DERECHOS DIGITALES

VENEZUELA 2024

Informe sobre la relación de la crisis política y social sobre el ejercicio de derechos fundamentales en entornos digitales

Mi principal preocupación es “que todo lo que digas, puede ser usado en tu contra, en un país sin estado de derecho, donde con solo un post, te pueden sentenciar a la cárcel, incluso, si solo compartes un post”

Testimonio de periodista

Índice

Resumen

El presente informe aborda la relación de la crisis política y social sobre el ejercicio de derechos fundamentales en entornos digitales en Venezuela, en un contexto

caracterizado por la censura, la vigilancia estatal y restricciones al acceso a la información, destacando que este estudio se centra en tres ejes: libertad de expresión en internet, la ciberviolencia institucional y la accesibilidad a la información.

Fue elaborado entre los meses a julio a noviembre con información recopilada en colaboración con defensores de derechos humanos, periodistas, líderes sindicales y observadores electorales de los estados Bolívar, Lara, Táchira y Yaracuy, utilizando una metodología que combina la revisión documental y los testimonios ciudadanos, no obstante, no sólo documenta la situación actual, sino que también busca proponer recomendaciones para promover un entorno digital más libre y justo, y fomentar un diálogo constructivo entre académicos, defensores de derechos humanos y la sociedad civil.

El informe sobre el monitoreo de derechos digitales en Venezuela en 2024 expone que el 90% de los defensores encuestados disminuyó la cantidad de sus publicaciones tras las elecciones presidenciales, y que se registraron al menos 33 bloqueos a portales web; por ello es un llamado a la acción y a la reflexión sobre el papel de la tecnología en las sociedades contemporáneas, a través de un análisis riguroso y colaborativo, con el que se propuso ofrecer un panorama claro de la realidad que enfrenta Venezuela en el ámbito digital, al tiempo que se abren espacios de diálogo y posibles soluciones para garantizar el respeto y la promoción de los derechos digitales en un entorno desafiante.

Contexto

La acelerada digitalización que ha transformado no solo la forma en que nos comunicamos, sino también cómo ejercemos nuestros derechos fundamentales, incluyendo los derechos digitales ha significado en Venezuela el atravesar por un fenómeno complejo, donde la crisis institucional y las restricciones a las libertades civiles se han visto comprometidas por una serie de decisiones emanadas desde el Estado venezolano, tanto de naturaleza como jurídica como extrajurídica. El año 2024 se erige como un momento crucial para reflexionar sobre el estado de los derechos digitales en el país, dado que se han incrementado las denuncias acerca de violaciones sistemáticas a la privacidad, la libertad de expresión, el acceso a la información, pero más preocupante aún, el uso del espacio digital para ejercer violencia institucional contra la ciudadanía.

En Venezuela, la crisis política y social ha ido acompañada de un control férreo por parte del Estado sobre el espacio digital, a través de la implementación de leyes que limitan el acceso a la información y la vigilancia masiva sobre los ciudadanos han configurado un entorno donde ejercer derechos digitales se ha vuelto riesgoso. La censura en medios de comunicación, tanto tradicionales como en plataformas digitales, ha ido en aumento, en un intento por silenciar a voces críticas, considerando que en el previo a la campaña para las elecciones presidenciales ya se tenían 53 sitios web de noticias bloqueados. Las políticas de bloqueo y filtrado de contenido han restringido el acceso a información relevante especialmente la organización de movimientos sociales que buscan defender los derechos humanos y la democracia.

El presente informe tuvo como objetivo principal realizar un análisis exhaustivo de la situación de los derechos digitales en Venezuela durante el año 2024, centrándose en tres ejes fundamentales: la libertad de expresión en internet, la ciudadanía como parte del grupo de víctimas de la ciberviolencia institucional y la accesibilidad a la información; para ello, se implementó una metodología que combina la revisión de material documental, incluyendo leyes, doctrinas y opiniones

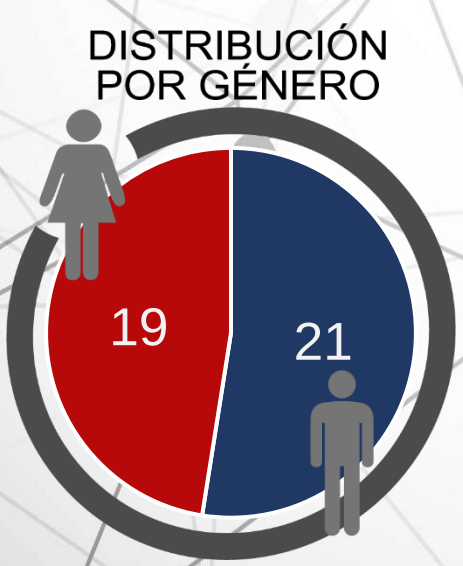
de organismos internacionales, así como una investigación de campo que permite captar la experiencia de los ciudadanos en su interacción con el espacio digital.

La investigación no fue exclusivamente centrada en documentar la situación actual, sino también en recomendar acciones que contribuyan a fortalecer los derechos digitales en Venezuela, en un momento donde la tecnología puede ser una herramienta poderosa para la defensa de los derechos humanos, es imperativo que estas herramientas sean utilizadas para empoderar a los ciudadanos y no para reprimir su voz.

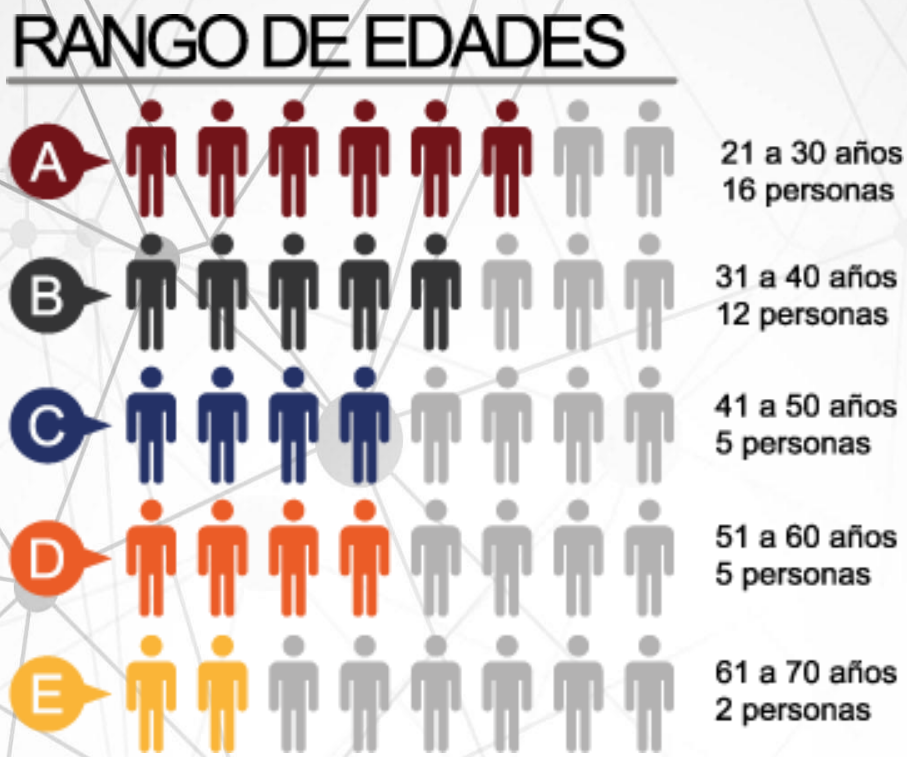
Ámbito de la investigación

Este estudio cuyo objetivo es analizar los efectos de la crisis política vinculada a las elecciones presidenciales sobre el ejercicio de derechos fundamentales en entornos digitales en Venezuela, se desarrolló en cuatro meses comprendidos entre julio a noviembre del año 2024.

Para ello se contó con la participación de 40 defensores de derechos humanos, entre ellos, periodistas, líderes sindicales, activistas de organizaciones no gubernamentales y observadores electorales distribuidos los encuestados en los estados Bolívar (30%), Lara (25%), Táchira (22,5%) y Yaracuy (22,5%).



Las edades de los sujetos de estudio están comprendidas entre los 21 y 65 años, predominado el grupo comprendido por los jóvenes (40% de la muestra), quedando expresada la distribución de la siguiente manera:



Estas entidades tienen en común una agenda sindical muy activa de larga data y han registrado casos de persecución hacia los trabajadores del sector público y en contra de la población en general debido a la tendencia a alzar su voz crítica ante las arbitrariedades del Estado hacia la población venezolana.

Asimismo, han sido objeto de constantes interrupciones eléctricas y fluctuaciones de voltaje, los cuales el gobierno de Nicolás Maduro ha atribuido a presuntos planes de la oposición para “desestabilizar” la sociedad y la economía, por lo que han ejercido acciones represivas y mantienen una política de intimidación en contra de aquellos que realicen denuncias sobre la situación de este servicio público, y en especial, haciendo uso de las redes sociales.

En los cuatro estados seleccionados se tiene presencia de los grupos considerados como objetos de estudio en la actual investigación, teniendo en cuenta que en el contexto de los comicios presidenciales se han ocupado de investigar, documentar, vigilar, denunciar e informar sobre cualquier evento irregular o que contraste con las declaraciones de las figuras del partido de gobierno.

Metodología

En Venezuela el levantamiento de información de derechos digitales relacionados con derechos humanos en Internet ha exigido la utilización de diversas metodologías para estudiar la relación entre la tecnología y la defensa de los derechos humanos.

En la presente investigación una de las más utilizadas ha sido la documentación de casos específicos sobre violaciones a los derechos digitales, que consistió en recopilar información sobre incidentes de censura, acoso en línea, violaciones a la privacidad y otros abusos.

Del mismo modo, se recurrió al uso de encuestas lo que nos permitió a diversas entidades medir la percepción de la población sobre la libertad de expresión y el acceso a la información en línea, obteniendo así datos cuantificables que permiten visualizar las tendencias en los derechos digitales.

Como complemento, también se optó por abordar un enfoque de investigación participativa, en el que se involucró a las comunidades afectadas en el proceso de recolección de datos, adaptándose al contexto que abarca la investigación, destacando que este método no sólo empodera a las personas en la documentación de sus experiencias, sino que también asegura que los datos recolectados sean representativos y contextualizados.

La utilización de herramientas de análisis de datos ha crecido en popularidad en el contexto de derechos digitales. Investigaciones que analizan patrones de censura o acoso en plataformas de redes sociales se han convertido en comunes.

Otra metodología relevante ha sido la realización de talleres de capacitación y workshops sobre protección digital y derechos humanos. A través de estas iniciativas, se capacitan a activistas y periodistas en la recolección y el manejo seguro de información, asegurando que entiendan la importancia de documentar y denunciar violaciones, así como las mejores prácticas para hacerlo.

La elaboración del informe sobre la situación de la libertad en Internet y los derechos humanos en Venezuela ha requerido un enfoque metodológico integral que combina una revisión exhaustiva de fuentes documentales y un análisis detallado de datos empíricos recogidos del trabajo de campo. Este proceso ha permitido comprender la complejidad del entorno digital en Venezuela, donde la censura y la represión son realidades palpables para los defensores de derechos humanos y ciudadanos en general.

Fuentes Documentales

Se llevó a cabo un análisis documental que abarcó múltiples fuentes, entre ellas: las leyes vigentes, normas regulatorias y políticas públicas que afectan la libertad de

expresión y el acceso a la información en el entorno digital, siendo fundamental para identificar las herramientas legislativas que el Estado ha utilizado para justificar la censura y la vigilancia sobre los ciudadanos. Además, se consultaron documentos elaborados por expertos en materia digital, investigaciones académicas y reportes de organizaciones no gubernamentales que han monitoreado la situación de los derechos humanos en Venezuela. Estos documentos proporcionaron un contexto crítico y evidencias sobre las políticas de control y represión que se implementan en el país.

Trabajo de campo y recopilación de opiniones

Se realizaron acciones de trabajo de campo que incluyeron la aplicación de encuestas a usuarios de Internet en diversas regiones de Venezuela. Estas encuestas fueron diseñadas para captar las experiencias y percepciones de los ciudadanos sobre la libertad en el espacio digital, así como para identificar los desafíos que enfrentan diariamente al intentar acceder a información y comunicarse en línea. Se incluyeron preguntas sobre la autocensura, el temor a represalias por expresar opiniones y la percepción sobre la seguridad digital.

Además, se realizaron entrevistas en profundidad con defensores de derechos humanos, activistas y especialistas en tecnología que han experimentado de manera directa la represión estatal en el entorno digital. Estas entrevistas proporcionaron información cualitativa valiosa, revelando tanto sus experiencias personales como su visión sobre las estrategias de resistencia ante la censura.

Análisis de Datos

Una vez recopilados los datos documentales y empíricos, se procedió a un análisis que combinó métodos cualitativos y cuantitativos. Los datos de las encuestas se analizaron estadísticamente para identificar tendencias y patrones, mientras que las entrevistas fueron analizadas mediante un enfoque cualitativo que permitió extraer temas recurrentes y narrativas significativas. Esta triangulación de metodologías garantizó una comprensión más profunda y robusta del fenómeno estudiado, al

integrar tanto la perspectiva legal como las vivencias reales de los ciudadanos en el contexto de la libertad en Internet.

Antecedentes de censura y bloqueo de internet en países de tendencia autoritaria

La censura en el ámbito digital es un fenómeno que se ha visto e intensificado en diversas partes del mundo, cada gobierno tiene sus propias justificaciones y métodos para implementarla. A continuación, se presentan algunos antecedentes relevantes en diferentes contextos y países:

China

1. *Gran Cortafuegos*: Se utiliza un sistema complejo de filtrado y censura en internet para bloquear el acceso a sitios web y controlar la información que circula en la red. Esto incluye plataformas de redes sociales extranjeras como Facebook y X. En noviembre de 2022 durante las protestas contra la política de confinamiento conocida “Covid cero”, del primer mandatario de ese país, Xi Jinping, este sistema se utilizó para censurar las imágenes de distintas redes sociales.

2. *Control de contenidos*: El gobierno chino controla de cerca los contenidos que se publican en plataformas nacionales, censurando cualquier crítica al Partido Comunista o a sus líderes. También ha usado estrategias como la compra de publicidad de manera abrumadora para mostrar su propaganda y narrativas, como ocurrió con Twitter hoy “X”, durante las protestas de Hong Kong de 2021, pese a que esta red está bloqueada en China desde el 2009.

Rusia

1. *Ley de blogs*: Desde 2014, Rusia implementó leyes que requieren que los bloggers y propietarios de sitios web que tienen más de 3.000 visitantes diarios se registren y cumplan con las regulaciones del Estado. Esto permite al gobierno monitorear y censurar contenidos.

2. *Control de redes sociales*: El Kremlin ha bloqueado o restringido el acceso a redes sociales como LinkedIn y ha amenazado con sanciones a plataformas que no cumplan con sus leyes de datos, es el caso de la agencia Roskomnadzor, que es El Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación, bloqueó Twitter y Facebook en 2022, durante el inicio de la invasión rusa a Ucrania.

Irán

1. *Censura estatal*: Irán bloquea regularmente el acceso a una serie de plataformas y sitios web, incluidos Facebook y Twitter, argumentando que son herramientas de desestabilización social y política. Distintos mandatarios del país se han encargado de filtrar información de internet que no esté alineado por la corriente islamista del partido de gobierno.

2. *Vigilancia*: El gobierno iraní también utiliza tecnología de vigilancia para monitorear y silenciar disidentes en línea, especialmente durante períodos de protestas.

Nicaragua

1. *Restricciones a la prensa*: Desde 2018, el gobierno de Nicaragua ha intensificado su control sobre los medios de comunicación y ha cerrado o censurado medios críticos. La represión se ha extendido a las plataformas digitales.

2. *Bloqueo de sitios*: Varias organizaciones han denunciado el bloqueo de portales de noticias y redes sociales, particularmente aquellos que informan sobre las violaciones de derechos humanos. El 27 de octubre de 2020, el gobierno de Nicaragua aprobó la Ley de Ciberdelitos en el congreso nicaragüense, para combatir lo que el gobierno de Ortega define como falsas noticias.

Cuba

1. *Control estricto*: El gobierno cubano controla el acceso a internet y limita las plataformas que permiten la libre expresión. Aunque se ha abierto el acceso a internet en los últimos años, la censura sigue siendo un problema.

2. *Desconexiones temporales*: Durante eventos de protestas o críticas, se han informado desconexiones temporales del servicio de internet. En 2019 entró en vigencia el decreto 370, que regula y penaliza el uso de internet para penalizar a quienes publiquen y compartan información que sea considerada contraria al gobierno.

En general, la censura digital es un fenómeno global que se manifiesta de diferentes maneras y con diferentes justificaciones. La tendencia es hacia un mayor control del Estado sobre la información digital, especialmente en contextos políticos tensos o en preparación para elecciones.

Legislación sobre DDHH Digitales en Venezuela

En Venezuela, varias leyes y regulaciones han sido consideradas como restrictivas de los derechos digitales y de la libertad de expresión en el entorno digital. A continuación, se destacan algunas de las leyes más relevantes en este contexto:

Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (Ley Resorte): Promulgada en 2004, esta ley regula el contenido de los medios de comunicación, incluyendo plataformas digitales. Establece requisitos estrictos sobre la transmisión de información y sanciona la difusión de contenido considerado "desestabilizador" o que contravenga los "valores" de la nación. Esto ha llevado a la censura y autocensura de muchos medios.

