Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Ciberataques como Estrategia Política: Un Análisis de su Impacto en la Libertad de Expresión Durante los Periodos de Inestabilidad Política del Ecuador (2019 -2024)

Cyberattacks as a Political Strategy: An Analysis of Their Impact on Freedom of Expression during Periods of Political Instability in Ecuador (2019-2024)

Diego Arturo Vinueza Miller[1]
Miembro de las Fuerzas Armadas
Ejército Ecuatoriano
diegovinueza.97@gmail.com
Rashid Patricio Jiménez[2]
Miembro de las Fuerzas Armadas
Ejército Ecuatoriano
rasho41@hotmail.com
Quito, Ecuador

Resumen

La presente investigación examina los efectos de los ataques cibernéticos en contextos de crisis política en relación al ejercicio de la libertad de expresión como un derecho fundamental. Usando un enfoque cualitativo, se revisan ejemplos recientes en los medios, para entender cómo estos eventos aquejan la libertad de expresión, la democracia y la polarización política. Se argumenta que estos ataques son más que simples hechos de ciberseguridad, siendo intencionales para influir en la opinión pública y favorecer intereses específicos, ya sean de

1 Magíster en Seguridad y Defensa, magíster en Planificación (proyectos). Es miembro de las Fuerzas Armadas –Fuerza Terrestre– del Ejército Ecuatoriano. Código ORCID: https://orcid.org/0009-0006-7608-2366
2 Magíster en Estrategia Militar Terrestre. Es miembro de las Fuerzas Armadas –Fuerza Terrestre– del Ejército Ecuatoriano.

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

aquellos que buscan tomar el poder como las élites que se conocen en la actualidad. Finalmente, se proponen estrategias prácticas basadas en políticas exitosas en contextos similares y recomendaciones derivadas de los estudios analizados.

Palabras clave: ciberataques, libertad de expresión, Ecuador, manipulación, democracia

Abstract

This research examines the effects of cyberattacks in contexts of political crisis on the exercise of freedom of expression as a fundamental right. Using a qualitative approach, recent media examples were reviewed to understand how these events impact freedom of expression, democracy, and political polarization. It is argued that these attacks are more than simple cybersecurity incidents, but are intentional and intended to influence public opinion and favor specific interests, whether those seeking to seize power or the current elites. Finally, practical strategies based on successful policies in similar contexts and recommendations derived from the analyzed studies are proposed.

***Keywords*:** cyberattacks, freedom of expression, Ecuador, manipulation, democracy.

Introducción

La utilización recurrente y casi indispensable de la tecnología y los medios digitales en la vida contemporánea genera múltiples riesgos para la comunicación y la opinión pública, tanto en el ámbito público como privado. Entre las amenazas que han ganado terreno, los ciberataques destacan como una herramienta cada vez más utilizada, ya sea para la represión política o para desafiar al Estado, de manera directa o encubierta. Estos incidentes van más allá de comprometer

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

la seguridad en línea de instituciones o empresas y de las personas; también atentan contra la libertad de expresión y la propia democracia (DeNardis, 2020), particularmente, en contextos sociales turbulentos o disruptivos, donde la política suele desempeñar un rol principal.

Esta realidad se ha vuelto recurrente en varios países de América Latina, una región caracterizada –en los últimos años– por la polarización e inestabilidad política, que tienen como factor principal una debilidad en la gestión institucional del Estado por parte de los gobiernos de turno (Izaguirre-Olmedo y León-Gavilánez, 2018). En esta región, los ciberataques han evolucionado hasta convertirse en una forma astuta y refinada de censura[3].

Con respecto a los ciberataques, o al contexto del ciberdelito en general, cabe mencionar que tanto los gobiernos como grupos fuera del Estado los usan a su favor, buscando mantener el control sobre las opiniones que favorecen los intereses de grupos de poder específicos (Human Rights Watch, 2023). Sin embargo, en contextos de turbulencia y lucha por el poder, también emergen intereses transnacionales relacionados con la polarización política e ideológica de la región (Santamaría, 2021), lo que introduce a otros actores cuyos intereses convergen con la corrupción y la desestabilización democrática.

3 Al respecto, la Organización de los Estados Americanos (OEA, 2023) presentó un informe denominado Informe regional sobre ciberseguridad 2023: Tendencias y amenazas en América Latina y el Caribe, que recoge detalles y preocupaciones de asociaciones latinoamericanas sobre las amenazas digitales en la región, lo que evidencia la escalada de estos hechos en los últimos años. Según el informe, "los ciberataques han aumentado notoriamente, afectando la seguridad y estabilidad de los países (Organización de los Estados Americanos, 2023, pág. 5)

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

El Ecuador por muchos años ha atravesado periodos de grave crisis social y política, esto se ha agravado con los reiterados ataques contra la prensa, lo cual ha pretendido atentar contra la democracia. Estos fenómenos también tienen incidencia con el crimen organizado, especialmente en estos últimos años donde se han intensificado los ataques cibernéticos por parte de los grupos de delincuencia organizada (Comisión Interamericana de Derechos Humanos, 2023). Un antecedente nefasto y trágico de estos tipos de ataques lo vivió el excandidato presidencial y periodista Fernando Villavicencio, quien –días antes de su fallecimiento– recibió una serie de amenazas y ataques en redes sociales, y esto se sigue observando hasta la actualidad.

Comprender este fenómeno es esencial porque afecta directamente la libertad de expresión, ya que es un derecho indispensable para una democracia consolidada, debido a que permite a los ciudadanos tomar decisiones, pedir cuentas y compartir ideas en todas las instituciones. Según el informe Freedom on the Net 2024, "los ciberataques contra periodistas y activistas son cada vez más comunes, especialmente en contextos de crisis política" (Freedom House, 2024). Estos ataques entorpecen el acceso a información verídica y los medios para comunicar, generando grupos donde las personas prefieren callar o limitar sus opiniones por temor a represalias de grupos élites.

La hipótesis que guía este trabajo sustenta que los ciberataques sobrepasan el desafío técnico: actúan como un instrumento político, destinado a intimidar voces, que cuestiona beneficios específicos, ya sean de ciertas élites o del mismo Estado, especialmente en períodos de crisis

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

o inestabilidad. Para sostener esta idea, se recurre a datos específicos que revelan cómo en países divididos por la política estos acontecimientos se utilizan para golpear a los oponentes o al gobierno, tergiversar información y, en última instancia, reforzar el control de los grupos élites que son quienes ostentan el poder.

En Ecuador, este esquema ha quedado demostrado en varias ocasiones con ataques organizados, dirigidos a medios independientes y periodistas, más aún cuando la política atraviesa períodos difíciles (Saltos-Ponce, 2023). Estas tareas son claramente definidas como una intención política de los grupos de poder en el país.

