

Revisión

# Periodismo de INVESTIGACIÓN en Ecuador:

## Análisis de prácticas en seguridad digital desde 2017

Daniela Saltos

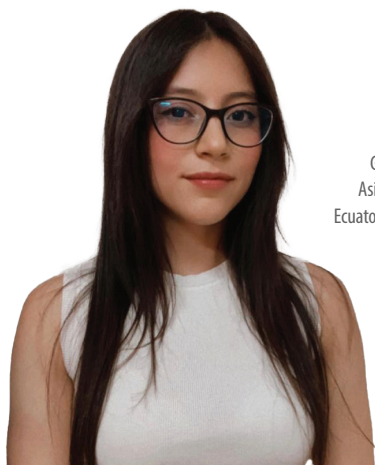
danielasaltosp@gmail.com

**Recibido:** 30 de abril de 2023 | **Aceptado:** 11 de octubre de 2023

**DOI:** <https://doi.org/10.18272/pd.v7i1.2967>

**Referencia de este artículo:**

Saltos, D. (2023). Periodismo de investigación en Ecuador: análisis de prácticas en seguridad digital desde 2017. *#PerDebate*, volumen 7 (pp. 142-163). Quito: USFQ PRESS.



Graduada de Periodismo en la Universidad San Francisco de Quito USFQ.  
Asistente de investigación en el Observatorio Interuniversitario de Medios  
Ecuatorianos (OIME). Ha publicado en medios como *La Hora*, *Primicias*, *Código  
Vidrio* y *Ecuador Chequea*.

### **Resumen**

Desde 2017, los cibercrimes a periodistas ecuatorianos han aumentado, incluyendo las cuentas de una periodista que dejó el país. El objetivo es registrar los resultados de un trabajo cualitativo que analizó las prácticas y la formación en seguridad digital de los periodistas de investigación mediante ocho entrevistas. El conocimiento se adquiere por medio de la experiencia debido a la falta de medidas estatales. Pero la responsabilidad recae tanto en los medios de comunicación como en los propios periodistas.

### **Palabras clave**

derecho informático, protección de datos, cibercrime, periodistas, Ecuador

## **Investigative journalism in Ecuador: analysis of digital security practices since 2017**

### **Abstract**

Since 2017, cybercrimes against Ecuadorian journalists have increased, including the accounts of a journalist who left the country. The objective is to record the results of a qualitative work that analyzed the practices and training in digital security of investigative journalists through eight interviews. Knowledge is acquired through experience due to the lack of state measures. But the responsibility lies with the media and journalists.

### **Key words**

computer law, data protection, cybercrime, journalists, Ecuador

## Introducción

El periodismo en Ecuador se ha transformado a partir de 2017 debido a los hechos históricos como el cambio de dos gobiernos, múltiples restricciones a la libertad de prensa como asesinatos a periodistas, el aumento de tecnologías, la pandemia de la covid-19 y el incremento de delitos cibernéticos. Estos, como el jaqueo y filtraciones, han aumentado exponencialmente desde 2017; sin embargo, los ataques de otro tipo contra periodistas han disminuido, a excepción de los años cuando existieron manifestaciones sociales (2019-2022). Este tipo de delitos son un riesgo para el periodismo de investigación debido a que trabaja con datos que son confidenciales, por lo que estas filtraciones pueden perjudicar el trabajo y vulnerar a los periodistas.

A causa de la globalización y la popularidad creciente de las tecnologías y redes sociales, una gran parte del periodismo ha migrado a los formatos digitales. Estas herramientas permiten un mejor análisis de datos, por lo que también las amenazas digitales aumentan. Desde 2017 hasta agosto de 2021, la Fiscalía General del Estado contabilizó 104 ciberdelitos en Ecuador (2021, p. 59). Ante esta realidad, se han implementado políticas tanto a escala global como en Ecuador para proteger a los usuarios.

En relación con la legislación ecuatoriana, el derecho informático protege el alcance de Internet y la seguridad para todos los usuarios. La Constitución de la República (2008) establece en el artículo 16 “el acceso universal a las tecnologías de información y comunicación”, complementándose con el artículo 66, numeral 19, que recalca la protección a la información de los usuarios. Once años después, en 2019, se implementó la Política Ecuador Digital por el Ministerio de Telecomunicaciones y de la Sociedad de Información (Mintel) con el fin de garantizar y evaluar el libre acceso a Internet de manera eficiente y segura. Asimismo, según el Sistema Económico Latinoamericano y del Caribe en América Latina los ciudadanos y gobiernos han invertido más en seguridad digital.

Esto evidencia que Ecuador reconoce la relevancia de la ciberseguridad. No obstante, las políticas no han sido suficientes para proteger la información de los periodistas. Existen pocas investigaciones y formación acerca de la protección de datos que beneficie el ejercicio periodístico. Uno de los pocos esfuerzos en este sentido es el foro “Seguridad para periodistas en situaciones de riesgo” del Consejo de Comunicación, que aborda también cuestiones de delitos en línea. La ciberseguridad se define como el conjunto de políticas, herramientas y programas que protegen la información y la integridad de los usuarios. Sin embargo, según Leyva-Méndez (2021, p. 1232), “la falta de decisión política y la limitación de recursos, no permiten promover una conciencia plena de prevención y mitigación”.