Ley Orgánica de Telecomunicaciones: Esta ley, vigente desde 2000 y reformada en varias ocasiones, otorga al Estado amplios poderes para regular las telecomunicaciones en el país. Permite la intervención del Estado en el acceso y

uso de internet, así como la posibilidad de bloquear sitios web y plataformas digitales bajo ciertas justificaciones.

Ley de Defensa de la Soberanía e Integridad Territorial: Promulgada en 2010, esta ley permite al gobierno tomar medidas contra cualquier contenido que considere que atenta contra la soberanía nacional, lo que incluye el monitoreo y bloqueo de plataformas digitales y redes sociales que difundan información que se considere perjudicial.

Ley de Delitos Informáticos: Estas leyes (existen varias propuestas y versiones) han sido criticadas por su posible uso para limitar la libertad de expresión y perseguir a quienes critican al gobierno. Las disposiciones sobre "crímenes cibernéticos" pueden ser interpretadas de manera amplia y potencialmente abusiva, lo que genera un clima de miedo para la libre expresión en línea.

Ley contra el Odio: La Ley Constitucional contra el Odio, la Intolerancia y por la Convivencia Pacífica, sancionada por la Asamblea Nacional Constituyente de Venezuela en 2017, es considerada una ley restrictiva de los derechos digitales. Esta ley ha sido objeto de críticas tanto a nivel nacional como internacional, ya que se argumenta que se utiliza para controlar la libertad de expresión y silenciar a opositores políticos, especialmente en el contexto de la disidencia en línea.

- Artículo 1 - Ámbito de la Ley

Establece que la ley tiene como objetivo sancionar y prevenir el odio y la intolerancia en todas sus formas, lo que proporciona una base amplia y ambigua para la interpretación y aplicación de la ley.

- Artículo 3 - Definición del derecho a la “Paz”

Introduce conceptos vagos y abiertos sobre lo que se considera "odio", "intolerancia" y "convivencia pacífica". Estas definiciones pueden ser utilizadas para restringir una amplia gama de expresiones y opiniones.

- Artículo 11 - Prohibición de la Incitación al Odio

Prohíbe la incitación al odio y a la violencia, pero su interpretación puede llevar a la censura de cualquier crítica o comentario negativo sobre el gobierno o figuras públicas, lo que afecta la libertad de expresión.

- Artículo 20 - Responsabilidad Penal

Establece sanciones penales para quienes sean considerados responsables de actos que promuevan el odio. Esto puede incluir desde información difundida en redes sociales hasta discursos políticos, lo cual crea un clima de miedo para quienes desean expresarse libremente.

- Artículo 21 - Agravantes

Permite la imposición del límite máximo de la pena, usando términos vagos y discrecionales que pueden ser considerados como agravantes, lo que puede llevar a la no discriminación adecuada de delitos relacionados.

- Artículo 22 - Sanciones económicas

Establece mecanismos para el seguimiento y control de la comunicación y publicaciones en medios públicos y privados, permitiendo un monitoreo constante de la actividad en espacios radiales y su eventual sanción en caso de permitir mensajes de odio en su plataforma.

- Artículo 23 - Obligación de colaborar

Obliga a las plataformas digitales a colaborar con el Estado en la difusión de mensajes para la promoción de la paz, así como a la eliminación de contenido que se considere ofensivo o de odio, lo que puede resultar en censura y eliminación arbitraria de publicaciones.

La Ley Constitucional contra el Odio ha sido denunciada por organizaciones de derechos humanos y libertades civiles como una herramienta para restringir la

libertad de expresión, especialmente en medios digitales. La vaguedad en las definiciones y la amplitud de las sanciones generan un ambiente propicio para la autocensura y limitan la discusión política y social en el país.

Ley contra el Fascismo y Expresiones Similares*:* La propuesta de Ley contra el Fascismo y Expresiones Similares, discutida por la Asamblea Nacional de Venezuela en 2021, ha sido considerada por muchos como un instrumento potencial de persecución y criminalización de derechos digitales. Aunque se presenta bajo el pretexto de combatir ideologías extremistas y proteger la convivencia pacífica, sus implicaciones para la libertad de expresión y los derechos digitales han generado serias preocupaciones.

Razones por las que se considera restrictiva:

- La propuesta de ley incluye definiciones amplias y vagas sobre lo que constituye "fascismo" y "expresiones similares", lo que permite una interpretación subjetiva y potencialmente abusiva. Esto podría llevar a la censura de cualquier crítica al gobierno o de ideas que se consideren contrarias a la narrativa oficial.
- Prevé sanciones penales para quienes sean acusados de promover ideologías que se consideren "fascistas", lo que podría incluir discursos políticos, comentarios en redes sociales y contenido en medios digitales. Esto crea un ambiente de miedo donde las personas podrían abstenerse de expresar opiniones críticas.
- Podría permitir un mayor control por parte del Estado sobre las plataformas de medios y las redes sociales, obligando a estas a colaborar en la identificación y eliminación de contenido considerado peligroso o inaceptable. Esto fomenta la autocensura y limita el intercambio de ideas.
- Existen preocupaciones de que esta ley se use como una herramienta para perseguir a opositores políticos, activistas y ciudadanos que critiquen al gobierno, promoviendo un clima de represión en lugar de un diálogo constructivo.

- La implementación de esta ley podría limitar gravemente la libertad de expresión en línea, afectando a periodistas, bloggers y usuarios comunes en sus capacidades de expresar opiniones y compartiendo información.
- La propuesta de Ley contra el Fascismo y Expresiones Similares se suma a un conjunto de normativas que han buscado restringir los derechos digitales y limitar la libertad de expresión en Venezuela. El ambiente político y social en el país ha sido marcado por la represión de voces disidentes, y tales leyes contribuyen a un marco jurídico que puede utilizarse para criminalizar la crítica y el disenso. Las organizaciones de derechos humanos y las voces críticas continúan denunciando estas iniciativas como violaciones a los derechos fundamentales de los ciudadanos.

Por otra parte, Nicolas Maduro en su plan de censura y control comunicacional en fecha 12 de agosto de 2024 mediante el **Decreto N° 4.975**, creó el Consejo Nacional de Ciberseguridad. Este Decreto se generó en medio de un contexto postelectoral donde las protestas, la represión desmedida y el malestar del país estaban en pleno desarrollo ante el anuncio del primer boletín oficial realizado por el Consejo Nacional Electoral.

Es importante destacar, que dicho decreto emitido por el ejecutivo venezolano plantea varias preocupaciones en relación con el ejercicio de los derechos digitales y la posible lesión de los derechos humanos. Algunos de los aspectos preocupantes que se pueden observar incluyen:

El decreto podría contener disposiciones que restringen la libertad de expresión, especialmente en medios digitales, lo que limitaría la capacidad de los ciudadanos para expresar sus opiniones y críticas hacia el gobierno. La mención de "eficacia política" puede implicar un aumento en la vigilancia del gobierno sobre las actividades en línea de los ciudadanos, lo que podría resultar en la monitorización de las comunicaciones digitales y la criminalización de opiniones disidentes y esto lleva a la falta de claridad en los términos y condiciones establecidos en el decreto puede llevar a abusos de poder, permitiendo a las autoridades actuar

arbitrariamente sin rendir cuentas, lo que afectaría la transparencia y el estado de derecho.

Del mismo modo si el decreto prevé restricciones sobre el acceso a plataformas digitales o información en línea, esto perjudica el derecho de los ciudadanos a informarse y comunicarse libremente, cualquier disposición que imponga sanciones severas por la difusión de información o la realización de actividades en línea consideradas "subversivas" podría llevar al temor a la autocensura entre los ciudadanos.

El decreto podría afectar de manera desproporcionada a defensores de derechos humanos y activistas que utilizan plataformas digitales para abogar por cambios sociales, exponiéndolos a represalias y acoso. Al igual que las restricciones digitales podrían impactar gravemente a los grupos ya vulnerables, negándoles la posibilidad de expresarse y defender sus derechos en un entorno seguro.

La interpretación amplia y ambigua de términos del decreto podría resultar en la aplicación indiscriminada y arbitraria de la ley, lo que generaría un clima de inseguridad jurídica.

Estas preocupaciones reflejan un contexto en el que la regulación del uso de tecnologías digitales puede ser utilizada como una herramienta de control social, limitando los derechos fundamentales de los ciudadanos en Venezuela.

En la continuación del Decreto N° 4.975, se pueden identificar otros aspectos preocupantes relacionados con el uso indebido de las tecnologías de comunicación e información, así como la potencial lesión de derechos fundamentales:

La referencia a la "ciberdelincuencia" puede ser utilizada como justificación para implementar medidas represivas que limiten el uso de internet y las telecomunicaciones, afectando libertades civiles. Es decir, la falta de claridad en la definición de qué constituye "ciberdelincuencia" puede dar lugar a una interpretación amplia y subjetiva, permitiendo la criminalización de actividades que no necesariamente son delictivas.

La implementación de una política estatal centrada en la seguridad digital puede llevar a una concentración de poder en manos del gobierno, debilitando la capacidad de los ciudadanos para desafiar o cuestionar estas políticas. El mayor control estatal sobre las tecnologías de comunicación puede resultar en la invasión de la privacidad de los ciudadanos, con potenciales violaciones a la confidencialidad de la información personal.

No es menos preocupante la mención de la cooperación internacional para enfrentar la ciberdelincuencia puede llevar a acuerdos que comprometan la soberanía del país y afecten la protección de datos y derechos de los ciudadanos, teniendo en cuenta un asunto no menor y es que las políticas de vigilancia y control pueden desincentivar la innovación en el sector digital, debido al temor de represalias o sanciones por actividades legítimas en línea.

Las herramientas y políticas destinadas a combatir la ciberdelincuencia pueden ser dirigidas también a organizaciones de la sociedad civil, restringiendo su capacidad para operar y abogar por los derechos humanos, al establecer un marco legal para "proteger" a la sociedad, es probable que se intensifiquen las prácticas de censura en línea, afectando el acceso a información diversa y crítica.

Es de resaltar también que no se menciona explícitamente la importancia de la educación y la alfabetización digital para los ciudadanos, lo cual es esencial para empoderar a la población y prevenir la ciberdelincuencia de manera efectiva. Por ello se afirma que la respuesta del Estado podría ser desproporcionada, enfocándose en el control de la población en lugar de abordar las causas subyacentes de la ciberdelincuencia.

Estos aspectos adicionales resaltan la preocupante posibilidad de que las medidas adoptadas bajo el pretexto de garantizar la seguridad nacional puedan, en realidad, socavar los derechos y libertades fundamentales de los ciudadanos.

Consejo Nacional de Ciberseguridad: En el artículo 1º del Decreto, se pueden identificar varios aspectos preocupantes, al ser un órgano asesor y de consulta

dependiente del presidente, hay un riesgo de que el Consejo esté alineado con los intereses políticos del gobierno, lo que puede comprometer su imparcialidad y objetividad. La naturaleza de este consejo como un organismo dependiente puede llevar a la falta de mecanismos independientes de supervisión, aumentando el riesgo de abusos de poder.

La creación de un consejo que se ocupa de la "prevención de los usos delictivos" puede dar pie a la interpretación amplia de lo que se considera delictivo, facilitando la represión de actividades que no son inherentemente ilegales. Dependiendo de su funcionamiento, el consejo podría proponer normativas que restrinjan aún más el acceso a internet y la libertad de expresión, en nombre de la seguridad cibernética.

La descripción del consejo no menciona la inclusión de representantes de la sociedad civil, lo que podría llevar a decisiones que no consideren las voces y preocupaciones de los ciudadanos. Concentrar el manejo de ciberseguridad en un solo consejo bajo el control del Ejecutivo puede llevar a una centralización de poder, limitando la diversidad de enfoques y soluciones ante riesgos cibernéticos. En este sentido el foco en la "prevención de usos delictivos" podría implicar la implementación de sistemas de vigilancia más estrictos y control sobre la información circulante, afectando la privacidad de los ciudadanos.

La existencia de este consejo podría sentar un precedente para la creación de otras estructuras que busquen criminalizar el uso de tecnologías de comunicación, afectando la innovación y el desarrollo digital. Se afirma esto porque el decreto no especifica claramente cuáles serán las competencias y atribuciones del consejo, lo que podría dar lugar a interpretaciones diversas y a la adopción de medidas poco transparentes. Aunque la intención es combatir delitos cibernéticos, la falta de un enfoque integral que incluya educación y prevención puede resultar en una respuesta reactiva y punitiva que no aborde las causas de la ciberdelincuencia.

Estos aspectos resaltan la necesidad de un debate más amplio y la consideración de mecanismos que garanticen el respeto a los derechos humanos y las libertades civiles en el marco de la ciberseguridad.

En el artículo 2º, que detalla las funciones del Consejo Nacional de Ciberseguridad, se pueden observar varios aspectos relevantes y preocupantes. Aquí algunos de ellos:

El consejo tiene la tarea de asesorar no solo al Presidente, sino también al Consejo de Defensa de la Nación, lo que puede dar lugar a una integración de la ciberseguridad con la defensa nacional, generando preocupaciones sobre la militarización de la ciberseguridad, al elevar propuestas de regulaciones y leyes relacionadas con el uso de tecnologías de la información, existe el riesgo de que se promulguen normativas que limiten libertades civiles y derechos fundamentales en nombre de la seguridad.

La mención de la prevención de "usos delictivos" de las tecnologías de la información podría llevar a una interpretación ambigua, permitiendo la criminalización de actividades que no son necesariamente ilícitas, afectando la libertad de expresión y el acceso a la información, en este sentido la función de verificar el grado de cumplimiento de los planes y regulaciones podría llevar a una vigilancia excesiva y a la creación de un ambiente de temor y autocensura, en lugar de promover una cultura de ciberseguridad responsable.

La obligación de formular propuestas en armonía con los "intereses y objetivos de la Nación" puede llevar a que las recomendaciones del consejo estén más alineadas con la agenda política del gobierno que con las necesidades reales de ciberseguridad de la población. La continua valoración de riesgos y amenazas en materia de seguridad informática debe ser realizada de manera transparente y objetiva; de lo contrario, podría ser utilizada como justificación para implementar medidas excesivas o represivas.

Asimismo, no se menciona la participación de sectores diversos (como la sociedad civil, académicos o expertos en tecnología) en la formulación de políticas, lo que podría limitar el enfoque hacia una seguridad inclusiva y efectiva, así como las funciones del consejo pueden estar en función del contexto político del momento, lo que puede afectar su efectividad y su capacidad para ofrecer soluciones adecuadas y oportunas a problemas de ciberseguridad emergentes.

Estos aspectos resaltan la necesidad de un marco regulatorio claro, equilibrado y respetuoso de los derechos humanos para guiar las funciones del Consejo Nacional de Ciberseguridad, así como una supervisión adecuada de sus actividades.

Los artículos tres, cuatro y cinco, establece cuáles son las instituciones que integrarán el consejo su mecanismo y cómo se quedará distribuida la representación de esta comisión para la ciberseguridad nacional que básicamente está integrado en su gran mayoría por organismos policiales militares que hacen evidente el carácter policial del Estado venezolano en materia de derechos digitales.

Libertad de expresión en internet

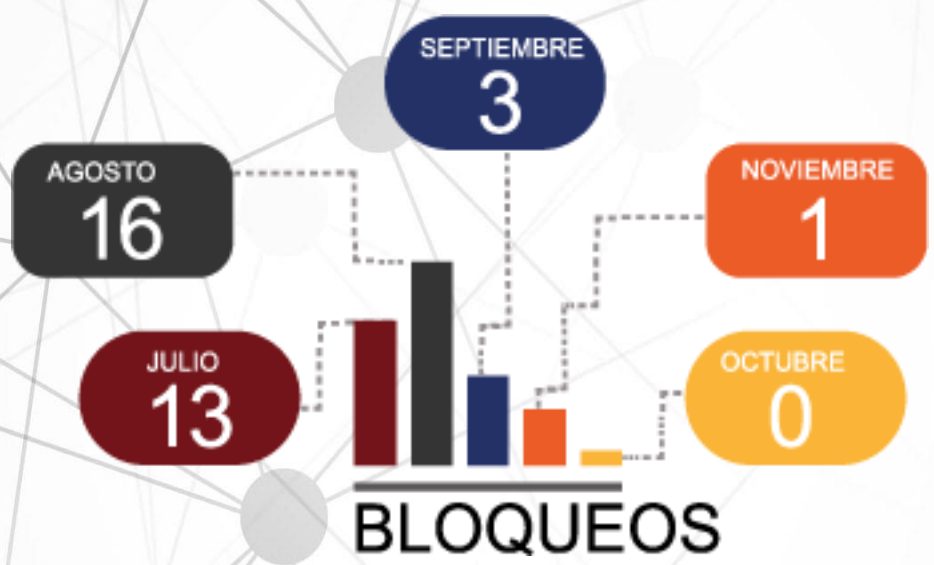
Bloqueo a portales web

El Estado venezolano en su visión hegemónica de controlar todos los medios de comunicación y de información, ha ejecutado una serie de bloqueos contra diferentes portales web a los cuales han tenido acceso los venezolanos en distintas esferas. Desde que Nicolás Maduro decretó el 23 de enero de 2024 la llamada “Furia Bolivariana”, se puso en práctica una razzia contra distintos medios informativos tanto radioeléctricos como digitales, siendo estos el mayor canal de información de los venezolanos a través de sus teléfonos inteligentes, tablets o computadores. En el caso de los portales web informativos (digitales), estos han representado espacios que habían logrado burlar la censura estatal.

Entre los decretos y decisiones arbitrarias del Estado destacan el bloqueo de las redes sociales X y Reddit, la imposición de restricciones para el uso de Signal, ordenados por Maduro el jueves 8 de agosto, y un llamado a dejar de utilizar

WhatsApp “voluntariamente”, argumentando que la plataforma está siendo utilizada para amenazar a miembros del chavismo.

