VISUAL REVIEW | Vol. 18, No. 8, 2026 | ISSN 2695-9631

International Visual Culture Review / Revista Internacional de Cultura Visual

https://doi.org/ 10.62161/revvisual.v18.6485

SEGURIDAD DIGITAL Y CIBERSEGURIDAD PERIODÍSTICA

Riesgos y desafíos: Caso Ecuador y Perú

Digital Security and Cybersecurity in Journalism.
Risks and Challenges: The Cases of Ecuador and Perú

KRUZKAYA ORDÓÑEZ [1]
kordonez@utpl.edu.ec
LUIS-ROLANDO ALARCÓN-LLONTOP[2],
luis.alarcon@upn.edu.pe
ABEL SUING [3],
arsuing@utpl.edu.ec
LUIS ORDÓÑEZ PINEDA [4]
loordonez@utpl.edu.ec
[1,3,4] Universidad Técnica Particular de Loja, Ecuador
[2]Universidad Privada del Norte, Perú

PALABRAS CLAVE

Periodismo
Ciberseguridad
Seguridad digital
Ciberviolencia
Protección de datos

RESUMEN

El periodista se enfrenta a un entorno digital de ataques cibernéticos, amenazas, robo de datos y extorsión en línea. Este estudio levanta un diagnóstico en Ecuador y Perú para indagar sobre los desafíos que encaran los periodistas y qué medidas de ciberseguridad están implementando. La metodología es mixta, se utiliza una encuesta diseñada sobre la base de las Estrategias de Ciberseguridad y las Leyes de Protección de Datos Personales, y una entrevista complementaria. Los resultados evidencian mayor presión y vulnerabilidad para el ejercicio periodístico y la ciberseguridad y la protección de datos se convierten en una dimensión estructural del periodismo.

Recibido: 03/ 07 / 2026
Aceptado: 20/ 10 / 2026

1. Introducción

La seguridad digital y la ciberseguridad requieren especial atención porque toda actividad y en este caso la periodística está ligada estrechamente al mundo digital, espacio en el que se gestan grandes cantidades de información que requieren observación e indagación y por el cual navegan los periodistas y las personas en general. Por lo tanto, la identificación de riesgos en el caso de los periodistas, se convierte en una acción fundamental debido a las crecientes amenazas que van desde ataques cibernéticos siendo la detección, inspección y remediación procesos preventivos importantes. Así también el robo de datos, acoso y extorsión en línea (Phillips, et. al. 2025), hasta la manipulación de información, situaciones que afectan la "libertad de medios de comunicación y la seguridad de las periodistas [que sufren] una peligrosa regresión en casi todas las regiones del mundo y que para Pauner Chulvi este retroceso se acentúa:

> […] en entornos no democráticos en los que los profesionales de los medios se enfrentan a una mayor intimidación por el uso indebido de leyes y por medidas adoptadas por las autoridades públicas para desacreditar su trabajo. […] El número de amenazas, ataques de espionaje digital y presiones contra ellos ha aumentado en los últimos años deteriorando gravemente su ámbito de trabajo (2024, p. 190).

Los riegos digitales que enfrentan los periodistas empiezan con las actividades diarias que dependen en gran medida de la mensajería utilizando sistemas como computadores, dispositivos móviles en los cuales, de forma escasa, utilizan sistemas de seguridad o codificación de datos, así lo señala la encuesta aplicada por Freedom House y el Centro Internacional de Periodistas en ciudad de México. A partir de estos resultados se recomienda, realizar estudios en cada territorio para medir el pulso de la seguridad digital y la incorporación de medidas de ciberseguridad para tomar acciones que contribuyan a "minimizar la vulnerabilidad de los periodistas y blogueros que cubren temas de alto riesgo tales como el narcotráfico, el crimen organizado, corrupción, violencia, abusos y violaciones a los derechos humanos" (Sierra, 2013, p.14).

Sobre violaciones a los derechos humanos un informe publicado por el Observatorio Latinoamericano de Amenazas digitales (2025) destaca que en Ecuador en el año 2023 se presentaron más de 300 ciberataques en especial en contra de un portal periodístico Indómita Media que publica temas relacionados con el deterioro de la situación de los derechos humanos. Estos informes de seguimiento los realiza en el Ecuador, Fundamedios, fundación que viene registrando una serie de ataques, como es el caso de las elecciones presidenciales del mismo año en el que, 23 periodistas y medios de comunicación fueron atacados por enjambres digitales a través de un troll center:

> que tienen la característica de activarse en determinadas coyunturas, cuando necesitan sentar un discurso o atacar un mensaje adversario. Se activaron en octubre de 2019, durante la pandemia del coronavirus para sembrar desinformación; durante la liberación del expresidente Jorge Glas —sentenciado por corrupción—, en abril de 2022; durante el paro nacional de junio de 2022 y […] a puertas de las elecciones seccionales, con un claro objetivo: de posicionar al correísmo y atacar a quienes van contra su construcción narrativa (2022, p.12).

En Perú, el escenario es similar, tanto los medios, periodistas, sectores estratégicos (manufactura, telecomunicaciones, salud y servicios financieros) ya no son víctimas colaterales, sino objetivos primarios de cibercriminales que buscan interrumpir servicios esenciales, robar datos sensibles. En este escenario la inteligencia artificial (IA) se ha convertido en un arma de doble filo "los atacantes recurren a sistemas FraundGPT o WormGPT para crear correos de phishing extremadamente realistas, automatizar campañas de ingeniería social y mapear superficies de ataque" (Meza Capcha, 2025).

Además, el escenario se agudiza porque solo el 27% de la población peruana escoge una carrera relacionada con la ciberseguridad e IA frente a un 31% de empresas que enfrentan

dificultades en el ámbito digital por la falta de profesionales con las competencias en estas áreas, en las que se incluyen a las empresas de medios (Forbes, 2025).

La violencia digital se expande vertiginosamente con el fin de atacar infraestructuras de la red o hacen uso de la tecnología digital para dañar a personas u organizaciones (Setyowati, 2023) acciones de las cuales no están excentos medios y periodistas. Por ello, es necesario que tengan una comprensión elevada sobre la importancia de la ciberseguridad para sortear ser blanco de ataques y minimizar el riesgo.