**Imagen 1.** La seguridad digital es un conjunto de herramientas, prácticas y procesos. Fuente: Pexels

Ese ejercicio consciente, por ejemplo, empieza con la identificación de las diferencias entre los términos ciberdelitos, ciberamenazas y ciberataques, que han sido definidos en estudios de seguridad digital. Una ciberamenaza es un riesgo que podría “explotar vulnerabilidades” (Instituto Federal de Telecomunicaciones, 2015), pero sin llegar a materializarse. En contraposición, según la misma fuente, el ciberataque representa un intento de dañar la integridad de la tecnología, pero sin completar en su totalidad el objetivo. Por último, el ciberdelito es el acto de afectar un sistema o herramienta dentro del ciberespacio cumpliendo su meta a cabalidad y siendo penado por la ley como si fuera un crimen tradicional.

### **Ciberdelitos en Ecuador: historia y estadísticas**

Una muestra de la escasez de recursos en seguridad digital para periodistas son las cifras de aumento en ciberdelitos en los últimos seis años pese a que la actual Constitución tiene un apartado sobre derecho a la comunicación y está vigente desde el 2008. En 2016, los ciberdelitos tenían el segundo lugar de ataques contra la libertad de expresión; no obstante, en 2017 la cifra aumentó a 59 casos de los 297 registrados (Fundamedios, 2017b). A partir de 2017, otro tipo de agresiones disminuyeron, pero los delitos en el entorno cibernético incrementaron.

Esta misma situación se vio reflejada en el 2018, cuando se registraron un total de 144 casos, de los que el 23,61 % eran aquellos que vulneraban la seguridad digital (2019a). Los periodistas que trataban información reservada que

comprometía a grupos de poder se vieron más afectados por esta falta de seguridad, que incluye el acceso a la información y reserva de datos personales. En ese año ocurrió el secuestro y asesinato del grupo periodístico de *El Comercio* en la frontera norte ecuatoriana por grupos criminales.

El año siguiente, 2019, fue el primer año desde 2017, según las siguientes estadísticas, que se registra una protesta social que incluye agresiones físicas, verbales y de discursos estigmatizantes para los periodistas ecuatorianos. Por esto, las agresiones aumentaron por encima de los ciberdelitos. Según Fundamedios (2019b), en este año se registraron un total de 212 agresiones y el 8,14 % fueron contra la seguridad digital (2019). A pesar de esto, estos últimos representaron el cuarto tipo de atentados.

Como se mencionó, en los seis años ocurrieron hechos que impulsaron cambios en el periodismo ecuatoriano. En 2020, la pandemia de la covid-19 causó que las actividades se volvieran más virtuales y, por la cantidad de personas conectadas a la red, aumentaron los ciberdelitos. Según Fundamedios (2020), de un total de 144 casos, el 18,75 % fueron en contra de sistemas informáticos de periodistas y redes sociales (2020). Los agresores incrementaron los métodos para vulnerar el ejercicio periodístico virtual y las políticas estatales no estaban preparadas para proteger la cantidad masiva de información.

Para el año 2021, las actividades virtuales continuaron, pero la seguridad digital tomó mayor importancia para los periodistas que manejaban información reservada. Además, la sociedad ecuatoriana vivió un nuevo cambio de gobierno, por lo que 12 casos de los 289 que se registraron fueron contra la seguridad digital (Fundamedios, 2021).

El 2022 registró una nueva protesta social en el país y, con ella, agresiones físicas, verbales y de discurso estigmatizante para los periodistas. Los ataques contra el ciberespacio fueron 28 y ocuparon el quinto lugar (Fundamedios, 2022). A pesar de esto, este tipo de agresiones ocuparon los primeros lugares de actos contra la libertad de expresión y las políticas no dieron una cobertura más amplia a los periodistas.

Asimismo, en 2023 se registraron dos hechos importantes que atentaron contra la seguridad de los periodistas. El primero es la recepción de memorias USB con carga explosiva en cinco medios de Ecuador, tres en Guayaquil y cinco en Quito (El Comercio, 2023). El segundo fue la salida de emergencia del país de Karol Noroña, periodista de *GK*, a causa de amenazas contra su vida. Un día antes su cuenta de Twitter sufrió un ciberataque (La Hora, 2023); por esto, los trabajos de investigación que tratan datos de carácter reservado tienden a ser más vulnerables a estos delitos, lo que representa un riesgo para la integridad del periodista.



Imagen 2. Salida del país de Karol Noroña anunciado por GK. Captura de pantalla

### Periodismo de investigación en Ecuador

A pesar de que el ejercicio periodístico requiere de un análisis que verifique los datos, existe un tipo que se especializa en profundizar los temas en una investigación que puede remontar hasta años. El periodismo de investigación es “aquel que persigue develar lo oculto” (Barahona, 2019, p. 15); por esto, la información que utiliza es confidencial y puede comprometer a grupos de poder que presentan irregularidades. De la misma manera, este ejercicio se define como una investigación en profundidad, original y con un sistema específico (The Center for International Media Assistance, 2013). Así, un ciberdelito contra los sistemas que guardan estos datos puede vulnerar la investigación y comprometer a periodistas a posibles riesgos.

A propósito de los trabajos periodísticos, estos suelen ser de carácter colaborativo como una medida de cubrir la información de manera más amplia. Por ejemplo, el Consorcio Internacional de Periodistas de Investigación (ICIJ) es una red con cerca de 280 periodistas de más de 100 países, (2023). En 2016, publicaron los *Panama Papers*, una investigación que empezó en 2015 y reveló millones de documentos acerca de la formación de sociedades *offshore*. De Ecuador participaron seis periodistas, por lo que fue un trabajo internacional que requirió de prácticas seguras.

