

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Comunicación y Artes Contemporáneas COCOA

**Periodismo de investigación y seguridad digital en Ecuador: Un
análisis de las prácticas periodísticas y la formación en la
protección de datos desde 2017**

Daniela Salomé Saltos Ponce

Periodismo

Trabajo de fin de carrera presentado como requisito
para la obtención del título de
periodista

Quito, 19 de mayo de 2023

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Comunicación y Artes Contemporáneas COCOA

**HOJA DE CALIFICACIÓN
DE TRABAJO DE FIN DE CARRERA**

**Periodismo de investigación y seguridad digital en Ecuador: Un
análisis de las prácticas periodísticas y la formación en la
protección de datos desde 2017**

Daniela Salomé Saltos Ponce

Nombre del profesor, Título académico

**Pamela Johana Cruz Páez, maestra en
Ciencias Sociales con mención en
Comunicación
Eric Samson, máster en Periodismo
Digital**

Quito, 19 de mayo de 2023

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en la Ley Orgánica de Educación Superior del Ecuador.

Nombres y apellidos: Daniela Salomé Saltos Ponce

Código: 00211713

Cédula de identidad: 1720729217

Lugar y fecha: Quito, 19 de mayo de 2023

ACLARACIÓN PARA PUBLICACIÓN

Nota: El presente trabajo, en su totalidad o cualquiera de sus partes, no debe ser considerado como una publicación, incluso a pesar de estar disponible sin restricciones a través de un repositorio institucional. Esta declaración se alinea con las prácticas y recomendaciones presentadas por el Committee on Publication Ethics COPE descritas por Barbour et al. (2017) Discussion document on best practice for issues around theses publishing, disponible en <http://bit.ly/COPETheses>.

UNPUBLISHED DOCUMENT

Note: The following capstone project is available through Universidad San Francisco de Quito USFQ institutional repository. Nonetheless, this project – in whole or in part – should not be considered a publication. This statement follows the recommendations presented by the Committee on Publication Ethics COPE described by Barbour et al. (2017) Discussion document on best practice for issues around theses publishing available on <http://bit.ly/COPETheses>.

RESUMEN

Este trabajo tuvo como objetivo 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, con el fin de fortalecer el ejercicio periodístico y fomentar la participación del país en nuevos trabajos. Tiene tres capítulos, en el primero a través de la definición de conceptos y la descripción del contexto de periodismo de investigación en el Ecuador, se desarrolló una metodología cualitativa cuyos resultados se registraron en el *paper* para la serie monográfica *#PerDebate*. Estos se obtuvieron a través de entrevistas a ocho periodistas ecuatorianos acerca de sus prácticas y su formación en protección en el espacio digital. Por otro lado, en el segundo capítulo se construyó el proyecto multimedia *The Safe Hack* en una página web con dos formatos, una infografía y un video, dirigidos a periodistas y usuarios interesados en el tema. Por último, en el tercer capítulo se registraron las conclusiones y recomendaciones del trabajo. Es decir, las reflexiones finales, limitaciones y sugerencias para ampliar el conocimiento en nuevas investigaciones. En resumen, las prácticas y la formación en seguridad digital son una necesidad propia para los periodistas de investigación, por lo que esta es una manera de contribuir a la difusión del tema. Como conclusión principal, se identificó que sí existen prácticas que se adquieren en el ejercicio de la profesión en un escenario de poca actuación por parte del Estado.

Palabras clave: Derecho informático, protección de datos, ciberdelito, periodistas, Ecuador.

ABSTRACT

This work aimed to analyze journalistic practices and data protection training of investigative journalists to combat the increase in cybercrimes in Ecuador since 2017, in order to strengthen the journalistic practice and encourage the country's participation in new jobs. It has three chapters, in the first, through the definition of concepts and the description of the context of investigative journalism in Ecuador, a qualitative methodology was developed whose results were recorded in the paper for the monographic series #PerDebate. These were obtained through interviews with eight Ecuadorian journalists about their practices and their training in protection in the digital space. On the other hand, in the second chapter, the multimedia project The Safe Hack was built on a web page with two formats, an infographic and a video, aimed at journalists and users interested in the subject. Finally, in the third chapter the conclusions and recommendations of the work were recorded. That is, the final reflections, limitations, and suggestions to expand knowledge in new research. In summary, internships and training in digital security are a necessity for investigative journalists, so this is a way to contribute to the dissemination of the topic. As a main conclusion, it was identified that there are practices that are acquired in the exercise of the profession in a scenario of little action by the State.

Key words: Computer law, data protection, cybercrime, journalists, Ecuador.

DEDICATORIA

A mi familia, incluido Tobías, cada uno dejó una parte de ustedes en este trabajo y en mí, soy quien soy por ustedes.

A los que se quedaron en el camino, a mi papi y papo, por creer en mí y enseñarme a que puedo hacer todo lo que me proponga. Lo estamos logrando.

AGRADECIMIENTOS

A Cristian y Michelle, gracias por ayudarme a aterrizar.

A mi fiel compañero y amigo en estos cuatro años, Sebastián, vamos juntos para la vida.

A mis profesores, Eric, Pamela y Tania, por enseñarme siempre con paciencia y motivarme a ser mejor cada día en estos últimos años.

TABLA DE CONTENIDOS

Comentado [PP1]: Los intertítulos como 1.1 deben estar a la izquierda del margen. Faltan los títulos de los anexos.

Introducción.....	10
Objetivos.....	13
Diseño metodológico.....	14
Capítulo 1	
Una radiografía del periodismo ecuatoriano de investigación desde la mirada de la protección de datos.....	18
1.1 Marco Contextual.....	18
1.2 Marco Referencial.....	23
1.3 El paper: Definición y estructura.....	26
1.4 El paper para #PerDebate.....	27
Capítulo 2	
The Safe Hack: Un ayudante para un periodismo digitalmente seguro.....	41
2.1 Cronograma y presupuesto.....	41
2.2 The Safe Hack: El proyecto multimedia.....	45
2.3 Formato 1.....	48
2.4 Formato 2.....	50
Capítulo 3	
Conclusiones y recomendaciones sobre seguridad digital: ¿Es necesaria para periodistas de investigación?.....	52
Referencias bibliográficas.....	56
Anexo A: Matriz de registro de información.....	60
Anexo B: Cuestionario para entrevistas.....	61
Anexo C: Carta de validación.....	63

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

Figura 1: Logo y nombre de la página web.....	46
Figura 2: Página de inicio del proyecto web <i>The Safe Hack</i>	48
Figura 3: Formato 1.....	49

Figura 4: Formato 2.....	51
Gráfico 1: Cibercrimes y amenazas en contra de los periodistas entrevistados.....	34
Gráfico 2: Fuentes de información sobre seguridad digital de los entrevistados.....	35
Gráfico 3: Rango de edad de los periodistas entrevistados.....	35
Gráfico 4: Nube de palabras sobre la definición de periodismo de investigación.....	36
Gráfico 5: Nube de palabras sobre la definición de seguridad digital.....	36
Tabla 1. Listado de periodistas de investigación entrevistados, según criterios de selección.....	15
Tabla 2. Cronograma de actividades para el trabajo de titulación, <i>paper</i> y proyecto multimedia.....	42
Tabla 3. Presupuesto.....	44

INTRODUCCIÓN

El trabajo periodístico en red alrededor de grandes cantidades de datos y de múltiples fuentes va en crecimiento. La experiencia más reciente fueron los *Pandora Papers*, en 2017. Más de 660 periodistas alrededor del mundo revelaron las redes construidas para mover dinero de 330 nombres de políticos y funcionarios de 90 países, incluido el Ecuador (Consortio Internacional de Periodistas de Investigación, 2017). Las compañías *offshore* secretas, lavado de dinero y evasión de impuestos fueron las conclusiones sacadas de esa investigación periodística. En el territorio ecuatoriano, los periodistas que participaron fueron Mónica Almeida y Paúl Mena del diario *El Universo* logrando involucrar al primer mandatario, Guillermo Lasso, en la investigación. Sin embargo, este no fue el primer trabajo colaborativo de investigación en el que aparece el país. En 2017, fue el caso *Paradise Papers*.

A partir de ese año, el periodismo en Ecuador pudo desarrollarse mejor en términos de acceso y tratamiento de la información, considerando que el gobierno de Rafael Correa se redujeron los espacios de investigaciones periodísticas (Levoyer, 2015). El periodismo de investigación se enfoca en construir un caso de interés público con información sensible que permanece oculta (2015). En el caso del país, los periodistas ecuatorianos han participado en investigaciones como *INA Papers* (2019), sobre la organización criminal encabezada por el expresidente Lenin Moreno, y *Pandora Papers* (2021) sobre las filtraciones de documentos sobre paraísos fiscales. Por esto, la obtención de datos y, aún más, su protección y tratamiento es de vital importancia en los proyectos. Por ejemplo, en los *Panama Papers* se trabajó con 300 mil registros de compañías en Panamá (Hidalgo & Torres, 2016) y en los *Pandora Papers* se trabajó con información de 29 mil usuarios (Consortio Internacional de Periodistas de Investigación, 2021).

También, la seguridad de los datos dentro del periodismo de investigación debe ser tomada en cuenta por la calidad de información que se trata. Generalmente, dentro de esta rama, se analizan datos reservados, por lo que su filtración puede provocar problemas sociales, políticos e incluso inconvenientes en la seguridad nacional. Un ejemplo internacional de las consecuencias de las filtraciones de información sensible es el caso de *Wikileaks*. A partir del jaqueo de Julian Assange a los sistemas del Gobierno estadounidense, se revelaron secretos nacionales que comprometían al país (Cevallos, 2022).

Aunque ese tipo de filtraciones masivas de documentos oficiales no se ha dado en el territorio ecuatoriano, la seguridad digital está en constante riesgo. El impacto del desarrollo tecnológico sin un control vulnera la información en la red. Según Leyva-Méndez (2021), “la falta de decisión política y la limitación de recursos, no permiten promover una conciencia plena de prevención y mitigación” (2021, p. 1232) sobre los ciberdelitos en el país. De esta manera, los

periodistas se ven afectados por las pocas medidas de protección de datos que pueden tomar en las investigaciones con contenido sensible.

Asimismo, la seguridad digital es parte del derecho de acceso al internet. Según la Fiscalía General del Estado, desde 2017 hasta agosto del 2021 se registraron 104 765 ciberdelitos, entre los que está la apropiación fraudulenta por medios electrónicos (10 393 casos), acceso no consentido a un sistema informático, telemático o de telecomunicaciones (1 265 casos), ataque a la integridad de sistemas informáticos (463 casos), interceptación ilegal de datos (298 casos), revelación ilegal de base de datos (153 casos) y delitos contra la información pública reservada legalmente (40 casos).