Distintas organizaciones venezolanas como Venezuela sin filtro, Espacio Público y Redes Ayuda han realizado un seguimiento constante a las restricciones que han sufrido los portales informativos, pero también sus portales web han sido blancos de bloqueos gubernamentales, al igual que los servicios de proveeduría de seguridad digital y redes sociales de gran envergadura como lo es el caso de X (antiguo Twitter).



En Venezuela se ha implementado una política estatal que está compuesta por una serie de tácticas para generar bloqueos informativos que limitan el acceso a información crítica y restringen tanto al derecho a la información como el derecho a la libertad de expresión. Este análisis técnico aborda las estrategias utilizadas y las empresas estatales involucradas en estos bloqueos, que han forzado a la población a descargar un VPN para mantenerse informados ante la ausencia de libertad de expresión en los medios de comunicación tradicionales.

Estrategias de Bloqueo Informativo

1. Bloqueo de Sitios Web: El gobierno utiliza técnicas de filtración a nivel de la red para bloquear el acceso a sitios web de noticias, plataformas de redes sociales y

portales de información que son críticos con el régimen. Esto se realiza a través de la implementación de listas negras de URL que son bloqueadas por proveedores de servicios de Internet (ISP).

2. Sistemas de Monitoreo y Censura: Se han implementado sistemas de monitoreo que permiten al gobierno identificar y censurar contenido en tiempo real. Esto incluye técnicas de inspección profunda de paquetes (DPI) que permiten al Estado supervisar el tráfico de Internet y bloquear contenido no deseado.

3. Interferencia en Redes Sociales: La interferencia en el funcionamiento de plataformas de redes sociales es otra táctica común. Esto incluye ralentizar la velocidad de acceso a estas plataformas o en algunos casos, bloquear completamente el acceso en momentos críticos, durante protestas o eventos políticos importantes como lo son los casos de “X” bloqueado el 9 de agosto y de TikTok bloqueado el 28 de septiembre de 2024 por el ejecutivo nacional venezolano.

4. Control de Proveedores de Servicios de Internet: El Estado ejerce control sobre los principales ISP del país, obligándolos a cumplir órdenes de censura y a facilitar el monitoreo del tráfico de datos. Esto incluye tanto empresas estatales como algunas privadas que operan bajo regulaciones estrictas, en las que bajo ninguna circunstancia ni la estatal CANTV, ni los servicios privados de proveeduría de internet pueden dejar de cumplir instrucciones de bloqueo.

5. Desinformación y Manipulación de Información: Además de los bloqueos, el Estado también ha utilizado técnicas de desinformación a través de medios de comunicación estatales y cuentas controladas en redes sociales para saturar el flujo informativo, promoviendo narrativas que favorecen al régimen y desplazando las voces críticas, que van desde campañas de estigmatización, hasta el uso de información no verificada o falsa para saturar la opinión pública.

Hashtags punitivos

El año 2024 se ha caracterizado por la coordinación entre el discurso oficial que se ha materializado en realidad, pero previamente ha existido una proyección en redes

sociales en donde se esgrime una narrativa que peligrosamente ha permeado en el mundo real.

Esta ha sido fundamentalmente la tendencia, que se puede analizar en varios periodos, puntualmente pudiéramos estar tres específicamente.

Se han podido desde el monitoreo analizar tres bloques de tiempo entre enero y abril, entre mayo y el 28 de julio y entre el 29 de julio hasta mediados de octubre del año en curso, con escenarios totalmente diferentes e incluso con discursos dirigidos específicamente hacia personas de ese grupo específicos

#LaFuriaBolivariana

Nuevamente traída a la realidad el 23 de enero del año 2024 durante una locución del presidente Nicolás Maduro, en donde ordenaba a sus bases del partido socialista Unido de Venezuela desatar la furia bolivariana. Ya en el año 2020 había sido implementada entre enero y abril de ese año, pero en el presente ha sido utilizada para según la narrativa oficial evitar que por vías de hecho el partido en gobierno cesar a sus funciones y por lo tanto sus bases tenían que vigilar y marcar a los opositores incluso en sus viviendas, esto también acompañado con la narrativa de presuntos ataques contra la integridad física del presidente Nicolás Maduro.

Durante este período, más que una etiqueta o hashtag, pasó a ser una frase en la que se acompañaba otras campañas ligadas a la narrativa oficial. Fue retomada como etiqueta de uso más frecuente comenzando los meses de octubre y en el mes de noviembre y principios de diciembre donde también se observó publicaciones con el referido término.

Durante el segundo periodo entre abril y Julio, las campañas fueron mayoritariamente dirigidas hacia descalificar la imagen tanto de la líder opositora María Corina Machado como de los integrantes de su partido político, también se observaron menciones descalificativas en redes sociales contra los integrantes de los diferentes voluntariados que participaron en el proceso electoral del 28 de julio del año 2024.

#TunTunLlegoLaPaz

La campaña más agresiva que se ha desarrollado desde el estado venezolano hacia la ciudadanía, con una agresiva campaña de despliegue policial contra las personas que participaron en el proceso electoral, aquellas que estuvieron también involucradas en las movilizaciones ciudadanas como las marchas, concentraciones y todo tipo de expresión popular y finalmente las personas que realizaron comentarios en sus redes personales contrarias al gobierno nacional.

Destacan durante los dos últimos días del mes de julio y las siguientes siete semanas tanto del mes de agosto como de septiembre, videos donde se sometió al escarnio público a opositores como el caso de María Oropeza quien fue arrestada en su vivienda en la ciudad de Guanare, estado Portuguesa, con un video proyectado con una música de fondo de una película de terror.

Los videos donde se sometían a burla a opositores que hacían llamados a la protesta y posteriormente eran presentados luego de haber sido arrestados, con la muy conocida broma o meme, de los “tres Doritos después”, utilizada en gran medida en deportes como el boxeo y el fútbol.

Al igual que estas otras etiquetas como #ComanditosDelTerror #TunTunSinLloradera #GuarimberoLloronPaTocoron, representan dentro del lenguaje agresivo en sí mismo una gran campaña de intimidación contra la población en los días más álgidos de protesta por los resultados del 28 de Julio presentados por el Consejo Nacional Electoral.

Se contabilizaron por lo menos 27 etiquetas en Twitter y TikTok, alusivas a intimidación, estigmatización y difamación contra opositores, de las cuales 11 de gran interacción se pudieron identificar dirigidas hacia la libre opositora María Corina Machado, dos contra la defensora de Derechos Humanos, Rocío San Miguel y el resto dirigidas a otro escenarios y personalidades del mundo de la política y de la sociedad civil venezolana.

Organismos y empresas del Estado venezolano involucrados

1. **CANTV (Compañía Anónima Nacional Teléfonos de Venezuela):** Es el principal proveedor de servicios de telecomunicaciones en el país y está bajo control estatal. Esta telefónica es responsable de la mayoría del tráfico de Internet en Venezuela, ha implementado bloqueos y censura siguiendo órdenes del gobierno.

2. **Movilnet:** Esta es la filial de CANTV dedicada a los servicios móviles. También ha sido utilizada para el acceso a información privada vía SMS y otros servicios de comunicación que facilitan la organización y difusión de información crítica.

3. **Ministerio del Poder Popular para la Comunicación y la Información:** Este ministerio supervisa la política de comunicación del Estado y es responsable de la regulación de los medios de comunicación en el país. Se encarga de emitir regulaciones sobre el contenido que pueden difundir los medios de comunicación y coordinar las acciones de censura.

4. **Sistema Nacional de Medios Públicos:** Comprende una red de medios de comunicación estatales que se utilizan para difundir información favorable al gobierno y desmentir o descalificar informaciones negativas.

5. **CONATEL (Comisión Nacional de Telecomunicaciones):** Es el ente regulador que supervisa los servicios de telecomunicaciones en Venezuela. CONATEL ejerce control sobre las concesiones de medios y frecuencias, además, puede imponer sanciones a medios de comunicación que no cumplan con las directrices del Estado.

El Estado venezolano ha desarrollado un sistema complejo de tácticas para generar bloqueos informativos, que combina la censura directa y el control de la infraestructura de telecomunicaciones con el uso de la desinformación. La combinación de empresas estatales como CANTV, Movilnet y CONATEL, entre otras, permite al gobierno ejercer un control efectivo sobre el flujo de información y limitar las libertades digitales de los ciudadanos. Las implicaciones de estas acciones son profundas, ya que afectan la capacidad de las personas para acceder a información veraz y participar en el discurso público.

Accesibilidad a la información

Afectación de la población por la crisis de servicios

Los cortes eléctricos han tenido un impacto significativo en la velocidad y calidad del acceso a Internet en el país. El registro de la velocidad de Internet en el país varía significativamente por regiones debido a factores como la infraestructura disponible, la calidad del servicio de los proveedores de Internet y los cortes de electricidad, en este contexto las interrupciones afectan a los activistas desde diferentes perspectivas: psicológica, económica, técnica y laboral.

Venezuela es uno de los países con el internet más lento, según Ookla, en el país para abril de 2024, la velocidad mediana de Internet fijo residencial fue de 45.84 Mbps para la carga y de 48.77 Mbps para descarga. En el caso de la velocidad mediana de Internet móvil fue de 6.29 para la carga y de 11.66 Mbps para descarga, factor por el cual existen personas que se han inhibido de hacer publicaciones en redes sociales.

- Impacto Psicológico:

Los apagones prolongados generan distintos tipos de reacciones en la sociedad, desde enojo, tristeza y ansiedad en los ciudadanos, situación que no es diferente en aquellos que dependen de la tecnología para llevar a cabo su labor de activismo. Activistas digitales, quienes suelen utilizar plataformas en línea para organizarse, comunicar sus ideas y difundir información, se enfrentan a un entorno hostil donde el servicio eléctrico y el acceso a internet son restrictivos. Esta falta de estabilidad puede provocar sentimientos de frustración, impotencia y desesperanza, afectando gravemente su capacidad para mantener un enfoque positivo en su misión.

Investigaciones recientes, como las realizadas por la Organización Mundial de la Salud (OMS) y otras instituciones, han demostrado que el estrés prolongado puede provocar no solo problemas de salud mental, como ansiedad y depresión, sino también un deterioro en el rendimiento cognitivo. En un país donde la inestabilidad

es la norma, los apagones se suman a la carga emocional que ya enfrentan los activistas, creando un círculo vicioso de desmotivación y desconfianza.

Es el caso de Mariana (seudónimo), periodista en Bolívar: "Cada apagón es una nueva ola de ansiedad. Nunca sabes cuándo volverá la luz, y eso me hace sentir impotente, a veces impotente pero otras resignada. Estoy constantemente preocupada por cómo seguir adelante con nuestras actividades en el diario. He tenido noches en las que simplemente mis horas de sueño se ven modificadas, pensando en todo lo que tenemos que hacer y cómo los apagones nos detienen. Me siento desgastada emocionalmente, a eso hay que sumarle que, para surtir combustible en Puerto Ordaz, en ocasiones hay que hacer colas de más de 4 horas. Lo que más me afecta es el calor cuando hay un apagón, te desgasta física y emocionalmente a un nivel que debes postergar lo que estás haciendo para otro día."

- Impacto Económico:

Desde el punto de vista económico, los apagones afectan la capacidad de los activistas digitales para desempeñar su labor. Muchos de ellos dependen de tecnologías digitales y acceso a internet para obtener financiamiento, gestionar campañas y colaborar con organizaciones internacionales. La falta de electricidad no solo limita su acceso a estas herramientas, sino que también aumenta los costos operativos.

Según el informe del Banco Mundial de 2021, la crisis económica en Venezuela ha sido exacerbada por la inestabilidad del transporte y la logística, en gran parte debido a la falta de energía. Activistas que buscan apoyo financiero a menudo enfrentan dificultades para comunicar sus necesidades de financiamiento a donantes potenciales, lo que los deja en una posición vulnerable, incapaces de llevar a cabo sus proyectos y de recibir apoyo adecuado.

Testimonio de "Giovanni", activista sindical y comerciante en el estado Yaracuy: "Los apagones no solo interrumpen nuestra comunicación, sino que también afectan

nuestro presupuesto como emprendedores. Tuvimos que gastar más en generadores y combustible, lo que ha limitado nuestra capacidad de llevar a cabo nuestra actividad, por lo que la capacidad de participar en asuntos cívicos se ve limitada y prácticamente nula".

- Impacto Técnico:

Desde un punto de vista técnico, los apagones también limitan el acceso a las herramientas digitales y a la infraestructura necesaria para el activismo. La falta de energía significa que no se puede acceder a servidores, plataformas de gestión de contenido y otros recursos digitales esenciales. Esto crea un vacío en la comunicación y en la organización de actividades, debilitando la capacidad de los activistas para movilizar a la sociedad civil y generar impactos efectivos.

Además, la repetida interrupción en el servicio eléctrico puede dañar equipos sensibles, como computadoras y dispositivos de almacenamiento, resultando en pérdidas irrecuperables de datos importantes para el activismo y la defensa de los derechos humanos. Como mencionó Winston Cabas, presidente de la Comisión eléctrica Nacional del Colegio de Ingenieros de Venezuela, las pérdidas por el daño de equipos son incontables, "Hay que decirle al país la verdad..., decirles a los venezolanos de qué hora a qué hora son los racionamientos para que desconecten sus equipos, para que cuando regrese el suministro, que es cuando se dañan los electrodomésticos, ya estén desconectados".

Testimonio de “Laura” activista del estado Táchira: "Cada vez que hay un apagón, perdemos mucho más que solo unos minutos de trabajo. He tenido que enfrentar la pérdida de datos esenciales. En una ocasión, mientras trabajábamos en un informe importante, se cortó la luz y perdimos horas de investigación. Intento hacer copias de seguridad, pero a veces es imposible acceder a los servidores. Esto ha debilitado nuestra capacidad para comunicarnos y colaborar efectivamente. Antes contábamos con financiamiento externo, pero al no poder mostrar resultados debido a la falta de luz y conexión, varios donantes han decidido suspender su apoyo. Nuestro trabajo se ha vuelto más costoso y difícil"

- Impacto Laboral:

Los apagones también tienen un impacto laboral en el sentido más amplio. Muchas organizaciones de la sociedad civil dependen de tareas digitales para su funcionamiento. Cuando el acceso a electricidad es irregular, se pone en riesgo la continuidad de proyectos que requieren un esfuerzo constante y bien planificado. Esto puede resultar en la pérdida de empleos y en el despido de personal que no puede cumplir con sus responsabilidades debido a la falta de recursos.

Testimonio de “Eduardo”, joven activista del sector humanitario en el estado Lara: "Soy parte de un equipo que trabaja en el sector humanitario, pero los apagones han sido devastadores para nosotros. Muchos de mis compañeros han tenido que dejar sus puestos porque no pueden cumplir con sus responsabilidades. Uno de mis mejores amigos se fue del país al sentirse frustrado por no poder hacer nada. La verdad es que cada vez veo menos futuro en esto, y cómo los apagones están causando que el talento se pierda. Me duele ver cómo la inestabilidad laboral afecta a tantos que solo quieren hacer un cambio.”

Patrones Históricos entre Cortes Eléctricos y Conectividad

Frecuencia de Cortes: Desde el colapso del sistema eléctrico en Venezuela, los cortes de energía se han vuelto frecuentes y prolongados, coincidiendo con una caída notable en la calidad y velocidad de Internet. En períodos de apagones prolongados, como el apagón nacional de marzo de 2019, se reportaron caídas drásticas en el acceso a Internet a nivel nacional.

Los cortes de electricidad provocan la interrupción del suministro a las infraestructuras críticas, como servidores, centros de datos y nodos de distribución de Internet. Esto resulta en la pérdida de conectividad por períodos prolongados, lo que impide el acceso a la red.

Cuando la electricidad se restablece, es común que haya un aumento repentino en la demanda de usuarios que intentan reconectar sus dispositivos y acceder a Internet. Esta sobrecarga puede afectar la velocidad de conexión, resultando en

lentitud y en la dificultad para acceder a servicios en línea. La situación subraya la necesidad urgente de una reforma integral en el sector eléctrico y de telecomunicaciones para garantizar un acceso estable y de calidad a Internet en Venezuela.

Estacionalidad: La conectividad a menudo mejora temporalmente durante las temporadas de mayor producción de electricidad (como en temporada de lluvias), pero se desploma en temporadas secas debido a la disminución en la capacidad de generación de energía de las hidroeléctricas, que son la principal fuente de electricidad en el país.

Desigualdades regionales: Las áreas rurales y menos desarrolladas generalmente sufren más debido a la inestabilidad en el suministro eléctrico, lo que se traduce en una conectividad deficiente y velocidades de Internet más bajas. Las zonas urbanas pueden experimentar interrupciones, pero a menudo tienen un acceso más constante a fuentes alternativas de energía, como generadores.

Desconexión de Equipos de Red: Equipos esenciales, incluidos routers, switches y otros dispositivos de red, requieren energía para funcionar. Durante los apagones, estos equipos se apagan, lo que puede llevar a caídas en la conectividad en áreas específicas.

Efectos en la productividad: La repetida inestabilidad del suministro de energía y su impacto en la conectividad ha llevado a numerosas complicaciones para los sectores productivos que dependen de Internet para operar, incluyendo empresas, comercios e instituciones educativas.

