las interrupciones en estas herramientas pueden afectar su capacidad para trabajar eficientemente. Llevar un registro de los recursos utilizados puede ser útil para mantener un control sobre lo que necesitan proteger.

Al planificar su seguridad, las y los periodistas deben ser conscientes de las posibles amenazas que pueden ir desde fallos técnicos, como el fallo de un disco duro, hasta ataques maliciosos por parte de actores interesados en interrumpir su trabajo. Identificar quiénes pueden desear interrumpir su labor y cuáles son sus motivaciones es fundamental. Esto incluye considerar tanto a actores estatales como a personas que pueden percibir el periodismo independiente como una amenaza. A medida que se desarrollan estrategias de seguridad, es recomendable adoptar herramientas y prácticas simples que sean fáciles de utilizar, ya que los sistemas tecnológicos complejos pueden ser difíciles de entender y provocar más problemas que soluciones. Con un enfoque claro y una comprensión de los riesgos, las y los periodistas pueden establecer medidas efectivas para proteger su información y continuar su labor con mayor seguridad y autonomía.

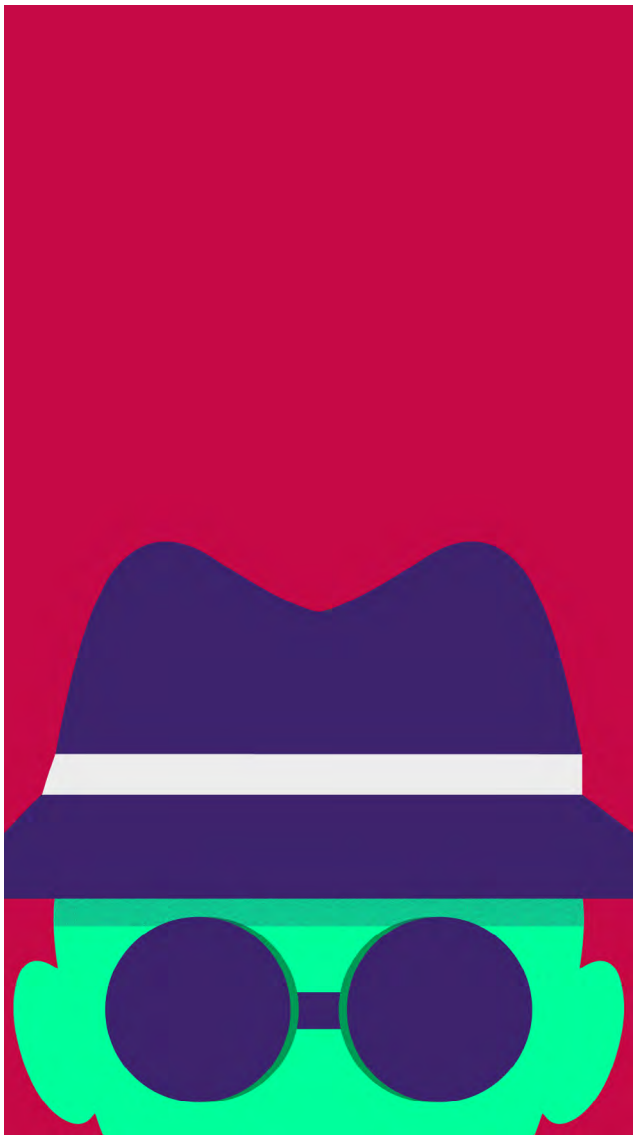
# BUENAS PRÁCTICAS EN SEGURIDAD DIGITAL



# 1 PROTECCIÓN DE FUENTES Y PERSONAS COLABORADORAS

## 1.1 ANONIMATO DE LAS FUENTES

Cuando registres imágenes potencialmente delicadas para su distribución pública, es importante que consideres la información sensible que podrías estar compartiendo. Si una persona es identificable en una fotografía de una manifestación, esto podría ponerla en peligro. Además, si alguien accede a los metadatos de las fotos que compartes, podrían identificarte a ti también.



El anonimato es una herramienta de protección y hay algunas aplicaciones móviles que pueden ayudar en ello:

- **ObscuraCam**[6] para difuminar los rostros de las personas que aparezcan en tus fotos.
- **Scrambled Exif**[7] para eliminar los metadatos de tus imágenes.

Para medios de comunicación y organizaciones que buscan recibir denuncias anónimas se sugieren sistemas más complejos pero seguros para la comunicación con sus fuentes y documentos clasificados.

- **SecureDrop**[8] es un sistema de código abierto para la presentación de denuncias que los medios de comunicación pueden instalar para aceptar de forma segura documentos de fuentes anónimas. Está disponible en 22 idiomas.
- **GlobalLeaks**[9] es una herramienta de código abierto que al igual que SecureDrop, se utiliza para enviar documentación cifrada y confidencial de las fuentes anónimas.

6 ObscuraCam. https://play.google.com/store/apps/details?id=org.witness.sscphase1&hl=en-US
7 Scramble Exif. https://play.google.com/store/apps/details?id=com.jarsilio.android.scrambledeggsif&hl=en-US
8 Securedrop. https://securedrop.org/
9 Globalleaks: https://www.globaleaks.org/

# 1.2 GESTIÓN DE INFORMACIÓN SENSIBLE

Establecer una directriz para el manejo seguro de la información proporcionada por las fuentes es esencial para que los periodistas puedan gestionar datos sensibles con mayor seguridad, minimizando el riesgo de filtraciones, ya sean accidentales o intencionadas. Con estas pautas, se protege tanto la confidencialidad de las fuentes como la integridad del trabajo periodístico.

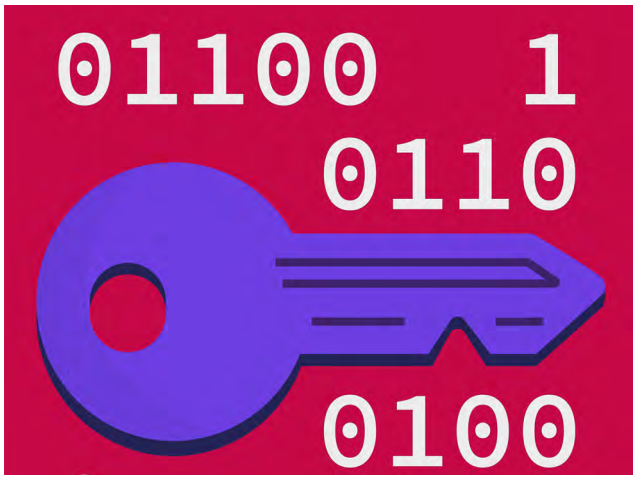
**1. Clasificación de la información:** Antes de almacenar o compartir cualquier información, se debe clasificar según su nivel de sensibilidad (por ejemplo, pública, confidencial, o altamente confidencial). Esto ayudará a determinar las medidas de protección necesarias.