Estos registros revelan la inseguridad digital del país, por lo que la protección de las bases de datos de los periodistas está en riesgo, pero no hay investigaciones al respecto. En cuanto a investigaciones relacionadas al periodismo investigativo, Juan Carlos Calderón en su libro *Periodismo de investigación* (2005) explica el proceso y las estrategias para esta tarea. También, Alejandro Querejeta (2011) desarrolla la metodología junto con profesionales que han participado en esta área. Por otra parte, los resultados de los proyectos periodísticos como *Rehenes: ¿Por qué ejecutaron a los periodistas de El Comercio?* (2019) de Arturo Torres y María Belén Arroyo, y *Migrantes de otro mundo* (2020) comparten el tratamiento a los datos obtenidos. En contraste, no hay revisiones de literatura sobre la seguridad digital para periodistas en Ecuador.

Como consecuencia de esta falta de estudio en ciberseguridad y el desarrollo de medidas, los ataques a mujeres periodistas en su lugar de trabajo han incrementado. Según *The Conversation* (2020), las agresiones llegan en modo de “discurso de odio y desinformación”. Además, el acoso *online* es el primer paso de un camino que termina en violencia *offline*. En 2022, se registraron 80 agresiones contra periodistas mujeres con discurso estigmatizante y ataques verbales, 34 casos más que en 2021 (Fundamedios, 2023). La información, tanto personal como

de investigación, está vulnerable dentro de los ataques por canales electrónicos a causa de las pocas medidas de regulación que se tiene en el mundo digital. Las bases de datos y sistemas informáticos están constantemente expuestos a los métodos de robo de información, como el *phishing*.

Por otro lado, el Sistema Económico Latinoamericano y del Caribe registró un aumento de inversión en ciberseguridad del 34.2% en 2022 en América Latina. A pesar de esto, según Leyva-Méndez (2021), en Ecuador no existe un protocolo específico para fortalecer la seguridad digital. Las medidas y estudios que se han realizado alrededor de esta materia son en el sector financiero. De igual manera, en el país se reconoce la vulnerabilidad de la prensa, especialmente en las páginas web. El Consejo de Comunicación realizó un foro virtual llamado “Seguridad para periodistas en situaciones de riesgo” que tuvo como producto final un documento con las ideas principales. Sin embargo, este no es un taller con alcance académico en la formación de los futuros periodistas.

Así, es importante realizar estudios a la protección de datos por la falta de metodologías en seguridad digital para periodistas, especialmente para aquellos de investigación, porque se trata información reservada. Además, los ciberdelitos han incrementado en el Ecuador, por lo que el trabajo periodístico se ve vulnerable a las filtraciones y es necesario analizar las medidas que los periodistas están tomando. Por esto, la pregunta que se busca responder es: ¿cuáles son 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 nuevos trabajos?

OBJETIVOS

A partir de la pregunta de investigación, el objetivo general es:

- 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, con el fin de fortalecer el ejercicio periodístico y fomentar la participación del país en nuevos trabajos.

Además, surgen los siguientes objetivos específicos:

- Describir la situación del periodismo de investigación ecuatoriano, enfatizando en los ciberdelitos u otros hechos relacionados con protección digital de datos, a partir de 2017.
- Definir el concepto de prácticas periodísticas en protección de datos para combatir el aumento de ciberdelitos en Ecuador desde la normativa de comunicación y de seguridad digital.
- Diseñar y ejecutar una metodología que permita evaluar la formación en seguridad digital para periodistas de investigación a partir de 2017 en Ecuador, cuyos resultados se registren en un *paper* y se desarrollen en un proyecto multimedia.

DISEÑO METODOLÓGICO

A partir de la pregunta cuáles son 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 nuevos casos de investigación, este trabajo es de tipo descriptivo porque “busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno” (Hernández-Sampieri, 2014, p. 98). En este caso, un grupo de periodistas de investigación fue parte del objeto de estudio del que se sacaron características en cuanto a las prácticas en protección de datos.

Para ello, el enfoque fue cualitativo. Según Niño (2011), este 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” (2011, p. 30). Así, este fue un proyecto centrado en las acciones de los periodistas de investigación alrededor de la seguridad digital.

Al no tener un número específico de profesionales especializados en este campo que formen parte de un listado oficial, se seleccionó a un grupo específico de periodistas de investigación para obtener información acerca de sus prácticas y sus formaciones en la protección de datos. En total fueron ocho los profesionales de la comunicación quienes fueron los informantes clave y se detallan a continuación:

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

N°	Nacionalidad	Trayectoria (premios)	Prácticas en seguridad digital
1	Ecuatoriana	Premios nacionales Jorge Mantilla Ortega y Fundamedios	Sí
2	Ecuatoriana	Premio nacional de periodismo Eugenio Espejo en la categoría investigación Premio Pulitzer por <i>Panama Papers</i>	Sí
3	Ecuatoriano	Premio Unión Nacional de Periodistas del Ecuador en investigación	Sí
4	Ecuatoriana	Mejor investigación del Premio Nacional de Periodismo Eugenio Espejo	Sí
5	Ecuatoriano	Mención especial en el premio Jorge Mantilla Ortega de <i>Diario El Comercio</i> , primer premio en el Segundo Concurso Interno de Periodismo de <i>Diario El Comercio</i> y colaborador de los <i>Panama Papers</i>	Sí
6	Ecuatoriano	Colaborador en los <i>Panama Papers</i> que obtuvo el premio <i>Pulitzer</i>	Sí

7	Ecuatoriano	Mejor trabajo escrito en el Concurso Jorge Mantilla Ortega Premio a la Mejor Investigación Periodística de un Caso de Corrupción (Premio IPYS) Premio Pulitzer por <i>Panama Papers</i>	Sí
8	Ecuatoriana	Premio Ortega y Gasset en la categoría Mejor historia o investigación periodística	Sí

Elaboración propia

En este sentido, los ocho periodistas constituyeron las unidades de análisis porque cumplieron con los siguientes criterios de selección: en primer lugar, la nacionalidad debido a que el objetivo general se centra en la indagación de la seguridad digital en Ecuador, por lo que estos debían ser ecuatorianos. En segundo lugar, la trayectoria en investigación periodística considerando los años y trabajos periodísticos de investigación, incluyendo premios. En tercer lugar, las prácticas en protección de datos, es decir la aplicación de herramientas y actividades sobre seguridad digital por la cantidad y características de los datos.

Es importante mencionar que en el grupo de unidades de análisis se incluyó la misma cantidad de periodistas mujeres como de hombres. Esto con el fin de incluir en el análisis la vulnerabilidad a la que el grupo femenino está expuesto y las medidas en seguridad digital que se deben tomar a propósito de los datos publicados en Fundamedios (2023).

La información, que fue obtenida de los informantes claves, se registró a través de entrevistas en profundidad. Según Sierra-Caballero (2019), en este tipo de entrevista “el objeto de investigación está constituido por la vida, experiencias, ideas, valores y estructura simbólica del entrevistado” (2019, p. 327). Es decir, el objetivo del análisis estuvo centrado en las prácticas periodísticas y la formación de los periodistas de investigación alrededor de la seguridad por las experiencias y trayectoria en su vida. Igualmente, dentro de este proceso se realizó observación a las medidas que apoye con información con respeto al tema.

Adicional a esto, la entrevista requirió de instrumentos para recolectar los datos. En este caso, se utilizó un cuestionario. Según Niño (2011), este es un “conjunto de preguntas técnicamente estructuradas y ordenadas” (2011, p. 89). Las preguntas estuvieron pensadas conforme a las categorías de selección. En otras palabras, las primeras fueron acerca del contexto del periodista, después las preguntas estuvieron relacionadas con su trayectoria en la investigación y para finalizar se relacionaron con el uso de herramientas de protección de datos. Agregando a lo anterior, se utilizó el formato de validación para evaluar las preguntas con un experto antes de realizar las entrevistas. Por último, se utilizó una matriz de codificación para analizar las respuestas. A partir de estas, las conclusiones sirvieron para desarrollar un proyecto multimedia dirigido a periodistas y a personas interesadas en la seguridad digital.

De igual manera, la investigación tuvo un alcance diacrónico, es decir, se analizó a través del tiempo. En este caso, el tiempo de estudio fue a partir de 2017 en Ecuador, debido a que el país enfrentó el cambio de un gobierno en el que existió persecución y el periodismo tuvo varias limitantes. Además, este fue un momento en el que se desarrollaron y publicaron varias investigaciones periodísticas colaborativas en las que participaron ecuatorianos y tuvieron un alcance internacional.

CAPÍTULO 1

UNA RADIOGRAFÍA DEL PERIODISMO ECUATORIANO DE INVESTIGACIÓN DESDE LA MIRADA DE LA PROTECCIÓN DE DATOS

En los últimos seis años, el periodismo de investigación ha evolucionado junto con el desarrollo de tecnologías. El Internet funciona como una herramienta de inmediatez y facilita el procesamiento de datos, especialmente estadísticos, en una investigación para obtener el análisis. Sin embargo, dentro de este ambiente también hay amenazas digitales que vulneran la confidencialidad de la información y el trabajo periodístico, tal como los hackeos o las filtraciones de datos. Este tipo de delitos han aumentado en el país a pesar de las políticas acerca de seguridad digital.

En este capítulo se cumplen los dos primeros objetivos específicos planteados en este trabajo: Describir la situación del periodismo de investigación ecuatoriano, enfatizando en los ciberdelitos u otros hechos relacionados con protección digital de datos, a partir de 2017; y definir el concepto de prácticas periodísticas en protección de datos para combatir el aumento de ciberdelitos en Ecuador desde la normativa de comunicación y de seguridad digital. Para ejecutarlos se tendrá cuatro secciones: marco contextual, marco referencial, *paper* a publicar y *paper* redactado.

1.1 Marco Contextual

En 2017, Ecuador tuvo un nuevo mandatario luego de diez años del gobierno de Rafael Correa (2007-2017). En este decenio, la administración se caracterizó por la represión y la persecución

al ejercicio periodístico con medidas adoptadas por la Superintendencia de Información y Comunicación (Supercom). Según Fundamedios (2017), ese año se cerró con menos agresiones que en el 2016; era la primera vez desde el 2008 que disminuían. Las cifras de hace seis años correspondieron a “297 agresiones a la libertad de expresión” (2017).

A pesar de esta disminución en agresiones, en lo que se refiere a la violación a los derechos digitales, como ciberamenazas, hackeos y censuras, fue todo lo contrario. En 2017, hubo 59 casos (2017). Este fue el principal ataque que se registró en el año, seguido de las agresiones verbales y abuso de poder estatal. Igualmente, los ciberataques han aumentado desde 2016, cuando ocuparon el segundo lugar en ataques contra la libertad de expresión (2017). Este incremento exponencial de cifras representa una deficiencia de los procesos y herramientas en materia de seguridad digital.

En 2017, 39 de los 67 casos de periodistas asesinados alrededor del mundo realizaban trabajo de investigación que se interponían a los intereses de grupos de poder (Endara, 2018). Este es un trabajo que requería de una protección de datos extra para mantener la información confidencial durante su tratamiento. Sin embargo, al no existir una política de seguridad la integridad de los periodistas se vio vulnerada.