Con referencia a este último punto, Di Salvo (2022), en su trabajo Seguridad de la información y periodismo, trae a colación las revelaciones realizadas en el año 2013 por Edward Snowden que pusieron en relieve las graves implicaciones de la vigilancia masiva y las amenazas digitales para la seguridad de los periodistas y sus fuentes.

Entre las amenazas más conocidas está el sofisticado software de espionaje y vigilancia Pegasus "aplicación que suele conocerse como Spyware [se instala en el móvil] a través de un enlace y aprovechándose de las vulnerabilidades de su sistema operativo se queda trabajando en segundo plano para permitir espiar remotamente" a través del celular o computador (Xataka, 2022). Con este software, de origen israelí, miles de periodistas y opositores de todo el mundo han sido espiados por gobiernos.

Lo que para Bradshaw y Howard son las ciber-tropas conceptaulizadas como "equipos gubernamentales, militares o de partidos políticos comprometidos con la manipulación de la opinión pública a través de las redes sociales" (2017, p. 3), siendo un fenómeno generalizado y global que responde a intereses de dominio político, económico y sobre todo de poder. Según lo autores los ataques digitales persiguen objetivos según el régimen político, en unos van orientados al control de la opinión pública.

En este sentido, los riesgos y desafíos que existen para los periodistas son inminentes ha medida del cómo se producen y difunden las noticias en el panorama mundial digital; así lo documenta Joyanes Aguilar en su obra dedicada a recoger "las noticias de ciberataques a ciudadanos, organizaciones y empresas, y hasta instalaciones críticas de países como plantas de energía química, centrales nucleares o fábricas de diferentes índoles" temas que se han vuelto habituales en las portadas de los diversos medios de comunicación "no solo escritos sino en radio, televisión y, naturalmente, los medios electrónicos de Internet" (2011, p. 15). Con el escenario adverso, el periodismo juega un papel fundamental por la información que genera, además han integrado en su trabajo dispositivos y acciones digitales lo que hace que su trabajo se centre en pensar en la seguridad digital de los periodistas, medios y fuentes.

Así también, "las nuevas tecnologías no solo permiten la vigilancia comercial y estatal, sino que ofrecen nuevas oportunidades para que los usuarios se protejan de la vigilancia"(Tsui y Lee, 2019) con acciones como el cifrado de datos. Estas acciones que se exponen para el común de las personas "plantea interrogantes sobre la concienciación y el conocimiento de los periodistas para usar estas herramientas para comunicarse de forma privada y segura con fuentes, colegas y editores" Tsui & Lee, 2019). Adicionalmente, los periodistas afirman en el estudio publicado por Waters (2018) que la vulnerabilidad, las amenazas reales o percibidas, de vigilancia gubernamental masiva, ha llevado a que su forma de trabajar cambie, lo que dificulta el trabajo y perjudica su comunicación con las fuentes. Hay que reconocer hasta que punto los periodistas poseen libertad digital.

1.1. Ciberseguridad y protección de datos

La ciberseguridad en el periodismo ha sido estudiada académica y científicamente desde distintos puntos de vista. En la región son importantes las investigaciones de Ordoñez y otros (2024) sobre el panorama legal de protección de datos en referencia al periodismo y el de Ordoñez y otros (2024) sobre las estrategias estatales llevadas a cabo para garantizar ciberseguridad al gremio. Otros trabajos han hurgado el tema de la ciberseguridad en relación a la desinformación acción concebida como un riesgo democrático (Rodríguez Fernández, 2020). También en Montañez Ramírez (2023) que aborda un estudio sobre las medidas preventivas de ciberseguridad, así mismo Mendoza Michilot, Dejo Vásquez y Najar-Ortega (2025) que indagan sobre el papel de los

medios frente al fraude informático, difusión, prevención y alfabetización. Con estas revisiones se ratifica la importancia de obtener la voz de los propios periodistas, sin embargo, no ha sido llamada para manifestarse sobre su propia ciberseguridad, lo que abre una brecha interesante e importante de cubrir con esta investigación.

Cuando se habla de ciberseguridad se establece una relación directa con la protección de datos y estos auntos son cruciales en el panorama digital, porque al comprender e implementar los principios para usar y utilizar las tecnologías emergentes, se garantiza la seguridad de los activos digitales y la información sensible y confidencial.

> La ciberseguridad propende por establecer medidas para evitar la ejecución de procesos no autorizados cuyos efectos pueden comprometer el sistema informático de una organización, [en otras palabras] busca blindar las infraestructuras tecnológicas que respaldan las operaciones de una organización que hace uso de hardware y software (Hernández Bejarano & Baquero Rey, 2025, p. 6).

La ciberseguridad posee estrategias y medidas para proteger, información, aparatos.y personas de ataques, vulneraciones y robos de información. Este accionar lleva a fundamentar principios como es la autenticación y control de acceso, cifrado y detección de amenazas, medidas y prácticas diseñadas para proteger los recursos en la nube del acceso no autorizado, las filtraciones de datos y otras actividades maliciosas (Tiwari, et.al, 2024).

Se incorporan a este proceso tecnologías emergentes: la IA y el blockchain que impulsan el crecimiento y poseen fortalezas significativas en el "análisis continuo de amenazas de detección de anomalías, la eliminación de fraude y el modelado predictvivo de eventos cibernéticos" que va más allá de la "compensación reactiva y se centra en la reducción proactiva de riesgos y el procesamiento automático de siniestros (Viji Gripsy, et-al. 2026).

Pero no solo la seguridad se concentra en la protección de ataques; sino, también en la defensa de los derechos de las personas, de los periodistas y sus redes, así como, la libertad de expresión, este último punto es cuestionable porque algunos Estados poseen el dominio absoluto de las redes y de los datos.

Desde el plano legal, la ciberseguridad de los periodistas de ambos países andinos que nos ocupa este estudio está resguardada por sendas leyes dirigidas a la protección general de datos personales. Sancionada en 2011, la Ley No 29733, Ley de Protección de Datos Personales (LPDP) en Perú, norma el tema para todos los ciudadanos sin distingos y por extensión para los periodistas (Congreso de la República del Perú, 2011). La Ley contempla un reglamento con acciones que se han implementado de a pocos, y en sus 15 años de vida ha conocido algunas modificatorias acordes, la mayoría, al acomodo de las potencialidades digitales progresivas. Una década después, Ecuador aprobó la Ley Orgínica de Protección de Datos Personales, garantizando a los ciudadanos el derecho a controlar su información personal extendiendo su regulación para la recolectar, usar los datos, estableciendo principios y derechos en torno al acceso, rectificación y eliminación) y obligaciones para los responsables del tratamiento aplicando el Reglamento expedido tres años (2023) despúes de la vigencia de la ley.