**2. Cifrado de datos:** Utiliza cifrado para proteger la información sensible, tanto en tránsito como en reposo. Asegúrate de que cualquier archivo, documento o comunicación que contenga datos sensibles esté cifrado para protegerlo de accesos no autorizados.

**3. Acceso controlado:** Limita el acceso a la información sensible solo a aquellas personas del equipo que realmente lo necesiten. Utiliza contraseñas fuertes y autenticación de dos factores para proteger las cuentas que acceden a esta información.

**4. Capacitación del personal:** Proporciona capacitación regular al equipo sobre la importancia de la seguridad de la información y las mejores prácticas para manejar datos sensibles. Asegurarse de que todas las personas comprendan las implicaciones de una posible filtración.

**5. Uso de canales seguros:** Siempre que sea posible, utiliza aplicaciones y plataformas de comunicación que ofrezcan cifrado de extremo a extremo para intercambiar información sensible. Esto incluye mensajería, correo electrónico y almacenamiento en la nube. Ten cuidado que cifrado a secas o cifrado en el transporte no son suficientes para las comunicaciones, es necesario cifrado de extremo a extremo.




**6. Revisiones de seguridad:** Realiza auditorías periódicas de seguridad para evaluar la efectividad de las medidas implementadas y realizar ajustes según sea necesario. Esto también incluye verificar la configuración de privacidad y seguridad de las herramientas utilizadas.

**7. Destrucción segura:** Almacena información sensible solo el tiempo necesario y destrúyela de manera segura cuando ya no sea necesaria. Esto puede incluir borrar archivos de forma permanente y deshacerse de documentos físicos de manera que no puedan ser reconstruidos.

**8. Protocolos de respuesta a incidentes:** Establece un protocolo claro para manejar incidentes de seguridad, incluyendo filtraciones accidentales o intencionadas. Esto debe incluir cómo notificar a las fuentes afectadas y tomar medidas para mitigar el daño.

**9. Conservación de registros:** Mantén un registro de todas las interacciones con las fuentes y la información que se comparte, para poder rastrear el origen de cualquier posible filtración y tomar medidas correctivas.

**10. Consentimiento informado:** Siempre que sea posible, obtén el consentimiento informado de las fuentes antes de utilizar su información, explicando cómo se manejará y protegerán su datos. Esto fomenta la confianza y puede ayudar a mitigar preocupaciones sobre la privacidad.

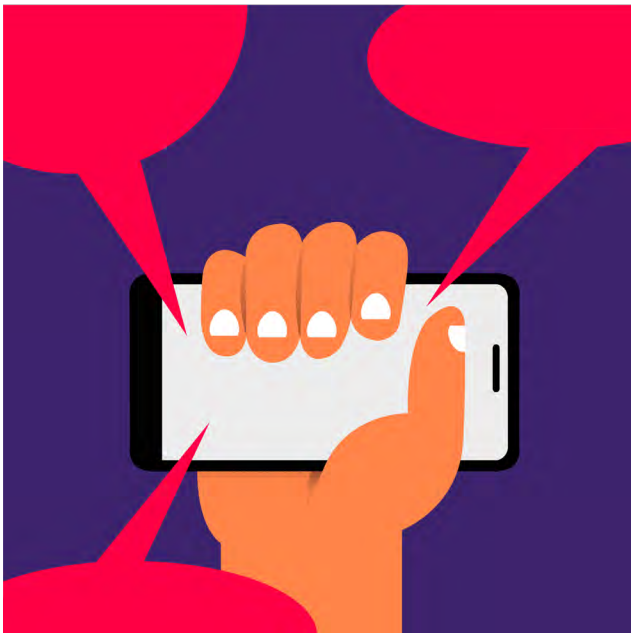
# 2 PROTECCIÓN CONTRA LA VIGILANCIA A PERIODISTAS

## 2.1 VIGILANCIA ESTATAL

Desde 2015, TEDIC se ha dedicado a documentar de manera exhaustiva la vigilancia de las comunicaciones en Paraguay[10], analizando no solo las adquisiciones de software de espionaje por parte del Estado y empresas, sino también las normativas que respaldan estas prácticas. Este trabajo revela un patrón preocupante de vigilancia masiva que en muchas ocasiones, resulta desproporcionada e innecesaria, afectando gravemente la privacidad y los derechos fundamentales de las personas. La labor de TEDIC pone de manifiesto la necesidad de un debate crítico sobre la justificación de estas medidas, y proporciona un contexto valioso para periodistas en el país, en un contexto donde la tecnología puede ser utilizada para controlar y silenciar voces disidentes.

Dada la creciente preocupación por la vigilancia de las comunicaciones, se presentan a continuación una serie de recomendaciones destinadas a fortalecer la seguridad de la comunicación de los periodistas con su entorno, que incluye fuentes, colegas, familiares y amigos. Estas sugerencias buscan crear un entorno más seguro y protegido para el intercambio de información sensible, garantizando así la confidencialidad y la integridad de las conversaciones en un contexto donde la privacidad es cada vez más vulnerable.

10 TEDIC. (2015) Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay. https://www.tedic.org/vigilancia-estatal-de-las-comunicaciones-y-derechos-fundamentales-en-paraguay/



### 2.1.1 Adquisición de dispositivos

Es fundamental que los periodistas adquieran sus dispositivos de manera segura y responsable, para evitar riesgos asociados con equipos comprometidos. El hardware, ya sea computadoras, teléfonos o dispositivos de almacenamiento, debe ser proporcionado por el medio de comunicación, el cual debe asegurarse de que hayan sido previamente analizados y sean seguros para su uso. Es fundamental que los y las periodistas eviten aceptar regalos o equipos de terceros, incluidas empresas, organizaciones o personas externas, ya que estos dispositivos podrían estar comprometidos o ser vulnerables a ataques. En caso de que la compra del equipo sea personal, el periodista debe tomar precauciones adicionales, como adquirirlo de fuentes confiables, asegurarse de que el hardware no esté alterado, y realizar análisis de seguridad antes de su uso.

### 2.1.2 Gestión de contraseñas

La gestión adecuada de contraseñas es fundamental para proteger la información sensible y las cuentas de las periodistas, especialmente ante el aumento de amenazas cibernéticas. Para comenzar, es fundamental crear contraseñas fuertes y complejas que incluyan una combinación de letras mayúsculas y minúsculas, números y símbolos, evitando palabras comunes o información fácilmente accesible. Una buena práctica es utilizar frases de paso, que son combinaciones de palabras largas y aleatorias, ya que son más seguras y fáciles de recordar. Además es importante no reutilizar contraseñas en diferentes cuentas, ya que si una contraseña se ve comprometida, todas las cuentas que la utilizan corren riesgo. Para reforzar la seguridad, se debe activar el doble factor de autenticación (2FA) siempre que sea posible, añadiendo una capa extra de protección (ver apartado siguiente).