En forma similar al año pasado en Ecuador, en 2018 las agresiones contra la libertad de expresión disminuyeron, con un total de 144 casos. Pero las violaciones a los derechos digitales siguieron en crecimiento con el 23,61 % de ataques (2019). Además, el inicio de este año quedó marcado por el secuestro y asesinato de tres periodistas de *El Comercio*, quienes realizaban una investigación sobre los delitos de los grupos criminales en la frontera norte del país. La falta de seguridad digital, que incluya el acceso a la información de manera segura, condiciona el aumento de violencia contra los periodistas, especialmente aquellos que investigan irregularidades de grupos de poder.

En contraste, en 2019 el patrón que se vio en los últimos años sobre las agresiones a periodistas y los ataques a la seguridad digital cambió. En total, se registraron 212 atentados a la prensa de los que 8,14% fueron contra los derechos digitales (2019). Este cambio se debe a la revuelta social que ocurrió en octubre por el decreto presidencial de eliminar el subsidio a la gasolina. En 11 días de protesta, se reportaron 138 periodistas agredidos (Plan V, 2022). A pesar de que los ataques se centraron en el paro nacional, las violaciones a la seguridad digital ocuparon el cuarto lugar. Esto evidencia la falta de atención en materia de ciberseguridad.

Por otro lado, el inicio de la pandemia por Covid-19 en el año 2020 marcó un cambio en el ejercicio periodístico en general. Los medios y profesionales de la comunicación tuvieron que trasladar todas las actividades presenciales a virtuales, por lo que requerían más seguridad para proteger los datos de investigaciones. En comparación al 2019, las agresiones a la libertad de expresión decrecieron a 144, pero los ciberataques aumentaron y representaron el 18,75% de los atentados, sobre todo las ciberamenazas, y acoso sistemático por redes y medios sociales (2020). Estas cifras indican que las políticas en ciberseguridad en el país no estaban reforzadas para soportar el cambio que trajo la crisis sanitaria.

De igual manera, la emergencia del Covid-19 continuó en 2021, por lo que la formación en seguridad digital se convirtió en una necesidad. Se registraron 289 casos de agresiones contra periodistas, 12 de los casos representaron restricciones en el espacio digital (2021). Posteriormente, en mayo se realizó el cambio de gobierno de Lenin Moreno en el que se reportaron 1702 agresiones en total a periodistas y medios de comunicación (2021).

Por el contrario, el 2022 registró una nueva crisis social causada por el descontento de las comunidades indígenas con el gobierno de Guillermo Lasso. Por esto, las agresiones físicas, amenazas, discurso estigmatizante y procesos judiciales fueron las principales agresiones contra los periodistas. Sin embargo, en quinto lugar están las restricciones en el espacio digital con 28 casos (2022). La seguridad digital es necesaria a causa del traslado permanente de

actividades a la modalidad virtual y es parte de los derechos informáticos, pero no se evidencia como una prioridad para proteger el ejercicio periodístico.

Además, dentro de los tres primeros meses del 2023 se ha registrado ataques en contra de los periodistas. Por un lado, cinco medios de comunicación ecuatorianos en Quito y Guayaquil recibieron pendrives con carga explosiva en un sobre. El Ministro del Interior, Juan Zapata, explicó que “sí pueden segar la vida de una persona o provocar la pérdida de una extremidad si llegasen a detonar completamente” (El Comercio, 2023). Por otro lado, la periodista ecuatoriana del medio GK Karol Noroña tuvo que salir del país al recibir amenazas contra su vida por las investigaciones sobre el crimen organizado. Esta fue una medida tomada del protocolo del medio, por lo que muestra la importancia de que los medios de comunicación tengan políticas internas de protección a los periodistas y a sus investigaciones.

A causa del incremento de tecnologías, parte de la información confidencial tratada en el periodismo de investigación se obtiene y se procesa a través de dispositivos conectados al internet. El acceso a esta red es un derecho establecido en las leyes ecuatorianas. Por ejemplo, en la Constitución de la República (2008) se establece que todas las personas tienen “el acceso universal a las tecnologías de información y comunicación” (art.16). Además, se asegura la protección de datos y la difusión solo con su autorización. (art. 66 numeral 19). En los últimos seis años este derecho ha estado en riesgo para los periodistas.

Igualmente, en el acuerdo ministerial No. 15-2019 del Ministerio de Telecomunicaciones y de la Sociedad de Información (MINTEL) se envió la “Política Ecuador Digital”, donde se propone tres programas: Ecuador conectado, Ecuador eficiente y ciberseguro, y Ecuador innovador y competitivo. Dentro de la política, la institución reconoce que la cultura y concientización de la ciberseguridad “no se ha consolidado en su totalidad” en el país (MINTEL, 2019, p. 24). No obstante, este acuerdo está diseñado para fortalecer los canales digitales.

Las políticas están diseñadas para proteger las actividades digitales; sin embargo esto no es suficiente para las investigaciones periodísticas que manejan datos reservados. Es importante considerar la calidad de información y los casos que se han desarrollado con participación de periodistas ecuatorianos. Así, en 2016 el Consorcio Internacional de Periodistas de Investigación (ICIJ) publicó una investigación realizada desde 2015 llamada *Panama Papers*. La filtración incluía “más de 11,5 millones de documentos de los servidores de Mossack Fonseca, un bufete de abogados panameño dedicado principalmente a la gestión de sociedades offshore” (Mateos-Robles, 2017, p. 3). En este trabajo periodístico participaron los ecuatorianos Arturo Torres, Andrés Jaramillo, Alberto Araujo, Mónica Almeida, Xavier Reyes y Paúl Mena.

De la misma forma, el año siguiente, en 2017 *Focus*, *PlanV*, *Milhojas* y *diario La Hora* publicaron la investigación acerca de un sobreprecio en grilletes chinos adquiridos con deuda externa pagada con petróleo. Los datos revelaron que dispositivos tenían una “diferencia de precios del 800% entre el precio de la empresa fabricante (Megastek) y la intermediaria (Ceiec)” (FocusEcuador, 2017). Este fue un proyecto periodístico colaborativo en el que debieron utilizar métodos de protección de datos para evitar filtraciones. En el mismo año, el ICIJ publicó los *Paradise Papers*, una investigación que vinculó a Guillermo Lasso con cuentas *offshore* (Erazo & Acosta, 2022).

Las investigaciones periodísticas de este tipo tardan varios años en recopilar toda la información. En 2019, se publicó el *caso Arroz verde* o también llamado *Sobornos 2012-2016*. Los ecuatorianos Fernando Villavicencio y Christian Zurita analizaron los “aportes entregados por empresas multinacionales al movimiento Alianza País” (GK City, 2021), partido político del expresidente Rafael Correa. Asimismo, en la plataforma de Periodismo de Investigación se encuentra el reportaje “Arroz verde en la salud: El reparto de los hospitales” sobre el reparto de poder en el gobierno de Lenin Moreno a través de insumos médicos (Puertas, 2019).

Adicional, se revelaron los *INA Papers* sobre irregularidades con empresas *offshore* relacionadas con Lenin Moreno y sus cercanos, una situación que continúa hasta la actualidad.

De la misma manera, en 2021 se publicaron los *Pandora Papers*. Como se mencionó anteriormente, esta fue una investigación realizada por 660 periodistas alrededor del mundo. Hasta enero del 2022, se publicaron nueve documentos que enlazan a varios funcionarios públicos de Ecuador (El Universo, 2022). Las herramientas de protección de datos deben ser reforzadas para evitar ciberataques durante el trabajo periodístico es de carácter internacional.

En la actualidad, los periodistas que conforman el medio digital *La Posta* publicaron “la existencia de una supuesta estructura narco criminal que involucra al cuñado del presidente [Guillermo Lasso] y a otros funcionarios públicos” (El Universo, 2023), incluso vincula a la empresa Osaka Fish, en Manta. Esta investigación se denominó *El gran informe*. El proceso se construyó a través de vigilancia y análisis de información hasta construir la historia, por lo que el uso de prácticas digitales seguras es importante para evitar su filtración y vulneración.

Finalmente, las investigaciones periodísticas colaborativas, como las presentadas anteriormente, continúan presentes al igual que el crecimiento de las amenazas digitales. Para entender estas últimas, se darán conceptos relacionados con la seguridad digital y el ejercicio periodístico.

1.2 Marco Referencial

La globalización, el desarrollo de tecnologías y el incremento de popularidad de las redes sociales han cambiado los formatos del periodismo. En definición, este es un ejercicio que se puede precisar por su producción. Según Pereira (2010), es “una práctica simbólica que construye socialmente la realidad” (2010, p. 102). Por otro lado, Emilio Filippi explica que se debe ir más allá de la descripción de los hechos, se debe interpretarla y profundizar en ella (en Martínez, 2010). Por esto, el periodismo se toma como una práctica que reproduce los hechos sociales con una contextualización y un análisis.

Este concepto indica que el periodismo se mueve al mismo tiempo que la sociedad, por lo que esta tiene diferentes aristas que deben ser cubiertas con un conocimiento específico. El periodismo especializado es un ejercicio que requiere un “tratamiento en profundidad” (Enguix-Oliver, 2015). Este tipo de periodismo se diferencia del generalizado porque busca investigar lo que hay detrás de los hechos y los interpreta según el contexto.

En referencia a la práctica periodística especializada, el periodismo de investigación es un ejemplo que tiene un gran impacto social. Según la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), este tipo de periodismo es aquel que “persigue develar lo oculto” (2019, p. 15). Por otro lado, Jordán-Correa et al. consideran que este puede ser un trabajo de rendición de cuentas (2020) porque revela datos que han estado restringidos y son de interés público. Así, los autores concluyen en el objetivo que tiene esta especialización. Para esta investigación, esta práctica se define como un tipo de periodismo que analiza de manera profunda un hecho de gran impacto con datos reservados.

A causa del incremento de tecnologías, esta información confidencial se obtiene y se procesa a través de dispositivos conectados al internet. Según Anzit, el derecho informático incluye a la sociedad de información y se define como las normas que controlan el área de tecnología de la información (en Aguilar, 2015). De igual forma, Aguilar (2015) explica el concepto como “el conjunto de normas jurídicas encargadas de regular los fenómenos jurídicos como producto de la utilización de los recursos informáticos” (2015, p. 20). En este caso, el derecho a la información es la normativa que protege el derecho del acceso al internet y la protección a los datos como recurso informático.

Agregando a lo anterior, parte de la normativa que regula el derecho al internet y a las tecnologías protege a los usuarios de las amenazas digitales. Este concepto se refiere a la ciberseguridad y tiene diferentes definiciones porque surgió por el incremento de tecnologías de la información y comunicación. Según el Instituto Federal de Telecomunicaciones IFT

(2015), es un conjunto de herramientas para proteger a los usuarios y a la información de amenazas en el ciberentorno. Por otro lado, la Asociación Global del Ecosistema Móvil (2018) la explica como una disciplina que se encarga de dar acceso a los recursos tecnológicos a las personas que deben tenerlo y quitarlo a quienes no. En este caso, la definición de ciberseguridad incluye sistemas, políticas, programas, tecnologías y procesos que protejan a los usuarios y a su alrededor tangible e intangible.