A través de este artículo, se busca desentrañar las características más comunes de los ciberataques en el contexto de crisis políticas, para comprender sus intenciones más allá del carácter técnico, con el objetivo de implantar opiniones y tendencias para favorecer intereses particulares. Además, mediante un análisis del contexto y de los mecanismos y estrategias que llevan a recurrir a esta forma de violencia, se pretende explorar cómo estos ataques están poniendo en jaque la libertad de expresión y, en última instancia, tambaleando la democracia misma.

Finalmente, utilizando una metodología cualitativa, se analizan casos específicos donde estas amenazas han estado presentes durante momentos de crisis o convulsión social. Estos incluyen eventos ocurridos en los últimos años en América Latina, como los de Ecuador, que tuvieron un impacto significativo en la sociedad y evidenciaron vulnerabilidades del Estado en cuanto a la estabilidad democrática (Comisión Interamericana de Derechos Humanos, 2023; Freedom House,

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

2024). Estos eventos pusieron en evidencia la facilidad con la que se recurre a los ciberataques para manipular la opinión pública o fomentar la censura, afectando directamente la libertad de expresión y el acceso a la información (Saltos-Ponce, 2023).

Este artículo también pretende contribuir al conocimiento científico y práctico respecto a cómo los ciberataques se han convertido en una herramienta de represión y hostigamiento contra medios, periodistas y ciudadanos que generan y buscan información en espacios digitales. Al vincular esta problemática con las dinámicas políticas y sociales que moldean la comunicación en la actualidad, el objetivo final es destacar la importancia de la libertad de expresión y el respeto a los derechos fundamentales para el futuro de la sociedad y la democracia en Ecuador.

Marco Teórico

Ciberataques

Los ciberataques –como herramienta para fines políticos– no son un fenómeno reciente. Desde principios del siglo XXI, han sido utilizados en movimientos como las denominadas "revoluciones de colores" en Europa del Este, donde actores estatales –y no estatales– emplearon estrategias digitales para movilizar protestas y desestabilizar gobiernos (Snegovaya, 2015). En Sudamérica, estas actividades se han adecuado a contenidos de polarización política, donde los ciberataques buscan no solo interferir infraestructuras, sino también manejar narrativas públicas (Salcedo-Albarán y Garay-Salamanca, 2016).

Los ciberataques son actividades y gestiones intencionadas dirigidas a comprometer sistemas digitales,

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

redes o infraestructuras tecnológicas con fines maliciosos (Schio, 2023). Estas actividades engloban agresiones que están distribuidas en denegación de servicio [DDoS], hackeos, phishing y ransomware, entre otros métodos, por mencionar los existentes en la actualidad (Ortiz-Prado y Gómez-Barreno, 2021). En el ámbito político, los ciberataques tienen un gran impacto estratégico, ya que su objetivo final es perturbar instituciones, callar voces críticas y utilizar la información de forma no adecuada (Santamaría, 2021). Según Freedom House (2023), en Sudamérica, estas acciones han servido para perjudicar y entorpecer campañas electorales, presentar datos reservados y más aún sensibles y, por ende, interferir y aislar plataformas digitales de comunicación en tiempos y temas de crisis políticas y sociales.

Libertad de Expresión

La libertad de expresión es un derecho humano primordial, completamente reconocido en instancias e instrumentos internacionales como la Declaración Universal de los Derechos Humanos [DUDH] y la Convención Americana sobre Derechos Humanos [CADH] (Naciones Unidas, 1948; Organización de los Estados Americanos, 1969). El artículo 19 de la DUDH establece que toda persona tiene derecho a opinar y expresarse libremente, buscar, recibir y compartir información e ideas sin represalias ni interferencias indebidas (Naciones Unidas, 1948). De manera similar, el artículo 13 de la CADH protege la libertad de pensamiento y expresión (Organización de los Estados Americanos, 1969). Sin embargo, en el mundo digital, este derecho enfrenta amenazas constantes debido a ciberataques, censura algorítmica y vigilancia masiva, que buscan influir en la opinión pública, las decisiones políticas

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

y las elecciones, ya sea para reforzar el poder establecido o para atentar contra él (Comisión Interamericana de Derechos Humanos, 2023; Freedom House, 2023).

Inestabilidad Política

La variación, el desequilibrio y la inseguridad política son un estado en el que las instituciones colapsan inmediatamente, palpable por conflictos internos, reemplazos abruptos en el poder o problemas sociales crecientes (Erkut, 2021). Mainwaring y Pérez-Liñán (2015) sustentan que este fenómeno apuesta a evidenciar la debilidad y fragilidad de las democracias, acompañada de la restringida capacidad que tienen los gobiernos para enfrentar las crisis, estableciendo situaciones para manifestaciones, protestas civiles, violencia generalizada, saqueos, destrozos a la infraestructura e incertidumbre política. En medio de este desorden, tanto actores políticos como aquellos que operan fuera del Estado recurren a tácticas como los ciberataques para fortalecer su posición, desprestigiar a sus rivales o manipular lo que la gente piensa.

Revisión de la Literatura

Ciberataques Como Herramienta Política

La literatura académica ha documentado ampliamente cómo los ciberataques se han consolidado como una herramienta política en diversos contextos globales. Deibert y Crete-Nishihata (2012) manifiestan que estos ataques trascienden la afectación de la seguridad digital, impactando profundamente la gobernanza democrática y los derechos humanos al facilitar la vigilancia, la censura y la manipulación de la información.

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Recientemente se ha podido evidenciar que todo tipo de actores estatales y no estatales usan ciberataques para detener disidencias y controlar narrativas públicas. Por ejemplo, Salcedo-Albarán y Garay-Salamanca (2016) recalcan cómo estas técnicas, utilizadas por redes criminales, se han incrementado en contextos de fragilidad institucional, afectando la libertad de expresión y el acceso a información oportuna y veraz. En el caso de Venezuela, una de las fuentes es la organización Reporteros Sin Fronteras (2024), que evidencia que los ciberataques en contra de medios independientes se han utilizado sistemáticamente para ocultar críticas al gobierno, especialmente durante eventos de crisis política y social, como se dieron las protestas de 2019 y las elecciones controvertidas del año 2020.

Las plataformas digitales hoy en día se constituyen en mecanismos clave para posicionar mensajes e ideologías de toda índole, incluyendo la desinformación y fake news (Wardle y Derakhshan, 2017). Sobre esto existen algunos estudios que han presentado resultados sobre el entorno adecuado de los contenidos polarizados y las campañas estratégicas para contrarrestar discursos gubernamentales (Badawy et al., 2018). Este suceso refleja la capacidad de los movimientos disidentes para reunir apoyo y aprovechar las vulnerabilidades tecnológicas existentes en beneficio de sus agendas políticas.