Con el contexto expuesto esta investigación persigue el objetivo de indagar sobre los riesgos y desafíos que enfrentan los periodistas ante los ataques, la ciberviolencia y qué medidas de ciberseguridad con equipos y datos están implementando. Los resultados servirán no sólo a levantar un marco referencial sobre la cuestión sino también para que el gremio periodístico en sí, pero también Estado, Academia y organizaciones de la sociedad civil dialoguen respecto a la situación que se halle y propongan mejoras integradas.

2. Metodología

La investigación se sostiene en el paradigma socio-crítico, que al combinar las perspectivas cuantitativa y cualitativa- marca evolución de la segunda superando lo exclusivamente cuantitativo (Finol de Franco & Vera Solórzano, 2020). El enfoque es, entonces, mixto: fusiona las perspectivas mencionadas haciéndolas interactuar y potenciándolas (Arispe et al., 2020). Desde lo cuantitativo, el alcance descriptivo centró en identificar, describir y analizar las características

de un fenómeno (Hernández-Sampieri & Mendoza Torres, 2023). En lo cualitativo, la tipología fenomenológica supuso investigar ese fenómeno desde la vivencia de los sujetos (Castillo, Romero & Mínguez, 2022). El diseño general es no experimental de corte transversal, pues no se intervino en las variables de estudio en ningún momento (Chuquiruna & Benites, 2019). El diseño específico fue mixto, cuantitativo con salida cualitativa para afrontar mejor un problema (Creswell, 2014; Cabrera, 2023). El tipo puntual de diseño mixto fue el secuencial explicativo, que se emplea cuando el investigador tiene una idea general del fenómeno y busca adentrarse en aspectos eventualmente causales (Barreto & Lezcano, 2023).

La unidad de análisis, "concepto abstracto/teórico/tautológico, representa una categoría analítica, no un caso concreto" y que hace trilogía con la unidad de observación y la unidad de información, (Barriga & Henríquez, 2011, p. 64), fue el colectivo de periodistas ecuatorianos y peruanos. Supone una población no finita, dadas las características laxas para ejercicio en general. Para el estudio se toman las datas oficiales de dos gremios reconocidos en ambas naciones, facilitadas tanto por el Consejo de la Comunicación del Ecuador (2025), como por el Colegio de Periodistas del Perú (2025): en el primer caso 983 y 11.696 en el segundo. Las muestras fueron no probabilísticas por conveniencia y por criterio, respectivamente próximas a los investigadores y bajo pautas viables de elección (Benites & Villanueva, 2015). Los criterios de inclusión fueron: 1) ser periodistas en ejercicio pleno, 2) representar a algún medio de comunicación directa o indirectamente y 3) tener independencia de funciones que supusieran conflictos de interés con el oficio. Los criterios de exclusión: 1) ser sujeto de sanción disciplinaria o administrativa por alguna institución gremial y 2) ser autor o coautor en estudios similares al presente.

La muestra fue de 358 periodistas; 203 del Ecuador y 155 de Perú. En la recolecciónde datos no se realiza distinción de sexo en razón que la investigación indaga el ámbito de la profesión.

La técnica cuantitativa para recolectar datos fue la encuesta, que en palabras de Wilson et. al.(2024) "[…] busca generar datos prácticos que informen y promuevan las prácticas educativas, las políticas y la investigación futura" (p. 1389). El instrumento fue un cuestionario, en línea, vía Google Forms, válido, moderno y útil en estos tiempos (Arias, 2021). El instrumento se compone de 12 preguntas agrupadas en bloques temáticos: a) Ataques en ciberviolencia, b) Conocimiento y desafíos con la ciberseguridad, c) Conocimiento e implementación de la Ley de datos personales, d) Tratamiento de información sensible. El instrumento se erigió sobre la base de las Estrategias de Ciberseguridad y las leyes: Ley de Protección de Datos Perú, No 29733; y la Ley Orgánica de Protección de Datos de Ecuador (21 de mayo de 2021).

Fueron dos versiones de un mismo instrumento que permitiese comparaciones validado en contenido por juicio de tres expertos, y se cumplió validez de criterio -el original comparte rasgos con instrumentos similares- y validez de constructo -se sostiene en amplia base teórica-. Tras aplicar una prueba piloto a 12 sujetos similares en características a la población, se sometió a prueba de confiabilidad por consistencia por Alfa de Cronbach, lo que dio un índice superior a 0.7, aceptable según la literatura.

El apartado cualitativo se sostuvo en la entrevista, acto seguido de la encuesta, técnica que acudió a la conversación abierta con objetivos puntuales (Armijo et al., 2021); y conveniente sobre todo en investigaciones de ciencias sociales y humanidades, para ampliar en una materia investigada (Lopezosa, Codina & Freixa, 2022). Para esta investigación la guía de la entrevista fijo tres preguntas ancla que giraron en torno a: 1) el resguardo de la confidencialidad de la información proveniente de las fuentes; 2) las medidas adoptadas para la protección de datos personales de fuentes, colaboradores y personas involucradas en el trabajo periodístico; y 3) la implementación de medidas para evitar la pérdida, el acceso no autorizado o el mal uso de datos sensibles.

De cara a analizar la información obtenida de la fase cuantitativa, se usó estadística descriptiva, como medidas de posición, de tendencia central y de dispersión (Armijo et al., 2021). Para analizar la fase cualitativa, se cumplió una trayectoria de análisis narrativo, (Arispe et al. 2020). Sobre las dimensiones y categorías de análisis, aplicando estrategias de triangulación, según se demanda para estudios mixtos los datos se integraron, con lo cual se pudo discutir hallazgos y arribar a conclusiones.

El estudio cumple los aspectos éticos prescritos en los tres principios de la ética en investigaciones con seres humanos: 1) respeto a las personas, respetando su autonomía y autodeterminación para decidir colaborar o no con el estudio; 2) beneficencia, o no maleficencia, el participar no supone riesgo de daños; y 3) justicia, ya que la selección de participante cuidó ser lo más equitativa en procedencias, estratos, géneros, etc. (Álvarez Viera, 2018).