Ahora bien, la materia de seguridad digital se enfoca en estudiar las amenazas digitales de las personas con acceso a internet. Alrededor de este evento surgen conceptos que tienden a ser confundidos en el área. Por ejemplo, ciberamenaza, ciberataque y ciberdelito. En primer lugar, la ciberamenaza es cuando se identifica un evento con “potencial de explotar vulnerabilidades” (IFT, 2015) en las tecnologías. Asimismo, según Villalba (2017) este concepto se define como un riesgo. Por lo que para esta investigación el concepto de ciberamenaza se identifica como un peligro que debe ser estudiado para evitar que se convierta en una acción.

En segundo lugar, los ciberataques pueden ser definidos como el “intento de dañar” (IFT, 2015), donde la acción tiene un claro propósito de interferir en la integridad de un sistema o entidad. Por el contrario, también puede ser definido como la acción cumplida de atacar con el propósito de robar información y atentar contra portales web (Coello-Ochoa, 2021). En este caso, la definición de ciberataque permanece en un intento, mas no la acción, con un objetivo malicioso evidente.

En tercer lugar, los ciberdelitos o delitos informáticos, según el Instituto de Ciencias Aplicadas y Tecnología (2022), son “figuras delictivas del crimen tradicional, pero adaptadas al ciberespacio” (2022, p. 14). De la misma forma, son definidos como crímenes relacionados con el Internet o tecnológicos que no tuvieran este recurso (Quevedo, 2017). En esta investigación, el concepto de ciberdelito es la acción de atentar contra un sistema o tecnología donde se logró el objetivo y se obtuvieron recursos privados.

Es importante definir estos conceptos relacionados con materia de seguridad digital debido a que su definición ha ido evolucionando a través de los años. Estos términos se relacionan directamente con los cambios de la sociedad, por lo que los elementos digitales han tomado mayor protagonismo con el aumento del uso de la tecnología y en el ejercicio periodístico.

1.3 El *paper*: Definición y estructura

Los resultados del análisis de las prácticas y la formación de los periodistas de investigación se registrarán en un *paper*. Según Arenas et al. (2014), este producto, o también llamado artículo científico, se define como “el producto de una investigación desarrollada en el marco de una disciplina del conocimiento, con temática y objetivos rigurosamente delimitados, bajo lineamientos teóricos y metodológicos específicos.” (2014, p. 2). En este caso, el documento siguió las mismas líneas y objetivos, pero se adaptó a los formatos de la revista donde se publicará.

El artículo científico se escribió con la estructura IMRyD (introducción, métodos, resultados y discusión). Este método permite “organizar y escribir su texto, y que ofrece una especie de mapa de carreteras claro para guiar a los directores, árbitros y, finalmente, lectores en la lectura” (Day, 2005, p. 7). Además, esta estructura ha sido recomendada por varios años debido a que cada parte responde a varias preguntas que permiten estructurar la investigación de manera coherente.

Se ha seleccionado la serie monográfica *#PerDebate* de la Universidad San Francisco de Quito (USFQ). Esta revista se centra en el “análisis y la reflexión de temas relacionados con la comunicación contemporánea, con especial énfasis en el periodismo” (Universidad San Francisco de Quito, 2023). La revista se encuentra en el volumen 7 sobre “Resiliencia e Innovación”. En este caso, el artículo estaría dentro de la sección *Alumni* donde los estudiantes graduados pueden publicar sus investigaciones.

El volumen actual de la serie monográfica acepta artículos relacionados con “narrativas inmersivas, nuevos formatos y modelos económicos del periodismo en tiempos de crisis” (Universidad San Francisco de Quito, 2023). El *paper* denominado “*Periodismo de investigación en Ecuador: análisis de prácticas en seguridad digital desde 2017*” se ajusta a la línea editorial con una extensión de 40 000 caracteres, formato APA y se compone de la introducción, que recoge el contexto y objetivos; la metodología, para posteriormente realizar el análisis de los resultados, y la discusión del tema que concluirá en un proyecto multimedia.

1.4 El paper para #PerDebate

Periodismo de investigación en Ecuador: análisis de prácticas en seguridad digital desde 2017

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

Daniela Salomé Saltos Ponce

Universidad San Francisco de Quito

ssaltos@estud.usfq.edu.ec

Resumen

Desde 2017, los ciberdelitos 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 a través de ocho entrevistas. El conocimiento se adquiere a través de la experiencia debido a la falta de medidas estatales. Pero, la responsabilidad está en los medios de comunicación y en los periodistas.

Palabras clave: Derecho informático, protección de datos, ciberdelito, periodistas, Ecuador.

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, el aumento de tecnologías, la pandemia del Covid-19 y el incremento de delitos cibernéticos. Estos, como el hackeo 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 tenido que trasladarse a los formatos digitales. De la misma manera, estas herramientas permiten un mejor análisis de datos, por lo que también las amenazas digitales aumentan; desde 2017 hasta agosto del 2021, la Fiscalía General del Estado registró 104 ciberdelitos en el Ecuador (2021, pg. 59). Por esto, se han desarrollado políticas alrededor del mundo y en Ecuador para proteger a los usuarios.

A propósito de la legislación ecuatoriana, el derecho informático protege el alcance del internet y la seguridad para todos los usuarios. Desde la Constitución de la República (2008), se establece en el artículo 16 “el acceso universal a las tecnologías de información y comunicación” (2008). Esta cláusula se complementa con la número 66 numeral 19 en la que recalca la protección a la información de los usuarios. Once años después, se realizó 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 seguro. Asimismo, según el Sistema Económico Latinoamericano y del Caribe en América Latina los ciudadanos y gobiernos han invertido más en seguridad digital.

De esta manera, se evidencia que Ecuador reconoce la importancia de la seguridad digital. 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 ellos es el foro “Seguridad para periodistas en situaciones de riesgo” del Consejo de Comunicación incluyendo el tema de delitos en línea. La ciberseguridad se define como una unión de políticas, herramientas y programas que protejan la información y la integridad de los usuarios; por esto, “la falta de decisión política y la limitación de recursos, no permiten promover una conciencia plena de prevención y mitigación” (Leyva-Méndez, 2021, p. 1232).

Ese ejercicio consciente, por ejemplo, empieza con la identificación de las diferencias entre ciberdelitos, ciberamenazas y ciberataques, y se han definido en los estudios sobre seguridad digital. Una ciberamenaza es un riesgo que podría “explotar vulnerabilidades” (Instituto Federal de Telecomunicaciones, 2015), pero que no llega a ser acción. Por otro lado, el ciberataque se convierte en un intento de dañar la integridad de la tecnología (2015), 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 Constitución, con un apartado sobre derecho a la comunicación, está vigente desde el 2008. En 2016, los ciberdelitos tenían el segundo lugar de ataques contra la libertad de expresión; sin embargo,

en 2017 la cifra aumentó a 59 casos de los 297 registrados (Fundamedios, 2017). 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. Se registraron un total de 144 casos, de los que el 23,61% eran aquellos que vulneraban la seguridad digital (2019). 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 este 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 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 (2019), 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 anteriormente, en los seis años ocurrieron muchos hechos que impulsaron cambios en el periodismo ecuatoriano. En 2020, la pandemia por 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 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 han ocupado 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 pendrives 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.

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” (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2019, p. 15); por esto, la información que utiliza es confidencial y puede comprometer a

grupos de poder con identificadas irregularidades. Así, un ciberdelito contra los sistemas que guardan estos datos puede vulnerar la investigación y a los periodistas.

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 (Consortio Internacional de Periodistas de Investigación, 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 “sobrepago en grilletes chinos adquiridos con deuda externa pagada con petróleo” (FocusEcuador, 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 para no vulnerar a 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*. Los datos que dos periodistas ecuatorianos, Fernando Villavicencio y Christian Zurita, recopilaron fueron acerca de contribuciones de multinacionales al entonces partido político del expresidente Rafael Correa, Alianza País (GK City, 2021). A partir de la publicación de esta información, se acusó a varios funcionarios con el delito de cohecho y el procesamiento continúa hasta la actualidad.

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* se publicó en 2019 y el sitio web con el mismo nombre continúa en circulación con más de 30 000 000 vistas (INA Papers, 2023). Este reveló la vinculación de empresas *offshore* con el entonces primer mandatario Lenin Moreno y su círculo cercano. Hasta la actualidad, el caso sigue siendo procesado y los mencionados enfrentan repercusiones.

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 y participaron dos periodistas ecuatorianos, 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 narco criminales 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 han sido audios y documentos que evidencian estas redes. Se requirió de seguridad digital para proteger la información de la investigación debido a que los periodistas deben protegerse tanto de las ciberamenazas como del ciberacoso.

A través de estos trabajos periodísticos colaborativos, se evidencia que los periodistas deben tomar medidas de seguridad por la cantidad y calidad 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 nivel 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 2022 cerró con 80 delitos en contra del personal femenino, lo que representó un incremento. El ciberacoso, en línea, puede transformarse en agresiones *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 muestran que la seguridad digital es importante en el periodismo. A pesar de que se han realizado políticas acerca de este tema para proteger a los ciudadanos, no se ha realizado 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 amparan su trabajo.

El propósito del *paper* es registrar los resultados de una investigación que analizó 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, con el fin de fortalecer el ejercicio periodístico y fomentar la participación del país en nuevos 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 a través de la experiencia.

Diseño metodológico

Esta investigación fue de carácter descriptivo porque se construyó alrededor del análisis de 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 nuevos trabajos. 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 a través de tres criterios al no tener un número oficial registrado de periodistas de investigación en el país. El primero, la nacionalidad, sirvió para enfocar el trabajo en el Ecuador. El segundo, la trayectoria, incluyó premios e investigaciones periodísticas colaborativas para conocer la experiencia profesional. Por último, el tercero,

las prácticas en protección de datos, sirvió para conocer las actividades y herramientas que usan en seguridad digital y cómo las han adquirido.

Tabla 1: Listado de periodistas de investigación entrevistados según criterios de selección

N°	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 en la categoría investigación Premio <i>Pulitzer</i> 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 <i>Diario El Comercio</i> , primer premio en el Segundo Concurso Interno de Periodismo de <i>Diario El Comercio</i> 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 Premio a la Mejor Investigación Periodística de un Caso de Corrupción (Premio IPYS)	Sí

		Premio Pulitzer por <i>Panama Papers</i>	
8	Ecuatoriana	Premio Ortega y Gasset en la categoría Mejor historia o investigación periodística	Sí

Elaboración propia

Al ser una investigación descriptiva, el proceso de recolección de información se hizo a través de las 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 esto, este tipo de entrevistas permitió recoger las prácticas en seguridad digital de las unidades de análisis desde su formación educativa como 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 sirvan 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 debió usar el formato de validación para confirmar que la estructura es 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 2017 por el cambio de mandatario, el cambio de políticas relacionadas con la comunicación que influyeron en el periodismo y las investigaciones colaborativas en las que los periodistas participaron; por esta razón, el alcance fue diacrónico.