Una gran parte de la literatura académica se concentra en la reprimenda impulsada por el Estado; los grupos de oposición, líderes sociales y grupos de poder, a menudo, respaldados por movimientos de izquierda o progresistas, han alcanzado un dominio comparable en varios países latinoamericanos. Estos grupos emplean herramientas

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

y mecanismos sistemáticos en redes sociales para crear tendencias y narrativas destinadas a influenciar en la opinión pública con intereses específicos (Bessi y Ferrara, 2016). Entre los grupos de poder claves en estas actividades están los denominados *trolls,* quienes actúan de manera sincronizada y organizada para incrementar mensajes y desinformación, afectando la apreciación colectiva (Badawy et al., 2018).

Para el Ministerio de Telecomunicaciones y de la Sociedad Civil (2022), el trabajo para evitar ciberataques es extenuante, aun cuando en contextos de graves crisis nacionales se han generado estrategias para impedir ataques a los sistemas públicos. Sin embargo, estas acciones aún enfrentan ciertas limitaciones como la generación de datos, ausencia de recursos económicos y un marco normativo amplio de regulación en materia electrónica, lo que impide una pronta y adecuada respuesta a las amenazas no estatales y transnacionales (Ordoñez-González, 2014).

Impacto en el ejercicio de la libertad de expresión como un derecho fundamental

En contextos donde el poder sobre los medios es casi total, completo y dominante, la censura por lo general deriva en autocensura impulsada por el miedo. Pérez-Martínez (2022) examina las causas de la censura, concluyendo que una de sus consecuencias es la omisión deliberada de opiniones debido a las amenazas y riesgos percibidos, no solo de acciones que ataquen de forma personal, sino también de sanciones administrativas y profesionales, lo que lleva a periodistas, activistas y personas en general a suprimir información sensible para evitar hackeos, campañas de desprestigio o acoso laboral, legal y personal.

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

En Ecuador se evidenció claramente en el caso del periodista Fernando Villavicencio, que, antes de su asesinato en agosto de 2023, sufrió una avalancha de ciberataques por presentar casos de corrupción en varias administraciones en el país. Reporteros Sin Fronteras (2024) explica cómo Villavicencio soportó un sinnúmero de ataques a sus cuentas de redes sociales y plataformas digitales, destinados a callar sus opiniones y desacreditarlo, especialmente debido a las investigaciones publicadas entre 2020 y 2023.

Según González-Bailón y Lelkes (2023), estas prácticas crean barreras para que periodistas y ciudadanos ejerzan su derecho a la libertad de expresión. Freedom House (2024) señala que la vigilancia total y la censura digital han ganado terreno en los últimos años, resultando en una constante en la mayoría de los países latinoamericanos. Este escenario afecta rigurosamente los derechos humanos, los medios independientes y los comunicadores, poniendo en riesgo las reglas democráticas agrupadas con la libertad de expresión garantizada por las normas, leyes y constituciones nacionales.

Contexto de Latinoamérica

En nuestro continente, los ataques cibernéticos se han convertido en un punto argüido de discusión, ya que su incremento va en un aumento considerable. Países como México, Brasil, Chile, Argentina, Ecuador y Colombia, se encuentran normando sus regulaciones. Para los autores Salcedo-Albarán y Garay-Salamanca (2016), los periodistas y medios de comunicación son los principales sujetos de ataques, seguidos por los líderes políticos; esto se da por cuanto gozan de confianza pública y atención de los ciudadanos, especialmente en procesos electorales.

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

En Brasil, Freedom House (2024) informa que, durante las elecciones de 2022, los ciberataques, incluyendo ataques DDoS y campañas de desinformación, afectan en gran escala la percepción pública sobre la veracidad del proceso electoral. En México y Colombia, los ciberataques se han utilizado para intimidar e influenciar a defensores de derechos humanos y medios independientes, aumentando la inseguridad institucional (Freedom House, 2023).

En Ecuador, existe un limitado acceso a sistemas o formas adecuadas para neutralizar los ataques cibernéticos; pese a no ser hechos nuevos en nuestra historia, no hemos avanzado en nuevas propuestas tecnológicas de seguridad digital, especialmente en tensiones políticas y sociales (Ordoñez-González, 2024).

La organización de derechos humanos Freedom House (2023) señala que, durante los disturbios suscitados en el 2019 en el Ecuador, el gobierno del expresidente Moreno limitó el acceso a plataformas digitales y censuró algunos contenidos comunicacionales con la intención de evitar un aumento de agresiones contra las fuerzas civiles y frenar discursos que aumentaban el disgusto social, como por ejemplo el aumento del precio de combustibles. Sin embargo, esta estrategia no resultó tan segura, pues los usuarios, principalmente manifestantes y líderes políticos, lo utilizaron de manera intensiva, logrando posicionar discursos de odio y de inestabilidad política hacia el mandatario y, lo más importante, declarar públicamente la resistencia de los protestantes (NetBlocks, 2019). Pérez-Martínez (2022) argumenta que, si bien las autoridades ecuatorianas han empleado la censura digital como recurso para neutralizar

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

a movimientos indígenas y opositores en coyunturas críticas, la persistencia de estos grupos en el manejo de herramientas digitales pone de manifiesto las fisuras de tales medidas, delineando un escenario de pugna por la hegemonía informativa en el ámbito virtual.

La región andina se encuentra cruzando una serie de actos de inestabilidad política y los ciberataques se han constituido en un arma de confrontación difícil de atacar. Human Rights Watch (2023) recalca casos como Bolivia y Honduras, donde los ciberataques se han utilizado para interferir en elecciones y callar a la oposición, aumentando la inestabilidad y violando los derechos humanos en la sociedad en general.

Pérez-Liñán y Mainwaring (2020) manifiestan que la mezcla de instituciones frágiles y el uso inadecuado de herramientas digitales por parte de los gobiernos, de forma constante, para difundir desinformación a través de medios estatales, ha minado aún más la confianza en la democracia en la región. Así, los ciberataques se han convertido en recursos estratégicos clave, casi como un arma importante, cuando los gobiernos enfrentan una popularidad en decadencia y declive.

Brecha de Conocimiento

Aunque el mundo académico tiene cada vez más atención al tema de los ciberataques y su efecto en la libertad de expresión, existe un vacío claro en la comprensión específica de la situación actual en Ecuador. Mientras que existen estudios de investigación a fondo, como los casos en países como Venezuela o Brasil, la investigación sobre Ecuador todavía sigue siendo superficial o limitada en alcance.