A partir de 2017, existieron varias publicaciones en las que participaron periodistas ecuatorianos, investigaciones tanto nacionales como internacionales. En ese año, cuatro medios nativos realizaron un trabajo colaborativo acerca del “sobrepeso en grilletos chinos adquiridos con deuda externa pagada con petróleo” (Focus Ecuador, 2017). Los datos que debían analizar tenían que ver con la diferencia de costos entre dos marcas de estos dispositivos, por lo que

involucraba a varios grupos de poder. De esta manera, se evidencia la importancia de la protección de información como medida de protección y seguridad de los periodistas.

La obtención de los datos reservados que pueden comprometer a grupos de poder son los que requieren de más tiempo para conseguirse; por esto, los proyectos periodísticos de este tipo pueden durar años desde su recolección hasta la construcción del reportaje o producto. Un ejemplo de esto fue en 2019 cuando se conoció el caso *Sobornos 2012-2016*. La información contenía las pruebas sobre las contribuciones de multinacionales que entregaron al entonces partido político Alianza País que dirigía el expresidente Rafael Correa. Evidencias recopiladas por Fernando Villavicencio y Christian Zurita (GK City, 2021). A partir de la publicación de esta información, se acusó a varios funcionarios con el delito de cohecho.

Asimismo, los proyectos periodísticos que incluyen una amplia investigación develan situaciones que son de interés público y pueden generar consecuencias legales para los involucrados. El caso de *INA Papers* (2019) y el sitio web con el mismo nombre continúa en circulación con más de 30 000 000 vistas. Este reveló la vinculación de empresas *offshore* con el entonces primer mandatario Lenin Moreno y su círculo cercano.



Imagen 3. Pandora Papers en la página de ICIJ. Captura de pantalla

En 2021, las investigaciones colaborativas seguían tomando fuerza con la ayuda del Consorcio Internacional de Periodistas de Investigación. Los *Pandora Papers* fueron un trabajo en conjunto de más de 660 periodistas que dieron a conocer redes de 330 funcionarios de 90 países en temas como lavado de dinero, paraísos fiscales y evasión tributaria (Consortio Internacional de

Periodistas de Investigación, 2021). El actual presidente del Ecuador, Guillermo Lasso, estuvo involucrado dentro del grupo investigado. La investigación, en el país, la realizó por el equipo de investigación de diario el Universo liderado en ese entonces por Mónica Almeida y Paúl Mena.

Una de las últimas publicaciones del periodismo de investigación fue el 13 de febrero del 2023 con *El gran informe*, realizado por el medio digital *La Posta*. La investigación se centró en las estructuras narcocriminales y la relación que estas tienen con el primer mandatario Guillermo Lasso, su cuñado, otros funcionarios e incluso una empresa en Manta (El Universo, 2023). Parte de la revelación de los periodistas fueron audios y documentos que evidencian estas redes. Se requirió de seguridad digital para proteger la información de la investigación de las ciberamenazas.



Imagen 4. Difusión en redes sobre El Gran Informe de la Posta. Captura de pantalla

Mediante estos trabajos periodísticos colaborativos, se evidencia que los periodistas deben tomar medidas de seguridad por la cantidad de información que procesan. Además, los delitos cibernéticos que atentan contra la libertad de prensa muestran que un riesgo virtual puede sobrepasar las pantallas. En 2017 se registraron 67 casos de periodistas asesinados a escala mundial. Según Endara (2018), 39 de ellos realizaban investigaciones que comprometían las acciones de personajes con influencias. Por esto, las prácticas en seguridad digital deben empezar en la formación, como un interés personal y del medio de comunicación en donde trabaja el periodista. Estos protocolos permiten que los profesionales contribuyan a la democracia.

De la misma manera, estos protocolos generales y propios deben cubrir la vulnerabilidad de cada grupo, por ejemplo, las amenazas a las que se enfrentan las periodistas mujeres. Según Fundamedios (2023), el año 2022 concluyó con 80 delitos contra el personal femenino, lo que representó un incremento. El



ciberacoso en línea puede transformarse en agresiones fuera de línea (*offline*); las prácticas y formación que tiene cada persona individualmente y en conjunto fortalecen la seguridad.

Las estadísticas acerca de agresiones contra periodistas de investigación y el carácter reservado de los datos que se analizan demuestran que la seguridad digital es fundamental en el periodismo. A pesar de que se han implementado políticas acerca de este tema para proteger a los ciudadanos, no se ha efectuado un análisis específico para los periodistas de investigación con el fin de preservar el cumplimiento del objetivo de la profesión. Por esto, es importante recalcar la responsabilidad del Estado ecuatoriano en esta protección, pero también las acciones de cada periodista y de los medios de comunicación que respaldan su trabajo.

El propósito del artículo es registrar los resultados de una investigación que respondió a la pregunta: ¿Cuáles son las prácticas periodísticas y la formación en protección de datos de los periodistas de investigación para combatir el incremento de los ciberdelitos en Ecuador desde 2017, que podrían afectar el ejercicio periodístico en nuevos trabajos? Esto se hace con el fin de fortalecer el ejercicio periodístico y fomentar la participación del país en futuros trabajos. A partir de una metodología cualitativa, se evidencia que las prácticas y la formación en seguridad digital son una necesidad personal que se adquiere por medio de la experiencia.

## Diseño metodológico

Esta investigación fue de carácter descriptivo porque el objetivo era analizar las prácticas periodísticas y la formación en protección de datos de los periodistas de investigación para combatir el aumento de los ciberdelitos en Ecuador desde 2017, que podrían afectar el ejercicio periodístico en trabajos futuros. Para el desarrollo se utilizó un enfoque cualitativo basado en las acciones de los periodistas de investigación alrededor de la seguridad digital.