Resultados

Durante el periodo de tiempo analizado, los ocho entrevistados confirmaron que participaron en investigaciones periodísticas a profundidad. Como se mencionó anteriormente, las unidades de análisis fueron elegidas en base a tres criterios: los ocho periodistas tienen nacionalidad ecuatoriana, cumplen con una trayectoria dentro del periodismo de investigación, incluyendo 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 el 50% a periodistas mujeres y el 50% a hombres; de esta manera, 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 puede observar en el siguiente gráfico, 35% recibieron amenazas como *phishing* o intento de hackeo 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 hackeo de su cuenta de correo electrónico y un caso no ha recibido ningún ataque.

Gráfico 1: Ciberdelitos y amenazas en contra de los periodistas entrevistados

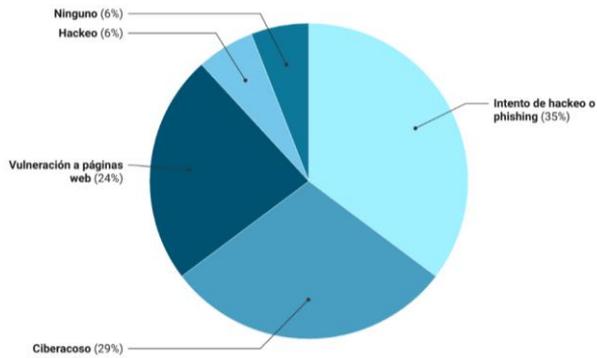


Gráfico: Daniela Saltos • Fuente: Daniela Saltos • Creado con Datawrapper

De la misma manera, seis de los ocho entrevistados son parte o colaboran con medios privados y en dos casos trabajan para una agencia de noticias y 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 puede evidenciar, el 35% tuvo cursos, 41% tuvo una necesidad propia de adquirir esta información y 24% recibió información del medio de comunicación.

Gráfico 2: Fuentes de información sobre seguridad digital de los entrevistados

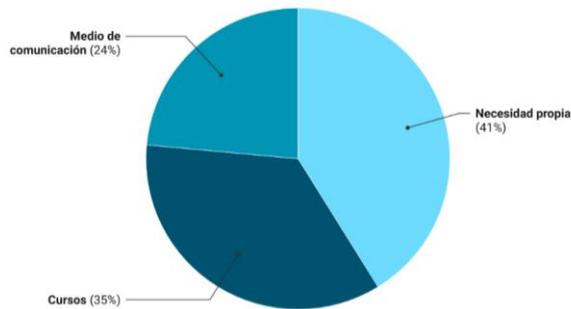
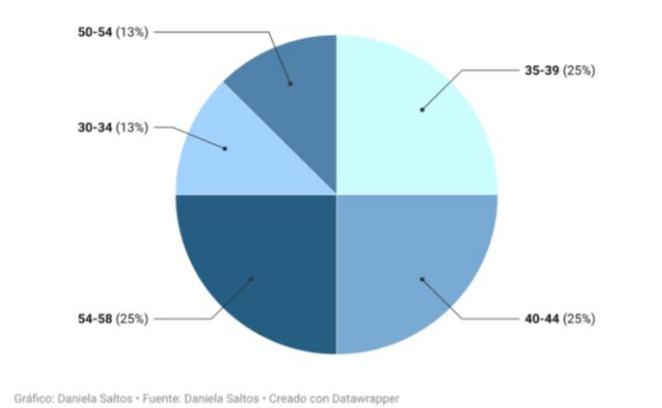


Gráfico: Daniela Saltos • Fuente: Periodistas entrevistados • Creado con Datawrapper

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 el siguiente gráfico, 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 tiene 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.

Gráfico 3: Rango de edad de los periodistas entrevistados



Los ocho entrevistados se refirieron sobre el periodismo de investigación en su definición y procesos. Como se presenta en la figura 4, esta especialización o 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 a través 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 realizaron en años.

Gráfico 4: Nube de palabras sobre la definición de periodismo de investigación



Por otro lado, los entrevistados coincidieron 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 estales y el acercamiento a las fuentes. También ha sido negativo en cuanto 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.

Gráfico 5: Nube de palabras sobre la definición de seguridad digital



Elaboración propia

Los entrevistados en su totalidad coincidieron en la importancia de la seguridad para periodistas de investigación debido a la información sensible que se maneja. Además, este no solo es un sistema de protección a los contenidos de las investigaciones sino que también lo es para el periodista. Estas herramientas son importantes 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, sin embargo también los riesgos.

Por esto, dentro de las respuestas de la primera entrevista, con una trayectoria de 19 años, se destaca los sujetos que tienen la responsabilidad de la seguridad digital. El sujeto 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 pasa a causa de la democracia débil en el país, los medios de comunicación deben tomar medidas y los periodistas deben ser autodidactas. Ahora bien, 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 tiene 30 años de experiencia y destacó que la materia en seguridad digital aún es un desconocido para los periodistas a pesar de que han pasado años desde que la tecnología se incorporó como necesidad. Sin embargo, es importante que las nuevas generaciones aprendan a utilizarla y generar prácticas para evitar vulnerar su trabajo y su marca personal como profesionales. Es importante tomar medidas de prevención debido a que confía que las aplicaciones no son 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 sujeto de análisis tiene una mayor relación con la tecnología, por lo que usa más herramienta como softwares para la protección digital. Entre las ventajas que tiene la tecnología están los repositorios digitales y estas herramientas permiten analizar de forma más fácil grandes cantidades de información, de la misma manera las fuentes y el periodista pueden proteger su conversación a través de 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 área 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 por el tipo de información vulnerable que utilizan, de esta manera se protege también al periodista que es vulnerable. Pero, estos protocolos dependen del nivel de exposición, en temas peligrosos como narcotráfico o 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.

Agregando a 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 tener seguridad digital. Existen herramientas que garantizan la protección de la identidad de un periodista e impiden que se registre la huella. 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 puede evitar riesgos si se tiene respaldos de esta manera y se alterna con la tecnología.

Para agregar a lo anterior, en la octava entrevista a un periodista con 15 años en el ejercicio, coincide 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. Como las prácticas básicas está el mantener el anonimato, hacer investigaciones colaborativas, el uso de verificaciones de dos pasos en redes sociales y cuentas de correo electrónico, un teléfono con la capacidad de traspasar 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 enfocó en las prácticas y formación en seguridad digital de los periodistas de investigación ecuatorianos. En cuanto a la educación, este es un tema que permanece fuera de las clases universitarias de periodismo. Las unidades de análisis desarrollaron este conocimiento a través de una necesidad propia en su mayoría, asistiendo a cursos o por

investigación propia. Sin embargo, solo una parte de los periodistas recibieron una capacitación de 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” (2015). 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, sino que se compone incluso de 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 mientras la tecnología se integre más a la vida de las personas; por esto, la Constitución de la República de 2008 habla en el artículo 16 acerca del derecho a “tecnologías de información y comunicación” (2008). 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, parte 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 por la revolución del mundo en un ambiente más digital.

Por esto, 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” (2022, pg. 208). Como se mencionó anteriormente, 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, esto es crucial para sortear los obstáculos.

En general, el periodismo se considera como los ojos de los ciudadanos, sin embargo, según la UNESCO, el periodismo de investigación tiene una mayor profundidad para revelar el tipo de información que el poder quiere ocultar (2019). 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; sin embargo, es muy necesario para cumplir con la democracia del país.

La importancia de la seguridad en el ciberespacio también es importante para proteger la vida de los periodistas, en especial los que tratan los temas que podrían interferir con los grupos de poder. Tomando los datos registrados por *The Conversation* (2020), existe una tendencia a recibir agresiones como discurso de odio y que traspasen la pantalla a la vida cotidiana. Como experiencias compartidas de algunos periodistas entrevistados, 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, se debe reforzar la protección a los periodistas, tanto digital como presencialmente.

Durante los últimos seis años, se han registrado varias amenazas digitales para los periodistas, incluso en los primeros meses del 2023 una periodista ha tenido 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” (2021, p. 1232-1233). De la misma manera, 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 que también en los protocolos que tomen los medios de comunicación y en los periodistas mismos.

Como se mencionó anteriormente, 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 la formación a través de foro, como el llamado “Seguridad para periodistas en situaciones de riesgo”, no ha tenido el suficiente impacto en los periodistas. En concreto, los entrevistados se han informado a través 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 través de las experiencias e ideas de periodistas de investigación con una trayectoria amplia. Por esto, 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 pueden vulnerar incluso su vida.

CAPÍTULO 2

THE SAFE HACK: UN AYUDANTE PARA UN PERIODISMO DIGITALMENTE SEGURO

A partir de las conclusiones de la investigación propuesta en el *paper*, se ha desarrollado el proyecto multimedia *The Safe Hack*. Este tiene el objetivo de diseñar productos periodísticos que apoyen la seguridad digital en periodistas y personas interesadas en el tema, además de sugerir herramientas para mejorar las prácticas contra los ciberdelitos. *The Safe Hack* (<https://salosaltos.wixsite.com/the-safe-hack>) tiene como plataforma base una página web creada en el sitio Wix donde se tendrán diferentes pestañas para cada producto multimedia.

El periodismo que se produce en el entorno cibernético se denomina periodismo digital. Según Guarnizo-Delgado et al. (2022), “la ventaja que tiene es que les llega más rápido a multitudes

Diseño metodológico					x													
Marco referencial y contextual						x	x											
Capítulo 1 de la investigación								x										
Planificación del proyecto web								x										
Avances de resultados									x									
Diseño de proyecto web y capítulo 2										x	x	x						
Primera versión del proyecto													x					
Segunda versión del proyecto														x				
Entrega de paper y proyecto																	x	
Presentación a evaluadores externos																	x	
Entrega final																		x

Elaboración propia

Como se puede ver, durante las dos primeras semanas se realizó la definición del tema de investigación a través de diferentes actividades que ayudaron a delimitar la idea en aquella que hable de sujetos, tiempo y área demográfica. Asimismo, hasta la semana cuatro se definieron las características básicas del trabajo, como la pregunta, los objetivos y la justificación. Además, se hizo la revisión de la literatura previa con el fin de dirigir el tema a un área diferente a las que ya han sido investigadas.

Durante las semanas cinco y seis en las que se realizó el diseño de la metodología para lograr los objetivos registrados previamente y el marco, se explican los conceptos y el contexto previo del tema de investigación. A partir de esto, desde la semana siete se realizó la redacción del capítulo 1, se presenta el *paper* para la revista elegida, en este caso la serie monográfica *#PerDebate* de la Universidad San Francisco de Quito. Al mismo tiempo, se empezó a utilizar la metodológica para obtener los resultados de las entrevistas a los ocho periodistas de investigación ecuatorianos.