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Salcedo-Albarán y Garay-Salamanca (2016) analizan cómo los ciberataques se han convertido en un arma política en América Latina, pero su enfoque principal está dirigido a naciones con mayor atención mediática internacional, como Argentina, Venezuela, Brasil o Colombia, dejando a Ecuador únicamente como un actor secundario. De manera similar, Freedom House (2023) analiza brevemente las restricciones digitales en Ecuador durante momentos críticos, como las protestas de 2019, pero no profundiza en los detalles de esos eventos, particularmente desde la perspectiva de las respuestas gubernamentales a los ataques de la oposición y los movimientos de izquierda, que jugaron un rol más allá del simple apoyo a las protestas.

La mayoría de los estudios existentes se centra en el impacto social o en las vulnerabilidades técnicas de la infraestructura institucional, dejando de lado las dinámicas políticas y sociales más profundas, como los vínculos con la represión, la inestabilidad y los intereses por desestabilizar para obtener impunidad (Deibert y Crete-Nishihata, 2012).

Esta brecha de investigación, muy marcada en el ámbito local, abre la puerta a nuevas contribuciones al debate académico y político sobre cómo los ciberataques se utilizan para perseguir agendas ocultas durante momentos de conmoción social y política, especialmente en un Ecuador, marcado por niveles de polarización social y política sin precedentes.

Metodología

La presente investigación se realiza bajo el enfoque cualitativo, por cuanto analiza una serie de documentos y los sintetiza al caso en estudio sobre ciberataques y libertad

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

de expresión. De igual manera, este trabajo recopila fuentes secundarias, como, por ejemplo, informes de los organismos de seguridad, reportajes de medios de comunicación y literatura académica, entre otros (Creswell, 2009). Esta metodología ayudó a identificar las principales causas, efectos y sujetos intervinientes en los ataques cibernéticos durante las protestas sociales y su incidencia con la libertad de expresión.

Resultados y Discusión

En esta sección, se plantea un análisis detallado de los casos más representativos, en los cuales se han detectado ciberataques relacionados con la libertad de expresión de los últimos años, para tratar de comprender cómo se han alzado como armas políticas para acallar voces y apuntalar el poder en medio de una marcada inestabilidad. También se explorarán los hilos que conectan a actores políticos con grupos armados y actividades ilícitas, con ejemplos palpables en países como Colombia, Venezuela y Ecuador.

Ciberataques Durante Las Protestas Indígenas de 2019

Las protestas indígenas de octubre de 2019 en Ecuador surgieron como respuesta a la eliminación del subsidio a los combustibles, medida adoptada por el gobierno de Lenín Moreno bajo el Decreto Ejecutivo 883 (Ortiz, 2020). Este escenario de conflicto social, de igual manera, se reflejó en el ámbito digital, con un incremento de actividades de desacreditar, desinformar y ciberataques dirigidos a instituciones públicas. Según un informe del Ministerio de Telecomunicaciones y de la Sociedad de la Información (2019), en los incidentes en los diferentes sectores se registraron intentos de vulneración a plataformas y sistemas estatales, afirmando una correlación entre el descontento de la sociedad en general y la actividad

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

desarrollada en el ciberespacio. Aunque en la actualidad no existen datos que concluyan sobre los orígenes de estos ataques, reportajes periodísticos de la época propusieron que en algunas ocasiones podrían haber provenido por la integración y manipulación de personas y servidores ubicados fuera del territorio ecuatoriano, lo que evidencia la urgente necesidad de cooperación internacional para poder abordar estas amenazas y riesgos transnacionales que en la actualidad enfrenta Ecuador (El Universo, 2019). Según NetBlocks (2019), en el desarrollo de las protestas se registraron intermitencias en la señal de internet que afectaron al 80% de las conexiones en Quito y otras ciudades, comprobando el impacto de los ciberataques en el acceso a la información.

Tabla 1

Tipos y consecuencias de ciberataques durante las protestas de 2019

Métodos utilizados	**Consecuencias**
Ataques DDoS que colapsaron servidores de medios digitales; Generación de medios improvisados con el fin de generar noticias falsas o exacerbar los ánimos de las protestas; Bots que, esparcieron fake news sobre las protestas; Hackeos que irrumpieron en las cuentas de líderes y periodistas; Censura a medios disidentes.	Silencio forzado en la cobertura de conformación, números de participantes, puntos de reunión, seguridad, amenazas detectadas y consecuencias de las protestas; Desconfianza generalizada sobre medios tradicionales y digitales; Incertidumbre por diversidad de versiones y fuentes de información; El miedo y la autocensura en comunicadores; Pánico en la población; Secuestro de policías y periodistas por parte de los manifestantes.

Nota: Elaboración propia con base en Fundamedios (2022) y Ortiz (2020)

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Este caso ilustra cómo los ciberataques se emplearon como una herramienta efectiva para silenciar voces disidentes y manipular la narrativa pública durante las protestas de octubre de 2019 en Ecuador, afectando el acceso a plataformas digitales y, con ello, la capacidad de los ciudadanos para informarse de manera adecuada, lo que repercutió directamente en la democracia participativa (Freedom House, 2020). Sin embargo, este impacto contrastó con la notable articulación y coordinación de acciones violentas por parte de los manifestantes, quienes aprovecharon el ciberespacio para organizar protestas y difundir sus mensajes sin restricciones aparentes, según lo reportado por NetBlocks (2019).

Medios internacionales como EFE, Agence France Presse y Swissinfo documentaron los ataques a la prensa y los ciberataques dirigidos a medios públicos y privados, los cuales, impulsados por *bots* y maniobras coordinadas, generaron desinformación y promovieron censura y autocensura por intimidación (Fundamedios, 2019). El ciberespacio, al tener doble uso –uno como arma de represión y el otro como una herramienta de resistencia– sustenta un actual debate referente a la necesidad de regular este aspecto, un contenido polémico y sensible en países de la Unión Europea y Estados Unidos de América, donde se analizan modelos de control responsable (Council of the European Union, 2023), como en contextos de América Latina donde existen democracias frágiles.

Los ciberataques ejercieron un papel muy importante en los debates públicos durante las manifestaciones de octubre de 2019 en Ecuador. Algunos representantes de los grupos de poder ocuparon campañas de desinformación y ataques digitales para influenciar en la percepción de los manifestantes y justificar la respuesta del estado (NetBlocks, 2019). En este

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

argumento, el movimiento político Revolución Ciudadana puso en duda la legitimidad del gobierno de Lenín Moreno y cuestionó las medidas económicas, mientras que el oficialismo argumentó que las manifestaciones estaban motivadas por beneficios políticos más que por un clamor masivo, genuino de la sociedad (Pazmiño, 2020). Según Freedom House (2020), en este lapso de tiempo se incrementaron las narrativas opuestas en los medios de comunicación y redes sociales, con actividades y estrategias diseñadas para desprestigiar tanto a los manifestantes como al gobierno. Así, los ataques no solo callaron voces de protestas, sino que debilitaron y disminuyeron los fundamentos democráticos al poner trabas al acceso de la información veraz y oportuna.