2. Resultados y Discusión

Tras la aplicación metodológica y efectuar el proceso de depuración de resultados, se realizó el análisis comparativo de la información recabada, aplicando la estadística descriptiva con las medidas de posición y tendencia central que se representan por la moda (categoría más frecuente) y la medida de dispersión por el conteo absoluto y relativo. El análisis cuantitativo se lo aplicó agrupando las preguntas en 4 bloques temáticos (preguntas 1 hasta la 12). Se complementó con el análisis cualitativo de la entrevista abierta (en orden, preguntas 13, 14 15) para recoger opiniones de los periodistas.

Los primeros resultados del conteo permitieron identificar que los medios híbridos (tradicionales y digitales) predominan en este estudio, se contabilizaron 119 (58,62%) en Ecuador y en Perú 97 (62,58%), mientras que los nativos digitales sumaron 84 (41,38%) y 58 (37,42%) respectivamente. Esto da cuenta que, los espacios de expresión de los periodistas continúan reconociendo la coexistencia de medios tradicionales como digitales considerados canales para amplificar la información, validando su accionar y la credibilidad en el entorno donde operan. Se aplicó la anonimización por temas de seguridad.

Una vez que se identificó el tipo de medio, el análisis temático se organizó en cuatro bloques, la primera categoría de estudio es la ciberviolencia para contabilizar los ataques y amenazas que los periodistas de Ecuador y Perú enfrentan (Tabla 1). Los resultados indican que en Ecuador existe una percepción mayor de todas las opciones (48%) -ataques digitales, vulneración de datos personales, robo de información y extorsión- en relación a Perú (46%).

Tabla 1. Registro de ciberviolencia

Categoría 1: Registro	Ecuador		Perú	
	F	%	F	%
Ataques digitales	47	23%	46	30%
Vulneración de datos personales	28	14%	12	8%
Robo de información	16	8%	16	10%
Extorsión	15	7%	10	7%
Todas las opciones	97	48%	71	46%
	203	100%	155	100%

Fuente: Elaboración propia

Entre los tipos de ataques digitales, el más reportado en Ecuador son las amenazas (37,9%), seguido de robos de datos (30,5%) esta precisión permite identificar ataques concretos, asociados a la intimidación, extorsión o pérdida de información esta última considerada en el ámbito periodístico un bien digital valioso. En Perú, los resultados indican que la categoría ninguna (27,1%), seguida de bloqueos (25,8%), resultan de una menor percepción e identificación de ataques digitales en relación a la mayor percepción, incidencia real, de ataques que se registra en Ecuador, lo que sugiere una mayor exposición de los periodistas ecuatorianos o en su defecto un mayor nivel de conciencia y capacidad de clasificación de ataques digitales, ante una menor percepción o identificación de ataques por parte de periodistas peruanos. Lo que supone no necesariamente la no ocurrencia de incidentes, sino la existencia de brechas en la percepción, el conocimiento o los mecanismos de reporte que se apliquen en las redacciones.

Tabla 2. Tipo de ataque digital

Categoría 1: Tipo	Ecuador		Perú	
	F	%	F	%
Amenazas	77	37,9%	35	22,5%
Robo de datos	62	30,5%	35	22,5%
Bloqueo	45	22,1%	40	25,8%

Intentos de ataque	6	2,9%	3	1,9%
Ninguna	13	6,4%	42	27,1%
	203	100%	155	100%

Fuente: Elaboración propia

La segunda categoría de análisis indaga sobre el nivel de conocimiento de ciberseguridad (Tabla 3) y los desafíos que en la era de la transformación digital se plantean en los distintos campos del ejercicio profesional (Tabla 4). Precisamente, en el ámbito periodístico, la ciberseguridad se presenta como un elemento técnico y jurídico que aporta a la seguridad digital, frente al tratamiento de la información. "Un claro ejemplo de esto es la publicación en 2016 de una investigación periodística titulada «Panama Pappers» en la cual se utilizaron bases de datos privados para revelar información de interés público" (Ramírez, 2020, p.48). p. 48). Desde esta perspectiva, a partir de los resultados obtenidos, resulta importante que exista un alto nivel de conocimientos relacionados con ciberseguridad, considerando los niveles de digitalización que, en la actualidad, aplican los medios de comunicación.

Con esta apreciación sugerente los resultados indican que los periodistas de ambos países afirman sí tener conocimientos sobre el tema (Tabla 3), sin embargo, entre los desafíos principales que se detectan (Tabla 4) es la falta de capacitación continua y especializada en Ecuador (47,78%) y Perú (36.77%) que limitan en algunos casos la gestión efectiva para la prevención de riesgos digitales que se presentan con: la vigilancia gubernamental y persecución del crimen organizado que en Ecuador y Perú se registran con el porcentaje del 21%, evidenciándose una preocupación compartida.

Otros de los desafíos que se observan y reportan con un 21%, en ambas naciones, es el manejo tecnológico que no precisamente es el adecuado y acertado para cada tipo de situación, lo que refleja limitaciones técnicas, infraestructura insuficiente y falta de personal especializado en ambos contextos.

Por otro lado, a los periodistas se les preguntó si han tenido acceso a recursos, información clara y oportuna que les permita enterarse del tema de ciberseguridad, los datos reflejan que en Perú existe mayor dificultad (9%) en relación a Ecuador (4,93%), estos resultados determinan la necesidad de organizar e instaurar equipos interdisciplinarios, en mayor medida en Perú (10.97%) en relación al pronunciamiento de los periodistas de Ecuador (4,43%). Esto conlleva a deducir que en Perú existe una elevada preocupación de integrar profesionales especializados técnicos y estrategas en gestión de ciberseguridad, así como profesionales especialistas en derecho y protección de datos.

De manera transversal en ambos países existe preocupación principalmente por la vigilancia del crimen organizado, la falta de capacitación y manejo tecnológico adecuado, que a la vez se convierten en desafíos relevantes lo que refuerza la acepción que la ciberseguridad no es un problema individual sino un fenómeno estructural que requiere la integración de capacidades técnicas y organizativas. Estos resultados permiten de forma parcial confirmar que, la falta de capacitación no es el principal ni único desafío que se presenta en el entorno periodístico.