El almacenamiento seguro de las contraseñas es vital, por ello se recomienda utilizar un gestor de contraseñas. **Bitwarden**[11], un gestor de contraseñas de código abierto, permite almacenar y sincronizar contraseñas de manera segura en múltiples dispositivos, ofreciendo cifrado de extremo a extremo y facilidad de uso. Cabe aclarar que algunos expertos en seguridad no recomiendan tener una base de contraseñas online.

Por otro lado, **KeePassXC**[12] es una opción excelente que almacena las contraseñas de forma local en el dispositivo, eliminando la necesidad de depender de servicios en la nube y garantizando un fuerte cifrado.

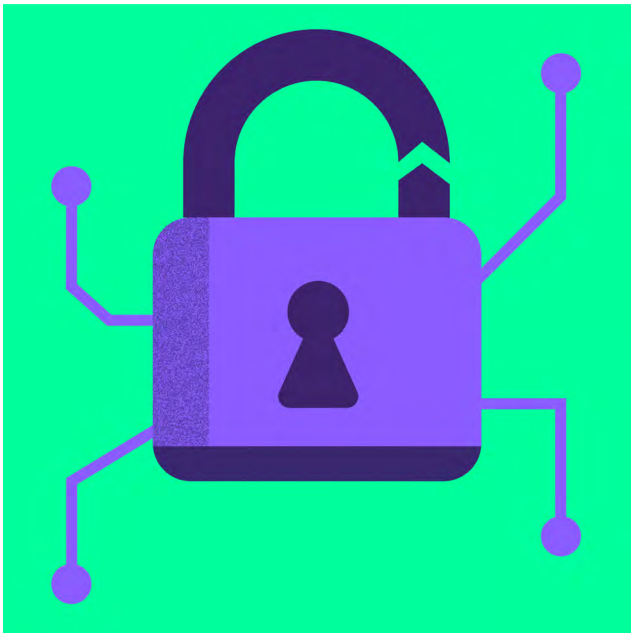
Además, es importante cambiar las contraseñas regularmente, especialmente para cuentas que manejan información sensible. Por último, la educación continua sobre las mejores prácticas en seguridad de contraseñas y nuevas amenazas es fundamental para adaptarse al panorama en evolución de la ciberseguridad. Al seguir estas directrices y utilizar herramientas efectivas como Bitwarden o KeePassXC, las y los periodistas pueden gestionar sus contraseñas de manera segura y proteger su información y la de sus fuentes en un entorno digital cada vez más peligroso.

11 Bitwarden: https://bitwarden.com/
12 KeePassXC: https://keepassxc.org/

### 2.1.3 Verificación de dos pasos

La "verificación en dos pasos" o "doble factor de autenticación" (2FA) es una medida de seguridad que añade una capa adicional de protección a tu cuenta. Esta segunda clave se requiere cuando se intenta acceder desde una ubicación o dispositivo no habituales. Generalmente se utiliza el teléfono móvil como forma de verificación, aunque también existen otras alternativas. Su principal utilidad radica en confirmar que la persona que intenta ingresar a la cuenta es quien dice ser, especialmente en situaciones inusuales. Sin embargo, si elegís recibir el código a través de un mensaje de texto o una llamada, existe el riesgo de quedarte sin acceso si pierdes tu teléfono o si te encuentras en un país donde no puedes conectarte a la red de telefonía móvil.

- Verificación de dos pasos en Instagram[13]
- Verificación de dos pasos en Facebook[14]
- Verificación de dos pasos en X[15]
- Verificación de dos pasos en Google/Gmail[16]



13 Instagram. https://www.facebook.com/help/instagram/566810106808145
14 Facebook: https://www.facebook.com/help/148233965247823
15 X (ex twitter): https://help.twitter.com/es/managing-your-account/two-factor-authentication
16 Google: https://www.google.com/landing/2step

### 2.1.4 Doble factor de autenticación basado en códigos temporales

El doble factor de autenticación (2FA) mediante códigos temporales se basa en una aplicación que se instala en el teléfono móvil y funciona como segunda verificación además de la contraseña. Cuando una persona intenta acceder a su cuenta, primero ingresa su contraseña y luego debe introducir un código que se genera en su propio teléfono y cambia cada minuto. Esto reduce significativamente el riesgo de acceso no autorizado, ya que incluso si un atacante obtiene la contraseña, necesitará también el código temporal para ingresar. Existen muchas aplicaciones que brindan esta funcionalidad y continuación te recomendamos un par:

#### Aegis para Android

Aegis[17] se destaca por su enfoque en la seguridad y facilidad de uso. Por cada plataforma que se vincula, generará los códigos temporales de manera local en el dispositivo, utilizando cifrado fuerte para proteger esta información. La aplicación es de código abierto y permite realizar copias de seguridad cifradas, lo que es ideal para usuarios que buscan una solución segura y confiable para gestionar sus códigos de autenticación.

Vale aclarar que este método es "local" por lo que si se pierde el dispositivo habrá que asegurar una forma de recuperación, sea a través de las claves de configuración de TOTP o de un respaldo.

#### 2FAS para IOS

Para usuarios de iPhone, 2FAS[18] es una buena alternativa para gestionar la autenticación de dos factores. Esta aplicación al igual que Aegis, permite configurar los códigos para cada plataforma y ofrece la opción de realizar respaldos de los accesos al iCloud, para el caso en que se pierda el dispositivo.

17 Aegis Authenticator https://getaegis.app/
18 2FAS: https://2fas.com/

### 2.1.5 Cifrado de las comunicaciones

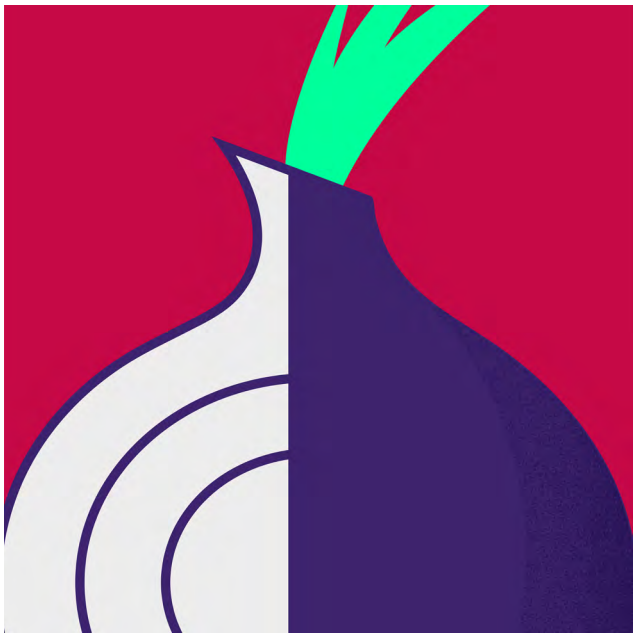
El cifrado es la única forma de garantizar el derecho a la privacidad y el ejercicio pleno de la libertad de expresión en el ámbito digital, especialmente en el caso de periodistas que cubren temas sensibles o de alto riesgo. En el caso de las comunicaciones hay que utilizar de extremo a extremo (E2E), lo que asegura que un mensaje esté protegido desde el momento en que sale del dispositivo hasta que llega a su destinatario, convirtiéndolo en un formato ilegible para cualquier tercero que logre interceptarlo (incluso en los servidores de la plataforma que corresponda). Solo la persona receptora puede restaurar el mensaje a su formato original y darle sentido.