Desde un punto de vista objetivo, observando ambas posturas, es evidente que la manipulación de la información siempre impide que la sociedad cuente con suficientes elementos para tener claro un criterio objetivo sobre la realidad del Ecuador (Freedom House, 2020). El contexto social y político ha propiciado, tanto a nivel local como regional, el establecimiento de bandos o posicionamientos radicalmente opuestos, lo que obstaculiza el diálogo y la búsqueda de soluciones para una sociedad atrapada entre los intereses de los grupos de poder (Pazmiño, 2020). Cabe destacar que diversas fuentes –entre ellas, el Banco Central del Ecuador– estimaron, junto con el Banco Mundial, que las pérdidas económicas para el país superaron los US$821,68 millones a escala nacional (Banco Central del Ecuador, 2020), recursos que podrían haberse destinado al desarrollo social, económico y productivo del país.

Ataques a Medios Digitales Durante el Paro Nacional de 2022

Las manifestaciones que se dieron en junio de 2022, lideradas por la CONAIE, originaron varios ciberataques contra medios digitales como Plan V y La Posta, identificados por su

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

postura de oposición crítica hacia el gobierno del entonces presidente Guillermo Lasso. Sus sitios web fueron hackeados, sus redes sociales afectadas y los datos personales de sus periodistas expuestos públicamente (Fundamedios, 2022). Según Fundamedios (2022), en los ciberataques que existieron durante el Paro Nacional se incluyeron patrones que sugieren la participación de personas y redes externas, probablemente, desde países vecinos, por lo que se debe fortalecer alianzas regionales en ciberseguridad. En las protestas se presentaron al menos 15 ciberataques a 15 medios digitales con 10.000 intentos de intrusión por hora, ilustrando la magnitud de estas amenazas. Datos recopilados por el Observatorio Latinoamericano de Amenazas Digitales (OLAD, 2024).

Tabla 2

Tipos y consecuencias de ciberataques durante las protestas de 2022

Métodos utilizados	Consecuencias
Ataques DDoS que tumbaron sitios web. Bots encargados de crear fakenews y viralizarlas. Filtraciones de correos y mensajes privados, de periodistas, opositores y funcionarios públicos. Hackeos de las cuentas de líderes opositores y periodistas. Censura a medios disidentes.	Silencio forzado en la cobertura de conformación, números de participantes, puntos de reunión, seguridad, amenazas detectadas y consecuencias de las protestas. Desconfianza generalizada sobre medios tradicionales y digitales. Incertidumbre por diversidad de versiones y fuentes de información. Casos de violencia inusual en la represión de las fuerzas del orden hacia los manifestantes. El miedo en comunicadores. Pánico en la población.

Nota. Elaboración propia con base en Observatorio Latinoamericano de Amenazas Digitales (OLAD, 2024).

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Este nuevo episodio de polarización política en Ecuador evidenció nuevamente un escenario en el que los ciberataques fueron utilizados como armas para amedrentar a quienes pretendían informar de manera independiente, sin importar su postura ideológica o política. Para esta instancia, el escenario ya era predecible, pero con las variantes de las lecciones aprendidas en las protestas de 2019, incluyendo el conocimiento de que los movimientos que respaldaban la protesta se encontraban fortalecidos por los eventos pasados, mientras que el gobierno de turno había sido debilitado por la ingobernabilidad determinada por las acciones de la oposición en la Asamblea Nacional y el Consejo de Participación Ciudadana y Control Social, en un contexto de creciente violencia donde ya se percibían las presiones de los Grupos de Delincuencia Organizada y el crimen transnacional en las cárceles, que también procuraban influir en la opinión pública y en la justicia mediante la coerción aplicada sistemáticamente a medios digitales, influencers, figuras públicas, jueces y funcionarios públicos (Kuhn-Ferreccio, 2024).

En este ambiente, las protestas escalaron durante más de dos semanas, desde el 13 hasta el 30 de junio de 2022, con casos y procedimientos similares en el contexto de los ciberataques a lo acontecido en 2019, lo que ocasionó un impacto en la gobernabilidad del Estado con respecto a la seguridad institucional y las vulnerabilidades que se acrecentaban en épocas de crisis, generando la necesidad de crear políticas y herramientas para enfrentar estos eventos disruptivos en el campo de la seguridad informática.

En ese mismo año se creó la Estrategia Nacional de Ciberseguridad (Ministerio de Telecomunicaciones y de la

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Información, 2022), que, entre otros objetivos, planteaba establecer un proceso integral para la gestión de riesgos de ciberseguridad y preparación para las crisis cibernéticas, con el fin de fortalecer dichas capacidades a nivel nacional y, de esta manera, robustecer a las instituciones públicas ante las crecientes amenazas en el ciberespacio.

El extremismo en la oposición, realidad latinoamericana de inicios de siglo

En América Latina, el panorama político no refleja una hegemonía constante de regímenes de izquierda, como podría sugerirse, sino un comportamiento pendular donde las ideologías de izquierda y derecha han alternado en el poder, con la presencia de gobiernos progresistas siendo más reciente y, salvo excepciones como Cuba, Venezuela y Nicaragua, de duración relativamente corta (Mainwaring y Pérez-Liñán, 2015). En este contexto, diversas evidencias señalan que el narcotráfico y el crimen organizado han permeado estructuras de poder, independientemente de la orientación ideológica de los regímenes, para favorecer sus actividades y vínculos ilícitos transnacionales (Briscoe et al., 2019). Aunque las investigaciones sobre estas conexiones son escasas y a menudo superficiales, los indicios disponibles —como los vínculos entre grupos criminales y élites políticas en varios países— tienden a ser opacados en un entorno académico donde las afinidades ideológicas, tanto de izquierda como de derecha, pueden influir en la visibilidad de estos fenómenos (Garay y Salcedo-Albarán, 2017).

Como ejemplo se puede mencionar el actuar del Ejército de Liberación Nacional [ELN] y las Fuerzas Armadas Revolucionarias de Colombia [FARC] en Colombia, grupos

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

que, en su intento por desestabilizar los procedimientos democráticos, les han ido vinculando con prácticas de fraude electoral, amedrentamiento y coerción durante diversos comicios electorales. Según Felbab-Brown (2019), estos grupos han empleado técnicas de intimidación física contra autoridades electorales y los electores, principalmente en regiones rurales, para adulterar resultados a favor de sus intereses o aliados políticos. Estas estrategias, al pasar el tiempo, han evolucionado hacia el ciberespacio, detectándose campañas de desinformación y ataques destinados a instituciones encargadas de la organización de las elecciones y medios de comunicación, como lo documenta InSight Crime (2021), que manifiesta el uso de bots y hackeos para influenciar en la percepción pública durante procesos electorales entre 2018 y 2020. Estas actividades, dirigidas hacia lo digital, reflejan un ajuste de sus tradicionales actividades contemporáneas de control político.

