Manual para desbloquear la censura digital

caja de herramientas para comprender e investigar los bloqueos en internet

Esta guía para periodistas y defensores de derechos digitales recoge conocimientos técnicos, periodísticos y de derechos humanos con la intención de acortar la curva de aprendizaje para rastrear y comprender la censura en internet.

Es una caja de herramientas que contiene datos e insumos experimentales que permiten analizar y seguirle el pulso al control del flujo de contenidos digitales y su impacto en el espacio cívico.

Este manual se sustenta en experiencias previas de investigación y periodismo de datos que permiten proporcionar un marco de referencia e insumos pedagógicos que sirven de orientación para monitorear, investigar y encontrar historias sobre los bloqueos en internet y otras restricciones a libertades en el entorno digital.

La hoja de ruta

El autoritarismo, cada vez más, toma fuerza en el entorno digital. Su objetivo es controlar ese flujo de contenidos que le permite a los ciudadanos armar el rompecabezas sobre la realidad local y global, como un proceso natural y espontáneo para la toma de decisiones libres, informadas con base en evidencias.

El control de contenidos en línea representa uno de estos mecanismos de cómo opera la censura en internet como estrategia del autoritarismo. Por eso vemos que el mundo se enfrenta a viejas prácticas de censura con nuevas tecnologías y con un mayor alcance, que hacen que las órdenes de silencio sean más sigilosas y menos visibles, pero con mayor alcance e impacto para los ciudadanos. Estas actuaciones no solo ocurren en países con regímenes que controlan las libertades sino también en algunos que practican la democracia.

Estos nuevos riesgos de control de contenido plantean grandes desafíos para el periodismo y la defensa de los derechos digitales. En un esfuerzo de comprender y sistematizar las experiencias previas y los conocimientos disponibles, hemos trabajado en este ***Manual para desbloquear la censura digital: caja de herramientas para comprender e investigar los bloqueos en internet***.

Para componer esta guía nos trazamos varios propósitos. La primera finalidad que nos convoca es proporcionar un marco de referencia que aporte conocimientos sobre el manejo básico de los principios de internet incluyente y derechos humanos y su relación con las estrategias de la censura digital. Por eso, nuestra tarea fue sistematizar conocimientos, metodologías y experiencias globales sobre los mecanismos y modalidades en los que operan los bloques digitales como una nueva estrategia de control del flujo de contenidos.

El segundo objetivo que nos ha movilizado ha sido la necesidad de encontrar hallazgos preliminares que logren identificar el comportamiento de la censura digital en Cuba. Para ello, nos basamos en la metodología y las fuentes de datos que ofrece el Open Observatory of Network Interference (OONI). En esta fase, la labor fue enriquecedora porque nos permitió construir, de forma experimental, una arquitectura de una base de datos que nos condujo a organizar unos primeros hallazgos que, sin duda, servirán de insumo o punto de partida para futuros proyectos. Aportamos, también, la visión de los periodistas locales que, en una encuesta exploratoria, nos permitieron levantar un diagnóstico sobre la navegación y el control de contenidos en su país.

En un tercer nivel propusimos mapear las fuentes globales de información y de datos existentes sobre los bloqueos digitales. Esta fase nos permitió organizar la información disponible que sustenta la labor de la comunidad global que le sigue el rastro a la censura digital. Esta experiencia fue útil para armar un glosario con la intención de ayudar a ser más precisos con el lenguaje que empleamos al hablar de los bloqueos digitales. De igual manera, esto nos permitió hacer un barrido de información sobre los aportes que han hecho diversas organizaciones para documentar los bloqueos digitales en Cuba.

En una cuarta fase, emprendimos un breve arqueo documental, de modo instruccional, sobre las técnicas y herramientas para la circunvención o sorteo de la censura en internet.

Con nuestras finalidades desglosamos las 10 secciones que componen este manual y que presentamos a continuación:

1 l Estándares para una internet sin bloqueos
2 l Operatividad de los bloqueos
3 l Fuentes de información, datos e iniciativas globales

1 l Estándares para una internet sin bloqueos

En tiempos de la sociedad-red, como lo ha llamado el sociólogo Manuel Castells, Internet se ha convertido como la nueva plaza pública, en ella transcurre una parte significativa de la vida social. La migración de las comunicaciones al entorno digital digital y la interconexión global ciudadana ha tenido como ideal la construcción de un espacio de intercambio basado en los principios democráticos.

La vida en Internet supone unas libertades digitales que, incluso, han estado bajo amenaza a escala global, según lo han demostrado diversos estudios internacionales. Algunos de estos riesgos han sido las obstrucciones en la circulación de información y el acceso a contenidos en Internet como una forma de control social. Estos hechos se expresan a través de bloqueos o episodios de filtrado de contenidos que configuran una forma de censura digital.

La Comisión Interamericana de Derechos Humanos (CIDH)[1] refiere que las interferencias y bloqueos en Internet pueden ser una forma arbitraria de ejercer el control de la red, principalmente, por parte de los Estados. Este organismo considera que "la interrupción del acceso a Internet" o a los contenidos que en ella circulan "aplicada a poblaciones enteras o a segmentos de la población nunca está justificada, ni siquiera por razones de seguridad nacional". Afirma que los bloqueos de contenidos "temporales o parciales afectan el ejercicio de los derechos humanos en línea". Para evitar estas prácticas de censura digital, la CIDH refiere que "el Estado tiene la obligación de adoptar medidas tendientes a asegurar que las empresas y organismos privados involucrados en la gestión y administración" de contenidos en Internet "no pongan barreras desproporcionadas" que obstáculicen la máxima posibilidad de buscar, recibir y difundir información en Internet.

En una declaración conjunta emitida en 2017, las relatorías de libertad de expresión de la CIDH y la ONU[2], mostraron su preocupación por las crecientes "maniobras de algunos gobiernos para intentar suprimir el disenso y controlar las comunicaciones públicas a través de medidas como normas represivas", entre las que consideraron los "controles técnicos a las tecnologías digitales como bloqueos, filtros, congestionamiento y cierre de espacios digitales".

Frente a las medidas de control de contenidos alertaron que "los sistemas de filtrado de contenidos impuestos por un gobierno que no sean controlados por el usuario final" representan una violación injustificada a la libertad de expresión. Explicaron que "el bloqueo de sitios web enteros, direcciones IP, puertos o protocolos de red dispuesto por el Estado es una medida extrema que solo podrá estar justificada cuando se estipule por ley y resulte necesaria para proteger un derecho humano u otro interés público legítimo, lo que incluye que sea proporcionada, no haya medidas alternativas menos invasivas que podrían preservar ese interés y que respete garantías mínimas de debido proceso".

Estas medidas atentan contra la libertad en Internet y de los principios que fundamentan los derechos digitales que, según la CIDH, deberían ser respetados por todos los actores que hacen parte del desenvolvimiento en la red.

En sus estándares, la CIDH y la Unesco refieren que Internet debe regirse por el criterios de derechos humanos y de libertad de expresión. Uno de ellos es la universalidad de Internet, que responde a un modelo integrador al servicio del interés público y orientado hacia la construcción de la sociedad del conocimiento. Por eso, el entorno digital se debe caracterizar por:

- Estar basado en los derechos humanos

---

[1] http://www.oas.org/es/cidh/expresion/docs/publicaciones/Internet_2016_ESP.pdf

[2] http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1056&IID=2

- Libertad
- Apertura
- Accesibilidad
- Multisectorialidad

Criterios de derechos humanos

La CIDH define unos principios para una Internet libre, abierta e incluyente, en la que no se admiten prácticas abusivas de bloqueos o filtrados con contenidos.

Se puede pensar, entonces, que cuando ocurre una medida de censura digital, que no responde a criterios de protección de las garantías ciudadanas, se interfieren los principios que sustentan en la libertad en la red, que están definido, por la CIDH, en los siguientes términos:

Principios	**Definición**
Apertura	***Las medidas de bloques interfieren el principio de apertura de la red.*** Este principio comprende la "necesidad de garantizar la conectividad y el acceso universal, ubicuo, equitativo, verdaderamente asequible y de calidad adecuada, a la infraestructura de Internet y a los servicios de las TIC, en todo el territorio del Estado".
Descentralización	***Los episodios de censura digital atentan contra el principio de descentralización de Internet.*** Este principio establece que los usuarios deben tener la libertad de "utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de Internet no esté condicionada, direccionada o restringida, por medio de bloqueo, filtración, o interferencia".
Neutralidad	***Los bloqueos digitales afectan el principio de neutralidad de Internet.*** Este principio representa una condición diferenciadora de Internet que se refiere a su capacidad de maximizar "la utilidad de las redes, tratando a todos los paquetes de datos en forma igualitaria sin distinción alguna. De ahí que en Internet se describa como una red boba cuya especialización se da en los extremos – el contenido o la aplicación se genera en un extremo, se traslada por la red en distintos paquetes, sin discriminación, y el contenido o la aplicación se rearma en el punto de destino".
Pluralismo y diversidad	***Los bloqueos digitales reducen la pluralidad y la diversidad de contenidos, otro de los principios de la libertad en Internet.*** El pluralismo y la diversidad son dos condiciones esenciales para "asegurar que no se introduzcan en la red cambios que tengan como consecuencia la reducción de voces y contenidos. Por eso, se debe "proteger la naturaleza multidireccional de la red", que se refiere a la libertad de emitir y la libertad de recibir información que tienen todos los ciudadanos. Esto implica la posibilidad de buscar y difundir "informaciones e ideas de toda índole, sin consideración de fronteras, en los términos del artículo 13 de la Convención Americana"

N o discriminación	***La censura digital configura un acto de discriminación.*** El principio de no discriminación comprende la obligación del Estado a "garantizar que todas las personas– especialmente aquellas que pertenecen a grupos vulnerables o que expresan visiones críticas sobre asuntos de interés público– puedan difundir contenidos y opiniones en igualdad de condiciones".
Privacidad	***El control del flujo de contenidos en Internet puede derivar, de manera indirecta, la protección personal y de elección de los usuarios digitales.*** El principio de privacidad se relaciona con la capacidad de elección de los usuarios y con la protección personal, en la "cual nadie puede ser objeto de injerencias arbitrarias o abusivas" durante su navegación en el entorno digital. La obligación del Estado es "crear un ambiente protegido para el ejercicio del derecho a la libertad de expresión, toda vez que la vulneración de la privacidad de las comunicaciones tiene un efecto inhibitorio y afecta el pleno ejercicio del derecho a comunicarse".
Gobernanza de Internet	***La censura digital va en contra de las buenas prácticas para la gobernanza de Internet.*** Es un principio de gobernanza es un eje transversal al funcionamiento de Internet, que debe orientar la responsabilidad del Estado para procurar la cooperación democrática en la gestión de Internet, con la intención de que todos los actores y las partes interesadas puedan ser tomados en cuenta en el diseño de políticas y la regulación de la red, con la fin de evitar el control exclusivo por parte del Estado. Esto quiere decir que los Estados tienen la obligación de trabajar conjuntamente con "el sector privado, el sector técnico, la sociedad civil y el sector académico, y fundamentalmente de los usuarios, para la regulación de Internet. "La multisectorialidad permite avanzar hacia la construcción de reglas comunes que garanticen la globalidad de Internet y mitiguen las violaciones o abusos a este importante recurso".
Fuente: Aportes de las CIDH	

Libertad de recepción

Estos principios que deben regir una Internet abierta, libre e incluyente, también impacta los derechos comunicacionales en su amplio sentido. El filósofo y comunicólogo venezolano, Antonio Pasquali[3], lo planteaba, en sus aportes teóricos, como el ejercicio de comunicar. Desde las plataformas digitales esto implica la igualdad de condiciones, la pluralidad de voces y de contenidos. Pasquali entendía Internet como un entorno para las libertades humanas, un bien universal y de servicio público. El ejercicio de comunicar en Internet no solo tiene que ver con la libertad de emisión, que era por lo que se caracterizaban los medios tradicionales, sino también la libertad de recepción, por eso él hablaba de la democracia de comunicar.

Esta reflexión de Antonio Pasquali permite pensar que la censura digital no solo afecta a la libertad de emisión (inherente a los medios o sitios afectados, sino que también afecta la libertad de recepción (una condición intrínseca a la capacidad de recibir y consultar contenidos por parte de la audiencia)

[3] https://prodavinci.com/Internet-en-la-memoria-y-la-propia-voz-de-antonio-pasquali/

El máximo acceso, condición relativa

Hay que tomar en cuenta que al igual que otros derechos humanos, la libertad en Internet, y la condición de máximo acceso a contenidos no puede ni debe ser absoluta. Por eso, antes de tomar medidas que deriven en bloqueos de contenidos y hechos de censura digital, los Estados y proveedores de Internet deberían aplicar una evaluación antes. Esto debe responder al criterio refiere que la libertad de circulación de contenidos en Internet es una condición relativa. Por eso, sus limitaciones o restricciones deberían aplicarse sólo en situaciones excepcionales y ser el resultado de un análisis basado en el ***test tripartito,*** que se aplica en el ámbito de derechos humanos, bajos las condiciones de legalidad, proporcionalidad y necesidad; y considerando también la responsabilidad ulterior.

La CIDH ofrece unas orientaciones para aplicar el test tripartito en los siguientes términos:

- **Legalidad:** la limitación debe ser "definida en forma precisa y clara a través de una ley formal y material y orientada al logro de objetivos imperiosos autorizados por la Convención Americana.

- **Proporcionalidad:** la limitación debe ajustarse a criterios delimitados" en tiempo, alcance e impacto.

- **Necesidad:** la limitación debe ser "idónea en una sociedad democrática para el logro de los fines imperiosos" para el respecto de los derechos humanos y la democracia.

- **Responsabilidad ulterior:** los posibles usos abusivos de las libertades en Internet "deben ser siempre ordenadas por un juez o autoridad jurisdiccional independiente e imparcial, respetando las garantías del debido proceso. Estas medidas en todos los casos deben ser proporcionales, no deben ser discriminatorias ni producir efectos discriminatorios, ni pueden constituir censura a través de medios indirectos, específicamente prohibidos por el artículo 13.3 de la Convención Americana".

Estos criterios para una Internet libre no solo forman parte de los estándares que deben guiar las buenas prácticas de los Estados, los proveedores de Internet y las plataformas que ofrecen servicio en el entorno digital, también forman parte de la lista de condiciones para monitorear la situación de los derechos humanos y aplicar estrategias de observancia internacional, especialmente por parte de organismos de Naciones Unidas y la OEA.