Sin embargo, aunque el cifrado E2E protege el contenido de los mensajes, la información asociada a las comunicaciones, habitualmente llamados metadatos pueden exponer detalles que hagan identificable al periodista o su fuente. Esto es especialmente preocupante en contextos donde la vigilancia y la monitorización digital son utilizados como herramientas de control o represión.

Por ello, es fundamental complementar el uso de cifrado, con otras medidas de protección, como la ofuscación de metadatos, el uso de redes privadas virtuales (VPN), redes de anonimización como TOR y la adopción de buenas prácticas en la gestión de dispositivos. Al combinar estas herramientas, los periodistas pueden fortalecer su resiliencia frente a vulnerabilidades y proteger no solo su trabajo, sino también su integridad personal y la de sus fuentes, resguardando su derecho a la privacidad en un entorno cada vez más expuesto a amenazas.

#### ■ TOR

TOR es una red de anonimato[19] que permite a las personas navegar por Internet de manera privada y segura, ocultando su ubicación, al encriptar el tráfico en múltiples capas y dirigir la conexión a través de una serie de nodos distribuidos por todo el mundo. Para los periodistas, TOR es una herramienta valiosa, especialmente cuando trabajan en entornos donde la vigilancia, la censura y la represión son comunes. Al utilizar TOR, los periodistas pueden acceder a información, realizar investigaciones, comunicarse con fuentes y publicar



contenidos sin revelar su identidad o ubicación, lo que es crucial cuando se enfrentan a gobiernos autoritarios o actores que buscan limitar la libertad de expresión.

Además es una herramienta clave para proteger la confidencialidad de las comunicaciones con fuentes sensibles o denunciantes, ya que previene que terceros rastreen las actividades en línea o intercepten el tráfico de datos. Esto es especialmente importante en la cobertura de temas delicados o en la obtención de información en países con restricciones al acceso a Internet. En resumen, TOR ofrece a los periodistas una capa adicional de seguridad, protegiendo su privacidad y fortaleciendo su capacidad para investigar y reportar sin temor a ser vigilados o expuestos.

TOR presenta varias ventajas en comparación con las VPNs (redes privadas virtuales). Una de las principales ventajas es su enfoque en el enmascaramiento de la identidad; mientras que una VPN puede ocultar la dirección IP del usuario y cifrar el tráfico de datos hacia un servidor específico, TOR distribuye el tráfico a través de múltiples nodos en su red, lo que hace que sea extremadamente difícil rastrear el origen de la conexión. Esta estructura en capas, donde cada nodo solo conoce la ubicación del nodo anterior y el siguiente, proporciona un nivel de anonimato superior.

19 Web del proyecto TOR: https://www.torproject.org/download/

Otra ventaja de TOR es que es completamente gratuito y de código abierto, lo que significa que su funcionamiento y seguridad pueden ser auditados por la comunidad. Esto contrasta con muchas VPNs, que pueden tener costos asociados y en algunos casos políticas de privacidad poco claras que podrían comprometer la información de las personas. Además, TOR permite el acceso a la "deep web", donde se pueden encontrar recursos e información que no están disponibles a través de navegadores convencionales, lo cual es especialmente útil para la investigación periodística.

Sin embargo, es importante tener en cuenta que, a diferencia de muchas VPNs que pueden ofrecer velocidades de conexión más rápidas, la navegación usando TOR puede ser más lenta debido a la forma en que redirige el tráfico. A pesar de esto, para periodistas y otras personas que priorizan la privacidad y el anonimato, las ventajas de TOR lo convierten en una herramienta muy valiosa en un entorno digital cada vez más vigilado.

### Mensajería y video llamadas cifradas

La mensajería y las video llamadas cifradas de extremo a extremo (E2E) son herramientas esenciales para garantizar la privacidad y la seguridad en la comunicación digital, especialmente para quienes trabajan en entornos de alto riesgo, como las y los periodistas. Este tipo de cifrado asegura que solo el remitente y el destinatario puedan acceder al contenido de los mensajes o las llamadas, impidiendo que terceros, incluidos proveedores de servicios y potenciales atacantes, intercepten o descifren la información transmitida. Plataformas como **Signal**[20], **Matrix/Element**[21] y **WhatsApp**[22] utilizan este enfoque, lo que no solo protege el contenido de las conversaciones, sino que también refuerza la confianza entre los comunicadores, permitiendo un intercambio de información más abierto y seguro.

Además, la implementación de este tipo de cifrado minimiza el riesgo de vigilancia y represalias, lo que resulta fundamental para quienes comparten información sensible o dependen de la confidencialidad para la protección de sus fuentes. En un mundo donde las amenazas a la privacidad son cada vez más comunes, la mensajería y las video llamadas cifradas E2E son herramientas indispensables para salvaguardar la libertad de expresión y la integridad de las comunicaciones.

A continuación brindamos algunos elementos sobre seguridad y protección digital para algunas aplicaciones de mensajería:

#### WHATSAPP

1. **Mensajes que desaparecen:** activa la opción de mensajes que desaparecen que provoca que los mensajes se autodestruyan después de cierto tiempo. Esto es útil para asegurar que la información sensible no quede almacenada indefinidamente.

▶ **Para activar:** abre un chat, toca el nombre del contacto o grupo, selecciona "Mensajes que desaparecen" y elige por ejemplo "24 horas".

2. **Privacidad de la cuenta:** configura la privacidad para que tu foto de perfil, estado y última vez en línea no sean visibles para personas que no están en tu lista de contactos.

▶ **Para activar:** ve a "Configuración" > "Cuenta" > "Privacidad" y ajusta la visibilidad de cada opción.

3. **Mensajes de un solo uso:** Utiliza la función de mensajes que desaparecen para enviar fotos, videos o audio que se autodestruyen después de ser vistos. Esto es útil para información confidencial que no debe ser almacenada, sin embargo debes tener en cuenta que no evita que la otra persona utilice diversas técnicas para almacenarla de todos modos.

▶ **Para activar:** Envía una foto o video y toca el ícono de "1" antes de enviarlo.