Capacitación a defensores sobre ciberseguridad

En el estado Lara se realizaron las capacitaciones de igual forma del 25 al 27 de julio de manera presencial, y otras que se realizaron de forma remota los días 12 y 13 de septiembre del 2024, con un total de 11 participantes. La formación estuvo a cargo del ingeniero José Millán, experto en realidad aumentada egresado de la universidad de Oriente. De igual forma, en Yaracuy se realizó la formación de 24

personas de manera presencial de los días 25 al 27 de julio y de forma online los días 12 y 13 de septiembre.

La capacitación estuvo a cargo del ingeniero José Millán, experto en realidad aumentada egresado de la Universidad de Oriente, y la temática abordada fue: nociones básicas sobre seguridad digital, herramientas para identificar riesgos en redes sociales, mensaje fraudulentos más comunes como el fishing y el spyware, así como una ilustración de cuáles son algunos de los medidas de protección que deben conocer los activistas de la sociedad civil para evitar ser blanco de la vigilancia en redes sociales, el robo de información, así también la protección de las cuentas bancarias como uno de los mecanismos de persecución hacia miembros de la sociedad civil.

Al respecto, en Táchira, se realizó una serie de talleres los días 25 y 26 de julio de manera presencial y adicionalmente una sesión virtual el 5 de septiembre, en los cuales se contó con la presencia de seis personas.

La formación estuvo a cargo del experto en redes sociales Adolfo Baptista, y el contenido impartido se centró en los mecanismos de protección en el área digital para ejercer la documentación, como una de las principales funciones de los defensores de Derechos Humanos. De igual modo, se facilitaron nociones básicas sobre seguridad digital como doble autenticación, uso de VPN e identificación de posibles amenazas.

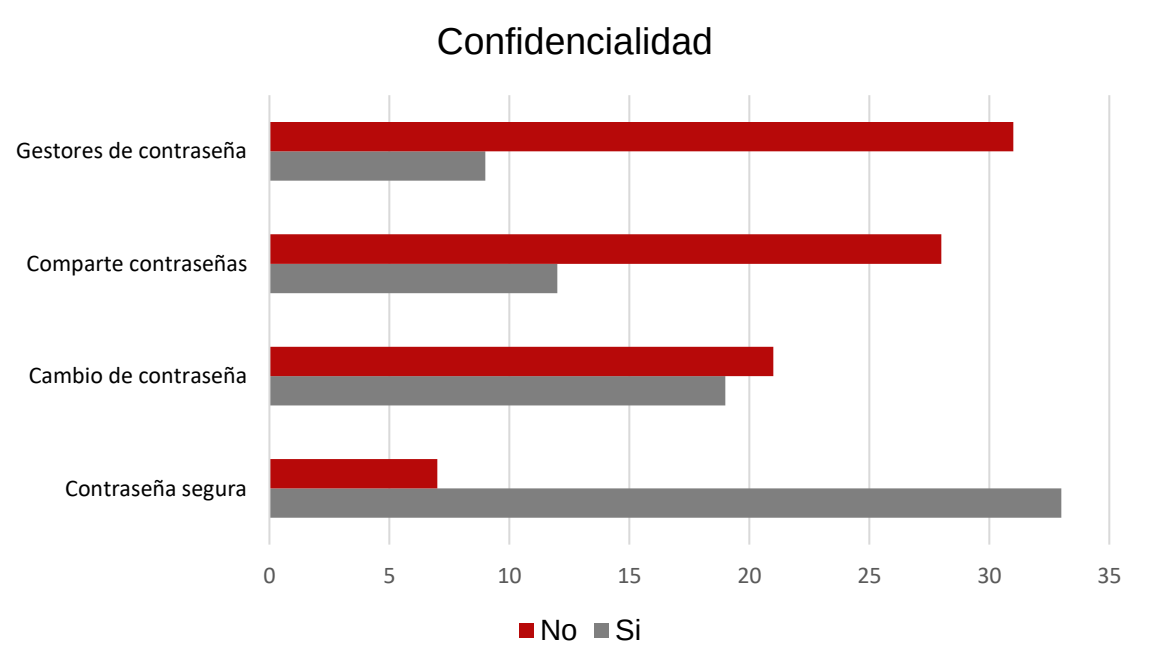
Por su parte, en el estado Bolívar se realizaron capacitaciones presenciales los días 26 y 27 de agosto, las cuales se complementaron posteriormente de manera remota, los días 29 y 30 de agosto, en las cuales se tuvo un total 11 participantes, bajo la tutoría de Simón Arreaza, experto en redes sociales de la Universidad Católica Andrés Bello, núcleo Guayana. En dicha participación se dictó una temática sobre el uso de conexiones seguras como el VPN, la doble autenticación para el ingreso a las cuentas personales e institucionales, así como nociones básicas para identificar posibles amenazas.

Percepción preelectoral sobre la seguridad digital

Para medir este indicador se realizaron dos encuestas, la primera el 25 de julio del 2024, previo a las elecciones presidenciales en el país a defensores de derechos humanos y comunicadores sociales, a fin de conocer su posición o expectativas sobre el manejo de las redes sociales en Venezuela y el riesgo de vigilancia o persecución por parte de las instituciones del Estado y afectos al partido de gobierno. Se obtuvieron los siguientes resultados:

Cuadro 1. Confidencialidad

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
1	¿Utiliza contraseñas seguras y únicas para sus cuentas?	33	82,5	7	17,4
2	¿Cambia regularmente sus contraseñas?	19	47,5	21	52,5
3	¿Ha compartido alguna vez contraseñas o información de inicio de sesión con otras personas?	12	30	28	70
4	¿Ha implementado medidas adicionales de seguridad como el uso de gestores de contraseña?	9	22,5	31	77,5

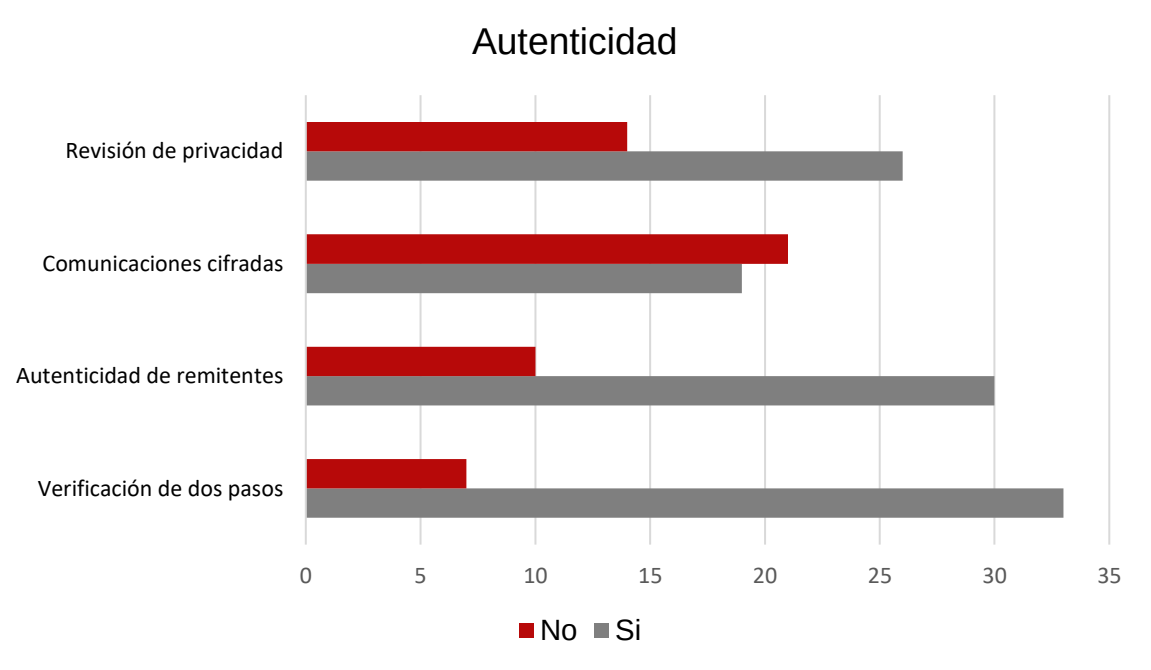


La confidencialidad se refiere a proteger la información del acceso no autorizado, estableciendo privacidad para los datos de la persona u organización, previniendo ciberataques o situaciones de espionaje.

Aun cuando la base de este pilar es el control de acceso mediante autenticación de contraseña, es importante que los encuestados manejen otros mecanismos como el escaneo biométrico y cifrado, debido a que han generado resultados favorables en este sentido, ya que un 30% ha compartido sus contraseñas.

Cuadro 2. Autenticidad

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
5	¿Habilita la autenticación de dos pasos en sus cuentas en línea?	33	82,5	7	17,5
6	¿Verifica la autenticidad de los remitentes antes de hacer clic en los enlaces?	30	75	10	25
7	¿Cifra sus comunicaciones sensibles cuando envía mensajes?	19	47,5	21	52,5
8	¿Revisa regularmente la configuración de privacidad de sus cuentas?	26	65	14	35

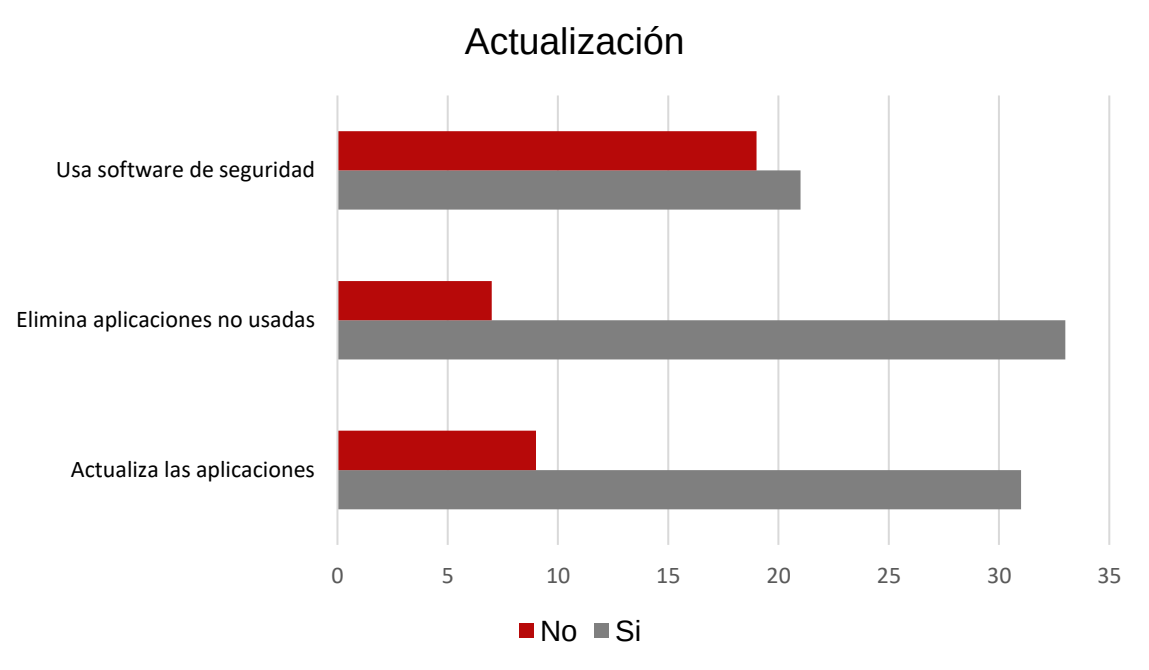


La autenticidad es la confirmación de que los datos tienen legitimidad, es decir, que no existe manipulación o intervenciones externas por parte de terceros que se hacen pasar por colaboradores. Para ello, es necesario documentar las acciones realizadas por los usuarios en la red y los sistemas.

Cabe destacar que menos de la mitad de los encuestados (47,5%) expresó que mantiene comunicaciones cifradas, lo que los coloca en una posición de vulnerabilidad ante posibles ataques de ciberseguridad a nivel personal y organizacional, recordando que los datos de las organizaciones deben tener procesos para identificar su autenticidad, para ello se recomienda la configuración de un registro de acceso que ayude a confirmar la veracidad de un registro en particular.

Cuadro 3. Actualización

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
9	¿Actualiza sus dispositivos y aplicaciones con regularidad?	31	77,5	9	22,5
10	¿Elimina las aplicaciones no utilizadas de sus dispositivos?	33	82,5	7	17,5
11	¿Utiliza software de seguridad actualizado en sus dispositivos?	21	52,5	19	47,5



Los resultados llaman la atención en cuanto al uso de software de seguridad actualizado por parte de los encuestados, debido a que solo un poco más de la mitad (52,5%) los implementa para el manejo de sus redes sociales, y se expone así a cualquier tipo de vulneración de sus cuentas o dispositivos con los que se dedica a la promoción, difusión y defensa de los derechos humanos en Venezuela.

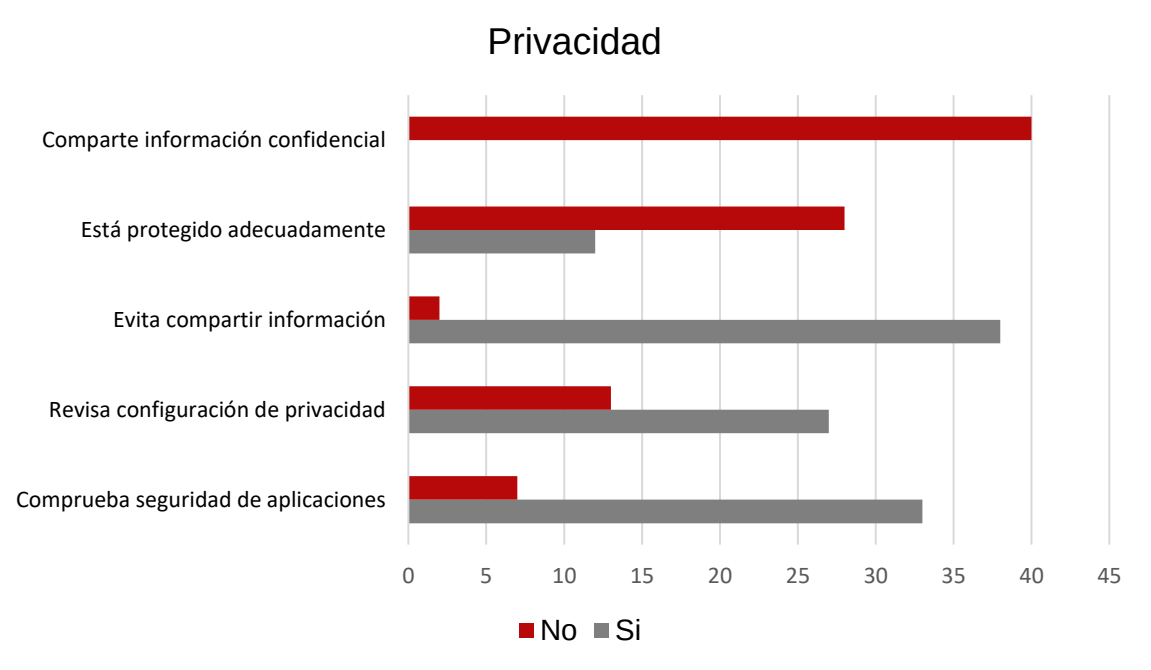
Según el Instituto Nacional de Ciberseguridad en España, es importante realizar actualizaciones frecuentes porque "*Los sistemas operativos, navegadores web, programas y aplicaciones son susceptibles de tener fallos de seguridad. Por este*

motivo, pueden necesitar ser actualizados, independientemente del dispositivo en el que se encuentren instalados. Esto incluye los programas y sistemas operativos de ordenadores, tablets, smartphones, consolas de videojuegos e incluso televisiones inteligentes."

Por otra parte, más de 75% de los elimina y actualiza las aplicaciones con frecuencia, lo que representa que realizan acciones que ayudan a reducir riesgos, permitiendo la verificación de código, cambios en codificación, evaluación de amenazas de codificación involuntarias, opciones de encriptación, permisos de auditoría y los derechos de acceso.

Cuadro 4. Privacidad

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
12	¿Comprueba la seguridad de una aplicación antes de descargarla?	33	82,5	7	17,5
13	¿Revisa con frecuencia la configuración de privacidad?	27	67,5	13	32,5
14	¿Evita compartir información personal sensible en línea?	38	95	2	5
15	¿Cree que su información personal en línea está adecuadamente protegida?	12	30	28	70
16	¿Ha compartido alguna vez información confidencial a través de una red social?	0	0	40	100



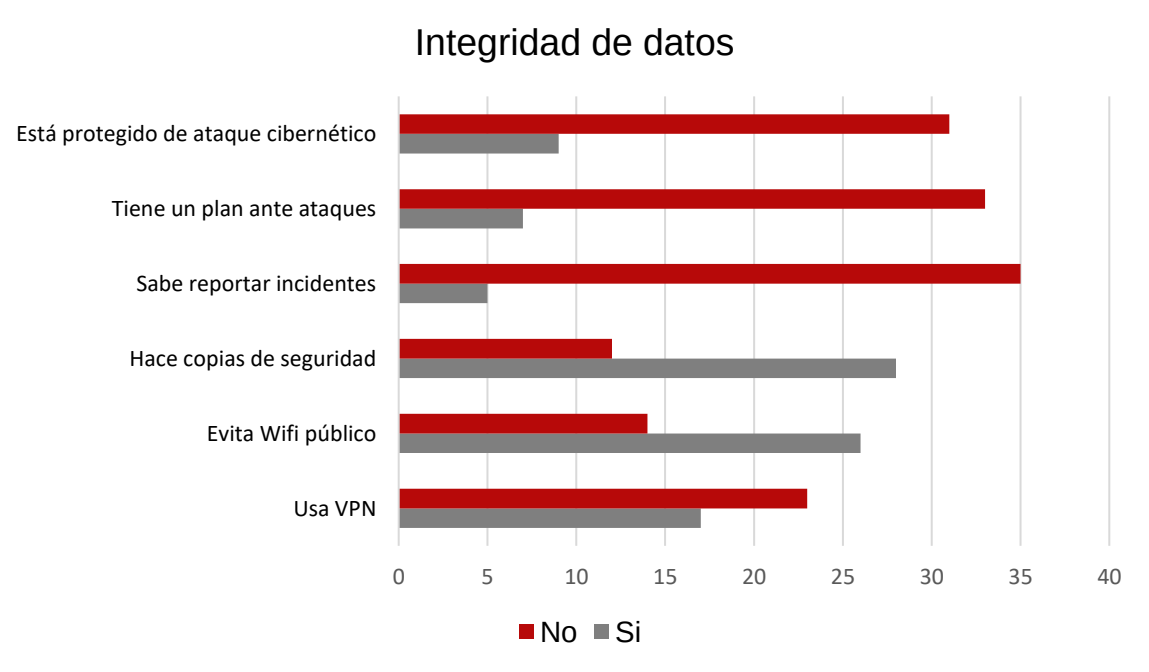
Las violaciones a la privacidad se refieren a los accesos no autorizados a cuentas de redes sociales, correo electrónicos y aplicaciones en línea, que pueden tener consecuencias graves para la intimidad de las personas y la confianza en las plataformas digitales.