Este tipo de metodología es “la exploración de un limitado pero detallado número de casos o ejemplos que se consideran interesantes o esclarecedores, y su meta es lograr “profundidad” (Niño, 2011, p. 30). Por esto, el trabajo se basó en las prácticas en seguridad digital de ocho unidades de análisis, cinco hombres y cinco mujeres periodistas de investigación.

Este grupo fue elegido por medio de tres criterios dado que no existe un número oficial registrado de periodistas de investigación en el país. El primero, la nacionalidad, sirvió para enfocar el trabajo en Ecuador. El segundo, la trayectoria, incluyó premios e investigaciones periodísticas colaborativas para conocer la experiencia profesional. Finalmente, el tercero, las prácticas en protección de datos, sirvió para conocer las actividades y herramientas que usan en seguridad digital y de qué

fuentes las han adquirido. Dentro del análisis se guardó el anonimato de los periodistas entrevistados para evitar vulnerar sus prácticas.

**Tabla 1.** Listado de periodistas de investigación entrevistados según criterios de selección

| N.º | Nacionalidad | Trayectoria (premios)  | Prácticas en seguridad digital |
|-----|--------------|--|--------------------------------|
| 1   | Ecuatoriana  | Premios nacionales Jorge Mantilla Ortega y Fundamedios 2011  | Sí                             |
| 2   | Ecuatoriana  | Premio Nacional de Periodismo Eugenio Espejo 2022, Categoría Investigación<br>Premio Pulitzer por <i>Panama Papers</i>   | Sí                             |
| 3   | Ecuatoriano  | Premio Unión Nacional de Periodistas del Ecuador en Investigación 2019   | Sí                             |
| 4   | Ecuatoriana  | Mejor Investigación del Premio Nacional de Periodismo Eugenio Espejo   | Sí                             |
| 5   | Ecuatoriano  | Mención especial en el Premio Jorge Mantilla Ortega de diario El Comercio, Primer Premio en el Segundo Concurso Interno de Periodismo de diario El Comercio y colaborador de los <i>Panama Papers</i>          | Sí                             |
| 6   | Ecuatoriano  | Colaborador en los <i>Panama Papers</i> que obtuvo el Premio Pulitzer  | Sí                             |
| 7   | Ecuatoriano  | Mejor trabajo escrito en la XXIX Edición del Concurso Jorge Mantilla Ortega<br>Premio a la Mejor Investigación Periodística de un Caso de Corrupción (Premio IPYS)<br>Premio Pulitzer por <i>Panama Papers</i> | Sí                             |
| 8   | Ecuatoriana  | Premio Ortega y Gasset en la categoría Mejor Historia o Investigación Periodística   | Sí                             |

Fuente y elaboración propias

Al ser una investigación descriptiva, el proceso de recolección de información se efectuó mediante entrevistas a profundidad. La diferencia que este proceso tiene con una entrevista enfocada es que en esta “el objeto de investigación está constituido por la vida, experiencias, ideas, valores y estructura simbólica del entrevistado” (Sierra-Caballero, 2019, p. 327). Por eso, este tipo de entrevistas permite recoger las prácticas en seguridad digital de las unidades de análisis, desde su formación educativa hasta su experiencia en medios e investigaciones colaborativas.

De la misma forma, para estructurar la entrevista fue necesario implementar el cuestionario de preguntas para que estas sean ordenadas y sirvieran como instrumento de recolección (Niño, 2011). En este caso, el cuestionario estuvo organizado por las tres categorías con las que se eligieron las unidades de análisis: datos personales, trayectoria y herramientas de protección de datos. Es importante recalcar que antes de realizar las entrevistas, se usó el formato de validación para confirmar que la estructura era adecuada para obtener información del tema. Posteriormente, una matriz de codificación permitió iniciar el análisis de las entrevistas.

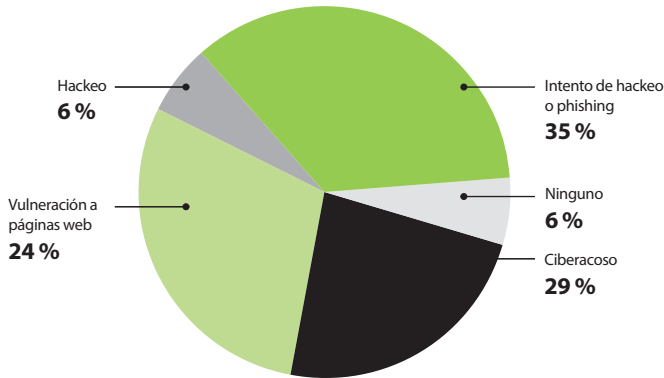
La metodología se basó en las prácticas en seguridad digital de periodistas de investigación ecuatorianos con una temporalidad específica. Es decir, las acciones a partir del año 2017 debido al cambio de mandatario, al cambio de políticas relacionadas con la comunicación que influyeron en el periodismo y a las investigaciones colaborativas en las que los periodistas participaron; por esta razón, el alcance fue diacrónico.

### 3. Resultados

Durante el período analizado, los ocho entrevistados confirmaron que participaron en investigaciones periodísticas a profundidad. Como se mencionó, las unidades de análisis fueron elegidas con tres criterios: nacionalidad ecuatoriana, trayectoria dentro del periodismo de investigación —que incluye premios y participaciones en investigaciones de alto impacto— y la aplicación de prácticas en seguridad digital, desde las más básicas hasta el uso de *softwares* o plataformas.