En la semana 10 se empezó con el diseño del proyecto multimedia a partir de las conclusiones obtenidas en el *paper*, incluyendo el nombre, la línea gráfica, la misión y la construcción de la página web. A partir de esta semana, se empezó a desarrollar los proyectos multimedia para incluirlos en la plataforma. Este proceso se continuó hasta la semana 15 y 16 con la entrega del proyecto y la presentación de resultados a evaluadores externos.

Además, este proyecto cumple con un presupuesto diseñado para el primer año de funcionamiento debido a que representa más gastos. El desglose de las categorías se incluye en la siguiente tabla:

Tabla 3. Presupuesto

Descripción	Cantidad	Tiempo	Precio	IVA/VAT 12%	Monto
Tecnología y marca					
Plan Conectar dominio Wix	1	12	\$14,50	\$1,74	\$35,38
Compra/renovación de dominio Wix (thesafehack.com)	1	1	\$14,95	\$1,79	\$36,48
Paquete de dos micrófonos lavalier	1	1	\$70,12	\$8,41	\$78,53
Cámara Canon T8i / 850D Kit lente 18-55mm	1	1	\$1.308,04	\$156,96	\$1.465,00
Trípode Steren MOV-049	1	1	\$26,51	\$3,18	\$29,69
Desarrollo de marca (logotipo, cromática, etc.)	1	1	\$460,00	\$12,00	\$472,00
Laptop Asus TUF Dash 15 (2022)	1	1	\$1.205,35	\$144,64	\$1.349,99
Adobe Creative Cloud	1	12	\$54,99	\$6,60	\$134,18
Canva (versión gratuita)	1	1	\$0,00	\$0,00	\$0,00
Google Workspace (Drive, correo electrónico, etc.)	1	1	\$10,80	\$1,30	\$12,10
Movilización					
Pasajes para reportería escala nacional	1	6	\$500,00		\$500,00
Gasolina	1	6	\$300,00		\$1.800,00
Peajes	1	6	\$30,00		\$180,00
Servicios básicos					

Celular	1	12	\$21,00		\$252,00
Agua	1	12	\$15,00		\$180,00
Luz	1	12	\$35,00		\$420,00
Servicio banda ancha (60Mbps)	1	12	\$36,50	\$4,38	\$62,78
Gastos varios					
Gastos varios					\$397,57
Personal					
Salario coordinador del proyecto	1	12	\$200,00	-	\$2.400,00
Salario web máster	1	12	\$150,00	-	\$1.800,00
Salarios colaboradores	2	12	\$150,00	-	\$1.800,00
TOTAL					\$13.405,70

Elaboración propia

Para comenzar con este proyecto multimedia, el presupuesto incluye la distribución de los gastos para poner en funcionamiento el sitio web. La cantidad de dinero total es de \$13.405,70.

Además, se dividió los costos por cinco categorías:

1. Tecnología y marca
2. Movilización
3. Servicios básicos
4. Gastos varios
5. Personal.

La primera categoría, tecnología y marca, es la que más presupuesto requiere. En esta se incluyen los implementos para realizar las coberturas, como micrófonos, cámara y computadora. De la misma manera, se cuenta con el diseño de la marca, como el manual donde se establece la tipografía, la cromática y el diseño de la página web y los formatos periodísticos. Sin embargo, estos gastos se consideran en su totalidad en el primer año, en los siguientes se puede reducir.

Por otro lado, también es importante considerar los gastos de movilización para realizar las coberturas, tanto para el desplazamiento vial como aéreo y elementos como la gasolina.

Igualmente, se toma en cuenta los gastos en servicios básicos debido a que son elementos necesarios para el trabajo periodístico, por ejemplo, la conexión a internet de buena calidad.

Además, se debe considerar los recursos humanos del proyecto. Para iniciar, se consideraron cuatro personas: el coordinador del proyecto, el webmaster que se encarga del funcionamiento de la página web y dos colaboradores. De esta manera, los contenidos podrán ser variados y según diferentes puntos de vista. Por último, se tomó en cuenta un porcentaje de gastos varios para considerar cualquier emergencia.

2.2 *The Safe Hack*: El proyecto multimedia

El proyecto multimedia *The Safe Hack* se construye a través de las conclusiones del *paper* acerca de la formación y prácticas en seguridad digital para periodistas de investigación ecuatorianos. Por esto, se identificó la falta de protocolos y herramientas que protejan los datos de investigación periodística, lo que se justifica por el aumento de ciberdelitos como una de las agresiones a la libertad de expresión en los últimos seis años en Ecuador.

A partir de esta necesidad, el proyecto multimedia desarrolla contenidos que incrementen la formación y prácticas en protección de datos. Así, tiene la siguiente misión: *The safe hack* es un proyecto periodístico basado en concientizar sobre la importancia de la seguridad digital y fomentar el uso de prácticas y herramientas de protección de datos para defender la confidencialidad de la información en el ciberespacio y en la vida offline. La propuesta de contenidos tiene un sentido dirigido a la formación, ética digital y profundidad para evitar los delitos cibernéticos. El sitio está dirigido a los periodistas y personas interesadas en seguridad, tanto en la educación como en las prácticas.

Para cumplir con esta misión, el eslogan que acompaña al nombre es “Un ayudante para un periodismo digitalmente seguro”. De esta manera, se comunicará la idea de que este es producto para promover la seguridad digital. Sin embargo, se refuerza que es un proyecto

periodístico con una base académica. Estos elementos se apoyan en la línea gráfica que fue pensada para lograr los objetivos propuestos.

Figura 1: Logo y nombre de la página web



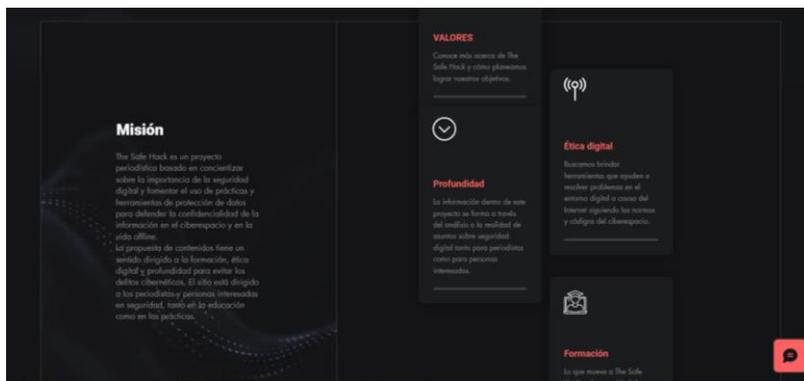
Como parte de la gráfica, el logo que será utilizado tiene como forma principal un escudo que representa la protección. Además, para comunicar que es un tema del entorno digital se utilizan las conexiones de la red inalámbrica dentro del escudo. Dentro de este, hay una cerradura para una llave y alrededor las manijas de una bóveda. En conjunto, representa el proyecto como una caja fuerte cibersegura.

En cuanto a la cromática, los colores son una gama de azules y morados al estilo del ciberpunk. Este es un movimiento cultural que surgió a partir de las preocupaciones sobre “las implicaciones que traen consigo la nueva tecnología” (Ramírez, 2022, pg. 131). De la misma manera, estos tonos representan el mundo digital, la tecnología y, al mismo tiempo, mantienen elegancia. Dentro del logo, es blanco # para contrastar con el fondo oscuro de la página web. Los tonos #3F4349, #FD6262, #889CE7 y #1862F7y # son parte de la cromática de la página y se utilizan en el proyecto multimedia y sus diferentes productos.

Por otro lado, la tipografía que se utiliza dentro de la página web está entre *Roboto* y *Futura light* y *regular* para los textos y subtítulos. La primera tiene un estilo *bold*, por lo que es utilizada para los títulos principales. Se escogió esta letra por sus características geométricas que caracterizan a las tipografías futuristas y se relaciona a la tecnología. Asimismo, se combina para los textos pequeño con la letra *Futura*, que tiene una característica sin serifa y terminaciones geométricas para lograr el ambiente del ciberespacio y el entorno digital.

En la página principal se colocaron elementos que creen un entorno tecnológico, pero también que se relacionan con el periodismo. En cuanto a los contenidos, se puede ver la misión y los valores del sitio web para que los usuarios tengan más información del sitio. Además, como un formato interactivo, se encuentra un resumen del primer formato con un enlace a la sección donde se encuentra, una línea de tiempo con las cifras de ciberdelitos en Ecuador de 2017 a 2021 y un resumen del segundo formato con un enlace directo a su sección. Adicional a esto, en la barra inferior se encuentran los datos de contacto y redes sociales.

Figura 2: Página de inicio de la página web *The Safe Hack*



2.3 Formato 1

El primer formato que se encuentra en la página web es una infografía interactiva que tiene los principales conceptos y recomendaciones sobre seguridad digital. Así, el tema se centra en crear una ayuda visual que sirva para disminuir los riesgos de navegar en el espacio digital; por esto está dirigido a una audiencia variada que muestre interés en la tecnología y en la protección de datos.

Este formato se realizó a partir de los resultados de la metodología del *paper*. Uno de los puntos que se identificó fue la falta de formación en este tema, por lo que cada uno de los periodistas adquirieron sus prácticas en seguridad digital por la experiencia. El objetivo de la infografía es

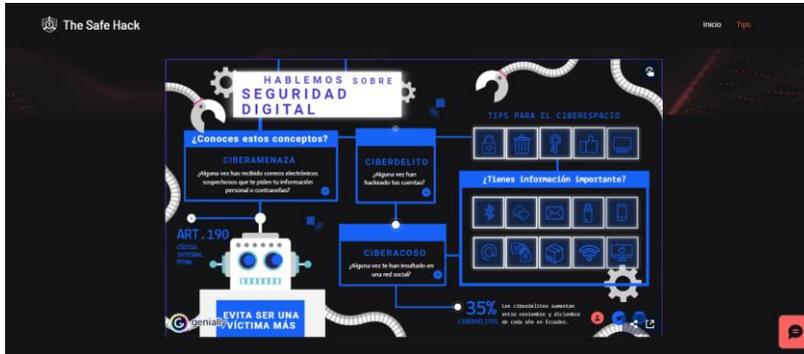
ser una recopilación de herramientas que disminuyan la posibilidad de ser víctima de un ciberdelito y contribuir a la educación de este tema para el público interesado.

Como se mencionó anteriormente, parte de la información, especialmente las recomendaciones vienen de seis entrevistas a periodistas de investigación ecuatorianos realizadas en el *paper* y del folleto Seguridad de los Sistemas de Información [Título original en francés: Sécurité des Systèmes de l'Information] de Erwan Chiloux. Por otro lado, también se presenta una sección de conceptos sacados de la sección de Marco Conceptual de este trabajo y del Instituto Federal de Telecomunicaciones.

Asimismo, se complementa la información con datos sobre ciberseguridad en Ecuador de la Unidad de Ciberdelitos de Ecuador de la Policía Nacional y el artículo 109 del Código Integral Penal que condena el uso fraudulento de un sistema informático para conocimiento general. De la misma manera, para asegurar la veracidad de los contenidos, la información fue verificada por Valentín Díaz, periodista especializado en investigación digital e investigación de software libre y el código abierto, la privacidad y ciberseguridad.