Estos supuestos que se enmarcan como desafíos tienen relación con las acciones que se deben implementar desde la propia institucionalidad de los medios de comunicación. Al respecto, se advierte —desde la perspectiva de la corresponsabilidad— la importancia del *compliance*, como una teoría que obliga a adoptar en las instituciones medidas de prevención, entre ellas, la formación y capacitación en líneas técnicas relacionadas con el tratamiento de la información. Naturalmente, en esta línea, queda resaltado —como un tercer supuesto— la función del Estado, en la función de represión de posibles afectaciones a la actividad periodística.

Tabla 3. Conocimientos sobre ciberseguridad

Categoría 2: Conocimiento	**Si**		**No**	
	F	**%**	**F**	**%**
Ecuador	146	71,92%	57	28,08%
Perú	121	78.06 %	34	21,94%

Fuente: Elaboración propia.

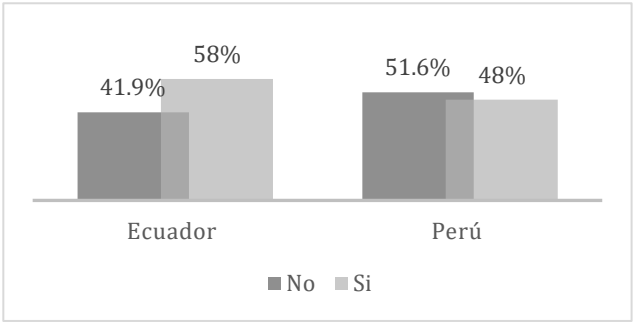
Tabla 4. Desafíos que enfrentan

Categoría 2: Desafíos	Ecuador		Perú	
	F	%	F	%
Falta de capacitación	97	47,78	57	36.77
Vigilancia y persecución del crimen organizado	44	21,67	34	21,94
Falta de manejo tecnológico adecuado	43	21,18	33	21,29
Acceso a información sobre ciberseguridad	10	4,93	14	9,03
Necesidad de organización con equipos interdisciplinarios	9	4,43	17	10,97

Fuente: Elaboración propia.

La tercera categoría se relaciona con el conocimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP- Ecuador y LPDP- Perú), los resultados indican que existe una opinión, relativamente, dividida respecto al conocimiento de la Ley (Figura 1.) En Ecuador el rango de conocimiento es del 58% frente a un 41.9% de desconocimiento. No obstante, llama la atención que prevalezca un criterio de desconocimiento en Perú, el no conocer registra un porcentaje mayor 51,6% en relación a los periodistas que sí (48%), considerando que la Ley de Protección de Datos Personales N.°29733 fue expedida en el año 2011. Al respecto, tendría que advertirse que, la autoridad de control tiene un papel importante, por cuanto, está destinada a "promover campañas de difusión y promoción sobre la protección de datos personales" —art. 33—; la brecha regional es de casi 10 puntos porcentuales a favor de Ecuador.

Figura 1. Conocimiento de la Ley de Protección de Datos



Fuente: Elaboración propia.

Continuando con la indagación, se preguntó sobre la implementación de las Leyes de Protección de Datos Personales en la empresa mediática (Tabla 5.), los resultados, basados en la escala de Likert ordinal, evalúan acciones de implementación según lo que establece la ley, los datos revelan un consenso en las respuestas de los periodistas de Ecuador y Perú, los porcentajes del totalmente de acuerdo y el acuerdo en sumatoria, se acercan al 100%. Esta tendencia representa medias entre 4,0 y 4,58 de respuestas "de acuerdo y totalmente de acuerdo", con desviación estándar baja; este patrón consolida la aceptación de la implementación de la LOPDP-Ecuador y LPDP- Perú y se descarta la ambivalencia significativa, al no observarse medias cercanas al punto neutral 3.

Aspectos de la LODP	Totalmente de acuerdo EC	De acuerdo EC	En desacuerdo EC	Totalmente de acuerdo PE	De acuerdo PE	En desacuerdo PE
Política Protección Datos	68.47%	30.05%	1.48%	45.81%	52.90%	1.29%
Política Seguridad Información	60.59%	38.92%	0.49%	49.03%	49.68%	1.29%
Consentimiento Uso Datos	55.67%	38.42%	5.91%	43.23%	54.19%	2.58%
Cláusulas Informativas	55.17%	38.42%	6.40%	43.87%	47.74%	8.39%
Interposición Quejas	50.74%	42.86%	6.40%	42.58%	52.90%	4.52%
Medidas Técnicas	61.08%	37.44%	1.48%	41.29%	53.55%	5.16%
Cláusulas Protección Datos	49.26%	46.80%	3.94%	40.00%	50.97%	9.03%
Notificaciones	54.19%	41.38%	4.43%	40.65%	53.55%	5.81%
Evaluación Impacto Datos	50.74%	44.83%	4.43%	40.65%	55.48%	3.87%
Capacitación Gestión Datos	63.05%	34.98%	1.97%	47.10%	49.03%	3.87%

Tabla 5. Cuadro comparativo de implementación de LOPDP (Ecuador)- LPDP (Perú)
Fuente: Elaboración propia.

Entre los aspectos prioritarios para los periodistas ecuatorianos se encuentra la implementación de la política de protección de datos personales (68,47%) que el Art. 13 menciona la publicación de políticas de privacidad como forma de cumplir con el deber de información al titular garantizando claridad en el tratamiento de datos, mención que va en concordancia con el segundo aspecto con mayor registro, capacitación sobre gestión de datos, como medida directa para la seguridad y el cumplimiento normativo (63,05%).

En Perú, los resultados se orientan a implementar medidas de evaluación de impacto del tratamiento de datos (55,48%). El Art. 13., señala que las políticas deben incluir mecanismos de evaluación del tratamiento para proteger derechos del titular. Así mismo, los periodistas están de acuerdo 53,55% con la adopción de medidas técnicas y organizativas y de seguridad para proteger los datos, el Art. 39 de la LPDP describe controles de acceso, registro de actividades y mecanismos de protección tecnológica que se cruza con el criterio de notificaciones de brechas de seguridad que incluye la obligación de tomar medidas ante riesgos o vulnerabilidades en el tratamiento de datos (Art. 16).