Criterios de notificación y transparencia

Los estándares de la CIDH[4] establecen una lista de condiciones con respecto a la responsabilidad de los intermediarios o proveedores de Internet, que también se pueden utilizar como una guía para analizar las decisiones públicas que derivan en bloqueos de contenidos digitales que, previamente, se ha dicho que solo debe ser aplicado de modo excepcional y cuando sean imperativo :

1. **Criterios de transparencia**: las medidas de restricción de contenidos deben incluir protocolos de transparencia, referente a las medidas y decisiones tomadas que derivan en censura. Esto debe incluir información pormenorizada sobre su necesidad y justificación.

[4] http://www.oas.org/es/cidh/expresion/docs/publicaciones/Internet_2016_ESP.pdf

2. **Garantías de protección:** se deben establecer garantías suficientes para la protección de la libertad de expresión.
3. **Debido proceso:** se debe garantizar el debido proceso y la presunción de inocencia de los gestores de contenidos y de los usuarios.
4. **Evitar represalia:** no se deben imponer medidas desproporcionadas a los proveedores de Internet o gestores de contenidos que estén involucrado en la difusión de contenidos.
5. **Régimen de notificación:** se debe aplicar un régimen de notificación que establezca el proceso para una notificación detallada, con fundamento jurídico en la que se explique la presunta falla o contenido ilícito que generó la censura.
6. **Régimen de contra-notificación:** se debe aplicar un régimen de contra-notificación, con garantías judiciales, que pueda ser ejercida por el afectado.

Desafíos para la próxima década

En 2019 la CIDH y la OEA, a través de sus relatorías para la libertad de expresión, establecieron un documento sobre los ***Desafíos de la libertad de expresión para la década*** (2020-2030)[5]. En él, incluyeron como prioridad de los Estados eliminar los controles para el flujo de contenido en Internet. Por eso advirtieron que los gobiernos y los diversos actores de los que depende el funcionamiento de Internet, deben "abstenerse de imponer interrupciones o bloqueos en la red de Internet o en la infraestructura de las telecomunicaciones". A su vez, pidieron avanzar el fortalecer la infraestructura digital para que sea "robusta, universal y cuya regulación garantice un espacio libre, accesible y abierto para todas las partes interesadas". Pidieron "proteger la libertad de expresión y el contenido en línea" y "respetar la neutralidad de red.

Las preocupaciones sobre la censura digital no solo han estado en la agenda panorámica de la libertad de expresión. Es un tema prioritario en otros escenarios

Bloqueos web en elecciones	La ONU y OEA, en una declaración conjunta publicada en 2020, incluyeron sus recomendaciones para evitar los bloqueos digitales como un mecanismo que incide en los procesos electorales. Por eso, advirtieron: "no debe haber censura previa de los medios de comunicación, lo que incluye el bloqueo administrativo de sitios web de medios y las interrupciones del servicio de Internet".

[5] http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1146&lID=2

Censura digital en pandemia	● La censura digital en pandemia ha estado en la lista de preocupaciones de Naciones Unidas. En las directrices de diversas agencias de la ONU para guiar la respuesta a la crisis de salud pública derivada por el COVID-19, consideraron “esencial que los gobiernos se abstengan de bloquear el acceso a Internet; en las situaciones en que se ha bloqueado el acceso a Internet, los gobiernos deben, con carácter prioritario, garantizar el acceso inmediato al servicio de Internet más rápido y amplio posible. Especialmente en un momento de emergencia, cuando el acceso a la información es de vital importancia, no se puede justificar la imposición de amplias restricciones al acceso a Internet por motivos de orden público o seguridad nacional”. ● Las oficinas para la libertad de expresión de Naciones Unidas, la Comisión Interamericana de Derechos Humanos y el Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa consideraron que “la reducción de contenidos y la censura, puede dar lugar a la limitación del acceso a información importante para la salud pública y sólo debe realizarse cuando se cumplan las normas de necesidad y proporcionalidad”. ● En la resolución de la CIDH sobre Pandemia y Derechos Humanos en las Américas, recomendaron a los Estados garantizar el acceso a la información, lo cual implica “respetar la prohibición de censura previa y abstenerse de bloquear total o parcialmente sitios de medios de comunicación, plataformas o cuentas particulares en Internet”.

2 I Operatividad de los bloqueos

Los bloqueos en Internet pueden definirse como una forma de censura digital que ocurren en un territorio geográfico determinado. Esto deriva en el filtrado de contenidos que ejecutan terceros, quienes deciden por el usuario y le quitan el control de decidir qué contenidos pueden o no consumir. Generalmente, quien toma la decisión de bloquear los contenidos son el Estado, el ente regulador o el proveedor de Internet. Hay algunas experiencias que indican que, en algunos casos, estos actores actúan de manera articulada para cerrar las puertas de la información y dejar en una posición de indefensión a los usuarios de Internet. La CIDH ha dicho que los sistemas de filtrado de contenidos que no sean controlados por el usuario son una forma de censura previa.

La censura digital también puede resumirse como una restricciones al flujo informativo, porque apunta a la reducción de la pluralidad y a minimizar diversidad de voces que deben ser escuchadas o consultadas en una sociedad.

Los bloqueos, además, suponen obstáculos en la emisión y recepción del proceso de comunicación, lo cual hace que se reduzcan las ventanas o las posibilidades para consultar contenidos y, por ende, afecta la posibilidad de los ciudadanos de tomar decisiones con respecto a asuntos públicos o privados, que impactan desde la dimensión política hasta la familiar.

Los bloqueos afectan la operatividad de diversos portales, la disponibilidad de contenidos y el derecho de los ciudadanos a consultar contenidos e información en las plataformas digitales.

En esta sección revisamos cómo opera la censura digital y cómo se puede identificar.

Tipología de los bloqueos		
	Identificación	**Nivel de censura**
Bloqueo por DNS lookup	- El usuario intenta abrir un dominio bloqueado y no logra conectarse - El servidor destinatario devuelve información incorrecta - Aparece un aviso que explica que el contenido se ha bloqueado o que ha habido un error de conexión - También puede aparecer un error que indica que servidor no existe; o puede aparecer el error: DNS	Bajo Es el bloqueo de menos costo en términos técnicos y el más fácil de evadir porque “no requieren herramientas adicionales más allá de las ya utilizadas normalmente por los proveedores de Internet (ISP) para poder proporcionar sus servicios, según lo han definido organizaciones civiles.

Bloqueo por HTTP / HTTPS	- Mecanismo que intercepta o redirige la navegación desde la propia ubicación en la web de la plataforma buscada. - Se aplica cuando se bloquean los paquetes del TLS handshake, los cuales se necesitan para lograr una conexión segura con un servidor de un sitio web. Lo ejecutan al aplicar un filtrado de paquetes del SNI (Server Name Indicación) que va al sitio web que el usuario desea consultar y no logra la conexión. -Este tipo de bloqueo impide que se establezca la conexión segura con el servidor del sitio web destinatario.	Medio Es más efectivo y costoso técnicamente que el DNS, porque amerita de un VPN para sortearlo.
Bloqueo por IP	Mecanismo que intercepta o redirige la navegación desde la propia ubicación en la web de la plataforma buscada. Funciona evitando que se encuentre el número de localizador o un puerto asignado a cada usuario para su conexión a Internet Generalmente, funciona por celdas o zonas, afectando a una región o comunidad determinada Bloquea el IP y su protocolo base.	Más efectivo y costoso que el DNS.

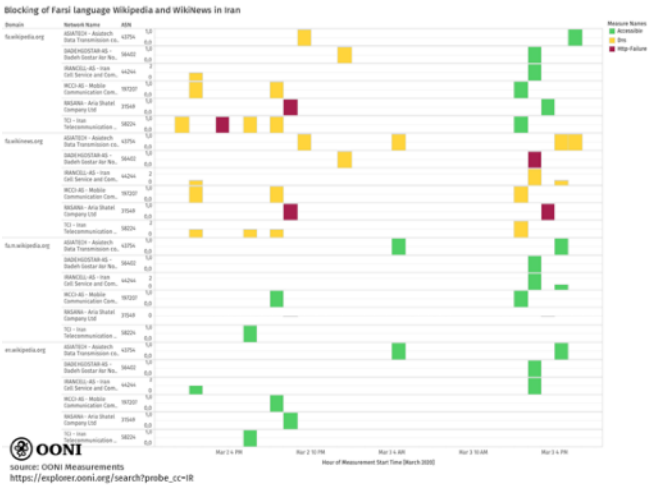
Patrones de bloqueo

Aunque no hay una clasificación global estandarizada, podemos entender que los bloqueos tienen distintas modalidades y dimensiones. Según la experiencia de documentación en países, se sugiere la siguiente caracterización.

Temporales: Son bloqueos momentáneos, que ocurren en un periodo específico de tiempo. Suele ocurrir que bloquean en un lapso específico ciertos sitios web y luego vuelven a estar accesibles. Ocurre, generalmente, con el bloqueo de las redes sociales o sitios de contenido global. Este tipo de bloqueo amerita una respuesta de monitoreo de rápida respuesta, debido a que puede cambiar el comportamiento de las pruebas en cortos bloques de horas.

Por ejemplo, en marzo de 2020, Wikipedia estuvo bloqueado temporalmente en Irán, de acuerdo con los hallazgos de OONI[6]

[6] https://ooni.org/post/2020-iran-blocks-farsi-wikipedia/



Ver: https://ooni.org/post/2020-iran-blocks-farsi-wikipedia/

Continuos: Son bloqueos que se mantienen en el tiempo y, generalmente, tienen pocas variaciones. Podrían entenderse como bloqueos fijos que mantienen su comportamiento por largos periodos de tiempo. Podría entenderse como un bloqueo continuo, por ejemplo, la restricción de contenidos relacionados a información de minorías étnicas en Pakistán, según las mediciones de OONI entre 2014 y 2017[7].

Probed ASN	Blocked URL	Blockpage
AS23674	http://www.BalochVoice.com	id-micronet-0
AS23674	http://www.BalochVoice.com	id-surf-safe-0
AS23674	http://balochwarna.org	id-micronet-0
AS23674	http://balochwarna.org	id-surf-safe-0
AS23674	http://www.bso-na.org	id-micronet-0
AS23674	http://www.bso-na.org	id-surf-safe-0
AS23674	http://www.ostoman.org	id-micronet-0
AS23674	http://www.ostoman.org	id-surf-safe-0
AS23674	http://www.radiobalochi.org	id-surf-safe-0
AS23674	http://governmentofbalochistan.blogspot.com	id-micronet-0
AS23674	http://www.BalochFront.com	id-micronet-0
AS23674	http://www.balochunitedfront.org	id-surf-safe-0
AS23674	http://www.balochwarna.com	id-micronet-0
AS23674	http://www.balochwarna.com	id-surf-safe-0
AS23674	http://www.thebalochhal.com	id-micronet-0
AS23674	http://www.thebalochhal.com	id-surf-safe-0

Ver: https://ooni.org/post/gambia-Internet-shutdown/

Selectivos: Pueden considerarse como bloqueos intermitentes, variaron según la ubicación geográfica, las horas y las conexiones de los usuarios. Apareció también una diversidad de las modalidades de bloqueos que aumentan los controles y que hacen más difícil sortear la censura. Es una modalidad que puede combinar una diversidad de patrones de bloqueos que puede varias por horas, por proveedor, por lista de sitios web, por días, zona geográfica y tipo de bloqueo. Ocurren en territorios con situaciones complejas de censura como las de Venezuela[8].

---

[7] https://ooni.org/post/pakistan-Internet-censorship/

[8] https://ipysvenezuela.org/intercortados/33-2/

Shutdowns: puede definirse de esta manera a apagones de la red o desconexiones arbitrarias de Internet. Ha ocurrido en varios países, muchas veces en momentos de alta conflictividad asociadas a protestas o elecciones. OONI reportó uno de estos casos durante las elecciones presidenciales de Gambia de 2016[9].
Hay que tomar en cuenta que los patrones del comportamiento de los bloqueos no son absolutos y que pueden variar o incluso pueden derivar en nuevas combinaciones, según el contexto y el entorno nacional donde ocurren.

Descartar las interferencias

Así como hay que entender el tipo de bloqueo, cómo se manifiesta y los patrones de la censura digital, también hay que considerar varios elementos que permiten descartar las interferencias de Internet. Por eso, presentamos una lista de chequeo que pueden ser útil repasarla antes de hacer un pronunciamiento o denuncia de bloqueo:

- No todas las interferencias de conexión representan un bloqueo
- Puede haber fallas de conexión a Internet que esté impidiendo la navegación, pero que no necesariamente es un bloqueo
- Puede existir fallas técnicas en la computadora o dispositivo de conexión del usuario y no necesariamente es un bloqueo
- El usuario puede tener interferencias que no son un bloqueo, si no que pueden estar asociadas a otras fallas relacionadas con las web que se consultan: fallas en los servidores, administradores o dominios, entre otros.
- Pueden haber impedimentos de consulta de contenidos que pueden estar relacionados con otros hechos como los ataques que atentan y vulneran la seguridad de una página web
- Los bloqueos no se derivan por ataques a los servidores de los sitios web o de denegación de servicio (DDOS)
- Los bloqueos de contenidos son ajenos a las fallas generales de pueden afectar a algunas plataformas, como las caídas globales de las redes sociales como las de Twitter, Instagram, por ejemplo

Antes de hacer conclusiones y denuncias, hay que buscar las evidencias:

- Haciendo mediciones propias en el terreno a través de aplicaciones de testeo como las de OONI
- Consultando con otras fuentes para determinar cuán generalizada es la restricción
- Consultando repositorios globales de evidencias
- Procurando la consulta a un técnico o especialista en asuntos electrónicos

[9] https://ooni.org/post/gambia-Internet-shutdown/

3 I Fuentes de información, datos e iniciativas globales

La comunidad técnica global ha trabajado en diversas iniciativas que sirven de apoyo para levantar evidencias, monitorear y emprender investigaciones sobre el estado del Internet en el mundo. Diversas fuentes son de utilidad para seguir los asuntos de censura digital. Incluso, las metodologías implementadas, mayormente, por la comunidad técnica tienen una enorme potencialidad para fines periodísticos y de defensa de los derechos digitales.

En este manual revisamos seis iniciativas que pueden ser de utilidad.

A.- OONI

La iniciativa más sólida para rastrear los asuntos de bloqueos digitales es la del Observatorio Abierto de Interferencia de Internet (OONI)[10]. Este es un proyecto que se comenzó a implementar en 2012 con la finalidad de asegurar una Internet libre y abierta, a través del aumento de la recolección de evidencias de censura con mecanismos de transparencia. OONI se considera un observatorio ciudadano con criterios técnicos, y ha levantado mediciones, a través de colaboradores en más de 200 países.

OONI[11] tiene una estructura de funcionamiento descentralizada, con una estrategia de medición que se basa en las tareas de medición de una comunidad global de voluntarios, quienes realizan pruebas de detección de censura desde el terreno.