20 Signal: https://signal.org/
21 Element: https://element.io/
22 WhatsApp: https://www.whatsapp.com/download

## SIGNAL

**1. Mensajes que desaparecen:** activa la opción de mensajes que desaparecen en Signal para que tus mensajes se autodestruyan después de cierto período de tiempo (por ejemplo, 24 horas).

▶ **Para activar:** abre un chat, toca el nombre del contacto y selecciona "Mensajes que desaparecen", luego elige la duración.

**2. Configuración de privacidad:** configura tu perfil para que solo tus contactos puedan ver tu foto de perfil y tu estado.

▶ **Para activar:** ve a "Configuración" > "Privacidad" y ajusta la visibilidad de tu perfil.

**3. Autodestrucción de medios:** en Signal, puedes enviar fotos y videos que se pueden ver una sola vez antes de autodestruirse, lo que es ideal para compartir información sensible.

▶ **Para activar:** envía un archivo de medios y selecciona la opción "Ver una vez" antes de enviarlo.

**4. Chatea sin exponer tu número de teléfono:** Signal ha incorporado la posibilidad de crear chats o conversaciones sin necesidad de brindar tu número de teléfono o requerir el de la otra persona. Esto es especialmente útil cuando es necesario proteger las identidades.

▶ **Para activar:** abre tu perfil en Signal y crea o edita un alias. Luego le entregas esa información a tu contraparte para que puedan conversar de forma segura.

## MATRIX/ELEMENT

Element es una plataforma de mensajería y colaboración que se basa en el protocolo Matrix, diseñado para ofrecer comunicación segura y descentralizada. Algunas de sus características más destacadas son:

**1. Cifrado de extremo a extremo:** Matrix/Element ofrece cifrado E2E de forma predeterminada, lo que garantiza que solo los participantes de una conversación pueden acceder al contenido de los mensajes. Esto es especialmente valioso para periodistas que manejan información sensible o confidencial.

**2. Interoperabilidad:** al estar basado en el protocolo Matrix, Element permite la interoperabilidad con otras aplicaciones y redes de mensajería que también utilizan este protocolo. Esto facilita la comunicación entre diferentes plataformas y aumenta la flexibilidad para los usuarios.

**3. Descentralización:** Matrix/Element se puede alojar en servidores propios o utilizar servidores públicos, lo que otorga a los usuarios más control sobre sus datos y la privacidad de sus comunicaciones. Esto es crucial para quienes desean evitar la vigilancia centralizada que puede ocurrir en otras plataformas.

**4. Funciones avanzadas:** además de mensajería, Matrix/Element ofrece funciones como video llamadas, intercambio de archivos, y la posibilidad de crear salas ilimitadas de chat públicas o privadas que a su vez se pueden agrupar en "espacios". Estas características son útiles para el trabajo colaborativo en equipos de periodistas.

**5. Código abierto:** Matrix/Element son plataformas de código abierto, lo que permite que la comunidad revise y mejore el software. Esto también brinda mayor transparencia respecto a la seguridad y la privacidad, ya que cualquier persona puede auditar el código.

## TELEGRAM

**Telegram[23] no ofrece cifrado de extremo a extremo de forma predeterminada en todos sus chats**, lo que limita significativamente su seguridad y privacidad. En los chats regulares, la información es cifrada en tránsito, pero puede ser accesible en los servidores de Telegram, lo que representa un riesgo si esos servidores son comprometidos. Lo mismo ocurre en los grupos. Esto contrasta con el cifrado E2E, donde solo el remitente y el destinatario tienen la clave para descifrar los mensajes.

Sin embargo, Telegram sí ofrece una opción de cifrado E2E en sus "chats secretos". En estos chats, los mensajes están protegidos de tal manera que ni siquiera Telegram puede acceder a ellos. No obstante, los usuarios deben iniciar manualmente un chat secreto para beneficiarse de esta función, lo que significa que la mayoría de las conversaciones no estarán tan protegidas de forma predeterminada. Además, los chats secretos no permiten la sincronización entre dispositivos, lo que puede ser una desventaja. Por lo tanto, quienes busquen un alto nivel de privacidad deben ser conscientes de estas limitaciones y considerar alternativas que ofrezcan cifrado de extremo a extremo en todas las conversaciones.

## CORREO CIFRADO E2E

Es posible utilizar correo E2E con casi cualquier plataforma de correos. El problema de este sistema es que requiere que la contraparte también realice el proceso de configuración y luego el intercambio de claves criptográficas se realiza de forma manual.

Para plataformas web como Gmail, existen herramientas Mailvelope[24] o FlowCrypt[25] que permiten habilitar ese tipo de configuración.

Por otra parte si utilizas el cliente Thunderbird[26], con cualquier proveedor de correo electrónico, puedes habilitar el cifrado E2E a través de OpenPGP[27] que ya viene incluido. Sin embargo ocurre lo que ya mencionamos anteriormente, que la contraparte debe configurar también su E2E y luego realizar manualmente el intercambio de claves de cifrado.

23 Telegram: https://desktop.telegram.org/

24 Mailvelope: https://mailvelope.com/
25 FlowCrypt: https://flowcrypt.com/
26 Thunderbird: https://www.thunderbird.net/es-ES/
27 OpenPGP: https://www.openpgp.org/

### 2.1.6 Sincronización remota

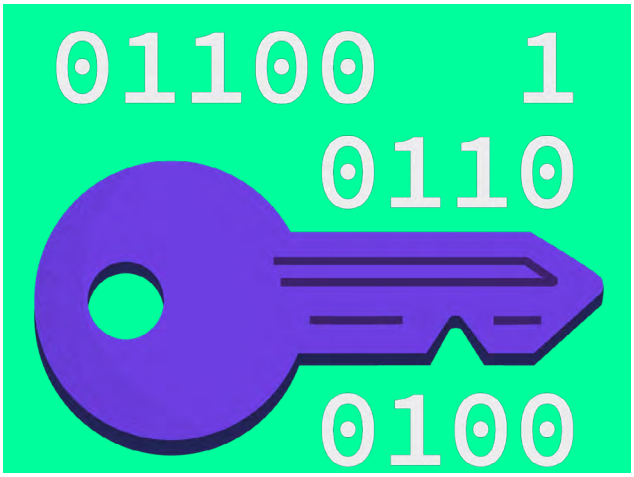
Realizar copias de seguridad remotas, en las que tus archivos locales se copian regularmente a un servidor remoto, es una práctica altamente recomendable para proteger tu información, especialmente en el ámbito periodístico, donde la pérdida de datos puede ser crítica. Este método te permite recuperar tu información en caso de que pierdas el acceso a tu máquina local. Aquí hay varios enfoques posibles:

#### Sincronización "en la nube"

Si utilizas plataformas como **Drive** de Google o **iCloud** de Apple, y trabajas "en la nube" seguramente parte o toda la información de tus dispositivos estará sincronizada con alguna de esas plataformas. Por otro lado, también hay alternativas libres como **NextCloud**, **OwnCloud** o **Filen**, que podrías configurar en tus propios servidores o buscar algún proveedor que brinde ese servicio.