En relación a las preguntas 11 y 12 con las cuales se indagó el uso de herramientas y procedimientos que aplican los periodistas para la protección de datos e información sensible, los resultados del análisis comparativo de entre 10 alternativas de respuesta con elección libre, indican que, la seguridad basada en *hadware* y *sofware* aplicada en Ecuador, la realizan con discos externos para el respaldo de información sensible que se combina con la autenticación y control, (contraseñas seguras) y no contestar llamadas de desconocidos, herramientas que, combinadas con procedimientos como verificación de fuentes, que lo apuntan como prioridad, seguido de no abrir correos extraños y cambio de claves de manera constante, permiten confirmar que existe una paralelismo significativo entre conocimientos de ciberseguridad y percepción de riesgo. La visualización de riesgo digital es latente porque son equipos que están vigilantes del monitoreo gubernamental y persecución del crimen organizado (22%) dato que resulta del análisis de la categoría de ciberviolencia, a esto se suma la preocupación por las posibles pérdidas o robo de información.

Tabla 6. Cuadro comparativo implementación de herramientas y procedimientos de ciberseguridad

Herramientas de protección	**Ecuador**	**Perú**
Contraseñas / Claves Seguras (Autenticación)	**69**	**59**
Respaldo en Discos Externos / Backup	58	40
No contestar llamadas/Números desconocidos (Conciencia)	**29**	**16**
Control de Acceso / Limitar Accesos	14	3
Almacenamiento en la nube	**14**	**3**
Servidor proxi con autenticación de dos pasos y escaneo de vulnerabilidad	10	1
Cifrado/Encriptación	**4**	**24**
Aplicación firewall	4	8
Otros	**2**	**0**
Procedimientos		
Verificación de fuentes	**77**	**26**
No abrir correos /enlaces extraños (Phishing)	56	46
Control de acceso a la información (permisos)	**32**	**32**
Instalación de Software Antivirus	12	4
Análisis de procedencia de correo	**11**	**30**
Doble capa de seguridad	8	6
Evitar contacto con redes externas	**7**	**11**

Fuente: Elaboración propia.

En el caso de Perú, la seguridad basada en *sofware* y *hadware* la combinan con la utilización de discos externos para resguardo de información, la autenticación y control de acceso (contraseñas seguras) y cifrado (encriptación de datos en equipo) que aplican los medios y periodistas para dinamizar la protección de los datos e información sensible (Tabla 6.). Entre los procedimientos para la protección de datos e información sensible al igual que en Ecuador, en Perú se destaca la acción de no abrir correos extraños y el control de acceso a la información (permisos) y con tercer paso la verificación de fuentes.

Vale destacar que tanto en Ecuador y Perú las herramientas de seguridad avanzadas como trabajar con servidor proxi con autenticación de dos pasos y escaneo de vulnerabilidad, así como, el respaldo encriptado en la nube con cifrado de punto final, aplicación firewall y limitación de accesos compartidos poseen un registro menor. Esto demuestra que los procedimientos con herramientas de seguridad tienen una connotación básica. Sin embargo, se destaca que la verificación de fuentes es tan importante como el control de acceso, lo que sugiere que los periodistas integran la seguridad del dato con su trabajo esencial de protección a la fuente.

Finalmente, este apartado se concluye con la percepción cualitativa de los periodistas (preguntas abiertas 13, 14 y 15). El análisis cualitativo ofrece hallazgos relevantes en ambos países; con respecto a las estrategias de confidencialidad, a más de la verificación de fuentes, primer paso inexorable en la práctica periodística y controles de seguridad básicos, recurren a la anonimización y minimización de datos, especialmente en equipos de periodistas peruanos, lo que favorece a la reserva de la identidad de las fuentes. Además, aplican la omisión intencionada de datos personales y como mecanismo de protección comparten información delicada. Estas prácticas reducen el riesgo de vulneración de información de las fuentes y de documentos, seguimiento a la huella o rastros de papel. Estas acciones se aplican para escenarios hostiles o de vigilancia acentuada.

Un dato importante que se recalca, en ambos países los mecanismos de seguridad avanzada son marginales, pese a los riesgos a los que expresan estar expuestos y a la necesidad que indican al menos los periodistas de Perú de adoptar medidas técnicas y organizativas adecuadas.

Asimismo, los periodistas de Ecuador y Perú reconocen no aplicar estrategias formales para la protección de datos sensibles, se limitan al control de la información de forma personal basados en la confianza individual o de equipo.

Los resultados cualitativos en su conjunto presentan un escenario positivo que se traduce en una elevada conciencia sobre la importancia de la protección de datos personales, la

confidencialidad de las fuentes y el mal uso de datos y documentos sensibles, lo que refleja un nivel de madurez digital combinado con prácticas tradicionales que en algunos casos limitan la expansión de la ciberseguridad en el ámbito periodístico.

3. Conclusiones

Es importante destacar que, en el conjunto de datos cuantitativos y cualitativos analizados, los periodistas de Ecuador y Perú, que ejercen la profesión en medios híbridos como digitales, están expuestos a un escenario de riesgo vinculado con ataques digitales, ciberviolencia y vulnerabilidades relacionadas con equipos y datos.

En Ecuador los periodistas tienen una mayor exposición digital en comparación con sus pares de Perú: este resultado permite confirmar que los periodistas en Ecuador enfrentan mayor civerviolencia que en Perú. La evidencia es el reporte de amenazas, robos de datos y ataques asociados a la intimidación y extorsión o pérdida de información, lo que sugiere un contexto de mayor presión y vulnerabilidad para el ejercicio periodístico. Ante este escenario la ciberseguridad y su relación directa con la protección de datos se convierte en una dimensión estructural del periodismo, especialmente en entornos marcados por riegos asociados a la vigilancia, persecución sistemática derivados de la exposición pública que marcan la pauta para la implementación de protocolos de seguridad digital.

En cuanto a la capacitación especializada en ciberseguridad que se plantea como desafío en ambos países los periodistas y medios admiten la ausencia de una cultura y procesos de formación continua y especializada, lo que conlleva a optar por aprendizajes autodidactas e informales. Esta realidad se agudiza con la escasez de recursos institucionales y el escaso nivel de conocimiento de ciberseguridad que limitan en algunos casos la gestión efectiva para la prevención de riesgos digitales, convirtiéndose estos asuntos en preocupaciones centrales del ejercicio periodístico.