La infografía está diseñada como un elemento de interactividad para mantener la atención de los usuarios. Por ejemplo, se usan botones que dirigen a los conceptos y a las recomendaciones en forma de íconos. Los textos mismos tienen una característica de hipertextualidad debido a que ciertas palabras dirigen a otras páginas que apoyan a la adquisición de la información en todos los dispositivos electrónicos.

Figura 3: Formato 1



2.4 Formato 2

El segundo formato es un video cuyo eje principal es el panorama de la seguridad digital para periodistas en investigaciones reservadas en Ecuador. En primer lugar, se habla sobre el contexto del país en protección de datos y los protocolos que hay de protección a los periodistas al igual que los problemas que se presentan. En segundo lugar, se muestra el funcionamiento a detalle de aplicaciones que sirven para que los periodistas se protejan y cuiden sus investigaciones en el espacio digital.

Debido a que este proyecto está basado en los resultados presentados en el *paper* para la serie monográfica #PerDebate, se identificó la falta de seguridad digital para los periodistas de investigación a pesar de que existen leyes para el ciberespacio. Una de las conclusiones fue que la responsabilidad no solo está en el Estado, sino en los medios de comunicación y los periodistas mismos. Por esto, el objetivo de este formato es servir como una guía para que los profesionales puedan ser autodidactas y conozcan el panorama ecuatoriano del tema en las acciones estatales.

Para realizar este formato, se dividió el video en dos partes: en primer lugar, el punto de vista de dos especialistas: María Daniela Álvarez, quien es experta en ciberseguridad en el

Ministerio del Interior en Ecuador, y Fausto Vasco, quien es director del departamento de Tecnologías de la Información en la Universidad San Francisco de Quito. Por otro lado, las cifras son importantes para evidenciar el incremento de estas amenazas; por lo que se utilizó los informes publicados por Fundamedios y la Fiscalía Nacional del Estado. En tercer lugar, se tienen los testimonios de los periodistas de investigación trabajando trabajos colaborativos con diferentes herramientas sobre seguridad digital. En el segundo video se incluye el funcionamiento de algunas aplicaciones con el seguimiento de Valentín Díaz.

Además, este formato incluye un texto que explica el eje principal de este con información y datos importantes que están enlazados a nuevos documentos que sirvan como material adicional para los periodistas. De esta manera, se asegura que este grupo específico tenga diferentes herramientas para cuidar sus proyectos y su integridad.

Figura 4: Formato 2



CAPÍTULO 3

CONCLUSIONES Y RECOMENDACIONES SOBRE SEGURIDAD DIGITAL: ¿ES NECESARIA PARA PERIODISTAS DE INVESTIGACIÓN?

La investigación se realizó a partir del aumento de ciberdelitos en Ecuador, como una amenaza al ejercicio periodístico especialmente de aquellos profesionales especializados con el trabajo con datos reservados. Alrededor de ellos, interesó el análisis de las prácticas y formación en seguridad digital que se adquieren a través de la experiencia. Los asuntos sobre protección de datos son importantes para evitar vulneraciones a la información de interés público y a la integridad de los actores de comunicación.

La pregunta con la que partió ese análisis fue cuáles son 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 nuevos trabajos. Esa interrogante se planteó en el contexto del aumento de los ciberdelitos en el país dirigidos al periodismo de investigación a partir de 2017 se trató en el Capítulo 1. En esa sección además se diferenció entre los conceptos del ciberdelito, ciberamenazas y ciberataques, diferencias conceptuales que se trasladaron a la metodología cualitativa. Con esta

información, se construyó el cuestionario de preguntas para las entrevistas que arrojaron los resultados para el artículo académico presentado a la serie monográfica *#PerDebate*.

A partir del análisis de estos resultados, se redactó el capítulo 2. En esta sección se construyó el proyecto multimedia *The Safe Hack* que tiene como base una página web con dos formatos dedicados a la seguridad digital. Este sitio cuenta con una identidad de marca que se enfoca en la tecnología y la protección de datos. Además, dentro de los formatos se buscó la interactividad, hipertextualidad y los elementos multimedia para llegar al público específico, en este caso, los periodistas y usuarios interesados, con el objetivo de ser una guía para navegar de manera segura en el ciberespacio.

Como se mencionó anteriormente, la conclusión principal es que la seguridad digital es importante para el periodismo de investigación debido a que los datos son reservados. Por esto, las prácticas y la formación en seguridad digital se han adquirido por una necesidad personal durante el ejercicio práctico a lo largo de los años. A pesar de que las herramientas no evitan por completo que los ciberdelitos ocurran, son una ayuda para disminuir los riesgos y evitar perjudicar las investigaciones e incluso al periodista.

A través de la investigación, se concluye que Ecuador reconoce la importancia de la seguridad digital; por lo que existen políticas como el artículo 109 del Código Penal que condena el uso fraudulento de los sistemas informáticos y el interés de crear un protocolo en el Consejo de Comunicación. Sin embargo, estas acciones no han sido suficientes para proteger a los periodistas. Como parte de los resultados, el Estado ecuatoriano tiene falencias que no le permiten concentrarse en la creación de medidas seguras para el ejercicio periodístico, tanto en el entorno digital como fuera de la pantalla.

No obstante, una de las conclusiones más importantes es que la responsabilidad no solo recae en el gobierno, sino que también en la importancia que le den los medios de comunicación y los periodistas. Aún existen profesionales y medios que no han desarrollado sus prácticas para

proteger la información sensible, por lo que se debe incentivar el conocimiento de este tema entre colegas también.

La importancia en la seguridad digital ha tomado más fuerza en los últimos seis años por el impacto que ha tenido la tecnología. Para el periodismo de investigación, ha facilitado diferentes áreas como la sistematización de datos y el acceso a la información. Pero, se debe tomar en cuenta que también se presentaron más riesgos, como el aumento de desinformación y ciberdelitos.

A lo que se refiere entre herramientas tecnológicas y periodistas de investigación, se concluyó que existe una perspectiva diferente según la edad y trayectoria. Los periodistas con más experiencia y edad tienen más prácticas relacionadas al comportamiento más que a las aplicaciones, incluso usan menos redes sociales. Por otro lado, reconocen que este es un tema que debe tener más alcance en las nuevas generaciones. Sin embargo, se concluye que lo más importante es la constancia que las prácticas deben tener, en esto radica su efectividad. Estas están compuestas entre comportamientos y aplicaciones, pero realizándolas constantemente.

Finalmente, las prácticas y formación en seguridad digital benefician también a que la violencia *online* no traspase la pantalla y atente a la integridad de los periodistas. El trabajo de investigación es necesario para construir la democracia, por lo que se debe garantizar la seguridad de los profesionales de comunicación en todas las áreas.

A partir de esta investigación, se recomienda utilizar los resultados en el tema de la formación de los periodistas en seguridad digital. Es decir, estudiar los planes de estudio en las universidades y tomar elementos importantes para fortalecer el conocimiento de este tema debido al constante aumento de la tecnología. De la misma manera, la información puede ser utilizada en diferentes cursos o programas especializados en este tema para difundir el contenido a más personas interesadas.

Por otro lado, el proyecto multimedia recogió prácticas y herramientas digitales para navegar de manera segura en la red, pero en futuras investigaciones los productos pueden tener mayor alcance. Por ejemplo, realizar investigaciones acerca del periodismo de investigación con violencia de género y otras áreas. Igualmente, se recomienda ahondar en el tema de los protocolos que pueden ser aplicados a medios de comunicación en todas sus áreas como una escala mayor y analizar en qué medida los periodistas y el personal los conocen. De esta manera, se logrará un mayor compromiso en la lucha por la ciberseguridad en el ejercicio periodístico.

REFERENCIAS BIBLIOGRÁFICAS

- Acuerdo Ministerial 006-2021 [Ministerio de Telecomunicaciones y de la Sociedad de la Información]. Política de Ciberseguridad. 17 de mayo de 2021.
- Aguilar, P. (2015). ¿derecho informático o informática jurídica?. *Revista de Investigación en Tecnologías de la Información: RITI*, 6(3), 19-24. <http://bit.ly/3IYfAc0>
- Arenas, S., Burgos, R., Lizcano-Rivera, C., Rebolledo-Muñoz, R., Barrero, N., Girón, S., Pataquiva, A. & Suárez, C. (2014). *El artículo científico*. Universidad Sergio Arboleda. <https://bit.ly/3YPZExt>
- Asociación Global del Ecosistema Móvil. (2018). Seguridad y privacidad en las redes móviles: Desafíos, propuestas y consideraciones para los gobiernos. GSMA Latin America. <https://bit.ly/41tWult>
- Calderón, J. (2005). *Periodismo de investigación*. Quito: Ciespal.
- 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/3IduyL5>
- Coello-Ochoa, I. (2021). Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos. <https://bit.ly/3kyG5M2>
- Consejo de Comunicación. (2020). *Segundo Ciclo Virtual “Seguridad para periodistas en situaciones de riesgo”*. Dirección de Comunicación. <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>
- Constitución de la República de Ecuador [Const]. Art. 16. 20 de octubre de 2008 (Ecuador). <https://bit.ly/3L9xeLJ>
- Day, R. (2005). *Cómo escribir y publicar trabajos científicos*. The Oryx Press. <https://bit.ly/3lged7>
- El Comercio. (2023). *Artefactos explosivos salieron desde Quinsaloma hasta medios de comunicación*. El Comercio. <https://bit.ly/43aPP0j>

- El Universo. (2022). *Resumen 2021: Las revelaciones de los Pandora Papers causan revuelo en Ecuador*. El Universo. <http://bit.ly/3JaBBUd>
- El Universo. (2023). *'La Posta' responsabiliza al Gobierno por su seguridad y gremios condenan amenazas al medio entre pedidos de no incurrir en un 'periodismo populista'*. El Universo. <http://bit.ly/3YSvp9f>
- El Universo. (2023). *¿Quién es el fiscal que recibió informe hecho público por La Posta sobre supuesta estructura narcocriminal?*. El Universo. <http://bit.ly/3ZVI4dh>
- Endara, R. (2018, enero 6). 65 bajas para el periodismo mundial en 2017. *Caja Negra*. <https://bit.ly/3Ep1797>
- Enguix-Oliver, S. (2015). Periodismo especializado y especialización política. *Mediaciones Sociales*, 1(14), 103-128, http://dx.doi.org/10.5209/rev_MESO.2015.n14.51561
- Erazo, V. & Acosta, A. (2022). Lasso, los Paradise Papers y los Pandora Papers. Nodal: Noticias de América Latina y el Caribe. <http://bit.ly/3T5xqNL>
- 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). *Sobreprecio en grilletos chinos adquiridos con deuda externa pagada con petróleo*. Focus Ecuador. <http://bit.ly/3ZRBx2g>
- Fundamedios. (2017). 2016: un clima negativo para la libertad de expresión en Ecuador. <http://bit.ly/3Yynu0m>
- Fundamedios. (2017). Agresiones a la libertad de expresión disminuyen en un 40%. Fundamedios. <http://bit.ly/3SK63ZC>
- Fundamedios. (2019). *¿El año del cambio de marea para la libertad de expresión?*. Fundamedios. <https://bit.ly/3yqijVS>
- Fundamedios. (2019). Paro: 37 casos de agresiones contra periodistas están en la Fiscalía. Fundamedios. <https://bit.ly/3YxjaPc>
- Fundamedios. (2020). 2020 un año entre las muertes por COVID y la desinformación. Fundamedios. <http://bit.ly/3ZzwP9G>
- Fundamedios. (2021). Durante el Gobierno de Lenin Moreno 1702 periodistas y medios de comunicación fueron agredidos. El asesinato de Nos Faltan 3 fue el caso emblemático. Fundamedios. <http://bit.ly/3ZFA27O>
- Fundamedios. (2021). Ecuador 2021: ...Y a los periodistas nos siguen pegando bajo. Fundamedios. <https://bit.ly/3Jt0L1K>
- Fundamedios. (2023). *El periodismo ecuatoriano, blanco del crimen organizado*. Fundamedios. <https://bit.ly/40U6rbL>
- GK City. (2021). *¿Qué es el caso Arroz Verde?*. GK City. <http://bit.ly/3mK4COY>