No estaría mal revisar si tu información está yendo donde tu crees, es decir, entrar en cualquiera de esas plataformas y ver si tu información está actualizada. Tanto tus dispositivos de escritorio como los móviles se pueden sincronizar con estas "nubes".

Aquí surgen un par de inconvenientes: por un lado, la corporación tiene acceso a la información y la capacidad "gratuita" de las mismas suele ser bastante acotada.




#### Cifrado primero luego nube

Para solucionar el primer problema, lo que podemos es utilizar algún software de cifrado para nuestros archivos y luego subirlo a cualquiera de estas nubes. En este sentido existen **VeraCrypt**[28] y **Cryptomator**[29].

VeraCrypt permite crear contenedores o volúmenes cifrados, particiones cifradas y hasta cifrar tu disco duro por completo. Es una herramienta muy potente de cifrado en el almacenamiento que solo funciona en dispositivos de escritorio.

Por otro lado Cryptomator permite crear volúmenes cifrados y los maneja de tal forma que hace más sencillo su uso con soluciones de "nube". Por lo que si quieres tener una sincronización entre tus dispositivos y una nube, pero evitar que los proveedores de nube puedan acceder a tu información, lo mejor sería utilizar Cryptomator para cifrar tus datos antes de cada subida.

Hay que tener mucho cuidado cuando se utilizan programas de cifrado como los dos antes mencionados: debes guardar de forma correcta y segura la clave de descifrado, de lo contrario, puedes perder toda tu información.

28 VeraCrypt: https://www.veracrypt.fr/en/Home.html
29 Cryptomator: https://cryptomator.org/

## Sincronización “sin nube”

Existe otra forma de sincronizar contenido que es usando mecanismos “peer-to-peer” o entre pares. Esto tiene como beneficio que no dependemos de proveedores externos o corporaciones, y el espacio en disco que puede usar en la sincronización ya depende de cada dispositivo.

Este método tiene como problema que para que el contenido entre los dispositivos se sincronice, ambos (o más si son más de dos) deben estar online al mismo tiempo.

Existen programas como **IPFS desktop app**[30], **Sia**[31] o **Syncthing**[32] que permiten configurar este tipo de sincronización.

## Respaldos

Cuando hablamos de respaldos, hablamos también de que sean incrementales, lo que ahorra espacio de almacenamiento y permite volver atrás cierto tiempo, según se haya configurado. Por ello no hay que confundir “sincronización” con “respaldos”.

Existen herramientas como **Duplicati**[33] que funciona en cualquier dispositivo de escritorio y permite crear diferentes configuraciones de respaldos, tanto a nivel local, a través de diversos protocolos de red o también “nube”.

Una buena estrategia de respaldos podría ser sincronizar los archivos de mi móvil con mi computadora de escritorio y luego realizar respaldos a un disco externo utilizando Duplicati.

30 IPFS: https://docs.ipfs.tech/install/ipfs-desktop/
31 SIA: https://sia.tech/
32 Syncthing: https://syncthing.net/
33 Duplicati: https://duplicati.com/

### 2.1.7 Cifrado de los dispositivos y bloqueo de pantalla

Es fundamental cifrar tu información para proteger la información confidencial de la persona que ejerce el periodismo. Existen herramientas que permiten cifrar el disco completo de tu dispositivo de escritorio: por un lado está **BitLocker**[34] para Windows, también **FileVault**[35] para MacOS, y para Linux existen **EncFS**[36] y **Luks**[37].

Sin embargo existe un programa que ya mencionamos en el apartado anterior llamado **VeraCrypt**[38] que permite crear contenedores cifrados. Esto puede ser útil en el escenario donde un mismo conjunto de datos debe ser abierto en cualquiera de los 3 sistemas operativos mencionados más arriba.

Los dispositivos iOS y Android también cuentan con funciones de cifrado que deben estar activadas. Para ello es muy importante elegir una frase de contraseña segura, ya que esta es la única barrera que protege los datos. Cada vez que se enciende tu móvil, te va a preguntar esa frase para luego descifrar y mostrar toda tu información personal; cuando el dispositivo se apaga, la información vuelve a estar cifrada.

También se sugiere configurar los bloqueos de pantalla, tanto en la computadora como en el dispositivo móvil, ya que estas medidas disuaden a observadores casuales. Sin embargo es importante asegurarse de apagar la computadora al abandonar el área de trabajo o, cuando se crea que podría ser revisada. Como ya se mencionó los dispositivos que cuenten con cifrado completo configurado, al estar apagados están protegidos por la contraseña maestra o clave de cifrado.

En algunos casos puede ser importante guardar información sensible en unidades USB cifradas, ya que es más fácil de transportar y ocultar. Estas también se pueden formatear con VeraCrypt.

Se sugiere mantener alerta a posibles observadores incluso en entornos de trabajo y evita usar computadoras públicas como las de bibliotecas u otros lugares similares.

### 2.1.8 Dispositivos satelitales y sus limitaciones

En Paraguay, donde la cobertura informativa puede verse obstaculizada por limitaciones de conectividad y, en ocasiones por la represión de las autoridades, la tecnología satelital se convierte en una herramienta fundamental para los y las periodistas que trabajan en situaciones adversas. Inspirados por el uso de teléfonos satelitales en conflictos como el de Siria en 2012[39], las personas reporteras de Paraguay pueden emplear estas tecnologías para mantenerse conectados y transmitir información, incluso en áreas donde las comunicaciones convencionales son poco fiables. Sin embargo, es importante que sean conscientes de los riesgos asociados al uso de tecnologías satelitales, como el posible rastreo de sus dispositivos por parte de las autoridades. Para maximizar su seguridad, los y las periodistas deben seguir protocolos estrictos, **como evitar transmitir desde la misma ubicación repetidamente, limitar la duración de las llamadas y apagar el dispositivo tan pronto como termine la transmisión**.

Además, es importante que los y las periodistas adopten medidas preventivas para proteger la información sensible. Aunque las transmisiones satelitales pueden estar cifradas, no son completamente resistentes a la interceptación. Por ello, se recomienda usar palabras clave en comunicaciones extremadamente delicadas y, en la medida de lo posible, evitar el uso de teléfonos satelitales para este tipo de conversaciones. En caso de que un dispositivo sea confiscado, las autoridades podrían acceder a información crítica, como registros de llamadas y datos de contacto, lo que representa un grave riesgo para la seguridad de las fuentes.