Por otro lado, en lo que refiere al conocimiento y aplicación de las Leyes de Protección de Datos Personales llama la atención que prevalezca el criterio de desconocimiento de periodistas peruanos, tomando en cuenta que la fecha de aprobación de la LPDP fue en el año 2011, lo que representa una ventaja ante Ecuador, cuya LOPDP fue expedida en el año 2021. Sin embargo, se destaca que periodistas de ambos países advierten la inclusión de políticas de protección de datos, medidas técnicas, evaluación de impacto y capacitación de gestión de datos, reglamentación que va en concordancia con las medidas de ciberseguridad de *hadware* y *sofware,* así como los procedimientos que implementan, entre los cuales se destaca la verificación de fuentes y documentos y el control de acceso lo que sugiere que los periodistas ecuatorianos valoran la seguridad del dato y la protección de fuentes. En Perú, también consideran estos procedimientos de apropiación relevante, sin embargo, su tendencia se orienta a la seguridad y protección de equipos. Finalmente, se sugiere la implementación de procedimientos de seguridad avanzada que permitan disminuir riesgos y vulnerabilidades en el ejercicio periodístico.

Esta investigación encuentra sus fortalezas tanto en la elección del tema abordado, de la máxima importancia porque se trata de las garantías primero y las prácticas para sostener aquellas luego respecto al ejercicio mismo periodístico en el orden de la seguridad digital en tiempos en que la digitalidad misma vive quizás sus momentos más intensos; así como en ofrecer una primera metodología de abordaje que aspira al enfoque mixto, desde el paradigma sociocrítico, basándose en una metodología de orden cuantitativo al inicio, para completarse con aportes cualitativos escudriñados sobre los protagonistas de la labor periodística misma, los periodistas, en una interesante muestra de los países estudiados. Con todo, el estudio reconoce limitaciones, como la imposibilidad de generalizar al 100% los resultados obtenidos al haber trabajado con una muestra no probabilística, o la ausencia de alguna otra técnica, como análisis documental, por ejemplo, que pudiera haber cruzado la información procedente de los periodistas y aportar así a una lectura más integral de la cuestión. Corresponde a otros investigadores superar estos puntos y continuar aportando en las líneas de investigación que se desprenden de la seguridad digital, en general, y la ciberseguridad periodística, en específico.

4. Agradecimientos

El presente texto nace en el marco de las líneas de investigación que mantiene el Grupo de Investigación en Comunicación y cultura audiovisual -Universidad Técnica Particular de Loja.

Referencias

Alvarez Viera, P. (2018). Ética e investigación. *Boletín Redipe* [Internet], 7 (2), 122-149. https://goo.su/QeaMUG

Arias Gonzales, J. L. (2021). *Métodos de investigación on line. Herramientas digitales para recolectar datos*. Enfoques Consulting EIRL.

Arispe Alburqueque, C. M., Yangali Vicente, J. S., Guerrero Bejarano, M. A., Rivera Lozada de Bonilla, O., Acuña Gamboa, L. A., & Arellano Sacramento, C. (2020). *La Investigación científica. Una aproximación para los estudios de posgrado.* Universidad Internacional del Ecuador.

Armijo, I., Aspíllaga, C., Bustos, C., Calderón, A., Cortés, C., Fossa, P. et al. (2021). Manual de metodología de la investigación 2021. Universidad del Desarrollo, 2021.

Asamblea Nacional del Ecuador (2021, 26 de marzo). *Ley Orgánica de Protección de Datos Personales.* Documento de acceso abierto en línea. https://short.do/kiLtUC

Barreto, J., & Lezcano, A. (2023). Análisis y fundamentación de los diseños de investigación: explorando los enfoques cuantitativos, cualitativos y mixtos basados en Creswell & Creswell (2018). *Revista Unida Científica, 7*(8), 110-117. https://goo.su/HWbRfH

Barriga, O.A. & Henríquez A., G. (2011). La relación Unidad de Análisis-Unidad de Observación-Unidad de Información: Una ampliación de la noción de la Matriz de Datos propuesta por Samaja. *Revista Latinoamericana de Metodología de la Investigación Social,* (1), 61-69. https://goo.su/zQJUEqg

Benites Romero, S. H., & Villanueva López, L. (2015). *Retroceder investigando ¡Nunca! Rendirse con la tesis ¡Jamás!* Fondo Editorial Cultura Peruana E.I.R.L.

Bradshaw, S. & Howard, F. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. University of Oxford. https://goo.su/OlaCrK

Cabrera, P. (2023). Nueva organización de los diseños de investigación. *South American Research Journal, 3*(1), 37-51. https://doi.org/10.5281/zenodo.8050508

Castillo López, M., Romero Sánchez, E., & Mínguez Vallejos, R. (2022). El método fenomenológico en investigación educativa: una revisión sistemática. *Latinoamericana de Estudios Educativos, 18*(2), 241–267. https://doi.org/10.17151/rlee.2023.18.2.11

Chuquiruna León, A. & Benites Romero, S. (2019*). Investigue. Usted también puede. Reseña de trabajos que cambiaron el mundo.* Imprenta Hesse EIRL.

Colegio de Periodistas del Perú (08 de febrero de 2025). *Data total colegiados a nivel nacional*. Documento respuesta ante pedido específico.

Congreso de la República del Perú (2011, 03 de julio). *Ley Nº 29733. Ley de Protección de datos personales.* Diario Oficial El Peruano. https://goo.su/EBxMR

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

Di Salvo, P. (2022). Seguridad de la información y periodismo: mapeo de un campo de investigación naciente. *Sociology Compass, 16*(3). https://doi.org/10.1111/soc4.12961

Finol de Franco, M. & Vera Solórzano, J.L. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. *Mundo Recursivo, 3*(1), 1-24. https://goo.su/JJp2

Forbes (8 de mayo de 2025). *El 76% de empleadores en el mundo no encuentran talento en IA y ciberseguridad.* https://goo.su/BezBRQe

Fundamedios (Publicación 2 de agosto de 2022). *Un troll center vuelve a hacer de las suyas en el país*. https://goo.su/7co19

Hernández Bejarano, M. & Baquero Rey, L. E. (2025). *Fundamentos de la ciberseguridad.* Escuela Tecnológica Instituto Técnico Central. https://goo.su/UhKlFd

Hernández-Sampieri, R. &Mendoza Torres, C. (2023). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill.