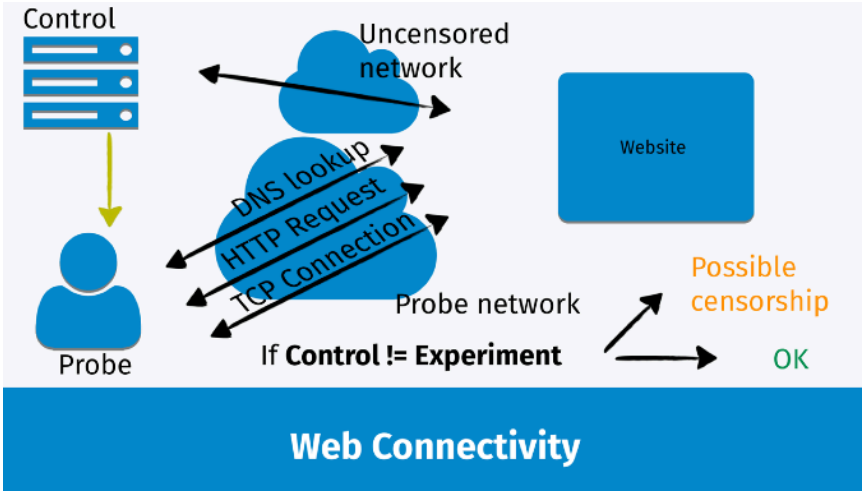
Sus metodologías, herramientas y mediciones son abiertas, transparentes y cumplen con el criterio de revisión previa por parte de la comunidad técnica. Su función principal es técnica y sus evidencias muestras posibles evidencias de censura, que deben ser comprobadas en el terreno o por la comunidad técnica.

Trabajan en función de recursos y herramientas de datos abiertos, ofrecen un archivo de datos abiertos de evidencias que se levantan en distintas partes del mundo sobre las interferencias de Internet, principalmente, relacionadas con bloqueos digitales.

---

[10] https://ooni.org/about/

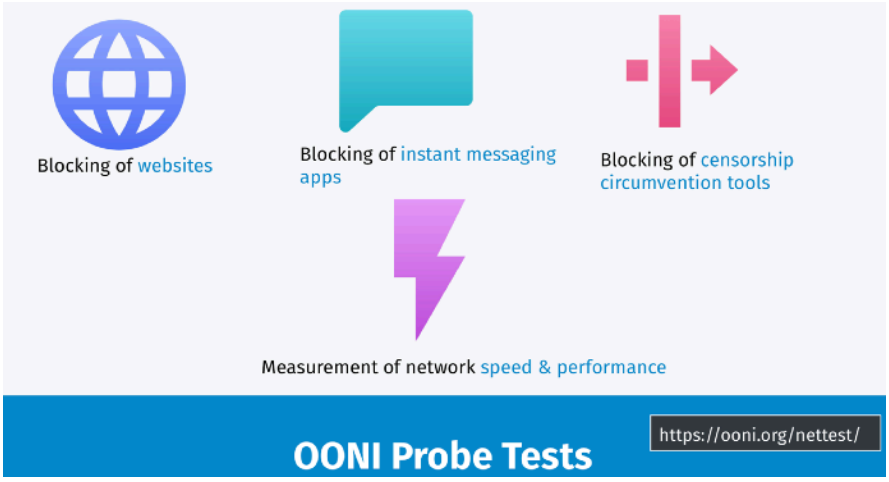
[11] https://ooni.org/post/2020-imv-slides-recordings/



Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

Los análisis que hace OONI están orientados a evaluar:

- Bloqueo de sitios web: ¿cuáles sitios web han sido bloqueados por ISP? ¿Cómo han sido bloqueados y cuáles han sido las técnicas de bloqueo?¿Cómo es el comportamiento de los bloqueos por sitios web en diferentes periodos de tiempo?
- Bloqueo de aplicaciones de mensajería instantánea como WhatsApp, Facebook Messenger y Telegram: ¿Estas plataformas han sido bloqueadas? ¿Cómo cambia el comportamiento de estos bloqueos por ISP y lapsos de tiempo?
- Bloqueo de herramientas de circunvención de la censura digital como, por ejemplo, Tor o Psiphon: ¿funcionan o no las herramientas de circunvención en la red que se está corriendo la prueba?
- Presencia de sistemas en la red que pueden ser responsables de censura o vigilancia:
- Mediciones de velocidad y estado de conectividad y acceso a Internet: ¿Cuál es la velocidad y el estado de la red? ¿Como se pueden observar cambios en el comportamiento de la red por días, zonas o fechas?



Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

La mayor fortaleza de OONI ha sido el desarrollo de un software de código abierto, que está en constante revisión y mejoramiento. Este observatorio tiene varias herramientas que pueden ser útiles para rastrear la censura digital.

- **OONI Probe**: es una aplicación que puede descargarse para celulares (con sistemas Android e iOS) y computadoras que puede utilizarse para recoger datos que pueden servir potencialmente como evidencias sobre la censura en Internet. Está diseñada para mostrar cómo, cuándo, dónde y por cuáles proveedores o plataformas están siendo implementadas las medidas de bloqueos en la red.

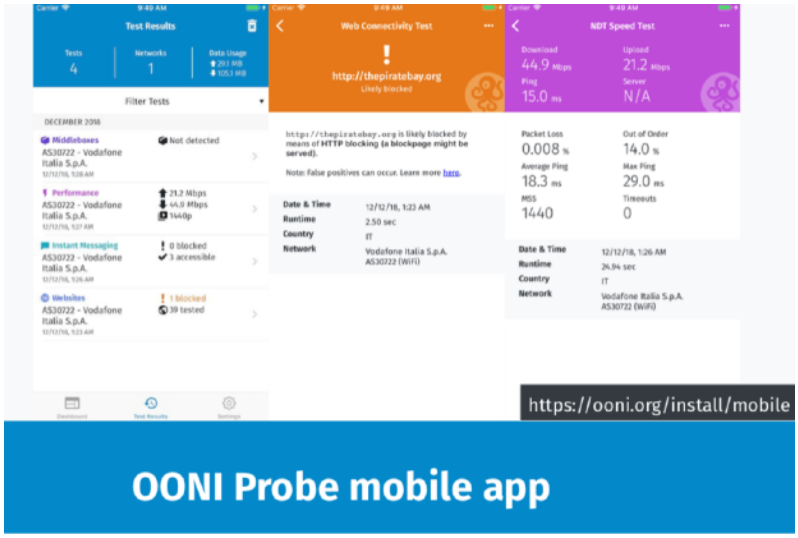
  OONI advierte que esta aplicación no es una herramienta privada, por lo que existe el riesgo de que alguien pueda monitorear la actividad en Internet de sus usuarios y podría determinar que están utilizando la herramienta de OONI Probe. También aclaran que incluyen diferentes tipos de URL para testear, entre las que se encuentran algunos contenidos que pueden ser objetables o provocativos en algunos entornos, como podrían ser sitios con información pornográfica. Además, por defecto las mediciones de OONI se publican bajo el criterio de transparencia y de datos abiertos, sin embargo, el usuario puede cambiar esta configuración al descargar o usar la aplicación.

  Un consejo que no se puede pasar por alto para el uso del OONI Probe es apagar el VPN, en el caso de que se esté utilizando, al momento de correr la prueba. Si el VPN está encendido no se recoge eficientemente la medición y no se levantan las evidencias de posibles bloqueos.

Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

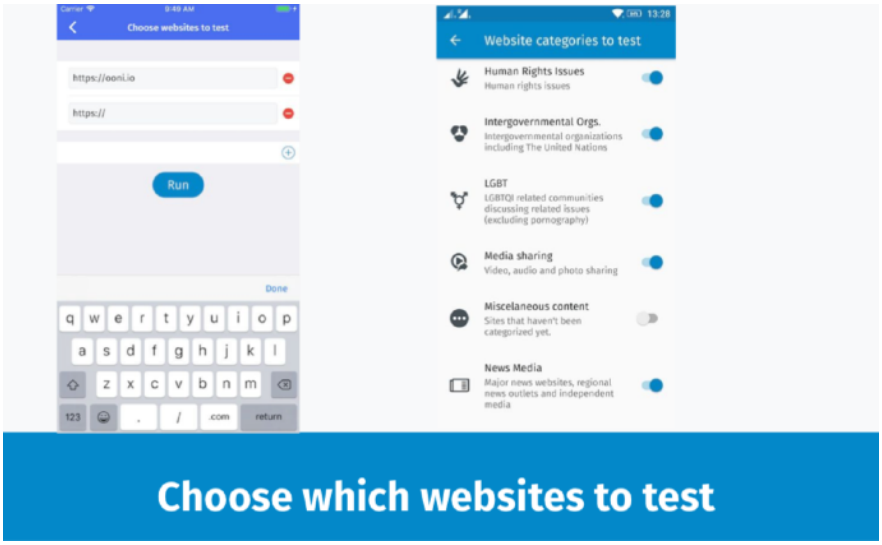
OONI Probe corre tres tipo de mediciones:

A. **Pruebas aleatorias**: son previamente configuradas por OONI, para correr en distintos momentos del día, rotando la lista de medición por país.



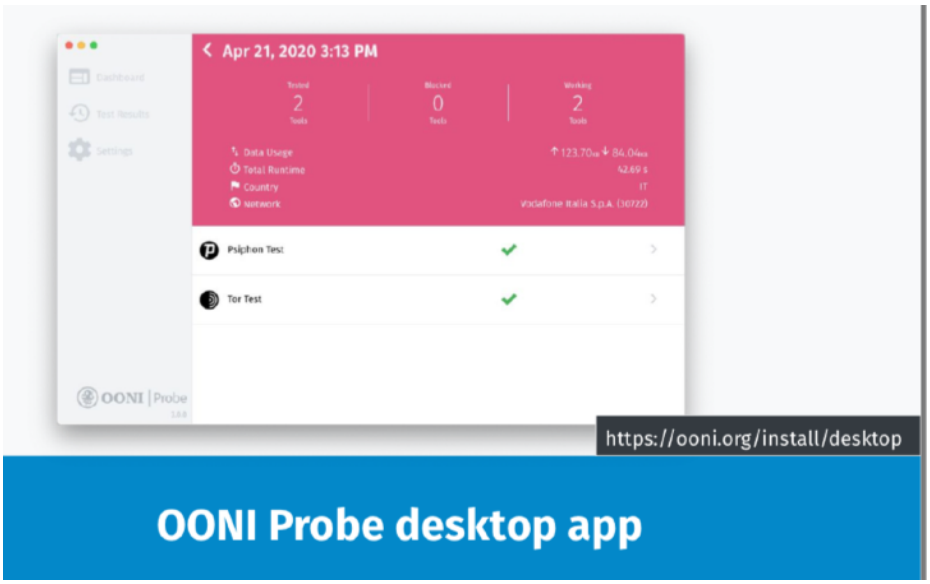
Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

B. **Pruebas personalizadas configuradas desde el celular o la computadora:** los usuarios pueden preparar sus lista personalizada de los sitios que desea analizar, correr la medición y obtener el resultado en tiempo real. Para repetir la prueba, debe configurar de nuevo la medición y volverla a correr.



Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

C. **Pruebas preconfiguradas para mediciones de campaña o coordinadas:** OONI permite preconfigurar listas de medición para ser compartida a través de enlaces que pueden distribuirse de manera pública o privada mediante un enlace. Esta opción se utiliza a través de otra herramienta que es la de OONI Run que explicaremos en la siguiente sección. Esta opción es recomendable para hacer mediciones en equipo y de manera colaborativa, en distintos puntos geográficos, por distintos proveedores, de manera simultánea, bajo un protocolo o criterios de investigación previamente acordados.



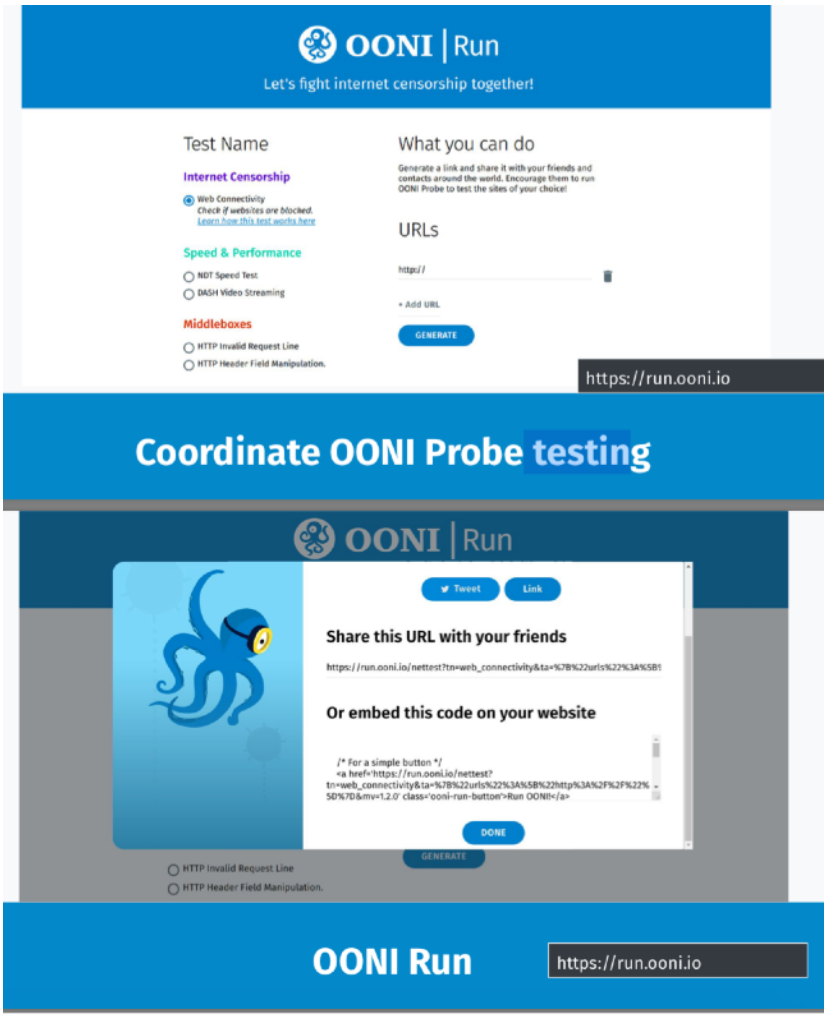
Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

Política de riesgos potenciales

OONI presenta una política de riesgos potenciales que deben ser tomadas en cuenta por sus usuarios, por lo cual piden tomar en cuenta ciertas condiciones:

- Las amenazas previas y el perfil de los usuarios pueden llamar la atención al usar esta api.
- Las leyes y regulaciones de cada país podrían tener disposiciones que afecten a los usuarios, por lo cual es mejor documentarse legalmente antes de usar esta aplicación.