34 Bitlocker drive encryption: https://support.microsoft.com/en-us/windows/bitlocker-drive-encryption-76b92ac9-1040-48d6-9f5f-d14b3c5fa178
35 FileVault: https://support.apple.com/es-es/guide/deployment/dep82064ec40/web
36 Encfs.Win: https://encfs.win/
37 Lunks: https://gitlab.com/cryptsetup/cryptsetup/
38 VeraCrypt: https://www.veracrypt.fr/code/VeraCrypt/
39 EFF. 2012. Satphones, Syria, and surveillance. https://www.eff.org/deeplinks/2012/02/satphones-syria-and-surveillance

### 2.1.9 Inteligencia de fuentes abiertas (OSINT)

Las técnicas OSINT (Open Source Intelligence)[40] implican la recolección y análisis de datos provenientes de fuentes de información de libre acceso, utilizadas con fines ofensivos o defensivos en la planificación de operaciones. Sin embargo, el uso abusivo de software OSINT puede vulnerar distintos derechos humanos, ya que estas herramientas poseen capacidades para realizar vigilancia masiva. Pueden monitorizar tendencias completas en redes sociales, clasificar contenido y perfilar a usuarios, o utilizar técnicas de web scraping para descargar grandes volúmenes de información disponible en Internet.

Este tipo de sistemas permite la creación de perfiles detallados mediante el cruce y análisis de información pública, incluyendo contactos, interacciones, ubicaciones geográficas, imágenes, entre otros. Además, algunos sistemas adquiridos por entidades estatales tienen la capacidad de geolocalizar y desanonimizar perfiles, exponiendo a las personas a mayores riesgos de vigilancia y violaciones a su privacidad.

Para evitar que terceros almacenen tu información de navegación, actividades en redes sociales, tus metadatos e información general que está en Internet, además de todo lo que ya se recomendó anteriormente, se sugiere:

- Evita exponer tu ubicación o hábitos. No publiques imágenes o videos que muestren lugares identificables y comparte actividades solo después de haberlas concluido y en lugares que no frecuentes regularmente.
- Analiza la sensibilidad de tu contenido en redes sociales. La información compartida, junto con datos asociados como ubicación, tipo de dispositivo, nombre de usuario y fecha y hora de publicación, puede ser recopilada por diversas entidades, incluyendo organismos estatales, empresas privadas y, en algunos casos, grupos delictivos. Es importante tener en cuenta que las herramientas OSINT permiten cruzar datos de diferentes redes sociales y bases de datos, lo que aumenta el riesgo de exposición de su información personal.
- Se debe tener cuidado con los perfiles desconocidos o seguidores sospechosos, ya que las herramientas OSINT suelen usar cuentas falsas para infiltrarse en grupos o acceder a información restringida.
- Mantén el anonimato en línea, especialmente si tus publicaciones pueden poner en riesgo su seguridad o la de otros. Usa perfiles anónimos desvinculados de tu identidad real y navega con una VPN o TOR para mayor seguridad.

40 OSINT Framework. https://osintframework.com/

### 2.1.10 Malware remotos (Pegasus y Finfisher)

Los malwares avanzados son diseñados para espiar dispositivos electrónicos de manera remota. Utilizados por gobiernos y entidades privadas, permiten acceder a la información privada de periodistas, activistas y otros usuarios, sin su conocimiento. Este tipo de programas infecta dispositivos iOS y Android, así como computadoras como Windows y macOS. Permiten acceder a mensajes, llamadas, correos, y pueden activar el micrófono y la cámara sin que la persona se de cuenta.

El malware puede instalarse a través de enlaces maliciosos, archivos adjuntos, aplicaciones comprometidas o vulnerabilidades del sistema operativo. En algunos casos, como con Pegasus, ni siquiera requiere interacción de la persona (lo que se conoce como "exploits zero click[41]"). Una vez instalado, el malware se conecta al servidor de control del atacante, permitiendo el acceso remoto al dispositivo. Esto permite que el atacante realice actividades sin que la persona usuaria lo note.

Algunos los malware más conocidos son **Pegasus**[42] y **Finfisher**[43], ambo sistemas tienen antecedentes de adquisiciones en Paraguay.

Para minimizar el riesgo de infección, se sugiere seguir algunos de estos pasos:

- Utiliza herramientas especializadas, como Mobile Verification Toolkit (MVT)[44] y shutdown.log[45], para verificar si tu dispositivo está comprometido
- Desconfía de enlaces o archivos sospechosos. Existen herramientas[46] que permiten hacer una verificación primaria de los enlaces.
- Estar atenta a aplicaciones que no se hayan instalado en los dispositivos: computadoras o celulares
- Es importante mantener siempre el sistema operativo y las aplicaciones actualizadas. Desinstala las aplicaciones que ya no utilices
- Si se sospecha que existe infección del dispositivo, se sugiere abandonar por completo tanto el hardware como cualquier cuenta asociada.

41 Kapersky. (s.f) ¿Qué es el malware de zero clic y cómo funcionan los ataques de zero clic? https://www.kaspersky.es/resource-center/definitions/what-is-zero-click-malware

42 Pegasus. https://en.wikipedia.org/wiki/Pegasus_(spyware)

43 TEDIC. (2016) Finfisher en Paraguay. Más preguntas y dudas sobre software malicioso adquirido por SENAD. https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/

44 Aunque hay aplicaciones específicas que prometen detectar spyware o malware, su eficacia puede variar, y a menudo es necesaria la ayuda de un profesional para una detección fiable, añade.

45 Securelist. (2024) A lightweight method to detect potential iOS malware. https://securelist.com/shutdown-log-lightweight-ios-malware-detection-method/111734/

46 En la web existe https://www.shouldiclick.org que permite realizar análisis externos de los enlaces sin correr el riesgo de visitarlos. También existe una app para Android con una funcionalidad similar: https://play.google.com/store/apps/details?id=com.trianguloy.urlchecker

# 3 COBERTURAS DE ALTO RIESGO

En coberturas de alto riesgo, si existe conectividad, lo mejor sería utilizar herramientas que permitan subir la información de forma instantánea a nubes como Drive, OneDrive, iCloud, NextCloud o similar.

En el caso de discos externos se recomienda utilizar cifrado completo mediante el uso de VeraCrypt. Si son tarjetas de memoria que se utilizan en cámaras, deberían descargarse al disco duro cifrado o subirse a alguna nube lo más rápidamente posible.

Los dispositivos móviles son mecanismos de vigilancia por excelencia, pero también son herramientas fundamentales para no quedar aislado y poder documentar cualquier cosa que ocurra.