Joyanes Aguilar, L. (2011). Introducción. Estado del arte de la ciberseguridad. *Cuadernos de estrategia*, (149),11-46. https://goo.su/fyKw12C

Lopezosa, C.; Codina, L. & Freixa, P. (2022) *ATLAS.ti para entrevistas semiestructuradas: Guía de uso para un análisis cualitativo eficaz*. DigiDoc Research Group / Pompeu Fabra University, https://goo.su/tsaLBkg

Meza Capcha, E. (27 de agosto de 2025). *Ciberataques en Perú superan los 748 millones de intentos en lo que va del 2025*. Infobae. https://goo.su/2Z6gZX

Mendoza Michilot, M., Dejo Vásquez, M., & Najar-Ortega, R. (2025). El papel de los medios frente al fraude informático. Difusión, prevención y alfabetización. *Contratexto, 43*, 221-248. https://doi.org/10.26439/contratexto2025.n43.7160

Montañez Ramírez, C. (2023). *Medidas preventivas de ciberseguridad que debe tener un adulto mayor en Colombia para acceder a los servicios de internet y sus servicios [Proyecto de Grado para optar el título de Especialista en Seguridad Informática,* Universidad Nacional Abierta y a Distancia]. Repositorio institucional de UNAD. https://goo.su/OkW5pn1

Observatorio Latinoamericano de Amenazas Digitales (2025). *En la mira: seguridad y principales amenazas digitales en América Latina.* OLAD https://goo.su/zHSTH57

OECD (2018). Manual Oslo 2018 Guidelines for Collecting, Reporting and Using Data on Innovation, 4th Edition. https://doi.org/10.1787/9789264304604-en

Ordóñez, K., Suing, A., Punín, M. I., Carpio, L. (2024). Ciberseguridad y Periodismo: Estrategias para garantizar la seguridad de la información. Revista Ibérica de Sistemas e Tecnologías RISTI. 382-392. https://short.do/9mXqzS

Ordóñez, K., Puertas, L., Suing, A. (2024). *Los datos sus usos e implicaciones en espacios democráticos.* Revista Ibérica de Sistemas e Tecnologías. RISTI, 102-114. https://short.do/DosHwl

Pauner Chulvi, C. (2024). La protección de las fuentes periodísticas en la era digital y el impulso regulatorio de la Unión Europea. *Teoría y Realidad Constitucional*, (54), 189-216. https://goo.su/XFoy

Phillips, S., Hansen, M., Matsilele, A. (2025). Análisis de alcance: El panorama de riesgos digitales y soluciones de ciberseguridad para periodistas. En N. Clarke & S. Furnell (eds.) Aspectos humanos de la seguridad y garantía de la información. *HAISA 2024. IFIP Avances en Tecnologías de la Información y la Comunicación, 721.* Springer, Cham. https://doi.org/10.1007/978-3-031-72559-3_3

Ramírez, D. (2020). *La inherente tensión entre los datos personales y el periodismo*. En: INAI. (eds.) Periodismo y la protección de los datos personales (págs. 43-61). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://short.do/hwHV9Z

Rodríguez Fernández, L. (2025) Desinformación y Ciberseguridad: Impacto en las organizaciones españolas 2025. En Sierra, J., Rodrigo Martín, J. , Muñoz de Luna, A. (2025). Realidades conectadas:Medios, cultura y sociedad en la era digital, 309, McGrawHill. https://short.do/XY1RCn

Setyowati, M. S, Desila Utami, N., Habib Saragih, A. & Hendrawan, A. (2023). Strategic factors in implementing blockchain technology in Indonesia's value-added tax system. *Technology in Society*. *72*, e102169. https://doi.org/10.1016/j.techsoc.2022.102169

Sierra, J. L. (2013). *Seguridad Digital y Móvil para periodistas y Blogueros. Resultados de la encuesta entre periodistas y blogueros mexicanos*. Freedom House y ICFJ Knight International Journalism Fellow. https://goo.su/DN27Yjt

Tejero, J. (2021) Técnicas de investigación cualitativa en los ámbitos sanitario y sociosanitario. Ediciones de la Universidad de Castilla – La Mancha. https://goo.su/0zs2j

Tiwari, M., Tiwari, T., Ticku, A., Dadhwall, H. & Singh, T. (2024). Metodologías y Desafíos de las Técnicas de Ciberseguridad en el Entorno de Computación en la Nube. *ICIMMI '23: Actas de la 5ª Conferencia Internacional sobre Gestión de la Información e Inteligencia Artificial*, (182), 1 – 7. https://doi.org/10.1145/3647444.3652492

Tsui, L. & Lee, F. (2019). Cómo los periodistas comprenden las amenazas y oportunidades de las nuevas tecnologías: Un estudio de las mentalidades de seguridad y sus implicaciones para la libertad de prensa. *Periodismo, 22* (6), 1317-1339. https://doi.org/10.1177/1464884919849418

Viji Gripsy, J., Lukose, B., Sheeba, L., Mesia Dhas, JT, Jayasree, R. & Brindha, NV (2026). Mejora del seguro de ciberseguridad a través de IA y Blockchain para una gestión proactiva de riesgos. En M. Alawida, A. Almomani & M. Alauthman (Eds.), *Innovaciones y marcos de seguros de ciberseguridad en la era de la IA* (págs. 349-376). Publicaciones científicas globales IGI. https://doi.org/10.4018/979-8-3373-1977-3.ch012

Waters, S. (2018). Los efectos de la vigilancia masiva en las relaciones de los periodistas con fuentes confidenciales: Un estudio comparativo constante. *Periodismo Digital, 6*(10), 1294–1313. https://doi.org/10.1080/21670811.2017.1365616

Wilson, A. B., Bay, B. H., Byram, J. N., Carroll, M. A., Finn, G. M., Hammer, N., Hildebrandt, S., Krebs, C., Wisco, J. J. & Organ, J. M. (2024). *Journal recommended guidelines for survey-based research. Anatomical Sciences Education, 17*(7), 1389–1391. https://doi.org/10.1002/ase.2499

Xataka (2 de mayo de 2024) *Qué es Pegasus: cómo se infecta, qué puede hacer y cómo detectarlo*. https://goo.su/fntY