Solo el 30% de los encuestados considera que está debidamente protegido ante una posible vulneración de su privacidad, lo que demuestra la necesidad de reforzar sus conocimientos en ciberseguridad, aunque el 100% de ellos no comparte información confidencial a través de sus cuentas en redes sociales.

Los motivos detrás de los ataques cibernéticos pueden variar, pero existen tres categorías principales: delictivos, políticos y personales, sin embargo, en Venezuela se ha registrado un mayor caso de atacantes con motivaciones delictivas que buscan beneficios económicos a través del robo de dinero, y con motivaciones políticas suelen asociarse con actores del Estado hacia organizaciones no gubernamentales o a la infraestructura de la oposición.

Cuadro 5. Integridad de datos

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
17	¿Utiliza una red virtual privada (VPN) para navegar de forma segura en línea?	17	42,5	23	57,5
18	¿Evita conectarse a redes Wifi públicas no seguras?	26	65	14	35
19	¿Hace copias de seguridad de sus datos de forma regular?	28	70	12	30
20	¿Sabe cómo reportar incidentes de seguridad digital a las autoridades pertinentes?	5	12,5	35	87,5
21	¿Cuenta con un plan de respuesta ante posibles incidentes de seguridad digital?	7	17,5	33	82,5
22	¿Cree que sus cuentas están protegidas contra posibles ataques cibernéticos?	9	22,5	31	77,5



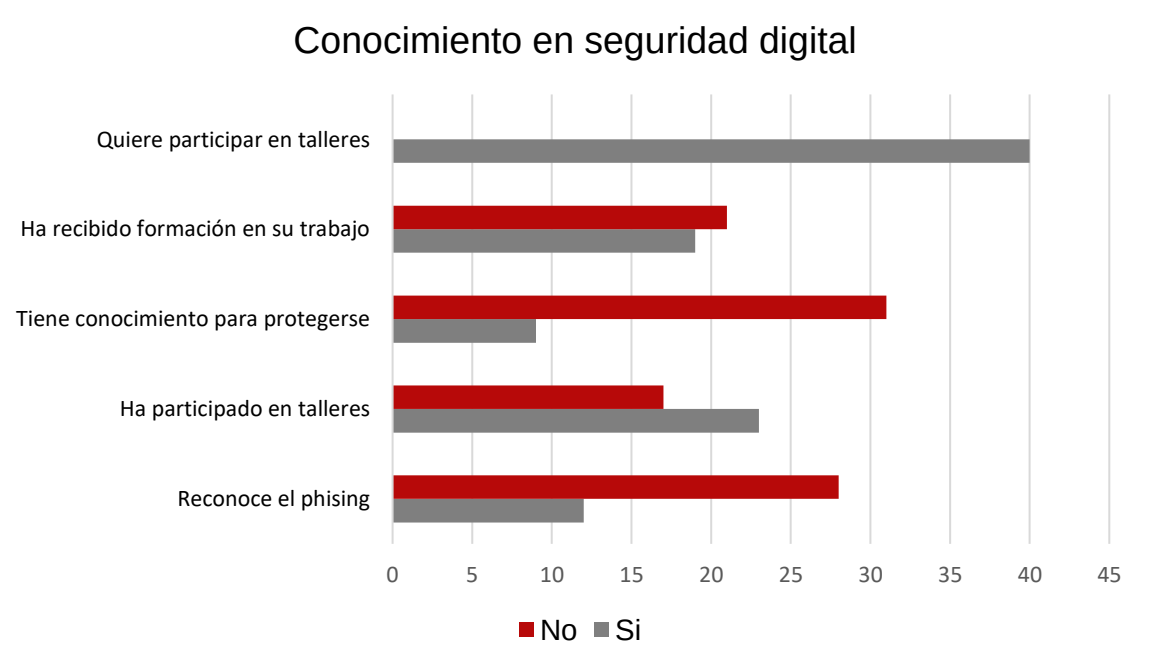
Con estos resultados se evidencia que los encuestados previo al 28 de julio evidenciaban una falta de medidas proactivas de seguridad digital, lo que los dejaba expuestos a de ser víctimas de ataques adicionales a los ya inherentes a su labor como defensores de derechos humanos, especialmente en un contexto donde hay preocupaciones sobre acoso, vigilancia y amenazas.

Hay que destacar que más del 80% de los sujetos no contaban con un plan de respuesta ante la violación de su ciberseguridad ni tenían conocimientos de cómo realizar los correspondientes reportes ante un eventual ataque digital.

Si existe una alteración indebida en los datos, significa que ha habido una pérdida de integridad, y es necesario implementar mecanismos de control para evitar la alteración no autorizada de la información.

Cuadro 6. Conocimiento en seguridad digital

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
23	¿Reconoce los signos de un posible ataque de phishing?	12	30	28	70
24	¿Ha participado en capacitaciones sobre seguridad digital?	23	57,5	17	42,5
25	¿Considera que su nivel de conocimiento en seguridad digital es suficiente para protegerse en línea?	9	22,5	31	75,5
26	¿Ha recibido formación específica sobre seguridad digital en su área de trabajo?	19	47,5	21	52,5
27	¿Está interesado en participar en un taller sobre seguridad digital?	40	100	0	0

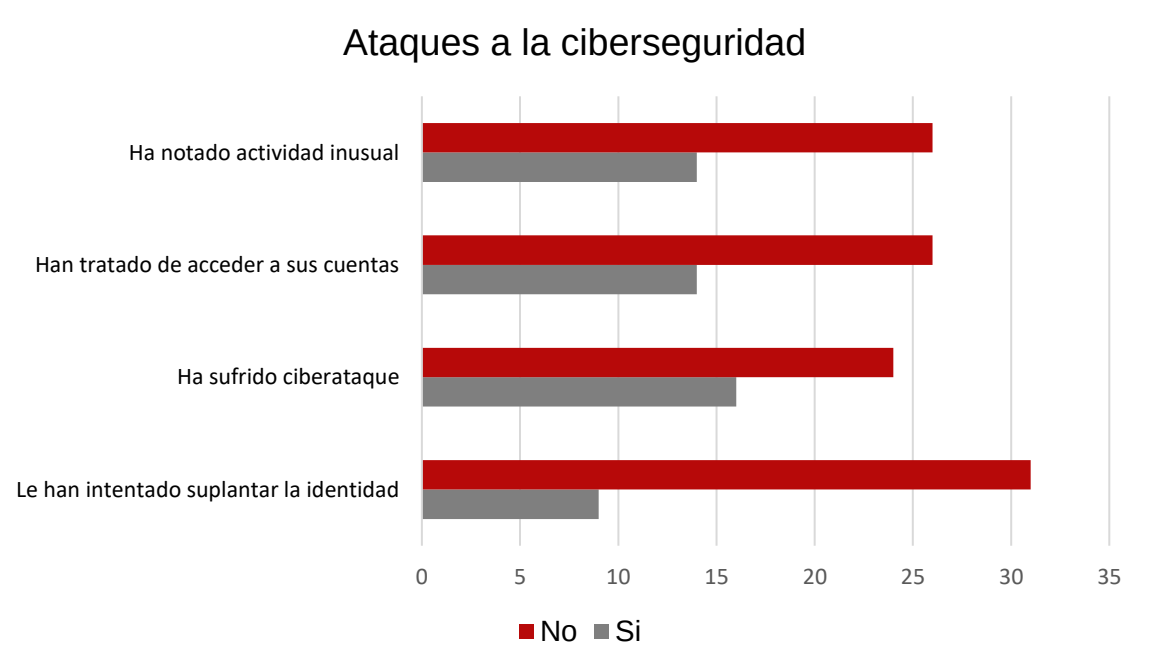


Tener conocimientos en ciberseguridad permite la reducción de pérdidas económicas, además de crear mecanismos de protección en procesos, tecnología y personas, no solo frente a ciberataques o fugas de información, sino también para garantizar la seguridad.

Al respecto, el 75,5% de los encuestados manifestó que su nivel de conocimiento en seguridad digital es suficiente para protegerse en línea, por lo que expresaron en un 100% que estaban interesados en recibir formación en ciberseguridad, a fin de poder minimizar su nivel de vulnerabilidad digital.

Cuadro 7. Ataques a la ciberseguridad

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
28	¿Ha experimentado alguna vez un intento de suplantación de identidad en línea?	9	22,5	31	77,5
29	¿Ha sido víctima de algún tipo de ciberataque?	16	40	24	60
30	¿Han intentado acceder a sus cuentas sin autorización previa?	14	35	26	65
31	¿Ha notado actividad inusual en sus cuentas que pudiera indicar una brecha de seguridad?	14	35	26	65

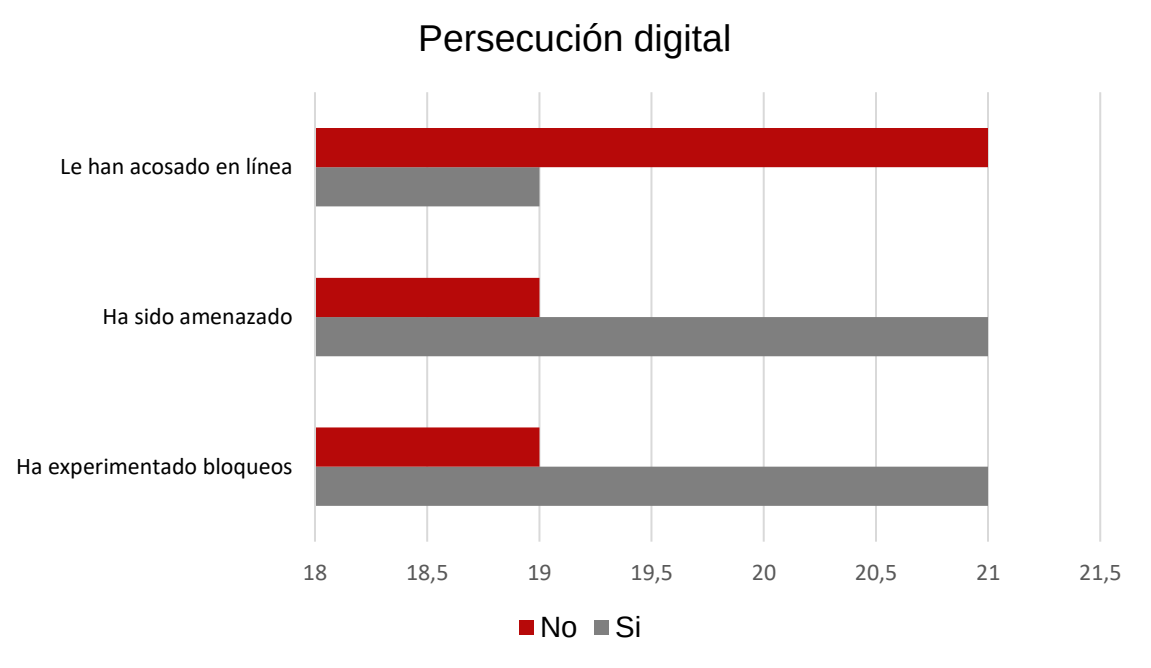


Antes de los comicios presidenciales en promedio, la mayoría de los encuestados no había experimentado intentos de suplantación de su identidad en las redes sociales, lo que puede indicar una confianza relativamente alta en sus prácticas de seguridad en línea o en la seguridad de las plataformas que utilizan. Sin embargo, debe ser objeto de atención aquellas personas que ya habían sido víctimas de este delito, debido a que se consideran amenazas directas.

Según la empresa de tecnología IBM "*un ataque cibernético es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital*."

Cuadro 8. Persecución digital

Ítem	En el manejo sus redes sociales y correo electrónico, usted:	Si		No	
		f	%	f	%
32	¿Ha experimentado bloqueos en línea al intentar acceder a cierto contenido?	21	52,5	19	47,5
33	¿Ha recibido amenazas en línea relacionadas con su labor?	21	52,5	19	47,5
34	¿Ha sido sujeto de acoso en línea en relación con su trabajo?	19	47,5	21	52,5



En relación a la recepción de amenazas o intimidaciones en línea entre defensores de derechos humanos laborales, periodistas y observadores electorales revelan que al menos la mitad de los encuestados ha recibido amenazas o intimidaciones en línea, lo que indica que enfrentan riesgos significativos en su trabajo. Esta cifra implica un entorno hostil para quienes se dedican a la defensa de derechos humanos, la actividad periodística y la observación electoral.

Las amenazas en línea pueden tener efectos paralizantes, afectando la capacidad de estos profesionales para llevar a cabo su labor. Esto podría resultar en autocensura, miedo a represalias, y un impacto negativo en la producción de contenido o en la defensa de causas importantes.

Según IBM, “los motivos detrás de los ataques cibernéticos pueden variar, pero existen tres categorías principales: delictivos, políticos y personales”, sin embargo, en Venezuela, la persecución ejercida por el Estado hacia la disidencia política se ha trasladado al ámbito digital, en especial en contra de los empleados públicos y defensores de derechos humanos.

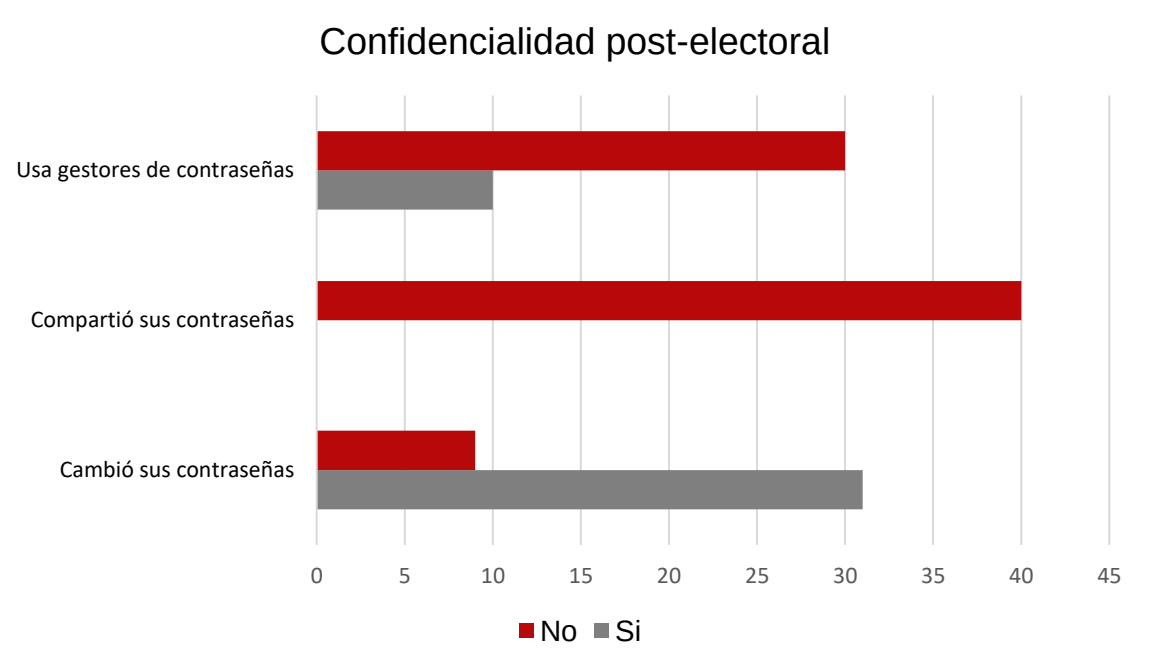
Ante esta situación, se hace urgente la implementación de medidas de protección, tanto a nivel personal como organizacional, esto incluye la capacitación en ciberseguridad, el uso de herramientas de protección y la creación de protocolos de respuesta ante amenazas.