Otro caso en el que se percibe la injerencia de la tecnología y los ciberataques sistematizados para influir en la opinión pública es el del régimen de Nicolás Maduro en Venezuela. Este gobierno, vinculado al "Cartel de los Soles", una red de narcotráfico con profundas raíces en el país (InSight Crime, 2020), ha empleado estrategias digitales para manipular narrativas públicas, especialmente en el contexto de las elecciones presidenciales de 2025 (Freedom House, 2024). Acciones como estas han provocado cuestionamientos y controversias a nivel mundial sobre la veracidad de dichos comicios, provocando el desconocimiento del gobierno por parte de algunos países y, por ende, la imposición de sanciones internacionales (Organización de los Estados Americanos, 2024).

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Aunque es un tema álgido, la percepción de la influencia del crimen organizado y el narcotráfico en la toma de decisiones de muchos gobiernos latinoamericanos es ampliamente reconocida (InSight Crime, 2019). Además, las vinculaciones con líderes y opositores a gobiernos de ideologías contrarias son una constante en la región. Las protestas sociales, muchas veces justificadas desde las necesidades sociales, han sido manipuladas por estos grupos, como se observó en Ecuador, Colombia y Chile entre 2018 y 2019 (Freedom House, 2020). Estos casos evidencian un cambio en las estrategias de control: del uso tradicional del poder estatal para silenciar protestas al empleo de ciberataques que trascienden lo técnico, utilizando la coerción, el amedrentamiento y la cancelación para inducir autocensura o incluso alterar radicalmente la opinión pública (Reporteros Sin Fronteras, 2019).

En Ecuador, se observa que las tácticas y técnicas para restringir la libertad de expresión no han sido ampliamente utilizadas en los gobiernos de turno de los últimos años, como los de Lenín Moreno y Guillermo Lasso, limitando su accionar a casos puntuales en medios tradicionales y dirigiéndose ampliamente en el ámbito de las redes sociales (Freedom House, 2023). Esto es totalmente contradictorio con los mecanismos empleados durante el gobierno de Rafael Correa (2007–2017), período en el cual se clausuraron estaciones de radio, televisión y medios digitales mediante el uso del dominio y atribuciones estatales, incluyendo a la Secretaría Nacional de Inteligencia (SENAIN) y el Servicio de Rentas Internas (SRI) para silenciar voces críticas (Fundamedios, 2017).

El propósito de este análisis no es adoptar una postura ideológica, más bien examinar cómo las críticas y oposición

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

que históricamente se dirigían a gobiernos autoritarios por emplear represión para proteger su ideología política han evolucionado con el tiempo. En la actualidad, estas manifestaciones se dan con mayor frecuencia en grupos de poder vinculados al crimen organizado que buscan influenciar directamente en el estado para proteger sus intereses o garantizar la impunidad de sus actividades (Garay y Salcedo-Albarán, 2017; InSight Crime, 2021). Este cambio se refleja en el ámbito de la ciberseguridad, donde se han identificado estrategias de manipulación de la información destinadas a moldear la opinión pública, según lo evidencian diversos estudios sobre América Latina (Freedom House, 2023). Estas dinámicas ilustran una transformación en los mecanismos utilizados para ejercer control, que ahora trascienden las acciones exclusivas de los gobiernos.

Los casos analizados muestran que los ciberataques, además de un problema técnico, son herramientas de poder que moldean el juego político. Al cercenar la libertad de expresión y distorsionar las narrativas, agravan la inestabilidad, especialmente cuando la sociedad ya está dividida por crisis o enfrentamientos ideológicos. Esto pone en evidencia una verdad incómoda que demanda fortalecer las defensas digitales y desarrollar regulaciones que protejan la información veraz como un pilar fundamental de la democracia.

Conclusiones

Los ciberataques que se reportaron durante las protestas sociales del 2029 contra la prensa ecuatoriana no solo se convirtieron en escenario de seguridad digital, sino que se libró otro campo como el mediático y político,

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

donde la prensa jugó un rol importante para los dos bandos confrontados, especialmente en el posicionamiento de discursos por parte del Gobierno de turno.

Al analizar casos concretos en Ecuador y otros países de América Latina, los resultados respaldan plenamente esta hipótesis. Se encontró que tanto gobiernos como grupos con intereses particulares han utilizado ciberataques de manera calculada para acallar a quienes difieren de sus políticas, ideologías o propósitos, moldeando la opinión pública siempre a su conveniencia. Esto afecta principalmente a instituciones, personas y medios de comunicación, pero sus consecuencias son tan profundas que debilitan los cimientos mismos de la democracia mediante el menoscabo institucional y de la gobernabilidad.

Los ejemplos revisados muestran claramente cómo los ciberataques se convierten en un arma para restringir la libertad de expresión y manipular deliberadamente la opinión pública. En Ecuador, por ejemplo, durante las protestas indígenas de 2019 y el Paro Nacional de 2022, estas estrategias digitales se usaron para desprestigiar a quienes se manifestaban, intimidar a periodistas, funcionarios públicos y medios de comunicación, pero también como una herramienta para generar conmoción en favor de la desestabilización de la democracia.

Se ha demostrado, a través de la revisión de casos y la literatura académica, que este tipo de ataques agrava las divisiones políticas existentes, creando diferencias abismales entre los medios que apoyan al poder de turno y los opositores. Asimismo, se evidencia que, en el contexto regional y local actual, estos últimos también buscan el

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

poder, aprovechando la convulsión social y las necesidades y protestas reales de la población, para desarrollar tácticas y estrategias orientadas a la desestabilización democrática. Para ello, generan rumores, noticias falsas y una desconfianza creciente hacia las instituciones y los procesos electorales.

El análisis también revela conexiones evidentes entre políticos, grupos armados y actividades ilegales como el narcotráfico y el crimen organizado, que recurren a los ciberataques para proteger sus propios intereses. Este hallazgo, aunque evidente, no ha sido abordado frontalmente en relación con el cambio de paradigma en el control de los medios, que ya no es exclusivo de quienes ostentan el poder gubernamental, sino que trasciende a esferas de poder que buscan el control e injerencia estatal desde la protesta social para satisfacer sus intereses de resguardar actividades ilícitas o garantizar impunidad a sus miembros y afines.