- **OONI Run:** está disponible en https://run.ooni.io, un espacio web de OONI que permite configurar jornadas o campañas de medición coordinadas, bien sean con carácter públicas o privadas, según los distintos tipos de pruebas que tiene disponible OONI**.** Permite pre-configurar una prueba con una lista de URL, o una opción de testeo, que se puede someter a un proceso de análisis o mediciones individuales o colectivas desde OONI Probe. OONI Run genera un enlace que luego puede ser compartido para hacer mediciones desde diversos puntos o lugares, preferiblemente, bajo un protocolo de medición y de investigación previamente diseñado y que sea robusto. OONI también, ofrece unas preconfiguraciones con enlaces temáticos para analizar algunos sectores que son de interés global. Estos enlaces se pueden tomar y reproducir por los usuarios a través de OONI Probe.



Ver: https://ooni.org/documents/imv2020-slides/ooni

Las 10 listas temáticas prediseñadas de OONI han sido creadas para colaborar en una respuesta rápida frente a eventos de emergencia de censura en Internet. Estas pueden ser utilizadas globalmente:

1. COVID-19 (25 URLS)
2. Redes sociales (39 URLS)
3. Sitios de noticia (47 URLS)
4. Vpns (21 URLS)
5. Wikipedia (28 URLS)
6. Derechos humanos (27 URLS)
7. Medio ambiente (20 URLS)
8. Lgbtqi (26 URLS)
9. Derechos reproductivos (4 URLS)
10. DNS y HTTPS (39 URLS)

- **OONI Explorer:** es un explorador de OONI con datos abiertos de evidencias técnicas de censura en Internet y otras interferencias digitales que se han presentado alrededor del mundo. Desde 2012, OONI ha alcanzado 280 millones de mediciones recolectadas en

233 países. Esta API, a través de su buscador, permite desagregar las búsquedas por países, proveedores, tipos de pruebas de censura, por URL, y períodos de tiempo. También, tiene un resumen breve de las mediciones por países y los últimos resultados más resaltantes.

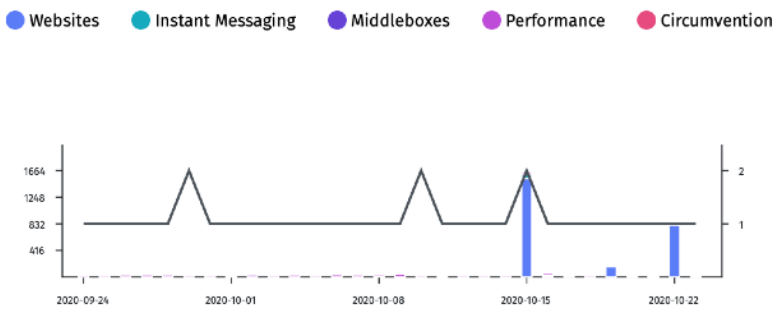
Las pruebas de bloqueos responden a tres categorías:

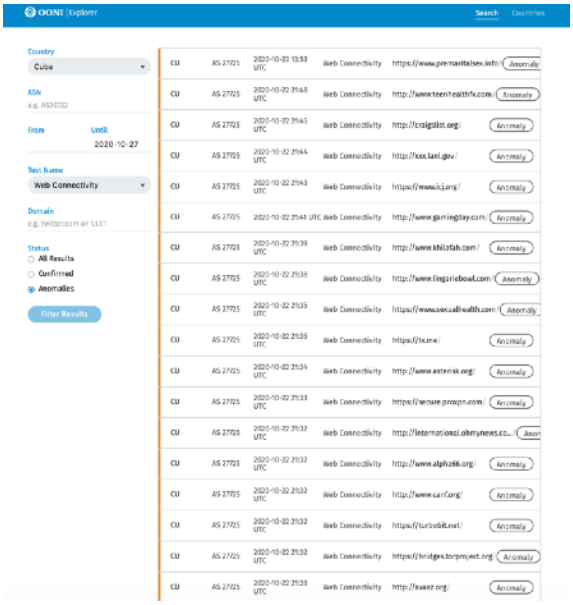
- **Normal o accesibles:** contenidos que no tienen evidencias de interferencias;
- **Confirmados:** evidencias de bloqueos en países en los que se ha confirmado, con un régimen legal o una información de fuentes directas que decreten esta censura digital
- **Anomalías:** evidencias de censura en situaciones no declaradas, por lo cual la medición sugiere interferencias o bloqueos. Pueden entenderse como una señal de que hay una señal errada para la accesibilidad. Pueden contener evidencias de censura pero hay que revisarlas con cuidado porque puede haber falsos positivos.

Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

Datos de Cuba

Los usuarios de OONI Probe han recogido más de 72 mil mediciones en cuatro ISP locales, la mayoría de ellas han sido pruebas del ISP de la Empresa de Telecomunicaciones de Cuba, en la cual se han testado más de 1500 URL.





Ver: https://ooni.org/documents/imv2020-slides/ooni.pdf

Lista de medición

OONI basa sus mediciones en una muestra de sitios web, que ellos denominan “listas de pruebas”. Existe dos:

- Lista de prueba global: contiene una amplia selección de sitios web que han sido considerados como relevantes a escala internacional.
- Listas de prueba específicas por país: aquí se han incluido sitios web relevantes para cada país. Una buena parte de esta muestra es aportada por los aliados y voluntarios locales.

Clasificación de los tipos de contenidos

Con el propósito de homologar criterios de medición y de investigación en la escala global, reducir el sesgo y facilitar la categorización de los sitios que se someten a las pruebas, OONI utiliza una lista de 30 categorías, que se ha perfeccionado desde 2012, y cuyo trabajo clasificación cuenta con el respaldo del Citizen Lab de la Universidad de Toronto, que lleva la administración y la clasificación de estas listas, y las ha puesto a disposición de GitHub, para la actualización en un modo colaborativo.

Esta categorización ha tomado en cuenta el conocimiento local, la comprensión de los contenidos que se consultan y el análisis del contexto político y social de cada país.

Esta categorización ha sido tomada en cuenta para caracterizar los sitios web que aparecen en las mediciones de OONI. Respondieron a estas 30 categorías, y cuyas siglas provienen del inglés:

- **ALDR (alcohol & drugs)**: sitios dedicados al uso, tráfico y venta de drogas y alcohol, independientemente de la legalidad local.
- **REL (religión)**: sitios dedicados a la discusión de asuntos religiosos, tanto de apoyo como críticas, así como a la discusión de grupos religiosos minoritarios.
- **PORN (pornografía)**: pornografía dura y blanda.

- **PROV (atuendo provocativo)**: sitios web que muestran atuendos provocativos y retratan a las mujeres de manera sexual con ropa mínima.
- **POLR (crítica política):** contenido que ofrece puntos de vista críticos sobre asuntos políticos. Incluye autores críticos y blogueros, así como organizaciones políticas de oposición. Incluye contenido a favor de la democracia, contenido anticorrupción, así como contenido que pide cambios en el liderazgo político, cuestiones de gobernanza y reforma legal, entre otros.
- **HUMR (human rights issues**): sitios dedicados a debatir cuestiones de derechos humanos en diversas perspectivas. Incluye los derechos de la mujer y los derechos de los grupos étnicos minoritarios.
- **ENV (medio ambiente)**: sitios relacionados con contaminación, tratados ambientales internacionales, deforestación, justicia ambiental, desastres.
- **MILX (terrorismo y militantes)**: sitios que promueven el terrorismo, militantes violentos o movimientos separatistas.
- **HATE (discurso de odio)**: contenido que desacredita a grupos o personas en particular por motivos de raza, sexo, sexualidad u otras características.
- **NEWS (medios de comunicación)**: incluye los principales medios de comunicación internacionales, así como los medios de comunicación regionales y los medios independientes.
- **XED (educación sexual)**: icontenido relacionado con anticoncepción, abstinencia, enfermedades de transmisión sexual, sexualidad saludable, embarazo adolescente, prevención de violaciones, aborto, derechos sexuales y servicios de salud sexual.
- **PUBH (salud pública):** contenidos relacionados con VIH, SARS, gripe aviar, centros para el control de enfermedades, Organización Mundial de la Salud, entre
- **GMB (juegos de azar):** sitios de juegos de apuestas en línea. Incluye juegos de casino, apuestas deportivas,
- **ANON (herramientas de anonimización y elusión)**: sitios que proporcionan herramientas que se utilizan para anonimización, elusión, servicios de proxy y cifrado de contenido.
- **DATE (citas en línea):** servicios de citas en línea que se pueden utilizar para conocer gente, publicar perfiles, chatear, entre otras actividades.
- **GRP (social networking)**: herramientas y plataformas de redes sociales.
- **LGBT (LGBT)**: una variedad de temas queer-gay-lesbianas-bisexuales-transgénero (No se toman en cuenta asuntos de pornografía)
- **FILE (intercambio de archivos):** sitios y herramientas utilizados para compartir archivos, incluido el almacenamiento de archivos en la nube, torrents y herramientas de intercambio de archivos P2P.
- **HACK (Herramientas de hacking)**: sitios dedicados a la seguridad informática, incluidas noticias y herramientas. Incluye contenido malicioso y no malicioso.
- C**OMT (herramientas de comunicación):** sitios y herramientas para la comunicación individual y grupal. Incluye aplicaciones de correo web, VoIP, mensajería instantánea, chat y mensajería móvil.
- **MMED (media sharing / redes sociales)**: plataformas para compartir videos, audio o fotos.
- **HOST (plataformas de alojamiento y blogs)**: servicios de alojamiento web, blogs y otras plataformas de publicación en línea.
- **SRCH (motores de búsqueda)**: motores de búsqueda.
- **GAME (juegos)**: juegos y plataformas de juegos en línea, excluidos los sitios de juegos de apuestas".
- **CULTR (Cultura):** contenido sobre entretenimiento, historia, literatura, música, cine, libros, sátira y humor.
- **ECON (economía)**: desarrollo económico general y temas relacionados con la pobreza, agencias y oportunidades de financiamiento.
- **GOVT (gobierno)**: sitios web gestionados por el gobierno, incluidos sitios militares.
- **COMM (comercio electrónico)**: sitios web de servicios y productos comerciales.

- **CTRL (control de contenido):** contenido benigno o inocuo utilizado para fines de control.
- **OIG (Organizaciones Intergubernamentales)**: sitios web de organizaciones intergubernamentales como las Naciones Unidas".

B.- Otras iniciativas:

- **CAIDA-IODA**
  https://ioda.caida.org

Esta es una iniciativa que se sostiene en un sistema operativo experimental que monitorea las redes de internet, casi en tiempo real. Es útil para identificar, analizar y mapear los cortes o apagones de internet.

Es una herramienta que "combina información de tres fuentes de datos, establece la relevancia de un evento y genera alertas. Los eventos de interrupción y las señales correspondientes obtenidas a través del análisis automatizado se muestran en paneles y gráficos interactivos que permiten al usuario inspeccionar más los datos"[12].

Es un proyecto cuenta con la metodología de la Universidad del Sur de California.

Se puede consultar información sobre Cuba.

- **Netblocks**
  https://netblocks.org

NetBlocks[13] se define como una sociedad civil de derechos digitales que aporta evidencias, a corto plazo, sobre bloqueos e interferencias de conectividad en varios países. Levantan reportes con evidencias sobre la proporción de accesibilidad de sitios web y de navegación. También, generan alertas en Twitter que son útiles para la documentación de denuncias.

- **Access Now - Keepiton**
  https://www.accessnow.org/keepiton/

La coalición #KeepItOn[14], es una iniciativa coordinada por Access Now, una de las organizaciones globales más importantes en asuntos de derechos digitales. Trabajan desde 2016 y han logrado sumar a más de 220 organizaciones de 99 países de todo el mundo. Su objetivo es denunciar cortes de internet a través de diversas estrategias. Coordinan el proyecto Shutdown ***Tracker Optimization Project (STOP)***. Generan un reporte anual que es muy útil para entender el contexto global de los bloqueos.

- **Measurement Lab (M-Lab)**
  https://speed.measurementlab.net/#/

---

[12] https://ioda.caida.org

[13] https://netblocks.org

[14] https://www.accessnow.org/keepiton/

Es una organización global que proporciona una amplia colección de datos abiertos con respecto al rendimiento de internet. Ofrece y promociona mediciones abiertas y verificables del rendimiento de la red global. Es útil para evaluar la calidad de la velocidad de internet. Tiene, también, un test de velocidad que es confiable.

- **Censored Planet**

  https://censoredplanet.org/projects

Censored Planet[15] es un laboratorio auspiciado por la Universidad de Michigan, con el trabajo de profesores, investigadores y estudiantes, que se dedica a investigar y producir mediciones sobre los diferentes tipos de violaciones a la privacidad y la seguridad en internet.

[15] https://censoredplanet.org/projects

4 I Cuba en los reportes internacionales

Para dimensionar las evidencias de censura digital que recogidos, de forma exploratoria, en el proceso de investigación, nos formulamos y tratamos de responder las interrogantes: ¿Dónde se ubica el país con respecto a los bloqueos? ¿Con qué países se puede comparar? ¿Qué muestran los organismos y reportes internacionales sobre los derechos digitales en Cuba?

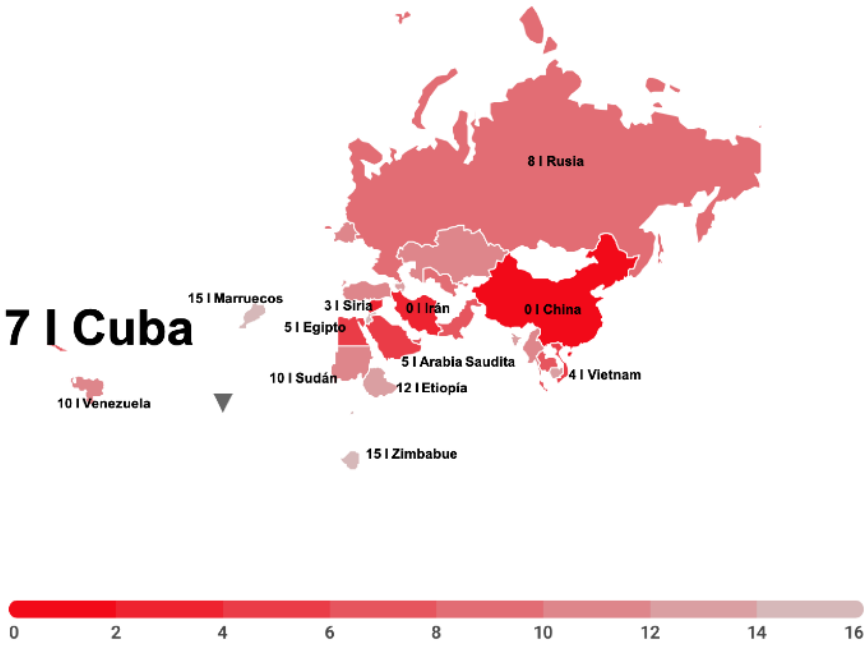
Las respuestas las encontramos en reportes de diversas instancias como Freedom House, Access Now, OONI, y la Comisión Interamericana de Derechos Humanos.