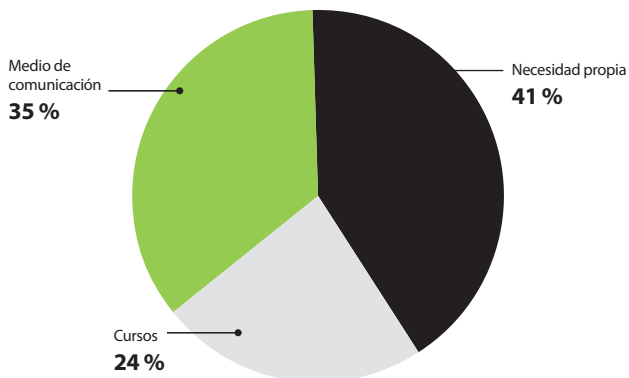
Con respecto al género de las unidades de análisis, los resultados corresponden a periodistas mujeres (50 %) y a hombres (50 %). De este modo, se analizan también los retos que las mujeres enfrentan al ejercer el periodismo de investigación en el espacio digital tomando en cuenta las cifras de agresiones a mujeres según Fundamedios (2023). Como se observa en la Figura 1,35 % recibió amenazas como *phishing* o intento de jaqueo de redes personales y 24 % experimentó la vulneración del medio en que trabajan o trabajaron realizando investigación. Por

otro lado, el 29 % recibió ciberacoso en las redes sociales por parte de funcionarios de gobierno y usuarios. Un caso (6 %) fue víctima de jaqueo de su cuenta de correo electrónico y un caso no recibió ningún ataque.



**Figura 1.** Ciberdelitos y amenazas en contra de los periodistas entrevistados Fuente y elaboración propias

Asimismo, seis de los ocho entrevistados son parte o colaboran con medios privados y en dos casos trabajan para una agencia de noticias y como *freelance*. Sin embargo, estos dos casos trabajaron anteriormente en medios privados donde desarrollaron investigaciones; por esto, es importante considerar el origen del conocimiento. Como se evidencia, el 35 % tuvo cursos, 41 % tuvo una necesidad propia de adquirir esta información y 24% recibió información del medio de comunicación.



**Figura 2.** Fuentes de información sobre seguridad digital de los entrevistados. Fuente y elaboración propias

Asimismo, los periodistas pertenecen a diferentes rangos de edad, lo que puede representar la relación que tienen con la tecnología y las redes sociales. Como se puede ver en la Figura 3, hay dos casos que pertenecen al rango de 40 a 44 años. Con respecto al periodista con menor edad, utiliza más herramientas digitales para la protección de datos. Por otro lado, hay una diferencia en el caso de 50 a 54 años quien utiliza las prácticas básicas en seguridad digital y uno de los casos de 54 a 58 años que ha decidido permanecer fuera de las redes sociales.

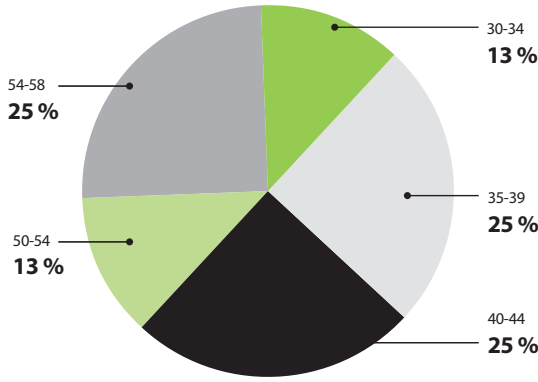


Figura 3. Rango de edad de los periodistas entrevistados. Fuente y elaboración propias

Los ocho entrevistados se refirieron al periodismo de investigación en su definición y procesos. Como se presenta en la Figura 4, esta especialización se define como una acción de revelar y profundizar hechos ocultos. Es una actividad que requiere una metodología específica que parte de una hipótesis que puede ser confirmada o negada por medio de evidencia verificada. Además, se destaca que para las investigaciones periodísticas de largo aliento es necesario el tiempo; por esto, las investigaciones realizadas a partir de 2017 se efectuaron a lo largo de varios años.



Figura 4. Nube de palabras sobre la definición de periodismo de investigación. Fuente y elaboración propias

Por otro lado, los entrevistados coincidieron en que el periodismo de profundidad ha cambiado con el impacto de la tecnología. Este impacto ha sido positivo en aspectos como el acceso a la información en plataformas web estables y el acercamiento a las fuentes. También ha sido negativo respecto al aumento de desinformación y la distribución masiva de contenidos falsos; por esto, los periodistas deben analizar este tipo de información de manera exhaustiva antes de incluirlo como evidencia.

Asimismo, con el aumento de tecnología las amenazas digitales también crecen, incluidos los ciberdelitos. Por esto, los entrevistados coincidieron en la composición de la seguridad digital para su definición y propósito. En otras palabras, la seguridad digital se compone de prácticas, educación, reglas y *softwares* para proteger la información y la identidad de los periodistas.