El caso de Ecuador es un reto global: la urgencia de regular y proteger el ciberespacio sin arriesgar los derechos fundamentales. En un ambiente donde los ciberataques sobrepasan fronteras, el debate sobre el seguimiento responsable de los medios digitales da más relevancia, especialmente en democracias delicadas donde las diversas ideologías políticas aumentan su impacto (Botero y Rivera, 2023). Estas acciones exigen equidad entre la seguridad digital y la protección de la libertad de expresión, un reto que trasciende el ámbito nacional.

Finalmente, se destaca que esta amenaza sobrepasa fronteras, ya que los ciberataques no se limitan a un solo país; sus consecuencias cruzan todo límite y amenazan la estabilidad de toda la región. Lo observado en Ecuador podría

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

difundirse en otros lugares si se consolida como un medio efectivo de desestabilización en la democracia, lo que podría aumentar las tensiones entre países y dividir aún más a las sociedades en general.

Recomendaciones

Para hacer frente a los desafíos de los ciberataques y salvaguardar la libertad de expresión, es primordial adoptar acciones y estrategias integras y coordinadas, teniendo en cuenta nuevos paradigmas como el planteado en esta investigación, abordando tanto las vulnerabilidades técnicas como las acciones políticas y sociales que permiten que estos altercados se utilicen como herramientas de represión.

Es urgente mejorar la normativa pertinente y adaptarla a la realidad regional y local. Esto significa implementar leyes nacionales e internacionales que regulen el uso de tecnologías digitales y crear mecanismos de rendición de cuentas que impidan a los gobiernos utilizar ciberataques como instrumentos de control político. En línea con el debate global, se recomienda establecer regulaciones equilibradas a la seguridad digital, en el marco de respeto a los derechos humanos, a través de modelos como los propuestos por la Organización de los Estados Americanos [OEA] (2023). Estas políticas deben incluir actividades de supervisión para evitar que utilicen la ciberseguridad como pretexto para restringir la libertad de expresión. Sin una norma, ley clara y sanciones efectivas, la impunidad seguirá siendo un obstáculo para la justicia.

La capacitación en ciberseguridad es fundamental. Periodistas, activistas, personas naturales y medios de comunicación deben tener programas de formación que les

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

permitan identificar, neutralizar y mitigar amenazas y riesgos como hackeos, *phishing* y filtraciones de datos; a través de herramientas de cifrado y anonimato, debe difundirse activamente para proteger la privacidad y la seguridad de quienes ejercen la libertad de expresión, tanto en instituciones públicas, privadas como en el contexto empresarial.

El apoyo internacional también desempeña un papel fundamental en esta lucha. Los ciberataques no saben de fronteras, por lo que es importante fomentar la colaboración entre países para combatir amenazas y riesgos transfronterizos y la unión con la delincuencia. La creación de redes regionales de apoyo mutuo puede ofrecer recursos y protección a periodistas y activistas en general que enfrentan ataques, fortaleciendo la resiliencia colectiva.

La protección de áreas e infraestructuras críticas y estratégicas no puede ser dejada a un lado, a pesar de las políticas de seguridad desarrolladas actualmente. Invertir en tecnología y personal capacitado para salvaguardar sistemas electorales y redes de comunicación pública es fundamental. De igual manera, adoptar protocolos de respuesta inmediata ayudará a mitigar los efectos de los ciberataques en tiempo real, minimizando su impacto.

La transparencia y la rendición de cuentas son elementos esenciales que deben guiar cualquier accionar estratégico orientado a la participación global y comunitaria en todas las instancias, ya sean estatales como privadas a nivel nacional e internacional. La creación de observatorios independientes para monitorear el uso de ciberataques por parte de actores políticos puede garantizar mayor transparencia en los procesos democráticos. Asimismo, resulta

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

fundamental apoyar investigaciones periodísticas y académicas que documenten casos de estos delitos informáticos y sus consecuencias, contribuyendo a un entendimiento más profundo del fenómeno.

Referencias

Badawy, A., Ferrara, E., y Lerman, K. (2018). Analyzing the digital traces of political manipulation: The 2016 Russian interference Twitter campaign. Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 258–265. https://doi.org/10.1109/ASONAM.2018.8508247

Banco Central del Ecuador. (2020, 17 de enero). Paralización de octubre de 2019 dejó daños y pérdidas por USD 821,68 millones. https://www.bce.fin.ec/boletines-de-prensa-archivo/paralizacion-de-octubre-de-2019-dejo-danos-y-perdidas-por-usd-82168-millones

Bessi, A. y Ferrara, E. (2016). Social bots distort the 2016 U.S. presidential election online discussion. First Monday, 21(11). https://doi.org/10.5210/fm.v21i11.7090

Botero, J. y Rivera, J. (2023). Regulating the digital public sphere: Balancing security and freedom in Latin America. Journal of Latin American Studies, 55(2), 123–145. https://doi.org/10.1080/17440572.2023.2184567

Briscoe, I., Perdomo, C., y Uribe-Burcher, C. (2019). Redes ilícitas y política en América Latina. Instituto Internacional para la Democracia y la Asistencia Electoral. https://nimd.org/wp-content/uploads/2025/02/Redes-ilicitas-Spanish.pdf

Comisión Interamericana de Derechos Humanos. (2023). Informe anual 2023: Situación de los derechos humanos

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

en Ecuador. https://www.oas.org/es/cidh/informes/pdfs/2023/informe_anual_2023_ecuador.pdf

Council of the European Union. (2023). Conclusions on the EU policy on cyber defence. https://www.consilium.europa.eu/media/63647/st08769-en23.pdf

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.). Sage Publications.

Deibert, R. y Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. Global Governance, 18(3), 339-361. https://www.jstor.org/stable/23269961

DeNardis, L. (2020). The internet in everything: Freedom and security in a world with no off switch. Yale University Press. https://doi.org/10.12987/yale/9780300233070.0001

El Universo. (2019, 10 de octubre). Ciberataques afectan plataformas estatales durante protestas en Ecuador. https://www.eluniverso.com/noticias/2019/10/10/nota/7567890/ciberataques-afectan-plataformas-estatales-durante-protestas-ecuador

Erkut, B. (2021). What is political instability and how does it affect international trade? En Impact of global issues on international trade (pp. 1-15). IGI Global. https://doi.org/10.4018/978-1-7998-8425-5.ch001

Felbab-Brown, V. (2019). Organized crime, illicit economies, and political violence in Colombia. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2019/10/FP_201910_colombia_crime.pdf

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Freedom House. (2020). Freedom on the Net 2020: The pandemic's digital shadow. https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow

Freedom House. (2023). Freedom on the Net 2023: The repressive power of artificial intelligence. https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence

Freedom House. (2024). Freedom on the Net 2024. https://freedomhouse.org/report/freedom-net