# 4 LÍNEAS DE APOYO PARA PERIODISTAS EN PARAGUAY

## TEDIC

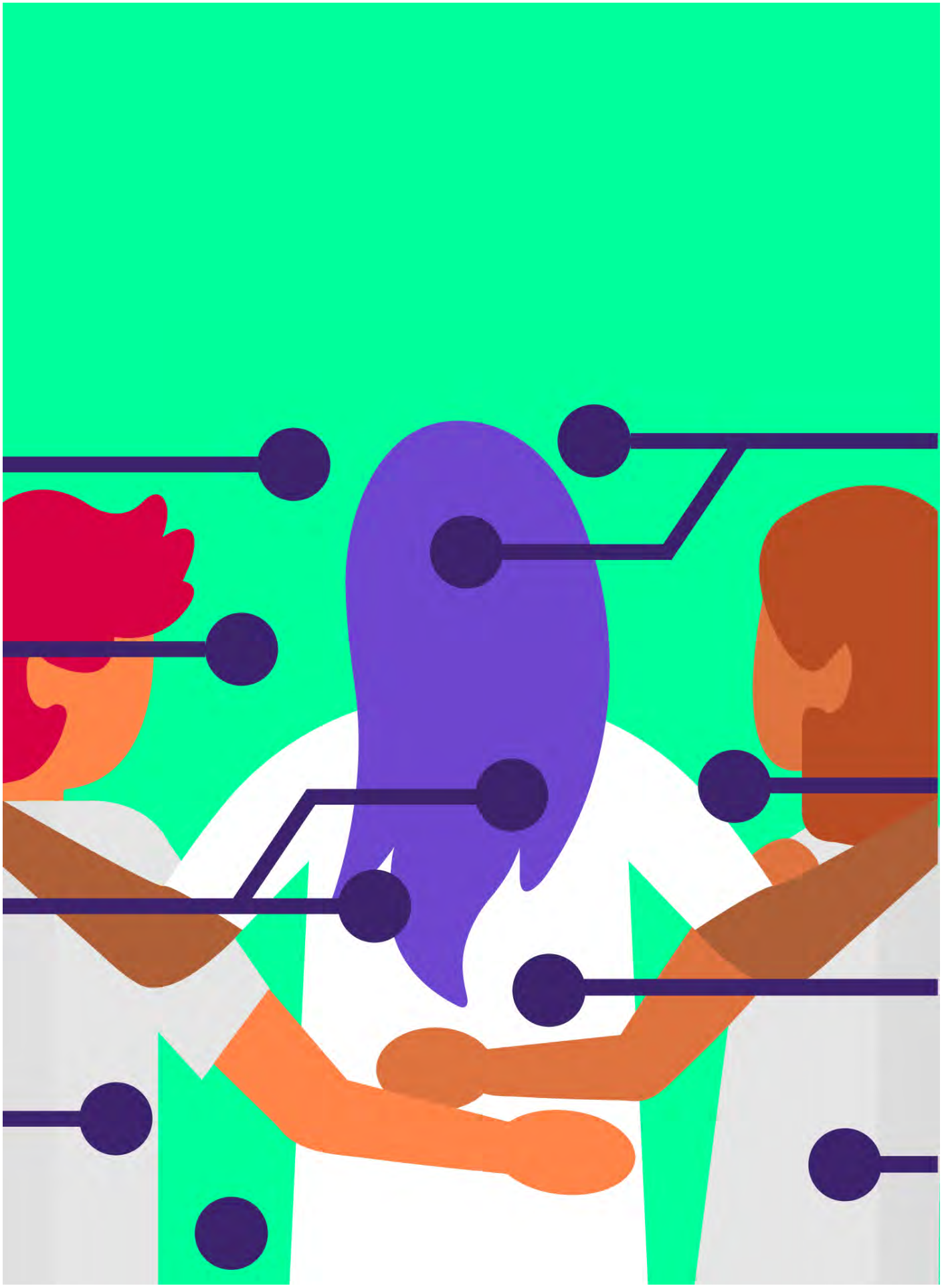
Línea de ayuda: hola@tedic.org

## ACCESS NOW

https://www.accessnow.org/help-es/

## AMNISTÍA INTERNACIONAL

https://securitylab.amnesty.org/



# REFERENCIAS BIBLIOGRÁFICAS


Artículo19 (2024). Seguridad integral para periodistas. Disponible en: https://seguridadintegral.articulo19.org/

CPJ (2020) Journalist security guide. Covering the news in a dangerous and changing world. Disponible en: https://cpj.org/wp-content/uploads/2020/05/guide.pdf

Free Press Unlimited (s.f.). TOTEM – en español. Disponible en: https://totem-project.org/es/

EFF (s,f) Surveillance Self-Defense. Disponible en: https://www.eff.org/pages/surveillance-self-defense

Feminist Tech Exchange. Evaluación de riesgo https://ftx.apc.org/books/es-ftx-reboot-de-seguridad-rnN/chapter/evaluacion-de-riesgos

IJNET (2024). Guía de supervivencia digital para periodistas. Disponible en: https://ijnet.org/es/story/gu%C3%ADa-de-supervivencia-digital-para-periodistas

Karisma (2024). Guía de divulgación de incidentes de seguridad digital para periodistas. Disponible en: https://web.karisma.org.co/wp-content/uploads/2024/02/Guia-de-divulgacion-de-incidentes-de-seguridad-digital.pdf

Karisma (2023). Chécheres, juguetes y armas. Disponible en: https://web.karisma.org.co/wp-content/uploads/2023/10/CHECHERES-JUGUETES-Y-ARMAS-1.pdf

SPP (2023). Manual para periodistas en situación de riesgo y/o amenaza. Disponible en: https://www.ohchr.org/sites/default/files/lib-docs/HRBodies/UPR/Documents/Session38/PY/A_HRC_WG.6_38_PRY_1_Paraguay_AnnexV_S.pdf

SocialTIC. ProtegeLA (s.f.). Disponible en: https://protege.la/

Small world news (2012). Safety using satphones. Disponible en https://smallworldnews.tv/Guide/Guide_SatPhone_English.pdf

TEDIC (2023) Violencia digital de género a periodistas en en Paraguay. Disponible en: https://www.tedic.org/wp-content/uploads/2023/10/Violencia-Genero-Periodistas-TEDIC-2023-web-2.pdf

TEDIC (2023). SOS Periodista: Kit de seguridad digital para periodistas. Disponible en: https://www.tedic.org/s-o-s-periodista-kit-de-seguridad-digital-para-periodistas/

TEDIC (2023). Videos de seguridad digital en idioma guaraní. Disponible en: https://www.tedic.org/videos-de-seguridad-digital-en-idioma-guarani/

TEDIC (2019) Gestor de contraseñas (offline). Disponible en: https://www.tedic.org/gestor-de-contrasenas-offline/

TEDIC (2019) El caos de las contraseñas: preguntas frecuentes. Disponible en: https://www.tedic.org/el-caos-de-las-contrasenas-preguntas-frecuentes/

UNESCO (2017). Manual de seguridad para periodistas. Guía práctica para reporteros en zonas de riesgo. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000243988

# S.O.S PERIODISTA