Situación postelectoral de la seguridad digital

Posterior a los comicios presidenciales se aplicó una encuesta de opciones múltiples referida nuevamente a la percepción de la seguridad en la utilización de canales digitales para la difusión, promoción y denuncia de hechos relacionados con los derechos humanos, de la cual se obtuvieron los siguientes resultados:

Cuadro 9. Confidencialidad post-electoral

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
1	¿Ha cambiado las contraseñas de sus cuentas en redes sociales?	31	77,5	9	22,5
2	¿Ha compartido sus contraseñas de redes sociales con otras personas?	0	0	40	100
3	¿Ha recurrido a gestores de contraseñas para proteger la seguridad de sus cuentas en RRSS?	10	25	30	75

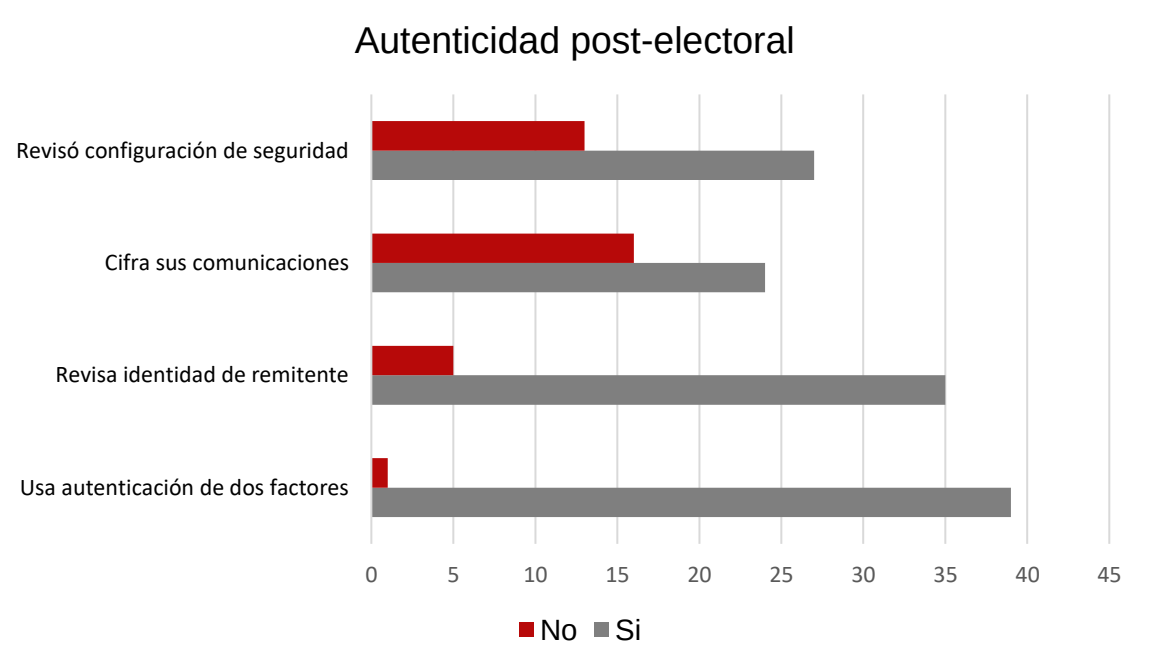


Luego de los comicios, el 77,5% los encuestados hicieron cambio de las contraseñas de sus redes sociales ante el incremento de la vigilancia sobre la actividad digital de los defensores de derechos humanos, en especial de los observadores electorales, sin embargo, se mantiene el alto porcentaje (75%) de ellos que no ha recurrido al uso de gestores de contraseñas como medida de ciberseguridad.

La Oficina de Seguridad del Internauta (OSI) define los gestores de contraseñas como “Aplicaciones que sirven para almacenar todas nuestras credenciales (usuarios, contraseñas, sitios web a los que corresponden, etc.) en una base de datos cifrada mediante una contraseña maestra”.

Cuadro 10. Autenticidad post-electoral

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
4	¿Ha habilitado la autenticación de dos factores para acceder a sus redes sociales?	39	97,5	1	2,5
5	¿Revisa la identidad del remitente de los correos electrónicos que recibe?	35	87,5	5	12,5
6	¿Tiene cifrada la configuración de sus comunicaciones en línea?	24	60	16	40
7	¿Revisa con regularidad la configuración de privacidad de sus redes sociales?	27	67,5	13	22,5

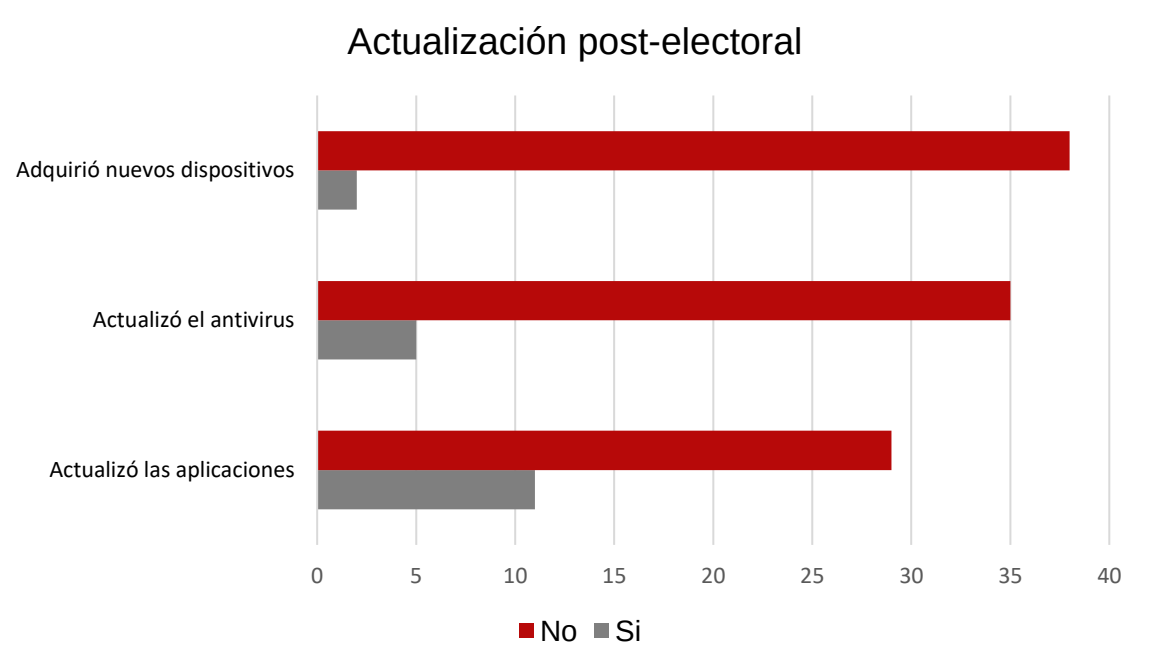


Con el aumento de las amenazas, los discursos de intimidación y los casos de detenciones tras la vigilancia digital ejercida por el Estado venezolano, casi la totalidad de los encuestados (97,5%) habilitó en sus cuentas de redes sociales y correo electrónico la autenticación de dos fatores, lo que indica que se preocuparon por protegerse de ataques a su ciberseguridad.

La verificación en dos pasos (a veces denominada autenticación multifactor) te ayuda a protegerte al dificultar que otra persona inicie sesión en tu cuenta. Usa dos formas diferentes de identidad: su contraseña y un método de contacto (también conocido como información de seguridad).

Cuadro 11. Actualización post-electoral

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
8	¿Realizó la actualización de las aplicaciones de sus redes sociales?	11	27,5	29	72,5
9	¿Actualizó el software de protección contra virus en sus dispositivos?	5	12,5	35	87,5
10	¿Adquirió nuevos dispositivos electrónicos para manejar sus redes sociales?	2	5	38	95

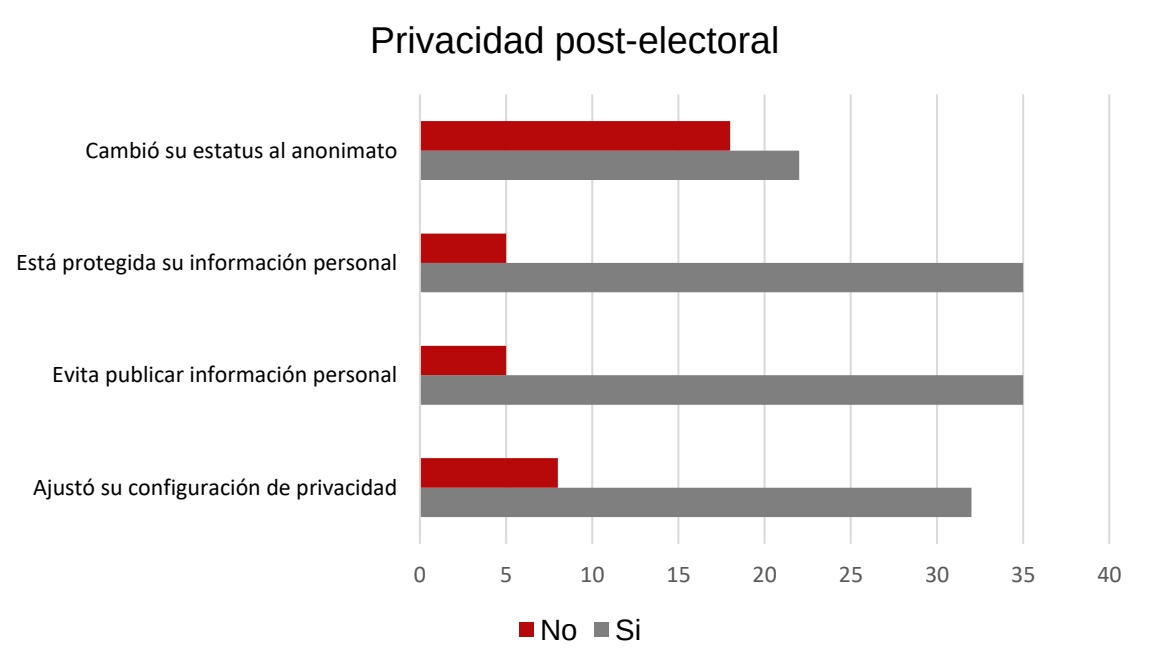


Ya sea se trate de un dispositivo personal o de una computadora de una organización, contar con una protección frente a amenazas es vital, y aun cuando existe una gran variedad de antivirus, cada uno con sus características y fortalezas, existe la necesidad de mantenerlos actualizados para tener acceso a mejoras que pueden ir desde el arreglo de bugs y fallas, hasta la suma de distintas herramientas y nuevas características.

Esto permite que el nivel de protección contra un ataque de tipo malware, sin embargo, la mayoría de los encuestados (87,5%) no lo ha tomado como una medida de ciberseguridad, teniendo en ese aspecto una debilidad en seguridad digital.

Cuadro 12. Privacidad post-electoral

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
11	¿Realizó ajustes a la configuración de privacidad de sus redes sociales?	32	80	8	20
12	¿Evita publicar información personal en sus cuentas?	35	87,5	5	12,5
13	¿Considera que su información personal está debidamente protegida?	35	87,5	5	12,5
14	¿Cambió al anonimato para publicar en las redes sociales?	22	55	18	45

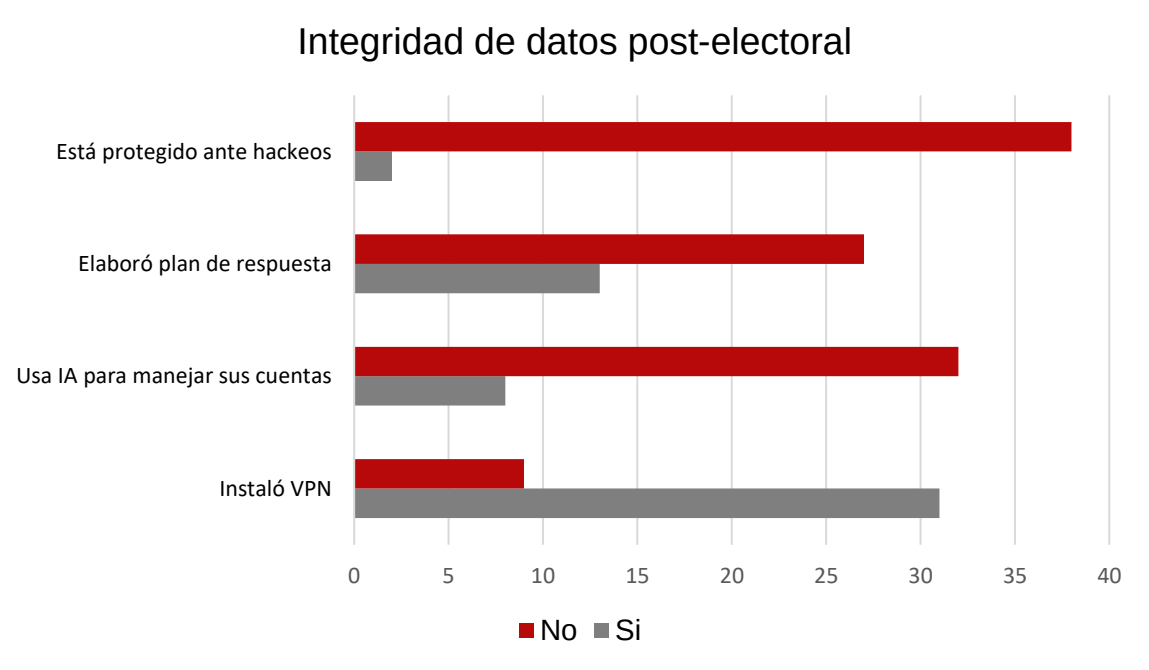


El anonimato en línea es la capacidad de utilizar Internet sin proporcionar ninguna información personal identificable. Esto significa que puedes hacer lo que quieras en Internet sin que nadie sepa quién eres, y en el caso de Venezuela, luego del 28 de julio de 2024, el 55% de los encuestado optó por esta modalidad para poder expresarse libremente sin revelar su identidad, y así evitar ser víctimas de vigilancia, amenazas o ataques directos por parte de actores del Estado.

Asimismo, el 87,5% de los entrevistados considera que realizó los ajustes correspondientes para proteger su información personal, lo que resulta un aspecto positivo para mantener su activismo digital.

Cuadro 13. Integridad de datos post-electoral

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
15	¿Instaló algún VPN para usar sus redes sociales?	31	77,5	9	22,5
16	¿Utiliza inteligencia artificial para manejar sus cuentas de redes sociales?	8	20	32	80
17	¿Elaboró un plan de respuesta ante posibles ataques a la seguridad de sus cuentas de RRSS?	13	32,5	27	67,5
18	¿Considera que sus dispositivos electrónicos están protegidos ante un hackeo?	2	5	38	95



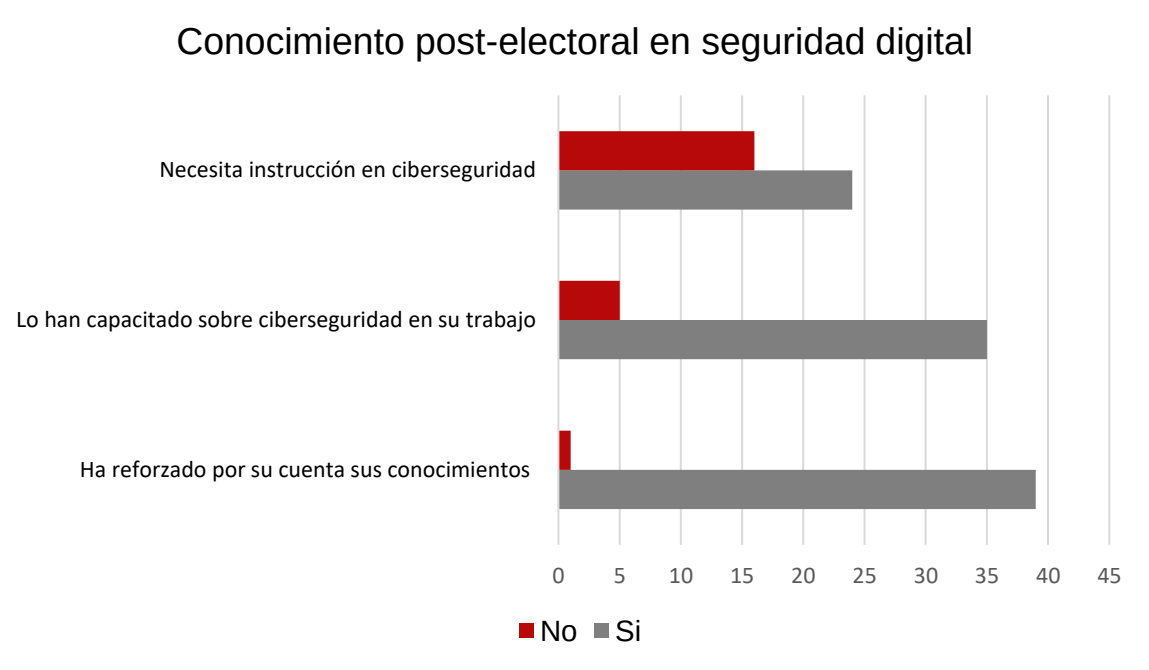
Luego del bloqueo de las redes sociales X, Reddit y TikTok en Venezuela ordenado por Nicolás Maduro, se volvió una necesidad la utilización de una red privada virtual (VPN) para acceder a la información imparcial publicada por medios de comunicación, organizaciones de derechos humanos y líderes políticos de oposición, pero además se le dio la importancia de protección de datos para quienes requerían publicar sin poner en riesgo su información personal.

Es relevante atender la necesidad de protección ante hackeos de cuentas manifestada por el 95% de los encuestados, debido a que esto es una debilidad que

puede ser aprovechada por aquellos que buscan coartar los derechos digitales de las personas, en especial de los defensores de derechos humanos, y además ayudarlos a crear un plan de respuesta ante posibles ataques a la ciberseguridad de sus organizaciones e integrantes, ya que solo el 32,5% expresó que cuenta con una planificación adecuada.