Fundación Andina para la Observación y Estudio de Medios [Fundamedios]. (2017). Informe sobre la libertad de prensa en Ecuador 2007–2017. https://www.fundamedios.org.ec/informes/informe-libertad-prensa-ecuador-2007-2017

Fundación Andina para la Observación y Estudio de Medios [Fundamedios]. (2019, 10 de octubre). La prensa fue blanco de los violentos: 138 periodistas agredidos en 12 días de protestas. https://www.fundamedios.org.ec/alertas/la-prensa-fue-uno-de-los-blancos-de-los-violentos-138-periodistas-agredidos-en-12-dias-de-protestas/

Fundación Andina para la Observación y Estudio de Medios [Fundamedios]. (2022, 25 de junio). El ataque a periodistas y activistas no cesa en el paro en Ecuador. https://www.fundamedios.org.ec/alertas/el-ataque-a-periodistas-y-activistas-no-cesa-en-el-paro-en-ecuador/

Garay, L. J. y Salcedo-Albarán, E. (2017). Narcotráfico, corrupción y estados: Cómo las redes ilícitas han reconfigurado las instituciones en Colombia, Guatemala y México. Vortex Foundation.

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

González-Bailón, S. y Lelkes, Y. (2023). Do social media undermine social cohesion? A critical review. Social Issues and Policy Review, 17(1), 155-180. https://doi.org/10.1111/sipr.12091

Human Rights Watch. (2023). Informe mundial 2023: Derechos humanos en tiempos de crisis. https://www.hrw.org/es/world-report/2023

InSight Crime. (2019). Organized crime and political instability in Latin America. https://insightcrime.org/investigations/organized-crime-political-instability-latin-america/

InSight Crime. (2020). Cartel de los Soles: Venezuela's narco-military network. https://insightcrime.org/investigations/cartel-de-los-soles-venezuelas-narco-military-network/

InSight Crime. (2021). The evolution of organized crime in Latin America. https://insightcrime.org/investigations/evolution-organized-crime-latin-america/

Izaguirre-Olmedo, J. y León-Gavilánez, F. (2018). Análisis de los ciberataques realizados en América Latina. Innova Research Journal, 3(9), 172-181. https://doi.org/10.33890/innova.v3.n9.2018.837

Kuhn-Ferreccio, M. (2024). Crimen organizado y su impacto en la gobernabilidad en Ecuador: Un análisis de los años 2019-2023. Revista Latinoamericana de Seguridad, 7(1), 45-62.

Mainwaring, S. y Pérez-Liñán, A. (2015). Inestabilidad política y colapso democrático en América Latina. Revista de Ciencia Política, 35(1), 123-148. https://doi.org/10.4067/S0718-090X2015000100007

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). Informe sobre incidentes

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

cibernéticos durante las protestas de octubre de 2019 en Ecuador. Quito, Ecuador.

Ministerio de Telecomunicaciones y de la Información. (2022). Estrategia Nacional de Ciberseguridad. https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Naciones Unidas. (1948). Declaración Universal de los Derechos Humanos. https://www.un.org/es/about-us/universal-declaration-of-human-rights

NetBlocks. (2019). Internet disrupted in Ecuador amid protests against austerity measures. https://netblocks.org/reports/internet-disrupted-in-ecuador-amid-protests-against-austerity-measures-8yAvkZ8Z

Observatorio Latinoamericano de Amenazas Digitales [OLAD]. (2024). En la mira: Seguridad y principales amenazas digitales en América Latina. Derechos Digitales.

Ordoñez-González, K. (2024). La ciberseguridad en Ecuador: La vulnerabilidad del periodismo en el espacio digital. IT Ahora. https://itahora.com/2024/08/02/la-ciberseguridad-en-ecuador-la-vulnerabilidad-del-periodismo-en-el-espacio-digital/

Organización de los Estados Americanos. (2023). Informe regional sobre ciberseguridad 2023: Tendencias y amenazas en América Latina y el Caribe. https://www.oas.org/es/sms/ciberseguridad/docs/Informe-Regional-Ciberseguridad-2023.pdf

Organización de los Estados Americanos. (2024). Informe sobre las elecciones presidenciales en Venezuela 2025. https://www.oas.org/es/informes/elecciones-venezuela-2025

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

Ortiz, P. (2020). Crisis social y respuesta estatal en Ecuador: Octubre de 2019. Revista Latinoamericana de Estudios Políticos, 12(1), 45–67.

Ortiz-Prado, E. y Gómez-Barreno, L. (2021). Tipos de ciberataques y su impacto en la seguridad digital en América Latina. Revista Latinoamericana de Seguridad Informática, 5(2), 34–45.

Pazmiño, D. (2020). Polarización política en las protestas de octubre de 2019: El caso de Ecuador. Revista de Estudios Latinoamericanos, 14(2), 78–92.

Pérez-Martínez, J. (2022). Rastros de censura y autocensura: Revelaciones del poder y el miedo sobre el periodismo (en Ecuador 2010–2016). Comunicación, 27, 31–49. https://doi.org/10.18566/comunica.n47.a03

Pérez-Liñán, A. y Mainwaring, S. (2020). Democracias y dictaduras en América Latina: Surgimiento, supervivencia y caída. Fondo de Cultura Económica.

Reporteros Sin Fronteras. (2019). Informe sobre censura digital en América Latina. https://rsf.org/es/informe-censura-digital-america-latina

Reporteros Sin Fronteras. (2024). Venezuela: Nuevo informe de RSF y organizaciones aliadas denuncia el miedo, la intimidación y la autocensura que rodean las elecciones presidenciales. https://rsf.org/es/venezuela-nuevo-informe-de-rsf-y-organizaciones-aliadas-denuncia-el-miedo-la-intimidaci%C3%B3n-y-la

Salcedo-Albarán, E. y Garay-Salamanca, L. (2016). Macro-criminalidad. iUniverse.

Saltos-Ponce, D. (2023). Periodismo de investigación en Ecuador: Análisis de prácticas de seguridad digital

Vinueza-Miller, D. A. y Jiménez, R. P.
pp. 261 - 295
Recibido: 14-03-2025
Aceptado: 30-04-2025
Publicado: 15-06-2025

desde 2017. Pódium, 85–100. https://doi.org/10.18272/pd.v7i1.2967

Santamaría, R. (2021). Polarización política y desestabilización democrática en América Latina: El rol de los intereses transnacionales. Latin American Research Review, 56(3), 589–604. https://doi.org/10.25222/larr.1234

Snegovaya, M. (2015). The role of digital media in the color revolutions. Europe–Asia Studies, 67(3), 397–417. https://doi.org/10.1080/09668136.2015.1030297

Wardle, C. y Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe. https://rm.coe.int/information-disorder-report-november-2017/1680764666