- Guarnizo-Delgado, J., Villaroel-Silva, D. & Romero-Quiroga, K. (2022). Transformación del periodismo hacia las plataformas digitales. *Revista RECIAMUC*. 6(3), 359-366. [10.26820/reciamuc/6.\(3\).julio.2022.359-366](https://doi.org/10.26820/reciamuc/6.(3).julio.2022.359-366)
- Hernández-Sampieri, R. (2014). *Metodología de la investigación*. McGRAW-HILL Education.
- Hidalgo, D. & Torres, F. (2016). La navaja suiza del reportero: Herramientas de investigación en la era de los datos masivos. Hapana Corp S.A.C. <https://bit.ly/3E1gMsp>
- Instituto de Ciencias Aplicadas y Tecnología. (2022). *Vigilancia tecnológica en Ciberseguridad*. <https://bit.ly/3IzvYyA>
- Instituto Federal de Telecomunicaciones. (2015). *Ciberseguridad*. <http://bit.ly/3ZoWKQX>
- Jordán-Correa, D., Samaniego-Rivas, G., Gutiérrez-Páez, D. & Rivera-Arreaga, A. (2020). El periodismo de investigación, un desafío en las aulas universitarias. *INNOVA Research Journal*, 3(5), 249-271, <https://doi.org/10.33890/innova.v5.n3.2.2020.1629>
- Levoyer, S. (2015). Periodismo de investigación, ¿el espacio perdido en el Ecuador?. *Universidad Andina Simón Bolívar*. <https://bit.ly/3YOPcXa>
- Leyva-Méndez, A. (2021). Análisis de políticas públicas de seguridad cibernética. *Revista Científica Polo del Conocimiento*. 6(3), 1229-1250. <http://dx.doi.org/10.23857/pc.v6i3.2431>
- Martínez, O. (2010). *Semillas de periodismo*. Monterrey: Universidad Autónoma de Nuevo León.
- Mateos-Robles, M. (2017). Análisis de los datos de los papeles de Panamá usando métodos de I.A. [Unpublished doctoral/master dissertation]. Universidad Autónoma de Madrid.
- Niño, V. (2011). *Metodología de la investigación: diseño y ejecución*. Ediciones de la U.
- Ordóñez, L. (2022). *Claves para presentar proyectos de investigación*. Universidad de Rosario. <https://bit.ly/3K2Awy4>
- Pereira, F. (2010). El mundo de los periodistas: aspectos teóricos y metodológicos. *Comunicación y Sociedad*, 1(13), 101-124. <https://bit.ly/3Zk5FmO>
- Puertas, M. (2019). *Arroz verde en la salud. El reparto de los hospitales (II)*. Periodismo de Investigación. <http://bit.ly/3T5tzjO>
- Querejeta, Alejandro. 2011. *Periodismo de Investigación*. Quito: Paradiso.
- Quevedo, J. (2017). *Investigación y prueba del cibercrimen*. [Unpublished doctoral dissertation]. Universidad de Barcelona.
- Ramírez-Gutiérrez, E. (2022). Cyberpunk: Crítica a la sociedad posmoderna en la primera calle de la soledad. *Revista Mitologías Hoy*. 27(1), 129-144. <https://doi.org/10.5565/rev/mitologias.723>
- Sierra-Caballero, F. (2019). La entrevista en profundidad: Función, sentido y técnica. In J.A González & C.M Krohling, *Arte y oficio de la investigación científica: Cuestiones*

epistemológicas y metodológicas (pp. 301-379). Ediciones Ciespal. <http://bit.ly/3ZV3ar7>

Sistema Económico Latinoamericano y del Caribe. (22, septiembre 26). La ciberseguridad superó el 50% de las inversiones de las empresas de América Latina en 2022. *Sistema Económico Latinoamericano y del Caribe*. <http://bit.ly/3jSwW0w>

The Conversation. (2020, noviembre 25). Los ataques en redes a mujeres periodistas se extienden cada vez más al mundo real. *The Conversation*. <http://bit.ly/3YnENCa>

UNESCO. (2019). Manual de periodismo de investigación: ética / narrativa / investigación / seguridad.

Universidad San Francisco de Quito. (2023). *Convocatoria Volumen 7 de la serie monográfica #PerDebate Resiliencia e Innovación*. <http://bit.ly/3JaL51q>

Villalba, A. (2017). Análisis de las ciberamenazas. *Cuadernos de estrategia*, 1(185), 97-138. <http://bit.ly/3y18SMI>

ANEXO A: MATRIZ DE REGISTRO DE INFORMACIÓN

Periodismo de investigación y seguridad digital en Ecuador: Un análisis de las prácticas periodísticas y la formación en la protección de datos desde 2017				
PROBLEMA	OBJETIVOS	PREGUNTA	CATEGORÍAS	METODOLOGÍA
1. Problema General	1. Objetivo General	1. Pregunta de Investigación	Categoría 1	1. Tipo de investigación
¿Cuáles son 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 nuevos trabajos?	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, con el fin de fortalecer el ejercicio periodístico y fomentar la participación del país en los casos de investigación.	¿Cuáles son los datos de identificación del periodista?	Nacionalidad, trayectoria, medio de comunicación	Cualitativa
	2. Objetivos Específicos		Categoría 2	2. Enfoque
	Describir la situación del periodismo de investigación ecuatoriano, enfatizando en los ciberdelitos u otros hechos relacionados con protección digital de datos, a partir de 2017.	¿Cuáles son las herramientas de protección de datos que utiliza el periodista en las investigaciones?	Uso de herramientas en protección de datos	Descriptiva
	Definir el concepto de prácticas periodísticas en protección de datos para combatir el aumento de ciberdelitos en Ecuador desde la normativa de comunicación y de seguridad digital.		Categoría 3	3. Método
	Diseñar y ejecutar una metodología			

ANEXO B: CUESTIONARIO PARA ENTREVISTAS

1. Perfil del entrevistado

- ¿Cuál es su nombre, edad y lugar de nacimiento?

- ¿Cuál es su cargo?
- ¿Cuál es el nombre de su medio y el tiempo de permanencia?

2. Trayectoria periodística

- ¿Cuántos años lleva ejerciendo el periodismo?
- ¿Qué es para usted periodismo de investigación?
- ¿Cómo ha cambiado el periodismo de investigación con el aumento de tecnología?
- ¿Qué investigaciones ha realizado desde 2017? ¿Con qué tipo de información ha trabajado? (cantidad de datos)
- Según su experiencia, ¿cómo era el periodismo de investigación en la época del gobierno de Rafael Correa y cómo es ahora?

3. Uso de herramientas en seguridad digital

- ¿Qué es para usted la seguridad digital?
- ¿Considera importante el uso de herramientas digitales para proteger sus datos en el periodismo de investigación?
- ¿Usa herramientas digitales para proteger la información?
- ¿Qué tipos de herramientas en seguridad digital utiliza y para qué (como almacenamiento de contraseñas o bóvedas de información)?
- ¿Recibió algún tipo de capacitación o clase sobre seguridad digital para el manejo de estas herramientas?
- ¿En el medio en el que está tienen protocolos de seguridad digital?
- ¿Usted ha tenido alguna experiencia sobre ciberataques? En caso de tenerla, ¿cuáles fueron las consecuencias?
- En caso de haber recibido amenazas, ¿alguna vez esas amenazas traspasaron la pantalla y dañaron su integridad física?
- ¿Qué haría en caso de ...?
 - Ciberataque
 - Ciberamenaza
 - Ciberacoso
- ¿Cómo trabajaría en un ambiente colaborativo para compartir información?

4. Derecho a la información

- ¿Son importantes las prácticas sobre seguridad para el ejercicio de los derechos de información y comunicación en el Ecuador?
- ¿Considera que la legislación del país protege a los periodistas de investigación?

ANEXO C: CARTA DE VALIDACIÓN

Esta carta de validación busca aprobar el cuestionario de preguntas para utilizarlos en entrevistas a profundidad con el fin de responder a la pregunta de investigación: ¿Cuáles son 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 nuevos trabajos?

1. Datos generales

Nombre: Eric Samson
Especialidad: Periodismo
Fecha: 13/03/2023

2. Observaciones en cuanto a:

1. Categorías

2. Contenido

3. Estructura de las preguntas

3. Observaciones en cuanto a:

1. Pregunta de investigación

2. Objetivo

4. Aportes y/o sugerencias:

Luego, de revisado el documento, procede a su aprobación.

SI

NO

Carta de validación

Esta carta de validación busca aprobar el cuestionario de preguntas para utilizarlos en entrevistas a profundidad con el fin de responder a la pregunta de investigación: ¿Cuáles son 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 nuevos trabajos?

1. Datos generales

Nombre: Eric Samson
Especialidad: Periodismo
Fecha: 16/03/2023

2. Observaciones en cuanto a:

- Categorías** Perfil: OK - Agregar el tiempo de permanencia en el último medio. ① Trayectoria ② Herramientas. Podría agregar una categoría sobre experiencias personales en ciberdelitos/no solo en una pregunta.
- Contenido** Agregar tiempo de permanencia en los medios en el 1 o 2 // En el 2, las preguntas sobre periodismo de investigación son algo generales, podría ir ex plico con la necesidad de protección de datos.
- Estructura de las preguntas** Faltaría una sobre las amenazas zarcadas o no en caso de haber sido víctima de ciberdelitos. Podría tener una pregunta específica por passwords y bitudes digitales.

3. Observaciones en cuanto a:

- Pregunta de investigación** Es la 4? la veo algo obvia, con respuesta obligatoria.
- Objetivo** Tema interesante y de actualidad.

- Aportes y/o sugerencias:** Son muchas preguntas. De repente, difícil que sus fuentes respondan a todo.

Luego, de revisado el documento, procede a su aprobación.

SI

NO