Cuadro 14. Conocimiento post-electoral en seguridad digital

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
19	¿Ha buscado reforzar por su cuenta sus conocimientos en ciberseguridad?	30	75	10	25
20	¿Ha participado en alguna capacitación sobre ciberseguridad organizada por su organización de trabajo?	16	40	24	60
21	¿Considera que necesita instrucción sobre seguridad digital?	22	55	18	45

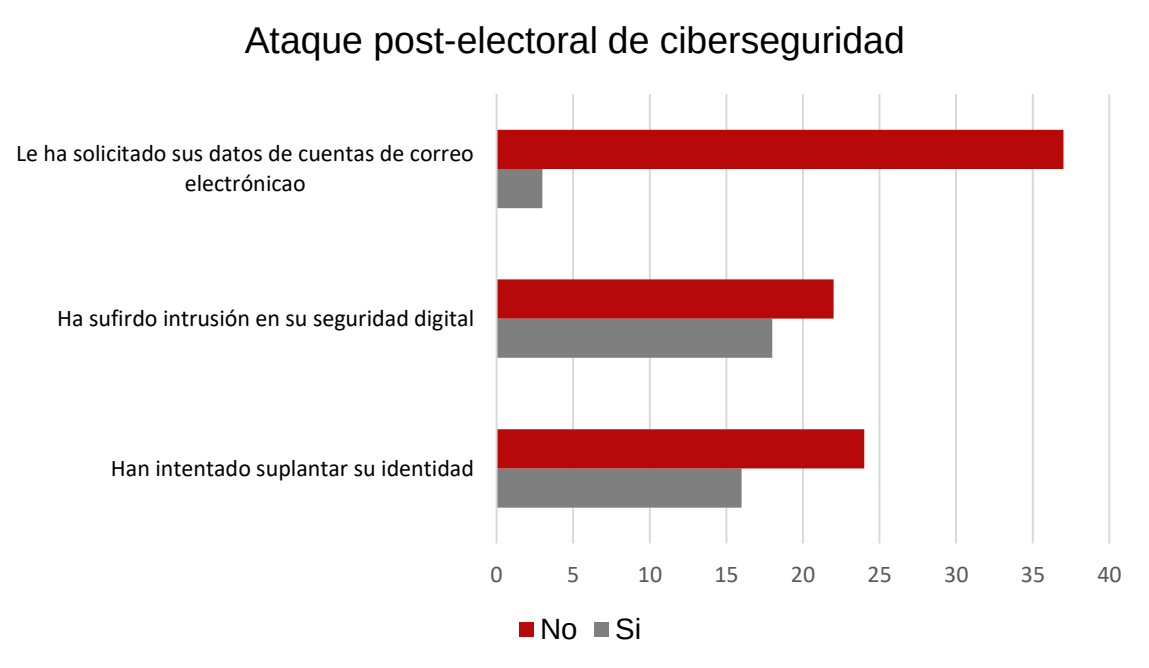


Aún cuando los encuestados han realizados esfuerzos por reforzar sus mecanismos de defensa electrónica, se hace necesario fortalecer los conocimientos en ciberseguridad debido a que luego de las elecciones este aspecto se volvió crucial para garantizar la integridad de las personas y organizaciones, es especial aquellos

dedicados a la defensa de los derechos humanos, debido a que en un 55% de los encuestados manifestó que requiere la instrucción apropiada ante los riesgos de vigilancia, persecución o ataque en el ámbito digital.

Cuadro 15. Ataque post-electoral de ciberseguridad

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
22	¿Le han intentado suplantar su identidad en las redes sociales?	16	40	24	60
23	¿Ha sido víctima de alguna intrusión a sus medidas de seguridad para acceder a sus redes sociales?	18	45	22	55
24	¿Le han solicitado datos personales relacionados con sus cuentas de correo electrónico?	3	7,5	37	92,5

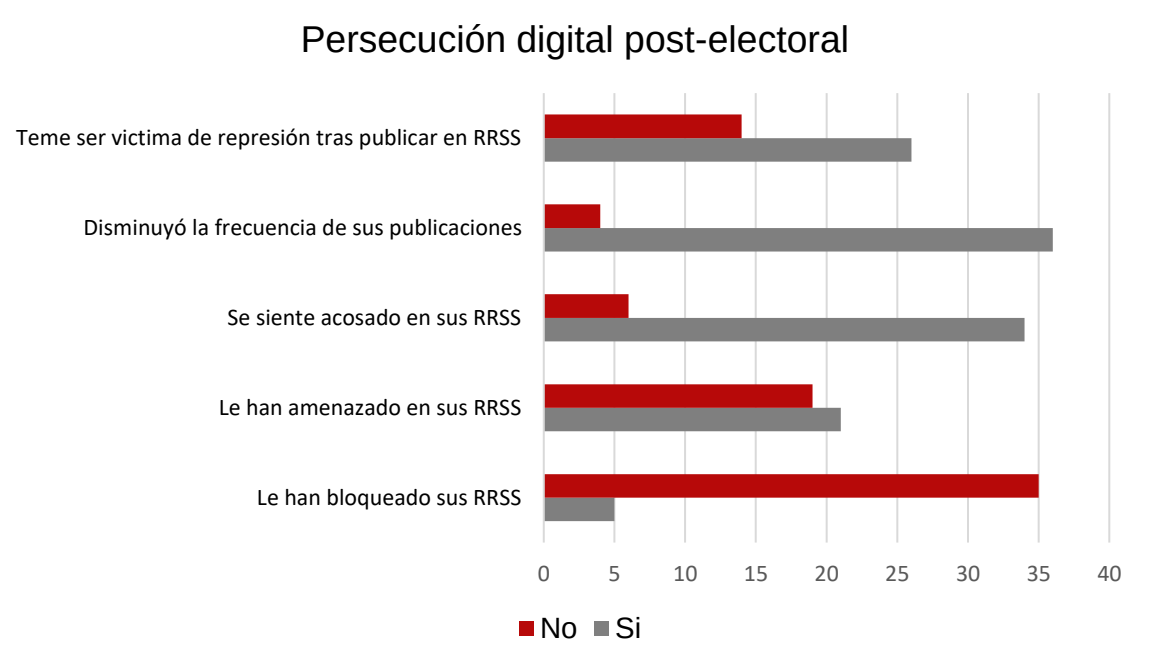


Estas respuestas reflejan un entorno complejo donde el riesgo y la vigilancia son omnipresentes, y la seguridad y la libertad de expresión son consideraciones críticas para la práctica de cada uno de estos grupos posterior al proceso electoral del 28 de julio. Las diferencias en sus respuestas subrayan la necesidad de abordar las

amenazas de manera contextualizada y desarrollar estrategias de protección adecuadas para cada sector.

Cuadro 16. Persecución digital post-electoral

Ítem	Después de las elecciones presidenciales en Venezuela del 28 de julio	Si		No	
		f	%	f	%
25	¿Alguna de sus cuentas en redes sociales ha sido bloqueada?	5	12,5	35	87,5
26	¿Ha sido objeto de amenazas a través de mensajes en redes sociales por ejercer su labor?	21	52,5	19	47,5
27	¿Se siente acosado a través de las redes sociales por publicar contenido sobre derechos humanos?	34	85	6	15
28	¿Disminuyó la frecuencia de sus publicaciones en redes sociales para evitar intimidaciones?	36	90	4	10
29	¿Teme a ser víctima de represión por parte del Estado si publica en las redes sociales?	26	65	14	35



El análisis de estas respuestas puede ofrecer una visión clara sobre el clima de inseguridad y miedo que enfrenta la población en Venezuela, especialmente en el contexto de la represión luego de los comicios presidenciales, debido a que el 90% de los encuestados ha disminuido la cantidad de publicaciones en las redes sociales

como medida de seguridad personal, sin embargo, también significa la pérdida de su capacidad de trabajar libremente sin temor a represalias.

El acoso y la vigilancia son prácticas comunes utilizadas para desincentivar la defensa de los derechos en el país, porque tienen un efecto paralizante en la actividad de quienes se dedican a la promoción y denuncia a través de las redes sociales.

Es de consideración que el 52,5% de los encuestados fue objeto de amenazas, siendo los observadores electorales uno de los grupos más afectados por la ola represiva desatada con la llamada Operación Tun-Tun, donde testigos de mesa fueron perseguidos en algunos casos, tras el seguimiento de las fuerzas de seguridad a través el uso de cuentas de redes sociales personales.

En general, todos los grupos experimentan algún grado de riesgo, pero los periodistas parecen estar en la situación más crítica con una percepción casi unánime de aumento del peligro. Esta percepción de riesgo y experiencias de acoso han afectado la voluntad de los sindicalistas y defensores de DDHH para participar en activismo en línea, además que la amenaza constante puede llevar a una auto-censura y limitar su capacidad de actuar en defensa de sus derechos o los de los demás.

Despido a trabajadores del sector público por el uso de redes posterior al 28 de julio

Tras el 28 de julio, día de las elecciones presidenciales, se evidenció el despido masivo de trabajadores del sector público debido al uso de redes sociales, teniendo que solo en el estado Apure un total de 5.000 trabajadores recibieron citaciones para comparecer ante la Zona Educativa, a cargo de la licenciada Mary Orasma, para notificarles de su despido por supuestas razones ideológicas, ya que expresaron su apoyo a Edmundo González Urrutia en las elecciones.

En dicha entidad llanera, se instruyó a la Secretaría de Gestión Interna del Centro de Desarrollo de la Calidad Educativa para que notificara a los ciudadanos

mencionados en un listado, a los que se les exigió presentarse en la coordinación de Gestión Interna, con el objeto de verificar el estatus laboral de los empleados, quienes debieron comparecer entre el 15 de agosto de 2024 y el 15 de septiembre de 2024, el listado emitido incluía a educadores, personal administrativo y obreros.

Nuevamente, resalta el día 15 de agosto, debido que el Sindicato Nacional de Trabajadores de la Prensa de Venezuela divulgó mediante su cuenta de “X” que los días 1 y 2 de agosto más de 40 empleados del canal de televisión estatal VTV fueron despedidos únicamente por haber dado "like" a publicaciones de María Corina Machado.

Estos despidos son considerados ilegítimos y afectan la estabilidad laboral de los trabajadores. "Rechazamos la represalia del Estado contra quienes piensan de manera diferente y se expresan al respecto. Demandamos que las inspectorías y la Organización Internacional del Trabajo (OIT) intervengan para restaurar los derechos de los afectados", concluye el mensaje.

“Los han botado de VTV y también de RNV. Hay terror en denunciar y algunos testimonios los hemos recogido en medio de llantos y susto. Los han despedido por darle "like" a cualquier publicación de María Corina Machado o por escribir "fraude" es sus estados de WhatsApp”, describe en X la cuenta del Sindicato Nacional de Trabajadores de la Prensa.

Además de estos casos, se han documentado casos de trabajadores que han sido forzados a presentar su renuncia. Mediante despidos masivos, amenazas y directrices que obligan a eliminar la aplicación WhatsApp de los teléfonos celulares, el gobierno nacional ha implementado medidas de represalia contra cientos de trabajadores del Instituto Nacional de Aviación Civil (INAC) y de las aerolíneas Conviasa y Aeropostal, quienes no apoyaron al mandatario Nicolás Maduro en las elecciones presidenciales.

En Conviasa, los despidos superaron los 190, mientras que en el INAC más de 100 empleados han sido despedidos. Hasta el momento, Aeropostal ha registrado cinco

despidos. Es importante señalar que estas acciones no solo afectan a obreros y empleados, sino que también impactan al personal administrativo, gerencial, pilotos y azafatas, quienes han sido identificados por expresar su rechazo al fraude electoral ocurrido el 28 de julio.

El gerente general de Seguridad Aeronáutica es el responsable de elaborar la "lista negra" en el INAC, y les ordenó que, a partir del 29 de julio, los empleados tienen la obligación de publicar fotos en sus teléfonos móviles o en redes sociales manifestando su apoyo a Maduro. Aquellos que se negaron a cumplir con dicha orden recibieron graves amenazas por parte de sus superiores, incluyendo el mencionado gerente de Seguridad Aeronáutica. Además de la coerción para que el personal trabajara durante los días en que la "oposición" convocaba concentraciones, también se están forzando a los empleados a eliminar la aplicación WhatsApp y, en su lugar, instalar la aplicación Wechat.

Patrones de persecución asociados con el ejercicio de derechos digitales

Despidos: A través de los 25 años que han estado en el poder, el chavismo la coacción a los empleados públicos como mecanismo de control social ha estado presente, fundamentalmente desde el año 2004 con el nacimiento de la lista estás con hasta los tiempos modernos.

Previo a los comicios presidenciales hubo amenazas y acciones para evitar que los trabajadores del sector público expresaran públicamente su simpatía hacia los candidatos de oposición. Sin embargo, esta acción de terminación arbitraria de la relación de trabajo entre el particular y el Estado que se ha visto a través del tiempo, en esta oportunidad se pudo observar en instituciones públicas y empresas estatales. Nuevamente la estatal petrolera petróleo de Venezuela en los días posteriores al 28 de julio ejerció esta práctica contra aquellos trabajadores que por publicar estados y opiniones en redes sociales como Instagram WhatsApp Facebook e incluso en “X”, resultaron despedidos de sus puestos de trabajo en estados como Falcón, pero también en Anzoátegui y Monagas.

Hostigamiento y amenazas: Siendo esta una práctica también conectada dentro de los patrones de violación de derechos laborales, se observa en esta oportunidad la misma retaliación por publicar en redes sociales contra trabajadores del sector público, aunque la medida que tomó el ejecutivo se tradujo en distintas prácticas la mayoría giro en función de mensajes de posibles traslados inconsultos o despidos, maltrato verbal en los sitios de trabajo, órdenes de borrar redes sociales de los trabajadores y hasta amenazas de llamado a las fuerzas de seguridad.

Traslados inconsultos: Se tiene reporte que en el estado Apure algunos trabajadores del sector educación fueron trasladados a distintas zonas diferentes a donde ya venían laborando, sin la previa solicitud del empleado como lo establece la ley.

Prohibición de ingreso al sitio de trabajo: Tanto en el estado Apure como en otros de las regiones del llano venezolano, hay reportes de trabajadores que posteriores 28 de Julio por sus opiniones en redes sociales no fueron notificados de despidos en su contra, pero tampoco se les permitía ingresar a su sitio de trabajo.

Hackeo de cuentas de redes sociales: Durante la segunda semana de septiembre, se reportaron varios hackeos e intentos de piratería mediante enlaces sospechosos o phishing, dirigidos a cuentas de periodistas y ciudadanos venezolanos. Uno de los perjudicados fue Andrés Rojas Jiménez, conductor de Unión Radio y editor del portal Petroguía. En la mañana del 14 de septiembre, recibió un mensaje de un usuario supuestamente identificado como Meta, el actual nombre de la empresa matriz de Facebook e Instagram. El mensaje advertía engañosamente sobre una posible inactivación de cuentas en Instagram por supuestas violaciones de las normas de la red social, como compartir contenido protegido por derechos de autor o mensajes spam. Luego, se indicaba que los usuarios debían completar un formulario de apelación, a través del cual los hackers podían obtener acceso a sus datos.

Violencia institucional hacia las mujeres que ejercen derechos digitales

El 12 de septiembre, la cuenta de X de la actriz venezolana Prakriti Maduro fue hackeada. Esta actriz, quien ha estado denunciando los patrones represivos que el régimen ha impuesto sobre la población desde las elecciones, reveló que en los días anteriores había sido víctima de un ataque a su cuenta personal en la misma plataforma. Esto ocurrió después de que publicara testimonios que le habían llegado a través de su mensajería privada sobre detenciones arbitrarias en el contexto de las protestas tras las elecciones. En una publicación en X, afirmó: "La dictadura logró hackear mi cuenta con el objetivo de continuar silenciando a los venezolanos. Para tranquilidad de todos, los testimonios que recibo por redes sociales los capturo y los elimino de inmediato. Por lo tanto, aunque me hackeen, no lograrán encontrar rastros de mis informantes".

Utilizando la herramienta online Brand 24, se hizo análisis sobre la estigmatización de dos figuras muy activas en redes sociales y personalidades de gran popularidad en Venezuela como lo es la líder política María Corina Machado y la defensora de Derechos Humanos Rocío San Miguel.

El informe generado para la etiqueta #CarcelParaLaSayona que desde las cuentas del gobierno nacional propiciaron contra la líder política María Corina Machado, se estableció entre 19 de julio y el 19 de septiembre de 2024 en un espacio de 92 días.

Se tiene que el volumen de impresiones superó las 28, asimismo el alcance en redes sociales de esta etiqueta llegó a estar por encima de los 375.000, el alcance fuera de las redes sociales fue de 4.434, la cantidad de interacciones fue de 38.789, y la cifra de “me gusta” fue de 19.355; cabe resaltar que a esta actividad se le invirtió el monto de 25.634 dólares para llegar a esa cantidad de personas.

Del mismo modo ocurrió con el caso de la defensora de derechos humanos Rocío San Miguel, en un análisis realizado por el observatorio venezolano de Cazadores de Fake News, al momento de su arresto el 9 de febrero del 2024 en el Aeropuerto Internacional Simón Bolívar de Maiquetía, siendo revictimizada por el Estado

venezolano con una campaña de descrédito por parte de cuentas trolls afines al oficialismo. Desde la plataforma cazamos Fake News explico en un hilo de Twitter el 11/02/24, explican que la cuenta #AsiSeDifamaEnVenezuela Rocío San Miguel @rociosanmiguel fue víctima de la campaña de estigmatización #*RocíoNoEsSanta, lo que se traduce en que no se trata de solo una etiqueta aislada; forma parte de una operación de información gubernamental. Esta táctica de descalificación no es nueva, sino parte de un patrón más amplio que busca desacreditar a aquellos que critican o se oponen a la administración actual.