Freedom House: Reporte 2020 Libertad en la red[16]

En el índice de Libertad en la red, entre 2019 y 2020, Cuba está entre los ocho países —de los 65 analizados— con menos libertad en Internet. Incluso, es el país con menos condiciones de acceso a Internet, unos de los cinco con mayores medidas de censura digital y control de contenidos. Algunos hallazgos que destacan:

- Continúan los bloqueos de sitios web y revistas de noticias cubanas, como 14 y medio,CiberCuba, Cubanet, ADN Cuba, Revista El Estornudo, y la Revista Tremenda Nota. Para este manual se pudo confirmar la aplicación de diversas técnicas de bloqueos de este grupo de medios que implicaron medidas de censura digital por HTTP, DNS e IP.
- Skype estuvo bloqueado en el pasado, pero los usuarios han utilizado otras alternativas similares como Imo, Facebook Messenger y Whatsapp.
- Sitios de noticias internacionales como la BBC estaban accesibles para el momento en el que se realizó este índice. Sin embargo, el registro de OONI que utilizamos para este manual muestra una evidencia de bloqueo por DNS de este medio internacional, con una prueba que se corrió en agosto de 2020.
- El sitio web de la revista ADN Cuba fue bloqueada en julio de 2019, según este reporte. Los datos analizados por OONI muestran cinco evidencias de bloqueo por HTTP, entre septiembre de 2019 y septiembre de 2020.

[16] https://freedomhouse.org/country/cuba/freedom-net/2020



OONI: Reporte 2017 Parknet, breve documentación sobre los bloqueos en Cuba[17]

Un equipo de investigadores hizo mediciones en Cuba, a partir de 8 puntos de medición en tres ciudades del país, y contabilizaron que 41 sitios web estaban bloqueados. Detectaron la implementación de DPI, paquetes de inspección de datos. Entre mayo y junio, la modalidad de bloqueo que OONI determinó fue la de HTTP, pero concluyeron que se podía eludir la censura a través del acceso de HTTPS, con el certificado de seguridad, de los sitios bloqueados.

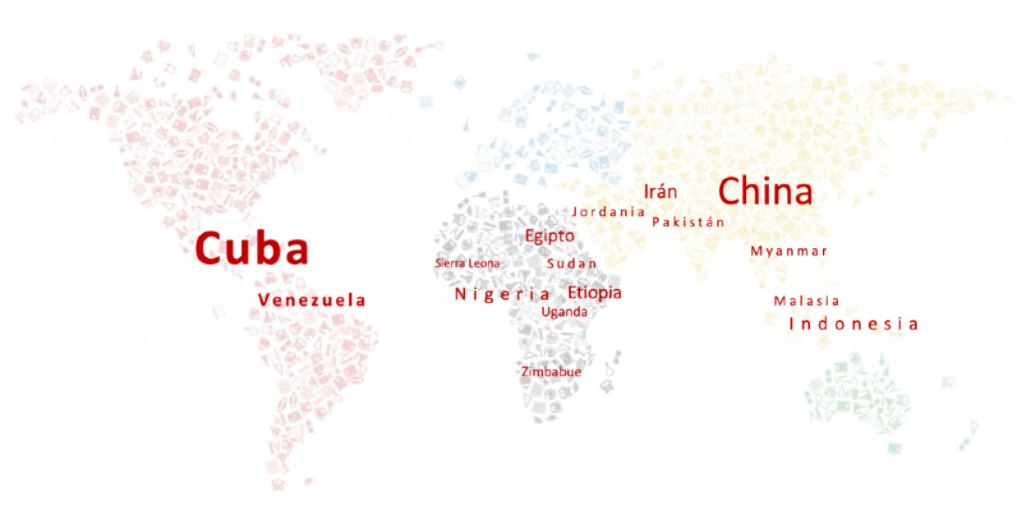
Establecieron algunas características:

- La mayoría de los sitios bloqueados se relacionaban con expresiones de críticas gubernamentales.
- Estaban bloqueados algunos medios de comunicación y blogs críticos y que difundían asuntos de derechos humanos en Cuba; sitios de ONG locales de libertad de expresión, y organizaciones internacionales como Freedom House
- El Proyecto de Prensa Libre de Cuba, que tiene como objetivo apoyar a periodistas y escritores independientes.
- Para ese momento, Skype fue la única herramienta de comunicación que encontraron bloqueada.
- Descubrieron que Google no permitió el acceso a su servicio App Engine a los usuarios cubanos.

OONI ha reportado situaciones de control del flujo de contenido digital similares a las que ocurren en otros países, los cuales conforman el mapa de países que sirven de guía para establecer comparaciones. Entre ellos está Venezuela, Sierra Leona, Nigeria, Uganda, Zimbabue, Sudán, Egipto, Jordania, Pakistán, Myanmar, Malasia, Indonesia, entre otros.

---

17 https://ooni.org/post/parknet-short-documentary-cuba/



CIDH: Reporte Libertad de expresión en Internet en Cuba[18]

La CIDH documentó las restricciones de la libertad de expresión en Internet en Cuba a través de medidas de censura digital que afectan a los medios de comunicación, principalmente, y también a los usuarios.

Con base en el informe, se puede evidenciar cómo los principios establecidos en los Estándares para una Internet libre, abierta e incluyente, se ven afectados en Cuba. A continuación presentamos una matriz de análisis en función de los aportes de la CIDH y los principios establecidos.

Principios afectado	**Análisis de la CIDH**
Apertura	"El acceso y uso de las redes por parte de la población cubana se ve seriamente obstaculizado por el bloqueo a sitios web críticos o disidentes del Partido del Gobierno. El bloqueo de sitios web de periodistas independientes, críticos del gobierno o relacionados con derechos humanos se ha mantenido a través de los años. Afectaría a blogs, páginas web o plataformas de contenidos gestionadas por voces críticas, ya se encuentren alojadas en el país o en el exterior".
Descentralización **Gobernanza multisectorial**	"Para la mayoría, la única opción sería la intranet cubana, que permite el acceso a los sitios web que están inscritos con el dominio .cu o que apoyan al gobierno cubano, pero como se señaló, la población mayoritaria no tendría acceso a la web global. La intranet nacional es una red controlada, en donde se puede navegar por sitios internacionales seleccionados, así como tener acceso al correo electrónico".

[18] http://www.oas.org/es/cidh/expresion/docs/informes/Cuba-es.pdf

Neutralidad	“La información disponible indica que desde el Ministerio de Informática y Comunicaciones se privilegiaría el acceso a páginas web que constituyen una especie de intranet nacional y que se orientan a replicar o a presentar una versión autóctona de servicios muy conocidos en el resto del mundo”.
Pluralismo y diversidad **No discriminación**	“Según diversas fuentes, una parte de los contenidos alojados en la Internet mundial no serían accesibles desde Cuba dado que son bloqueados o filtrados por las autoridades. En algunos casos se trataría de bloqueos temporales, pero en otros se habría constatado la imposibilidad de acceso a páginas web, plataformas o redes sociales como Facebook, Twitter, Youtube, Yahoo, MSN o Hotmail”.

La CIDH concluyó que “lejos de estos estándares para una red libre, abierta e inclusiva, el despliegue normativo y prácticas en Cuba generan un espacio controlado y sesgado”.

Este organismo hizo tres recomendaciones con la finalidad de que orienten las políticas públicas para eliminar el impacto de la censura digital.

- Adecuar la normativa local de conformidad con los principios señalados de acceso en igualdad de condiciones, el pluralismo, la no discriminación y la privacidad, así como la neutralidad de la red y la gobernanza multisectorial como componentes transversales de estos principios.
- Levantar en el más breve plazo el bloqueo de contenidos y en especial, el de los medios independientes censurados.
- Asegurarse de que los intermediarios no estén sujetos a un régimen que establezca su responsabilidad objetiva por el contenido que distribuyan o les obligue a ejercer funciones de supervisión del mismo.

ONU: Procedimientos especiales[19]

Las implicaciones de la censura digital en Cuba pueden ir más allá de los bloqueos de sitios web. Representantes de la ONU alertaron sobre el bloqueo y filtrado de contenidos a través de mensajerías de texto.

Relatores de Naciones Unidas emitieron una comunicación en 2019, a través de los procedimientos especiales, para alertar “el supuesto filtrado y bloqueo de mensajes llamando al voto negativo en el referéndum constitucional que se celebrará el 24 de febrero de 2019, enviados a través del servicio de mensajes cortos (SMS) de la empresa pública ETECSA (Empresa de Telecomunicaciones de Cuba, Sociedad Anónima)”. Hicieron notar que era necesario que el Estado de “Cuba adoptara todas las medidas necesarias para proteger los derechos y las libertades”. Consideraron que “la opinión pública tiene que ser informada sobre las implicaciones potenciales relacionadas” con las restricciones a la libertad de expresión.

En este mismo contexto, periodistas locales consultados comentaron, por ejemplo, que cuando el debate constitucional que aconteció entre 2018 y 2019 para la nueva Constitución había un monitoreo para bloquear a páginas que impulsaran la etiqueta #YoVotoNo, un hecho que también estuvo entre las preocupaciones de los expertos de la ONU.

---

[19] https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24316

Penalizaciones relacionadas al uso del Internet en Cuba

Los organismos internacionales también han denunciado otras formas de restringir las libertades digitales que han derivado en censura. Uno de los hechos significativos ha sido que Cuba cuenta con una regulación que busca controlar arbitrariamente el funcionamiento y el acceso a Internet. El Decreto Ley 370 entró en vigencia el 4 de julio de 2018 y establece un control amplio por parte del régimen cubano sobre el Internet.

El decreto establece como ilícitos, en su artículo 68, los siguientes actos[20]:

a) Comercializar programas, aplicaciones y servicios informáticos asociados a estos sin la autorización de los organismos competentes de acuerdo con la legislación vigente;

b) fabricar, comercializar, transferir, instalar equipos y demás dispositivos para brindar, facilitar o recibir servicios asociados a las TIC, sin la correspondiente autorización;

c) diseñar, distribuir o intercambiar códigos de virus informáticos u otros programas malignos entre personas naturales o jurídicas; se exceptúa la información enviada por usuarios a la autoridad competente para su análisis e investigación;

d) adicionar algún equipo de telecomunicaciones/TIC o introducir cualquier tipo de programas y aplicaciones informáticas en una red de datos, ya sea a través de soportes removibles o mediante acceso a redes externas sin la autorización del titular, o no garantizar su compatibilización con las medidas de seguridad establecidas para la protección de la red de datos;

e) acceder sin la autorización o agredir a cualquier sistema de cómputo conectado a las redes públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios debidamente autorizados;

f) hospedar un sitio en servidores ubicados en un país extranjero, que no sea como espejo o réplica del sitio principal en servidores ubicados en territorio nacional;

g) interferir, interceptar, alterar, dañar o destruir datos, información, soportes informáticos, programas o sistemas de información y comunicación de servicios públicos, sociales y administrativos;

h) realizar acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros, sin la debida autorización; y

i) difundir, a través de las redes públicas de transmisión de datos, información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas.

Las penalizaciones van desde el pago de multas hasta el decomiso de los equipos y medios utilizados y la remoción de licencias que autorizan a la prestación de servicios de forma temporal o definitiva.

---

[20] http://juriscuba.com/decreto-ley-no-370/

Organizaciones internacionales han mostrado su preocupación en relación al uso que se le puede dar al decreto. La Comisión Interamericana de Derechos Humanos (CIDH) consideró que el Decreto Ley 370 “podría generar restricciones indebidas al ejercicio de los derechos a la libertad de expresión y reunión a través de Internet, afectando la libre circulación de información."[21]

La CIDH ha advertido que las actividades de vigilancia en Internet son contrarias al derecho a la privacidad y protección de datos personales. Mostró preocupación porque este tipo de seguimiento en línea estaría siendo utilizado como un medio para la identificación de periodistas independientes y disidentes políticos, lo que llevaría al uso de patrones de hostigamiento contra estas personas.[22]

Por otra parte, en Cuba también existe la ley 88, también conocida como Ley Mordaza, que ha sido usada para reprimir el periodismo independiente en la isla y a toda acción que apoye, facilite, o colabore con los objetivos de la Ley Helms-Burton, ley estadounidense que refuerza el embargo a la isla.

A pesar de que es una ley de 1999, mucho antes de la llegada del Internet a la isla, el presidente del Tribunal Supremo Popular de Cuba, Rubén Remigio Ferro, amenazó desde su cuenta en Twitter, a mediados del 2019, con recrudecer la aplicación de esta ley.

Haciendo uso de la Ley Mordaza, en marzo de 2003, el régimen de Fidel Castro metió a la cárcel a 74 hombres y una mujer, de ellos 27 eran periodistas. Estos sucesos se conocen como la primavera negra.

5 I En datos: los bloqueos digitales en Cuba

En este proyecto, nos propusimos iniciar el proceso de diagnóstico para identificar cómo es el comportamiento de los bloqueos en Cuba y así obtener una caracterización preliminar útil para los periodistas y defensores de derechos digitales.

Empezamos utilizando la técnica de scraping, haciendo uso de la herramienta gratuita web scraper, se descargaron todas las anomalías reportadas por OONI, entre el 1 de septiembre de 2019 al 1 de septiembre de 2020, pertenecientes a la isla de Cuba.

Aunque no se utilizó en este caso, tal como se ha comentado en el punto 3 de este informe, OONI también tiene una API disponible que permite realizar su propio análisis de los datos.

En total, se descargaron 315 anomalías que incluían el dominio, el número de ASN, la fecha y hora, y el enlace al reporte de Ooni. Esta información se utilizó luego como base para la creación de una hoja de cálculo con estructura propia. La estructura consistía en una columna para el número de bloqueo, otras para la fecha, el año, mes, día, nombre del afectado, el dominio y la categoría. También se añadió el tipo de ataque reportado (si era de DNS, HTTP o IP), la empresa telefónica desde donde se reportó el bloqueo (ASN), el número de veces que aparece un afectado durante el período de tiempo analizado y el enlace al reporte.

En el caso de las categorías, se tomaron como referencia las indicadas por el Citizen Lab de la Universidad de Toronto. Estas categorías van desde los medios de comunicación, el activismo, la cultura y los derechos humanos hasta las más provocativas u objetables, como la pornografía.

---

[21] http://www.oas.org/es/cidh/informes/pdfs/Cuba2020-es.pdf.