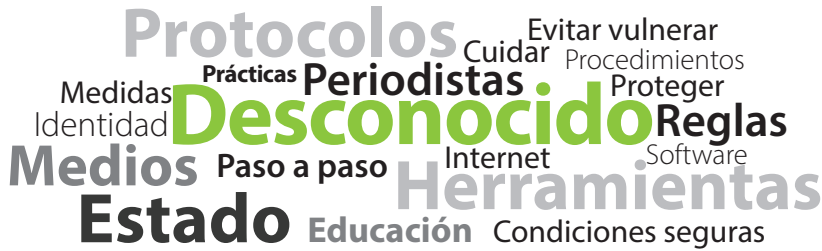


Figura 5. Nube de palabras sobre la definición de seguridad digital. Fuente y elaboración propias

Los entrevistados coincidieron unánimemente en la importancia de la seguridad para los periodistas de investigación, debido a la naturaleza sensible de la información que manejan. Este sistema no solo protege el contenido de las investigaciones, sino también al periodista. Estas herramientas son cruciales para proteger su integridad y, de la misma forma, la marca personal que cada uno tiene. Con el uso de tecnología y redes sociales, se ha incrementado la presencia de estos protocolos, aunque también los riesgos.

Por eso, en las respuestas de la primera entrevista, con una trayectoria de 19 años, se destacan los sujetos que tienen la responsabilidad de la seguridad digital. El entrevistado considera que el Estado debe estar siempre atento a la seguridad de los periodistas porque son los ojos de la ciudadanía. Sin embargo, cuando esto no ocurre debido a la debilidad democrática en el país, los medios de comunicación deben tomar medidas y los periodistas deben ser autodidactas. Cabe señalar que ninguna aplicación o *software* funciona completamente si no se convierte en una práctica constante.

Del mismo modo, en la segunda entrevista, con una trayectoria de 35 años en el periodismo, la idea principal para mantener seguridad en el espacio digital se basa en desconfiar y en mantener el secreto de las investigaciones. En primer lugar, es importante considerar que cuando se tiene información reservada sobre grupos de poder, el periodista ya es vulnerable, por lo que debe tener su propio sistema, desde el uso de las contraseñas hasta las bóvedas de información. Además, ninguna herramienta digital funciona en su totalidad si el periodista no mantiene el silencio.

Igualmente, el periodista de la tercera entrevista, con 30 años de experiencia, destaca que la seguridad digital aún es un terreno desconocido para los periodistas, a pesar de los años transcurridos desde que la tecnología se incorporó como una necesidad. Sin embargo, subraya la importancia de que las nuevas generaciones aprendan a utilizarla y generen prácticas para evitar poner en riesgo su trabajo y su marca personal como profesionales. Recalca la importancia de tomar medidas de prevención, ya que confía en que las aplicaciones no brindan suficiente protección una vez que el periodista está en riesgo, no solo en el ámbito digital, sino también en su integridad.

Por otra parte, en la cuarta entrevista, con una trayectoria de 12 años, el entrevistado tiene una mayor relación con la tecnología, por lo que usa más herramientas, como *software* para la protección digital. Entre las ventajas que ofrece la tecnología se encuentran los repositorios digitales, que permiten analizar de forma más fácil grandes cantidades de información. De la misma manera, las fuentes y el periodista pueden proteger su conversación mediante aplicaciones de comunicación encriptada. Las contraseñas son una llave para acceder a la información privada de los sistemas digitales, por lo que se pueden proteger tanto por mecanismos digitales como físicos.

Desde otra perspectiva de la seguridad digital, en la quinta entrevista, con 17 años de experiencia, el periodista considera que estas medidas de protección son necesarias para los periodistas de investigación debido al tipo de información sensible que manejan, protegiendo así al periodista que es vulnerable. No obstante, estos protocolos dependen del nivel de exposición; en temas peligrosos como el narcotráfico o las bandas en el país, el muro de seguridad debe ser más alto. En cualquier caso, los profesionales de la comunicación deben tener conocimiento de este tema.

Complementando lo anterior, en la sexta entrevista, con 19 años de trayectoria en el periodismo, el entrevistado recalca la importancia del anonimato como un pilar para mantener la seguridad digital. Existen herramientas que garantizan la protección de la identidad de un periodista e impiden que se registre la huella digital. De la misma forma, la actitud también es parte de las

prácticas en protección de datos, porque el objetivo en un proyecto periodístico no debe ser el protagonismo del investigador, sino cumplir con la revelación de los hechos.

Además, en la séptima entrevista, el periodista de 30 años de trayectoria reconoce la importancia de tomar medidas alternativas. Es decir, alternar los métodos entre digitales como tradicionales para mantener una mayor seguridad en las investigaciones. Mantener la información en papel puede ser considerado antiguo; sin embargo, se pueden evitar riesgos si se tienen respaldos de esta manera y se alternan con la tecnología.

Para agregar a lo anterior, en la octava entrevista a un periodista con 15 años de experiencia, coincide en la importancia de usar la tecnología en beneficio del trabajo periodístico y el manejo de *big data*. Asimismo, se puede trabajar en nuevos formatos que contribuyan a las investigaciones y mantengan la seguridad del periodista.

En resumen, las prácticas en seguridad digital se componen de varios aspectos que incluyen las aplicaciones tecnológicas y la actitud de los periodistas. Entre las prácticas básicas están mantener el anonimato, efectuar investigaciones colaborativas, el uso de verificaciones de dos pasos en redes sociales y cuentas de correo electrónico, un teléfono con la capacidad de transferir información por *bluetooth* o *AirDrop*. No tener las cuentas conectadas a ningún dispositivo, limpiar *cookies*, tener contraseñas de más de 16 caracteres difíciles de rastrear, no publicar datos personales en redes sociales, tener respaldos, no abrir correos de personas desconocidas. Para la navegación, es recomendable desactivar la opción de historial.