La campaña en su contra buscaba vincularla con supuestos planes de magnicidio, acusaciones que fueron propiciadas por Tarek William Saab y que jugaron un papel crucial en la difusión de mensajes en redes sociales. Frases como "trama conspirativa" (con 52 menciones), "trama brazalete" (con 37 menciones) e "intento de magnicidio" (con 22 menciones) fueron utilizadas para referirse a Rocío San Miguel, centrando la búsqueda en estas palabras clave mencionadas.

Disposiciones legales violentadas

El Estado venezolano, al ejercer prácticas de bloqueo a portales informativos y redes sociales, está violando varios pactos y tratados internacionales en materia de derechos humanos y derechos digitales, suscritos y ratificados por la República Bolivariana de Venezuela.

Estos bloqueos digitales dificultan la capacidad de las personas para comunicarse de manera efectiva y acceder a información crítica, lo cual es vital en cualquier democracia funcional. Asimismo, afectan la capacidad de las organizaciones de la sociedad civil para operar, monitorear violaciones de derechos humanos y educar a la población.

A continuación, se mencionan algunos de los principales instrumentos internacionales que Venezuela vulnera al ejecutar bloqueos:

1. Pacto Internacional de Derechos Civiles y Políticos (PIDCP)

Artículo 19: Establece el derecho a la libertad de expresión, que incluye la libertad de buscar, recibir y difundir información e ideas de todo tipo. Los bloqueos a portales informativos o redes sociales restringen este derecho fundamental y el derecho a la información.

2. Convención Americana sobre Derechos Humanos

Artículo 13: Reconoce el derecho a la libertad de pensamiento y de expresión. Esto incluye la obligación del Estado de garantizar el acceso a la información y la prohibición de la censura.

3. Declaración Universal de Derechos Humanos

Artículo 19: Similar al PIDCP, establece que toda persona tiene derecho a la libertad de opinión y de expresión, así como a buscar, recibir y difundir información e ideas por cualquier medio.

4. Principios de Naciones Unidas sobre la Aplicación de los Derechos Humanos en la Internet: Estos principios establecen que los derechos humanos deben ser protegidos y promovidos en el entorno digital, lo que incluye la prohibición de la censura y la garantía del acceso a la información.

5. Convención sobre los Derechos del Niño: Si bien se centra en los derechos de los menores, esta convención también subraya la importancia del acceso a la información y la libre expresión, que se verían comprometidos por los bloqueos a los medios digitales.

Las prácticas de censura y bloqueos en Venezuela no solo contravienen normas nacionales, sino que también desafían estándares internacionales ampliamente aceptados en relación con la libertad de expresión y el acceso a la información. Esto pone de relieve la necesidad de mayor vigilancia y presión internacional para garantizar el respeto a los derechos digitales.

6. Constitución de la República Bolivariana de Venezuela: Promulgada en 1999, establece diversos derechos fundamentales que el Estado debe garantizar a todas las personas, pero al ejercer prácticas de censura a los medios digitales, el Estado venezolano está violando varios aspectos y artículos de esta Constitución.

Artículo 49 - Derecho a la Defensa: Aunque se refiere principalmente a derechos en procesos judiciales, la censura puede afectar el derecho a la defensa y la posibilidad de recibir información veraz y oportuna.

Artículo 57 - Derecho a la Libertad de Expresión: Este artículo establece que toda persona tiene derecho a expresar libremente sus pensamientos, ideas y opiniones. También garantiza el derecho a buscar, recibir y difundir informaciones e ideas de todo tipo, lo que se ve directamente afectado por la censura de medios digitales.

Artículo 58 - Derecho a la Información: Este artículo garantiza el derecho de toda persona a recibir información veraz y oportuna. La censura de portales informativos y redes sociales impide que la población tenga acceso a información necesaria para una toma de decisiones informada.

Artículo 59 - Prohibición de Censura: Establece expresamente que no se puede imponer censura a los medios de comunicación. Esto implica que cualquier intento de bloquear páginas web o restringir el acceso a redes sociales puede ser considerado una forma de censura prohibida.

Artículo 70 - Protección a la Libertad de Comunicación: Este artículo protege la comunicación e información como derechos fundamentales del pueblo. Limitar el acceso a medios digitales y redes sociales tiene un impacto directo sobre este derecho.

Artículo 108 - Derecho a la Libertad de Pensamiento y Expresión: Reitera que se garantiza la libertad de pensamiento y expresión en cualquier forma de comunicación, siendo esto esencial para el ejercicio del derecho a la libertad de expresión y el acceso a la información.

Artículo 126 - Papel del Estado en la Comunicación: Este artículo establece que el Estado debe promover y garantizar el derecho a la comunicación y la información. Las prácticas de censura van en contra de esta obligación del Estado.

Artículo 337- De los Estados de Excepción: El Presidente o Presidenta de la República, en Consejo de Ministros, podrá decretar los estados de excepción. Se califican expresamente como tales las circunstancias de orden social, económico, político, natural o ecológico, que afecten gravemente la seguridad de la Nación, de las instituciones y de los ciudadanos y ciudadanas, a cuyo respecto resultan insuficientes las facultades de las cuales se disponen para hacer frente a tales hechos. En tal caso, podrán ser restringidas temporalmente las garantías consagradas en esta Constitución, salvo las referidas a los derechos a la vida, prohibición de incomunicación o tortura, el derecho al debido proceso, el derecho a la información y los demás derechos humanos intangibles.

Recordemos que tanto la Constitución de la República Bolivariana de Venezuela como la Ley Orgánica sobre Estados de Excepción (artículo 7 numeral 14), establecen que el derecho a la información no puede ser restringido.

La censura en Venezuela no solo afecta los derechos individuales, sino que también tiene un impacto en los derechos colectivos de la sociedad iberoamericana ya que genera un mal precedente, visto los abusos y restricciones impuestos por otros países del mundo y de la región, adaptados con sus propias estrategias.

Además, la vigilancia y la restricción de los medios digitales se produce en medio de un clima de miedo generalizado, donde el venezolano se inhibe de ejercer la libertad de expresión y la participación ciudadana o por lo menos es lo que el Estado intenta imponer.

Conclusiones

El análisis de la situación de los derechos digitales en Venezuela en el año 2024 revela una realidad alarmante que refleja la complejidad del entorno sociopolítico del país. Las conclusiones de este informe se centran en varios hallazgos clave que

no solo documentan el estado actual de los derechos digitales, sino que también enfatizan la necesidad urgente de abordar y mitigar las problemáticas observadas.

Se evidenció que la libertad de expresión en el ámbito digital se enfrenta a desafíos significativos, la censura de los medios de comunicación y la represión de las voces críticas han llevado a una atmósfera de miedo e incertidumbre entre los ciudadanos. Muchas personas han optado por la autocensura, evitando expresar sus opiniones y participar en debates públicos por temor a represalias, teniendo que el 55% de los encuestados (22 personas) cambiaron su estatus en línea al anonimato y el 90% de estos disminuyó la cantidad de sus publicaciones tras las elecciones presidenciales.

La protección de los datos personales ha sido otro de los ejes analizados en la investigación, debido a que la falta de legislación clara en materia de privacidad y la implementación de prácticas de vigilancia masiva han expuesto a los ciudadanos a riesgos constantes. Muchos venezolanos desconocen cómo se recopila, utiliza y almacena su información en línea, lo que los deja vulnerables al abuso de sus datos por parte de actores estatales y no estatales.

Esta situación exige un debate urgente sobre la necesidad de establecer marcos legales que regulen adecuadamente la protección de datos y que garanticen los derechos de los ciudadanos en el entorno digital. Al respecto, llama la atención que el cifrado de las comunicaciones de los encuestados pasó de un 47,5% previo a las elecciones del 28 de julio a un 60% luego de los comicios, en un intento personal de incrementar su ciberseguridad.

Un aspecto preocupante que ha emergido con fuerza en esta investigación es la violencia institucional digitalizada, un fenómeno que se manifiesta a través de herramientas tecnológicas utilizadas por el Estado para ejercer control y represión. Esta forma de violencia se traduce en mecanismos de monitoreo y seguimiento de las actividades digitales de los ciudadanos, creando un ambiente de vigilancia constante que inhibe la libertad de reunión y de asociación. Al respecto, después del 28 de julio, el 65% de los encuestados manifestó que teme ser objeto de algún

tipo de represalia por parte del ejecutivo nacional vinculado a su actividad en las redes sociales como parte de su función como defensor de derechos humanos.

Además, las amenazas a la seguridad digital, como los ataques cibernéticos a opositores y organizaciones de la sociedad civil, reflejan una estrategia sistemática del Estado para silenciar toda crítica. La coexistencia de herramientas tecnológicas sofisticadas junto a la falta de una infraestructura adecuada para proteger a los ciudadanos ha contribuido a un entorno en el que la violencia digital se convierte en un mecanismo de control y represión.

El informe también resalta la necesidad de fomentar la alfabetización digital entre la población, a fin de fortalecer las capacidades de los ciudadanos para navegar por el entorno digital de manera segura y efectiva es crucial para empoderarlos en la defensa de sus derechos. En referencia a este aspecto, el 100% de los entrevistados expresó su deseo de fortalecer sus conocimientos en ciberseguridad, ya sea a través de programas de capacitación o recursos educativos, que sirvan para enseñarles a utilizar las herramientas digitales como instrumentos de defensa y promoción de sus libertades.

Además, es imperativo que la comunidad internacional preste atención a la situación de los derechos digitales en Venezuela, por ello la cooperación entre países y organizaciones no gubernamentales es esencial para crear redes de apoyo que puedan ayudar a los ciudadanos a enfrentar los desafíos que plantean la censura y la violencia institucional digitalizada.

En conclusión, los resultados sobre el monitoreo de derechos digitales en Venezuela en 2024 es un llamado a la acción, que evidencia la urgente necesidad de abordar la violencia institucional digitalizada y sus implicaciones. Es fundamental adoptar un enfoque integral que promueva los derechos digitales como parte esencial de la lucha por la democracia y el respeto a los derechos humanos en el país, así como fomentar un diálogo constructivo y colaborativo que involucre a todos los actores de la sociedad.

Recomendaciones

Este ambiente ha creado una sociedad donde la comunicación y el intercambio de ideas son severamente restringidos, afectando no solo la dinámica democrática, sino también la capacidad de la población para informarse y organizarse en torno a causas comunes, por ello se hacen las siguientes recomendaciones a la Comunidad Internacional:

- Establecer mecanismos de monitoreo y documentación de los casos de violencia institucional digitalizada en Venezuela, asegurando que las violaciones a los derechos humanos sean registradas y denunciadas.
- Proporcionar asistencia legal a las víctimas de violaciones de derechos digitales, apoyando a organizaciones locales que trabajan en la defensa de los derechos humanos y protegiendo a los activistas.
- Utilizar canales diplomáticos para instar al Estado venezolano a que cese las prácticas de vigilancia y represión digital, promoviendo la libertad de expresión y el respeto por los derechos digitales.
- Apoyar financieramente proyectos que fomenten la alfabetización digital y la educación sobre derechos digitales en Venezuela, facilitando recursos para capacitar a la ciudadanía.
- Crear coaliciones internacionales de organizaciones de derechos humanos que trabajen conjuntamente para abordar la violencia institucional digitalizada en diferentes contextos, incluida Venezuela.

Las plataformas digitales se han convertido en espacios de riesgo, donde la disidencia es perseguida y donde los ciudadanos temen ser objeto de represalias, como detenciones arbitrarias o acosos, es por ello que se exhorta al Estado Venezolano a:

- Reformar y derogar leyes como la Ley contra el Odio, en aras de establecer un marco legal sólido que proteja los derechos digitales de los ciudadanos, incorporando medidas específicas contra la violencia institucional y el abuso de poder en el entorno digital.

- Promover la transparencia en la gestión de datos personales y establecer políticas de privacidad claras que respeten los derechos de los ciudadanos, evitando el uso indebido de la información.
- Implementar programas de capacitación para funcionarios del gobierno sobre derechos digitales y requisitos éticos relacionados con la privacidad y la protección de datos.
- El cese inmediato del acoso a través de las plataformas digitales hacia organizaciones de la sociedad civil políticas y de diferentes índoles que no están alineadas con el partido y gobierno de modo que la violencia en redes sociales se traduzca en violencia física hacia la disidencia política.

Las recomendaciones formuladas en este informe buscan orientar a los responsables de formular políticas, así como a las organizaciones de derechos humanos, hacia acciones que fortalezcan la protección de los derechos digitales en el país, pero también se impulsa a la ciudadanía a:

- Promover talleres y campañas de concientización sobre seguridad digital, enseñando a los ciudadanos herramientas y prácticas para proteger su información personal y evitar la manipulación en línea.
- Informar a la población sobre los riesgos de la autocensura, alentando a los ciudadanos a expresar libremente sus opiniones y compartir información, a la vez que los empodera para hacerlo de forma segura.
- Establecer redes de apoyo entre ciudadanos y activistas que compartan información y estrategias sobre cómo enfrentar la violencia institucional digitalizada, fortaleciendo la solidaridad y la colaboración en la defensa de los derechos.

Referencias bibliográficas

Argos Hub LLC. (2020). *¿Qué es Ciberseguridad? Objetivos, elementos e impacto en 2020*. Texas, EEUU. Artículo en línea. Disponible en: https://www.argoshub.com/que-es-ciberseguridad/

Asamblea Nacional de Venezuela. (2009). Constitución de la República Bolivariana de Venezuela. Disponible en: https://www.cgr.gob.ve/assets/pdf/leyes/Constitucion.pdf

Asamblea Nacional de Venezuela. (2018). Ley Orgánica de Seguridad de la Nación. Disponible en: https://www.observatoriodeconflictos.org.ve/oc/wp-content/uploads/2018/09/Ley-Organica-de-Seguridad-de-la-NAci%C3%B2n.pdf

Asamblea Nacional de Venezuela. (2019). Anteproyecto de Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela. Disponible en: https://www.accessnow.org/wp-content/uploads/2019/01/ley-del-ciberespacio-venezuela.pdf

Asamblea Nacional de Venezuela. (2020). Ley Orgánica de Telecomunicaciones. Disponible en: https://www.oas.org/juridico/spanish/cyb_ven_ley_telecomunicaciones.pdf

Asamblea Nacional de Venezuela. (2024). Ley contra el Fascismo, Neofascismo y Expresiones Similares. Disponible en: https://www.observatoriodeconflictos.org.ve/oc/wp-content/uploads/2024/05/Ley-antifascismo-Venezuela.pdf

Asamblea Nacional de Venezuela. Ley Contra El Odio la Intolerancia y por la Convivencia Pacífica. Disponible en: https://espaciopublico.ong/wp-content/uploads/2017/10/Borrador-Ley-contra-el-odio-la-intolerancia-y-por-la-convivencia-pac%C3%ADfica.pdf

Asamblea Nacional de Venezuela. Ley de responsabilidad social en radio, televisión y medios electrónicos. Disponible en: http://mippci.gob.ve/wp-content/uploads/2023/03/1-Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf

Cyberzaintza. (s/f). *Integridad*. Gobierno Vasco. Artículo en línea. Disponible en: https://www.ciberseguridad.eus/ciberglosario/integridad#:~:text=En%20ciberseguridad%2C%20la%20integridad%20hace,datos%20en%20tr%C3%A1nsito%20o%20reposo.

Gobierno Bolivariano de Venezuela. (2024). Decreto N° 4.975, mediante el cual se crea el Consejo Nacional de Ciberseguridad. Disponible en: https://pandectasdigital.blogspot.com/2024/08/decreto-n-4975-mediante-el-cual-se-crea.html

IBM (s/f). *¿Qué es un ataque cibernético?.* México. Artículo en línea. Disponible en: https://www.ibm.com/mx-es/topics/cyber-attack#:~:text=el%20siguiente%20paso-,%C2%BFQu%C3%A9%20es%20un%20ataque%20cibern%C3%A9tico%3F,sistema%20inform%C3%A1tico%20o%20dispositivo%20digital.

Instituto Nacional de Ciberseguridad. (s/f). *La importancia de las actualizaciones de seguridad*. España. Artículo en línea. Disponible en: https://www.incibe.es/ciudadania/tematicas/configuraciones-dispositivos/actualizaciones-de-seguridad

Organización de Estados Americanos. (1978). Convención Americana sobre Derechos Humanos. Disponible en: https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Organización de las Naciones Unidas (ONU). (1976). Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Disponible en:

https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr_SP.pdf

Organización de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos. Disponible en: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/spn.pdf

Organización de las Naciones Unidas. (2006). Convención sobre los Derechos del Niño. Disponible en: https://www.un.org/es/events/childrenday/pdf/derechos.pdf

Organización de las Naciones Unidas. Principios de Naciones Unidas sobre la Aplicación de los Derechos Humanos en la Internet. Disponible en: https://www.un.org/sites/un2.un.org/files/principios_globales_onu_integridad_informacion.pdf

Serra, J. (2023). *¿Por qué es tan importante la actualización de antivirus? Te enseñamos cómo hacerla*. Artículo en línea para Ciberseguridadtips. Disponible en: https://ciberseguridadtips.com/actualizacion-de-antivirus/

WeLiveSecurity. (2022). *Autenticación en dos pasos: qué es y por qué es clave para evitar el robo de cuentas*. ESET Latinoamérica. Artículo en línea. Disponible en: https://www.welivesecurity.com/la-es/2022/12/22/doble-factor-autenticacion-que-es-porque-lo-necesito/

Zendesk. (2024). *¿Qué es la ciberseguridad y cuál es su relación con la IA?.* Artículo en línea. Disponible en: https://www.zendesk.com.mx/blog/ciberseguridad/