[22]https://freedomhouse.org/es/article/apoyo-internacional-la-peticion-para-declarar-inconstitucional-el-decreto-ley-370-en-cuba

En cuanto al ASN, número de sistema autónomo o identificador único, OONI Probe los recopila para identificar la red en la que se realizó cada prueba.

Un proveedor de servicios de Internet (ISP) generalmente tiene un ASN registrado oficialmente (y puede tener más de un ASN). Si buscamos un número ASN en un motor de búsqueda web (como Google) se mostrará a qué ISP corresponde. Por ejemplo, la búsqueda de "AS 27725" debería devolver "Empresa de Telecomunicaciones de Cuba, S.A".

Todas las anomalías registradas, en este caso, pertenecen al mismo proveedor de servicios de Internet: La empresa de Telecomunicaciones de Cuba.

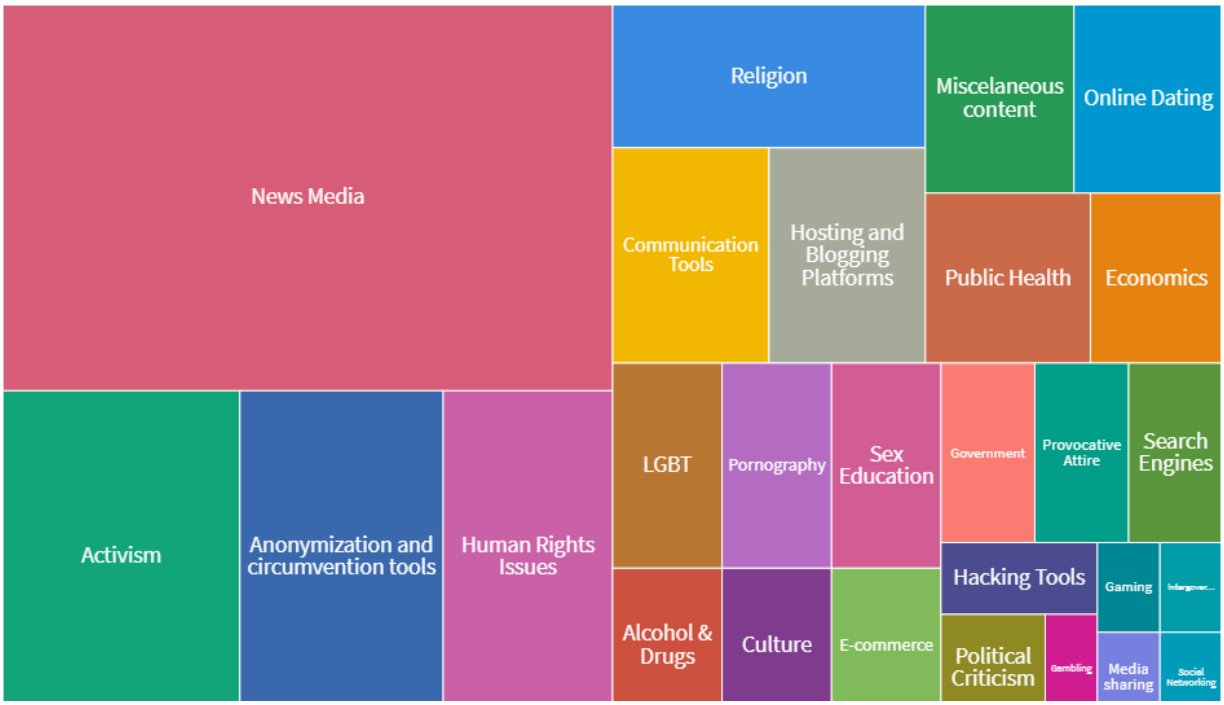
Hallazgos y evidencias de bloqueos en Cuba

Esta hoja de cálculo trajo consigo una serie de hallazgos que mencionaremos a continuación. Se realizaron tablas dinámicas para obtener los resultados mencionados.

En cuanto al número de bloqueos por categoría, podemos concluir que los medios de comunicación (News Media) son la categoría más afectada. Se reportaron 45 bloqueos durante el período de 12 meses recopilado. Es decir, casi el 27% de los reportes recogidos.

Le siguen los dominios relacionados con la categoría de activismo (activism), con 14 bloqueos, y la categoría de herramientas de anonimización y elusión (Anonymization and circumvention tools) con 12 bloqueos. Por el contrario, las categorías que reportan menor número de bloqueos son las de apuestas (gambling), juegos (gaming), uso compartido de medios (media sharing) y redes sociales (social networking). Cada una de estas categorías solo reportan un bloqueo durante el período de un año.

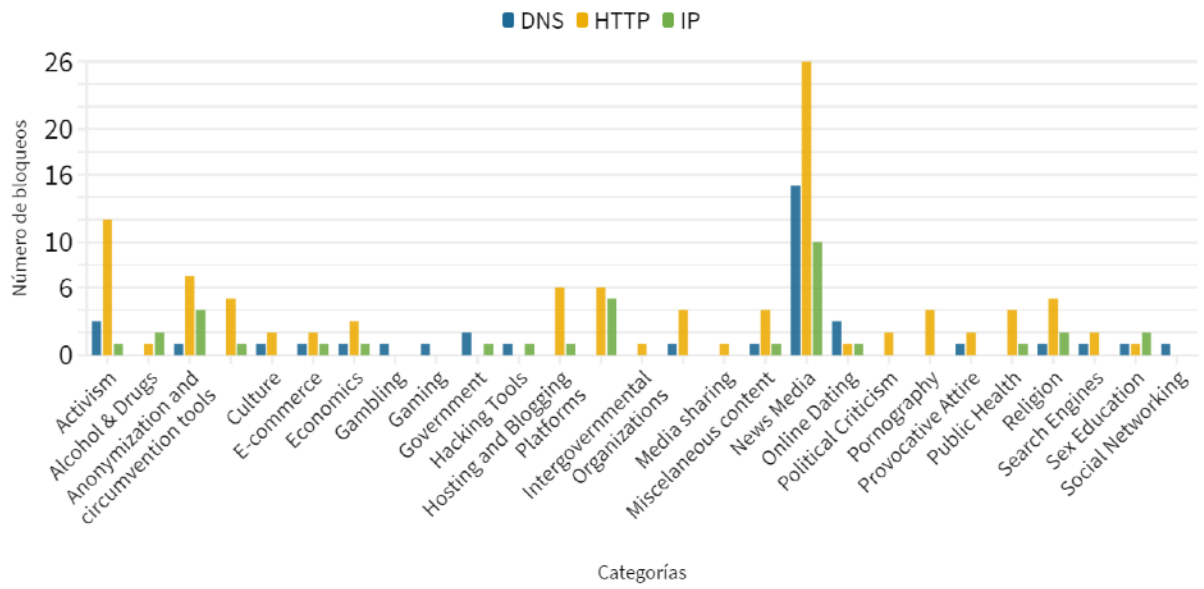
Número de bloqueos por categoría



https://public.flourish.studio/visualisation/4128738/

Al hablar de tipos de bloqueos por categorías, encontramos que la mayoría de los bloqueos son de HTTP, en 101 ocasiones se repiten. La categoría de medios de comunicación (News Media) recibió 16 ataques de HTTP, 15 de DNS y 10 de IPs. El bloqueo de DNS es el segundo favorito, con 37 reportados, seguido muy de cerca por el bloqueo de IPs que se repite en 35 ocasiones.
En la categoría de activismo (activism) también son los bloqueos de HTTP los que lideran, seguidos por los DNS y luego los de IPs.

Tipos de bloqueos por categoría

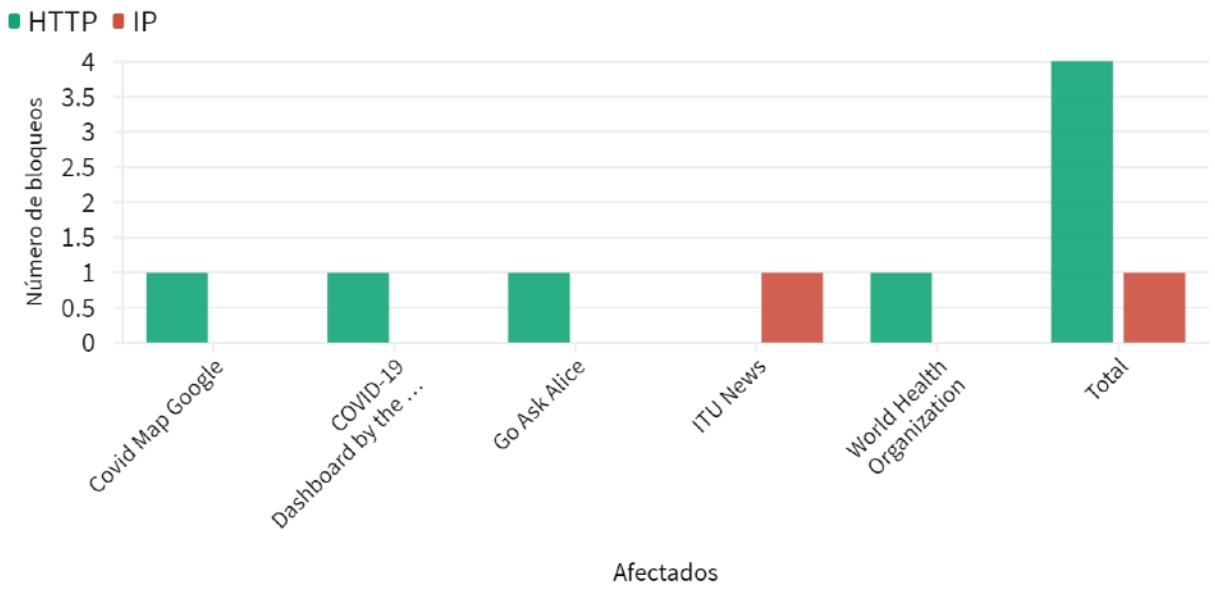


https://public.flourish.studio/visualisation/4128865/

Cabe destacar que en los datos recogidos hemos observado dominios atacados con información sobre salud y el COVID-19, la pandemia que afecta al mundo actualmente. Algunos de los dominios afectados son los correspondientes al Covid Map Google, COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University, Go Ask Alice, ITU News y World Health Organization. En su mayoría se reportan bloqueos de HTTP, solo al ITU News le corresponde un bloqueo de IP.

Periodistas consultados comentaron que la información que reciben sobre la COVID-19 la controla el Estado, y que no tienen forma de contrastar las versiones oficiales.

Tipo de bloqueos en páginas con información sobre COVID



https://public.flourish.studio/visualisation/4129208/

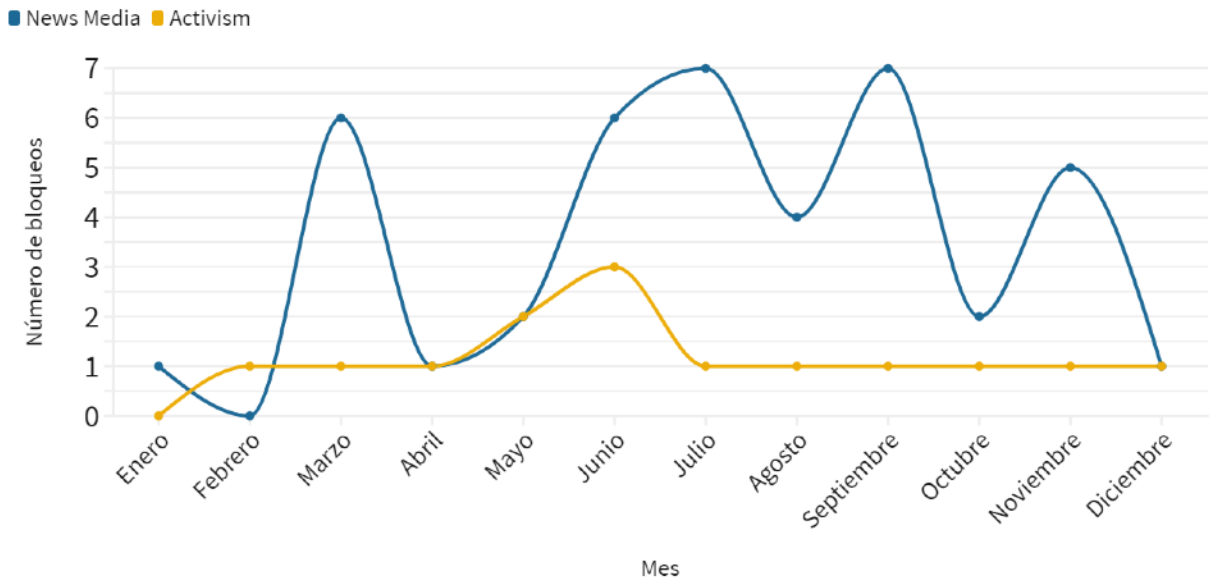
Tal como se precisó anteriormente, los dominios correspondientes a los medios de comunicación (News Media) son los más afectados por bloqueos. Pueden sufrir tanto bloqueos de DNS, como de HTTP e IP al mismo tiempo. Un ejemplo es el medio Cubanet que se reporta ha sufrido esos tres tipos de bloqueos. Hemos a su vez categorizado a los medios por locales o internacionales. En 26 medios locales se reportan bloqueos así como en 16 medios internacionales.

Afectado	Tipo de medio	HTTP	DNS	IP
14 y medio	Local		1	1
9/11 facts	Local		1	
ADN Cuba	Local	1		
Asere	Local		1	
BBC News	Internacional		1	
Ciber Cuba (http)	Local		1	1
Ciber Cuba (https)	Local			1
Convivencia	Local	1		
Cuba debate (español)	Local		1	
Cuba debate Inglés	Local	1		
Cuba Democracia y Vida	Local	1		
Cuba Encuentro	Local	1		
Cuba Posible	Local		1	
Cuban Art News	Local		1	
Cubanet	Local	1	1	1
Cubanology	Local	1		
Diario de Cuba (http)	Local	1		
Diario de Cuba (https)	Local	1		
Fundación Gabo	Internacional	1		
Fundación Nuevo Periodismo	Internacional	1		
Gawker	Internacional	1		
Global Investigative Journalism Network	Internacional	1		1
Global Voices	Internacional	1		
Journalism Courses	Internacional			1
Korean Central News Agency	Internacional	1		
Los Angeles Times	Internacional			1
Miscelaneas de Cuba	Local		1	
Net for Cuba	Local	1		
News Feed	Internacional	1	1	
Nieman Foundation	Internacional			1
Nuevo acción	Local	1		
Periodico Cubano	Local	1	1	
Proceso	Internacional	1		
Radio Televisión Martí	Local		1	
Revista El Estornudo	Local	1		
Revista Gatopardo	Internacional			1
Revista Ideal	Local	1		
Revista Tremenda Nota	Local			1
The Real Cuba	Local	1		
UN News	Internacional	1		
Vitral	Internacional	1		
Voa News	Internacional	1	1	
Total		26	14	10

https://public.flourish.studio/visualisation/4129339/

Se hizo también un análisis mes a mes de los bloqueos en las principales categorías afectadas: News Media y Activism. En el mes de julio y el mes de septiembre se observa el mayor número de bloqueos para medios de comunicación (7 en cada mes). Seguido del mes de julio y el mes de marzo (con 6 bloqueos). En el caso de los dominios con corte activista, el mes de julio fue el más afectado (con 6 bloqueos). Los demás meses se notaron estables. Por lo tanto, no se encuentra ningún patrón de bloqueo a nivel mensual.