Además, las aplicaciones también son un apoyo; por ejemplo, no hacer llamadas de teléfono abierto sino encriptadas como en WhatsApp o Signal. También se pueden cifrar los correos en sitios verificados como Proton Mail o MIT PGP Public Key Server, un directorio de claves públicas del programa Pretty Good Privacy (PGP). KeePass Password Safe funciona como un gestor de contraseñas. También se puede utilizar el token físico como Yubikey que es una llave de seguridad. Pinpoint como repositorio para grandes cantidades de información y la navegación en modo incógnito. En suma, este conjunto de prácticas se adquirió en su mayoría por la experiencia de las investigaciones, por lo que aún hay una necesidad de conocer este tema.

## Discusión

Este artículo se centró en las prácticas y formación en seguridad digital de los periodistas de investigación ecuatorianos. Respecto a la educación, este



es un tema que permanece fuera de las clases universitarias de periodismo. Las unidades de análisis desarrollaron este conocimiento en su mayoría por necesidad propia. Sin embargo, solo una parte de los periodistas recibió capacitación por parte de los medios de comunicación a los que pertenecen o pertenecían al momento de realizar investigaciones de largo aliento, y pocos de estos medios mantienen protocolos de seguridad digital.

Para desarrollar esta investigación, la ciberseguridad fue el concepto principal. Según el Instituto Federal de Telecomunicaciones (2015), hay varios elementos que componen este término, como “herramientas políticas, conceptos, acciones, prácticas idóneas y tecnologías”. Al comparar esta definición con los términos expuestos por las unidades de análisis, se encuentra una concordancia en que la seguridad digital va más allá que las aplicaciones, e incluye incluso la actitud que tienen los mismos periodistas. Además, se recalca la constancia que deben tener estas prácticas para ser efectivas.

La seguridad digital aumenta su importancia a medida que la tecnología se integra más a la vida de las personas; por esto, la Constitución de la República (2008) habla en el artículo 16 acerca del derecho a “tecnologías de información y comunicación”. Dentro de las respuestas de las unidades de análisis en esta investigación, se destaca que el uso de tecnología ha facilitado el ejercicio periodístico, debido a que se tiene un mayor acceso a los datos de las distintas entidades y un mayor acercamiento a las personas. Sin embargo, se debe considerar el uso y control de estas tecnologías con respecto a la desinformación y distribución de contenidos falsos.

Asimismo, uno de los riesgos del uso de las tecnologías de información y comunicación es el aumento de ciberdelitos. Según los datos de agresiones a la libertad de expresión registrados por Fundamedios en los últimos seis años, estos han estado dentro de los cinco delitos más frecuentes. En concordancia con esto, los entrevistados han tenido experiencias en ciberdelitos, ciberamenazas o ciberacoso, y en su totalidad reconocen la importancia de tener conocimiento en seguridad digital debido a la revolución del mundo hacia un ambiente más digital.

Por eso, las prácticas que han desarrollado también incluyen el uso de aplicaciones. Según Cevallos-Villamarín (2022), “hay herramientas digitales gratuitas que todos los periodistas pueden usar para sortear casi cualquier obstáculo” (p. 208). Como se mencionó, la seguridad digital es un conjunto de varios elementos. Por esto, las herramientas, como aplicaciones o *software*, no son suficientes sin la constancia y el comportamiento de cada periodista, lo cual es crucial para sortear los obstáculos.

En general, el periodismo se considera como los ojos de los ciudadanos, sin embargo, según Barahona (2019), el periodismo de investigación tiene una mayor profundidad para revelar el tipo de información que el poder quiere ocultar. En correspondencia con la definición formada a partir de las entrevistas a las unidades de análisis, este tipo de investigaciones requieren de tiempo. Por la experiencia de los entrevistados, este es un ejercicio que se está perdiendo debido a los riesgos, los recursos y la necesidad de la inmediatez; no obstante, es muy necesario para cumplir con la democracia del país.

La importancia de la seguridad en el ciberespacio es crucial para proteger la vida de los periodistas, especialmente de quienes tratan los temas que podrían interferir con los grupos de poder. Según los datos registrados por *The Conversation* (2020), existe una tendencia a recibir agresiones como discurso de odio que traspasen la pantalla a la vida cotidiana. Algunos periodistas entrevistados compartieron experiencias de cómo, al publicar los *Panama Papers*, estuvieron expuestos a que las personas transformaran el ciberacoso de las redes a la vida real, esperándoles fuera de su medio de comunicación para agredirlos. Por esto, es necesario reforzar la protección a los periodistas, tanto digital como presencialmente.

Durante los últimos seis años, se registraron varias amenazas digitales para los periodistas. Incluso en los primeros meses de 2023, una periodista tuvo que salir del país por amenazas, a pesar de que existen legislaciones sobre ciberseguridad. Según Leyva-Méndez (2021), en Ecuador existe una debilidad en generar “estrategias concretas en el ámbito de seguridad cibernética, planes que protejan la infraestructura crítica o un organismo bien desarrollado que asuma el comando y control de la seguridad cibernética” (pp. 1232-1233). Del mismo modo, los periodistas entrevistados consideran que no hay una protección digital por parte del Estado ecuatoriano. No obstante, la responsabilidad no solo recae en el Gobierno, sino también en los protocolos que adopten los medios de comunicación y en los propios periodistas.

Como se mencionó, los periodistas entrevistados sintieron la necesidad de conocer más sobre seguridad digital mientras realizaban sus investigaciones, por lo que asistieron a cursos y algunos recibieron información del medio de comunicación. A pesar de que el Consejo de Comunicación tenga un programa de seguridad para periodistas que incluya formación mediante foros, como el llamado “Seguridad para periodistas en situaciones de riesgo”, este no ha tenido el suficiente impacto en los periodistas. En concreto, los entrevistados se han informado por medio de cursos o charlas de organizaciones como la Fundación Periodistas Sin Cadenas, Fundamedios, Border Hub, Fundación GABO, Knight Foundation y Red de Periodistas Libres.