Bloqueos mes a mes a páginas de medios de comunicación y de corte activista



https://public.flourish.studio/visualisation/4131116/

De igual manera, se realizó una tabla dinámica para determinar cuáles eran las páginas que más se repiten en los bloqueos reportados por Ooni. Se determinó que change.org, una plataforma de peticiones donde se inician campañas para recolectar dinero, aparece en 15 ocasiones con bloqueos de HTTP y DNS. Le sigue la propia página de Ooni que aparece en 9 ocasiones con bloqueos de HTTP e IP. Y medios de comunicación locales como Cubanet, Diario de Cuba y Periodico Cubano que aparecen en 6 ocasiones cada uno. Algunos de estos bloqueos fueron también identificados por periodistas de la isla que fueron consultados para este manual.

Con la plataforma de Ooni no hay manera de determinar si un bloqueo es temporal o permanente. Sin embargo, el número de repeticiones permite dar luces sobre la recurrencia de los bloqueos.

Páginas que más se repiten en los bloqueos reportados por Ooni

https://public.flourish.studio/visualisation/4162962/

Un punto que nos llamó la atención es que, durante el periodo de tiempo analizado, no se observaron bloqueos recurrentes a redes sociales. Solo a la plataforma de Tik Tok que aparece en 3 ocasiones con bloqueos de DNS

En cuanto a las herramientas de comunicación o mensajería de texto bloqueadas aparecen Zoom, Google Group, ambas con bloqueos de HTTP, y Textra SMS con bloqueo de IP. Durante este periodo de un año, de septiembre de 2019 a septiembre de 2020, no se reportaron bloqueos a Telegram ni a Whatsapp.

Sin embargo, desde mediados de octubre de 2020, Ooni comenzó a reportar anomalías en Telegram ..Las pruebas de octubre indicaban que el app móvil de Telegram y interfaz web presentaron signos de bloqueos por parte de la Empresa de Telecomunicaciones de Cuba, S.A. Dichos bloqueos fueron denunciados también en redes sociales por activistas y periodistas de la isla. Sin embargo, un meses después periodistas cubanos que fueron consultados refirieron que el bloqueo no había mantenido la misma magnitud en el tiempo que se mantienen hasta la finalización de este informe.

5.1 I Percepción de los bloqueos desde la isla. Entrevistas a periodistas cubanos.

Entrevistamos a cuatro periodistas cubanos que se encuentran trabajando desde la isla, tres desde la Habana y un periodista en la provincia. Exploramos su percepción sobre los bloqueos digitales, cómo estos afectan su trabajo periodístico y qué vías toman o qué herramientas utilizan para sortearlos.

Compartimos los aportes de los periodistas, a quienes se les protege su identidad.

Noticias censuradas

Con respecto a las páginas que identificaron como bloqueadas en la isla y si se trataban de bloqueos temporales o continuos, los consultados refirieron varios medios, entre ellos, 14 y medio, Diario Revista, Paparazzi Cubano, Cubanet, Diario de Cuba, revista El Estornudo, Adn Cuba y Cibercuba. Dicen que en general todos los medios independientes alternativos están bloqueados. También hablaron de páginas

donde se hacen peticiones como el caso de Change.org, ya que “el régimen cubano no quiere que las personas se movilicen a raíz de una petición o de una causa”, según una de las entrevistadas.

Otras de las nombradas fueron, en general, páginas de becas en el extranjero, páginas de partidos políticos no reconocidos legalmente en Cuba y sitios web culturales independientes.

Refirieron que son sitios que se encuentran bloqueados de forma permanente. Sin embargo, sí han identificado que en algunas ocasiones pueden acceder a estas páginas, por periodos de tiempo muy cortos, sin uso de VPNs. No saben por qué suceden estos “desbloqueos” momentáneos.

Telegram bloqueado

Otro bloqueo que describieron fue el de Telegram, que ocurrió en octubre de 2020. Los periodistas ubicados en La Habana aseguraron que, para el momento de la consulta (un mes después cuando ocurrió esta censura), el bloqueo a Telegram ya se había levantado pero en ciertas ocasiones tenían dificultades para descargar fotos o archivos. Sin embargo, la periodista que se encuentra en la provincia dice que el bloqueo se mantiene.

Telegram es una app que ha visto incrementado su uso en Cuba porque se puede utilizar sin número de teléfono (solo para el registro) o sin necesidad de una tarjeta SIM aportando un mayor nivel de privacidad, debido al control Estatal sobre las redes de telecomunicaciones. También, Telegram se está utilizando mucho para crear y entrar a grupos. Sobre todo grupos de compra y venta (comercio electrónico) pero también grupos con tintes culturales o políticos. Telegram permite crear grupos de hasta 200 mil personas.

Los periodistas entrevistados especulan que por la expansión de estos grupos y el intercambio de información masiva que se está haciendo a través de Telegram es que el gobierno cubano busca bloquearla. Whatsapp es otra de las aplicaciones de mensajería que se utiliza con regularidad en la isla, ya que es la forma más sencilla de comunicarse con familiares que están en el exterior. Aplicaciones seguras como Signal no están tan masificadas ni son muy usadas. Pero, cada vez más periodistas y activistas la usan.

El bloqueo a Telegram trajo consigo que los ciudadanos cubanos sintieran más de cerca los bloqueos digitales. Inclusive empezaron a rodar por redes sociales links de descargas a VPNs y muchas más personas comenzaron a utilizarlos. De acuerdo a la información obtenida, esto también generó bloqueos a páginas de VPNs. Uno de los periodistas entrevistados usaba de manera gratuita “Secure VPN” y aseguró que la aplicación dejó de funcionar luego de los bloqueos de mediados de octubre de 2020.

“El bloqueo de Telegram nos permitió conectar con la gente. El bloqueo hizo que las personas se dieran cuenta que nosotros sufrimos este tipo de bloqueo y también que entendieran cómo es que se le puede restringir el acceso a la información. De alguna manera, en mi opinión personal, celebro un poco que haya ocurrido este apagón de Telegram para que las personas despertaran en este sentido y entendieran que el régimen tiene también diversas maneras de poder cortarle el acceso a la información”, contó uno de los periodistas de la Habana entrevistado.

Un periodista de la provincia nos comentó que el VPN que más utiliza es Psiphon y es el que ha visto a más personas utilizando por ser gratuito. La mayoría de los cubanos no pueden acceder a VPNs de pago por sus altos costos, si se comparan con el salario promedio de Cuba, y por la imposibilidad de hacer pagos online.

Según los periodistas entrevistados, los ciudadanos cubanos cada vez usan más los VPNs gratuitos al momento de acceder a Internet. Lo hacen de manera automática, muchas veces sin saber si una página está bloqueada o no, sobre todo para acceder a contenido de otros países. Los consiguen usualmente en la Google Store.

A pesar del reciente bloqueo de Telegram, los periodistas entrevistados comentaron que, hasta noviembre de 2020, las redes sociales no estaban bloqueadas en la isla. Por ejemplo, Facebook o Twitter podían utilizarse sin problemas. Para ese momento, lo que sí sucedía eran bloqueos a ciertos grupos o perfiles en redes sociales.

Bloqueos intermitentes

Los periodistas también refirieron intermitencias en los bloqueos. Expresaron que las páginas de noticias, por ejemplo, no siempre estaban bloqueadas. Pero, sí destacaron que hay momentos específicos donde hay bloqueos o mayor control por parte del gobierno.

Suspensión de la conectividad

Los consultados aseguraron que el pasado 20 de octubre, día de la cultura nacional en Cuba, a muchos periodistas y activistas les quitaron los datos móviles. Ese día iba a haber una gran movilización por las redes sociales y también en actividades culturales auspiciadas por proyectos independientes.

El quitar acceso a datos móviles es otra de las formas de censura impuestas por el gobierno cubano. La Empresa de Telecomunicaciones de Cuba (ETECSA) es la única que proporciona servicio de telefonía móvil e Internet en el país y está manejada por el gobierno. Los periodistas denunciaron la falta de señal para acceder a datos móviles en ciertos momentos y también la desaparición de crédito para uso de Internet dentro del teléfono, sobre todo cuando se trata de bonos de crédito obtenidos por pagos que se realizan desde el exterior.

Actualmente en Cuba, gran parte de los ciudadanos se conectan desde su teléfono móvil, y los llamados puntos de WIFI se utilizan menos.

Las imágenes que en su momento se veían de las personas tratando de conectarse en masa desde los parques o plazas al WIFI han quedado atrás. Los periodistas comentaron que desde la llegada de la telefonía móvil 2g y 3g, en 2018, los ciudadanos prefieren conectarse desde la comodidad y seguridad de su casa. A pesar que acceder a datos móviles es más costoso que acceder al WIFI en sitios públicos.

Los puntos de WIFI en lugares públicos siguen utilizándose cuando se quieren descargar archivos pesados como películas, vídeos o música. Pero, no para temas o conversaciones delicadas debido a que los agentes de seguridad del Estado monitorean estos espacios, aseguraron. Para el momento de la consulta, se encontraban limitados por las restricciones de la pandemia.

Lo otro son los altos precios para acceder a Internet. El acceso a 1GB de datos móviles puede costar 10 dólares, cuando el salario mínimo cubano equivale a 15 dólares. Así que los altos precios más los bloqueos digitales dificultan el acceso a los ciudadanos a información considerada contra a la revolución..

Restricciones en pandemia

El control de contenido se amolda al contexto. Así ha pasado con respecto a la posibilidad de consultar información digital en relación a la pandemia del coronavirus.que la única fuente que tenían, hasta

noviembre de 2020, para acceder a datos oficiales es el Ministerio de Salud Pública y sus informes. Sin embargo, el problema era que no había manera de contrastar esa información. Informaron que sí había datos disponibles ,pero los ciudadanos no confiaban en su veracidad. También consideraron que el bloqueo no ocurría, necesariamente, por la pandemia sino porque es una política de Estado el bloquear páginas informativas.

En el capítulo 4 de este informe, se habló sobre el uso del decreto 370 para restringir el acceso libre al Internet en la isla y como una manera de punir a los medios digitales. Los periodistas entrevistados comentaron que este decreto se ha aplicado en pocas ocasiones en Cuba y que se utiliza más como una forma de coacción. De igual manera, como con la Ley Mordaza que se usa para amenazar al periodismo independiente.

Sin embargo, los periodistas entrevistados se preocupan más por la presión que ejercen los agentes de seguridad del Estado. “Ocurre denigración social en el entorno donde vivimos, sometimiento a interrogatorios, interrogatorio a familiares y amigos”, describieron los periodistas. Hay muchas maneras de castigar e intimidar fuera del entorno digital. “Nos obstaculizan cosas tan sencillas como que un albañil vaya a tu casa o que alguien te alquile una vivienda”, dijo uno de los consultados

Los periodistas entrevistados lamentaron que sus publicaciones se puedan leer más en el exterior que dentro de sus comunidades. Creen que ese es el mayor impacto de los bloqueos: que los ciudadanos cubanos dentro de la isla no puedan tener acceso al periodismo independiente sin uso de un VPN o proxy.

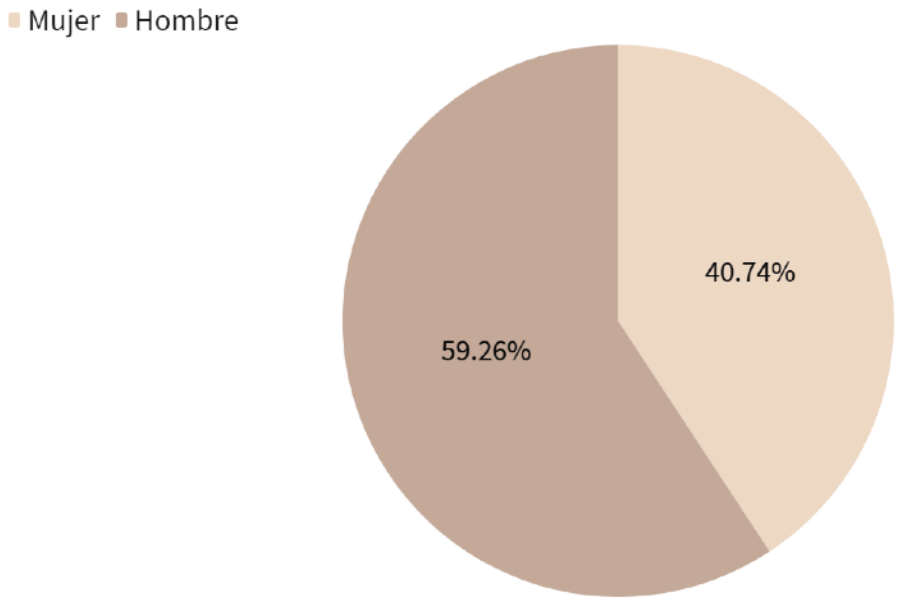
Para conocer más al respecto y tener un panorama general de la situación, decidimos realizar una consulta exploratoria con un número mayor de periodistas.

6 | Consulta exploratoria con periodistas cubanos: restricciones de conectividad y flujo de contenido

A la par de chequear los bloqueos reportados por OONI, sistematizar lo que han reportado organismos internacionales y hacer las entrevistas con estos cuatro periodistas, para este proyecto realizamos una encuesta a trabajadores de medios digitales en Cuba, para así tener un panorama más amplio de la disponibilidad del acceso a Internet y la frecuencia de los bloqueos.