Por último, este trabajo se ha construido a partir de las experiencias e ideas de periodistas de investigación con una trayectoria amplia. Por tanto, se puede concluir que aún hay un camino largo para encontrar un mecanismo de seguridad digital que satisfaga a la comunidad de periodistas, especialmente aquellos que usan información reservada y que pueden poner en riesgo incluso su vida.

## Referencias

- Barahona, M. W. (2019). *Manual de periodismo de investigación: ética / narrativa / investigación / seguridad*. Unesco. <https://bit.ly/46q7i6h>
- Cevallos-Villamarín, N. (2022). El periodismo de investigación en la era del *big data*. *Revista Enfoques de la Comunicación*, 1(7), 203-249. <https://bit.ly/3lduyL5>
- Consejo de Comunicación. (2020). *Segundo Ciclo Virtual "Seguridad para periodistas en situaciones de riesgo": Memorias*. Unesco. <https://bit.ly/3xvRoar>
- Consortio Internacional de Periodistas de Investigación. (2021). Pandora Papers: ¿Cómo se hizo la investigación y por qué es importante para América Latina? <https://bit.ly/3YFk8sR>
- \_\_\_\_\_. (2023). Acerca de. <http://bit.ly/3Lxjtq8>
- Constitución de la República de Ecuador. (2008, 20 de octubre). Asamblea de Montecristi. Registro Oficial 449. <https://bit.ly/3L9xeLJ>
- El Comercio. (2023). Artefactos explosivos salieron desde Quinsaloma hasta medios de comunicación. <https://bit.ly/43aPP0j>
- El Universo. (2023). ¿Quién es el fiscal que recibió informe hecho público por La Posta sobre supuesta estructura narcocriminal? <http://bit.ly/3ZVI4dh>
- Endara, R. (2018, 6 de enero). 65 bajas para el periodismo mundial en 2017. *Caja Negra*.
- Fiscalía General del Estado. (2021). Ciberdelitos. *Revista Científica de Ciencias Jurídicas: Criminología y Seguridad*, 1(30), 1-33. <https://bit.ly/3Xp4PUm>
- Focus Ecuador. (2017, 20 de noviembre). Sobreprecio en grilletes chinos adquiridos con deuda externa pagada con petróleo. <http://bit.ly/3ZRBx2g>
- Fundamedios. (2017a, 1 de enero). 2016: Un clima negativo para la libertad de expresión en Ecuador. <http://bit.ly/3Yynu0m>
- \_\_\_\_\_. (2017b, 28 de diciembre). Agresiones a la libertad de expresión disminuyen en un 40%. <http://bit.ly/3SK63ZC>

- \_\_\_\_\_. (2019a). *¿El año del cambio de marea para la libertad de expresión?* <https://bit.ly/3yqijVS>
- \_\_\_\_\_. (2019b). Los malos tiempos continúan: Informe 2019. <https://bit.ly/3YxjaPc>
- \_\_\_\_\_. (2020, 22 de diciembre). 2020 un año entre las muertes por COVID y la desinformación. <http://bit.ly/3ZzwP9G>
- \_\_\_\_\_. (2021, 22 de mayo). Durante el gobierno de Lenin Moreno 1702 periodistas y medios de comunicación fueron agredidos: El asesinato de Nos Faltan 3 fue el caso emblemático. <http://bit.ly/3ZFA270>
- \_\_\_\_\_. (2021). Ecuador 2021: ... Y a los periodistas nos siguen pegando bajo. <https://bit.ly/3Jt0L1K>
- \_\_\_\_\_. (2023). El periodismo ecuatoriano, blanco del crimen organizado: Informe libertad de expresión 2022. <https://bit.ly/40U6rbL>
- GK City. (2021, 24 de noviembre). *¿Qué es el caso Arroz Verde?* <http://bit.ly/3mK4COY>
- INA Papers. (2019, marzo). INA PAPERS: Los documentos sobre la corrupción presidencial en el Ecuador. <http://bit.ly/40ln4fj>
- Instituto Federal de Telecomunicaciones (IFT). (2015). Ciberseguridad. <http://bit.ly/3ZoWKQX>
- La Hora. (2023, 28 de marzo). Karol Noroña, periodista de GK, tuvo que abandonar el país tras amenazas de muerte. <http://bit.ly/414CuF3>
- Leyva-Méndez, A. (2021). Análisis de políticas públicas de seguridad cibernética. *Polo del conocimiento: Revista científico-profesional* 6(3), 1229-1250. <https://dialnet.unirioja.es/servlet/articulo?codigo=7926828>
- Niño, V. (2011). *Metodología de la investigación: diseño y ejecución*. Ediciones de la U.
- Posetti, J., Harrison, J. y Waisbod, S. (2020, 25 de noviembre). Los ataques en redes a mujeres periodistas se extienden cada vez más al mundo real. *The Conversation*. <http://bit.ly/3YnENCa>

Sierra-Caballero, F. (2019). La entrevista en profundidad: Función, sentido y técnica. En J.A González y C.M Krohling, *Arte y oficio de la investigación científica: Cuestiones epistemológicas y metodológicas* (pp. 301-379). Ediciones Ciespal. <http://bit.ly/3ZV3ar7>

The Center for International Media Assistance. (2013). Global Investigative Journalism: Strategies for Support. <https://bit.ly/407rzLH>