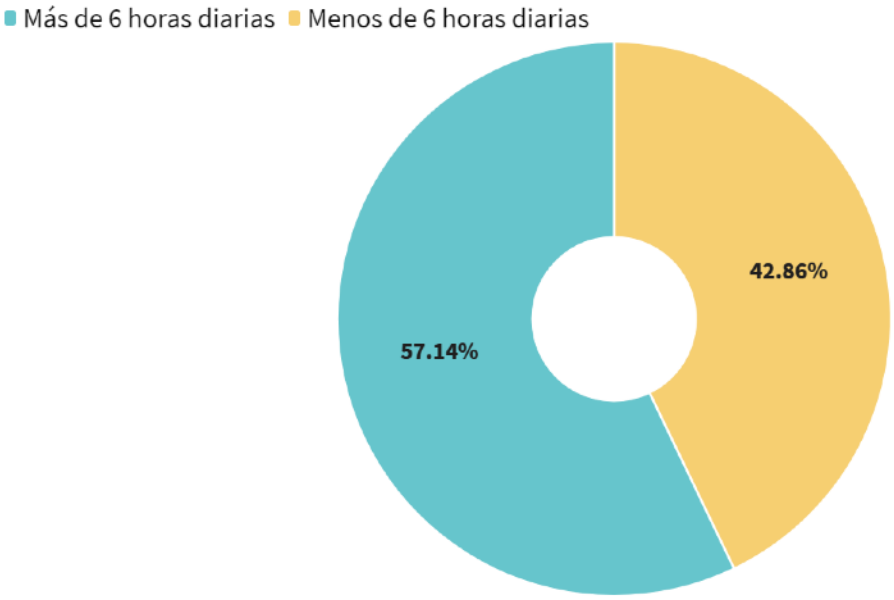
La encuesta fue respondida por 28 personas, en su mayoría del sexo masculino. Cabe destacar que se proporcionaron también las opciones de “otro género” o “prefiero no responder”.

Género de los encuestados



La segunda pregunta que se proporcionó, ya entrando en materia, se refería a la frecuencia de conectividad a Internet. Las opciones dadas fueron: más de 6 horas diarias, menos de 6 horas diarias, cada dos o tres días, cada cuatro o seis días, una vez por semana y menos de una vez por semana. Las respuestas se dividieron solo entre la primera y la segunda opción. Así que se puede concluir que se tiene acceso a Internet diariamente.

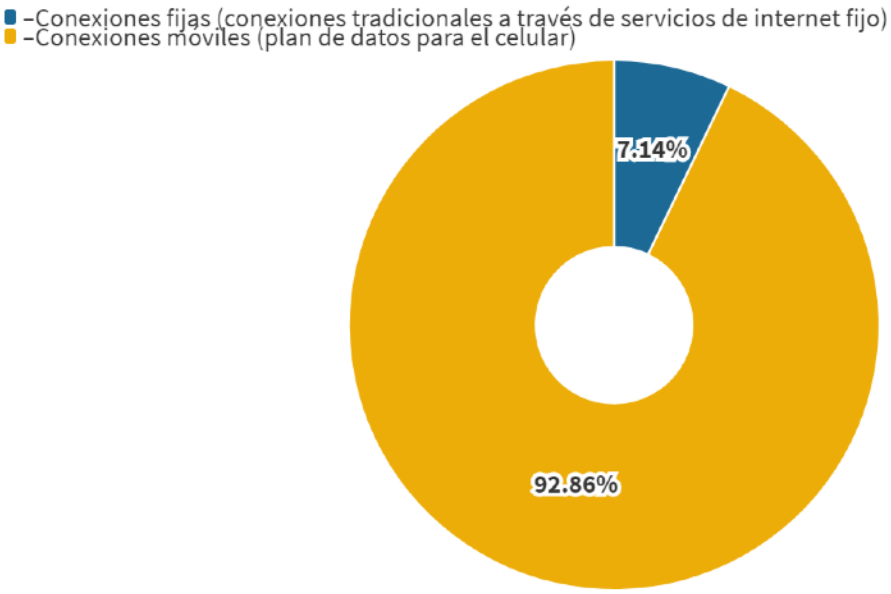
¿Cuál es su frecuencia de conectividad a Internet?



https://public.flourish.studio/visualisation/4141976/

La siguiente pregunta tenía como objetivo saber cuál es la banda por la que se conectan a Internet con frecuencia. Si se hacía uso de conexiones móviles, conexiones fijas o conexiones públicas. El 92,82% respondió que se conecta a Internet con mayor frecuencia a través de conexiones móviles o planes de datos para el teléfono celular. Seguido de solo un 7,4% que respondió conexiones fijas. Ninguno de los encuestados respondió que usa con frecuencia los puntos de wifi públicos.

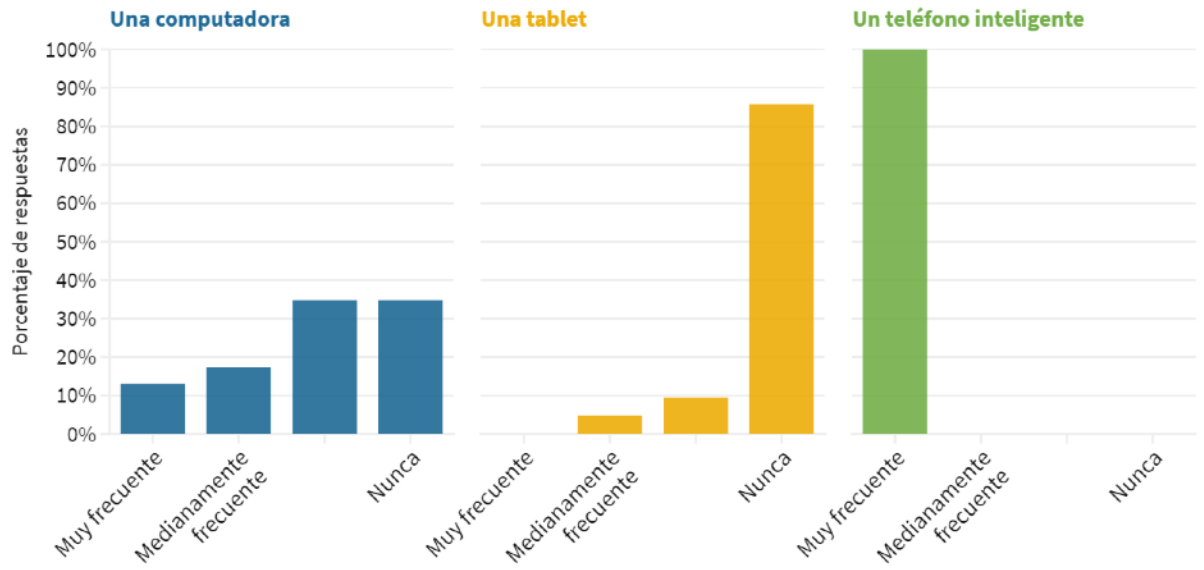
¿Cuál es la banda por la que se conecta a Internet con frecuencia?



https://app.flourish.studio/visualisation/4142113/edit?

La cuarta pregunta buscaba conocer qué dispositivos en Cuba se utilizan con más frecuencia para navegar en Internet. Se dieron como opciones de comparación una computadora, una tablet y un teléfono inteligente. El móvil se sitúa como el dispositivo usado con mayor frecuencia, seguido de la computadora y por último la tablet.

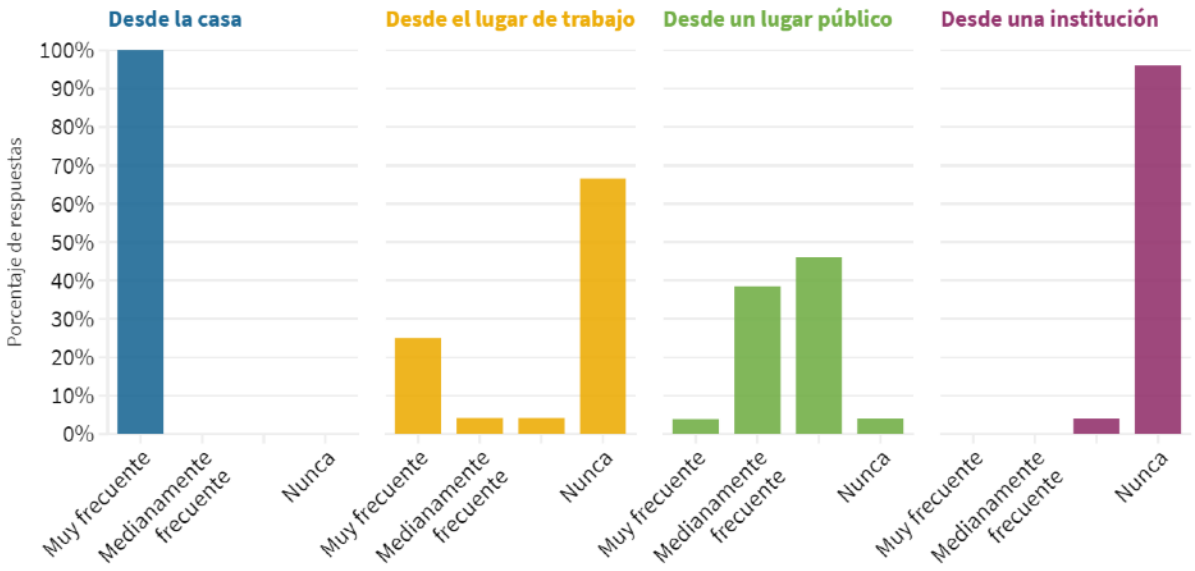
¿Qué dispositivos y con qué frecuencia los utiliza para navegar en Internet?



https://public.flourish.studio/visualisation/4142208/

También se le realizó una pregunta sobre el lugar desde que se conectaban a Internet y la frecuencia. Se les presentó cuatro opciones: desde la casa, desde el lugar de trabajo, desde un lugar público con un WIFI público (Plaza, por ejemplo) o desde una institución del Estado. En este caso, todos los encuestados respondieron que la casa es el lugar desde donde se conectan a la web con mayor frecuencia y una institución del gobierno es la opción menos frecuente o casi inexistente.

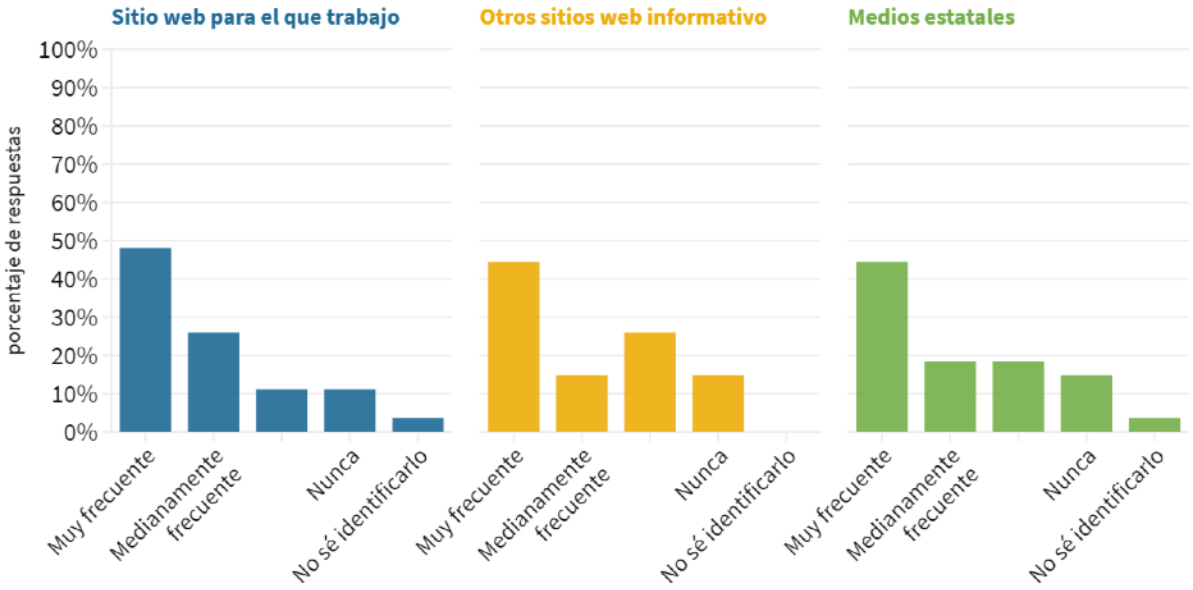
¿Desde qué lugar y con qué frecuencia tiene acceso a Internet?



https://public.flourish.studio/visualisation/4143060/

Otra pregunta que hicimos, relacionada también a la anterior, era con qué frecuencia se puede acceder a los medios de comunicación. Queríamos comparar la posibilidad de acceso a medios estatales con otros también de carácter informativo. Esta pregunta tuvo respuestas más equitativas por lo que no se puede llegar a una conclusión certera.

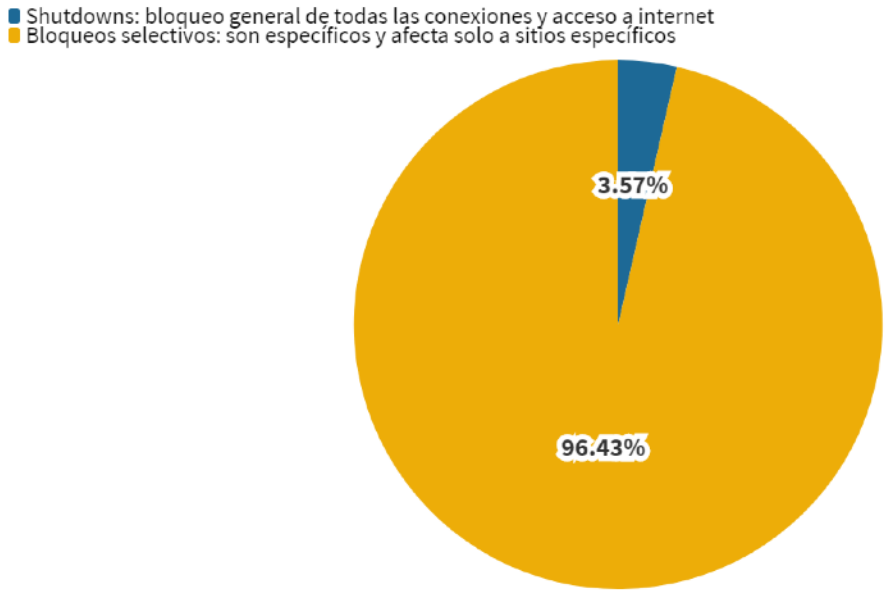
¿Con qué frecuencia puede acceder a los medios de comunicación más próximos a usted?



https://public.flourish.studio/visualisation/4154216/

También nos interesaba saber cuál era la percepción de los locales sobre los bloqueos en Internet y conocer más sus experiencias de navegación. El 96,43% de los encuestados respondieron que los bloqueos son selectivos, es decir, que son específicos y afecta solo a sitios específicos. Solo un 3,57% respondió que describiría a los bloqueos como shutdowns, es decir, bloqueos generales de todas las conexiones y acceso a Internet. Se tenían también otras dos opciones de respuesta: “Bloqueos masivos: son generalizados” y “Bloqueos intermitentes: a veces está disponible cierto sitios web y otras veces no” pero ninguno de los encuestados señaló estas opciones para describir los bloqueos en la isla.

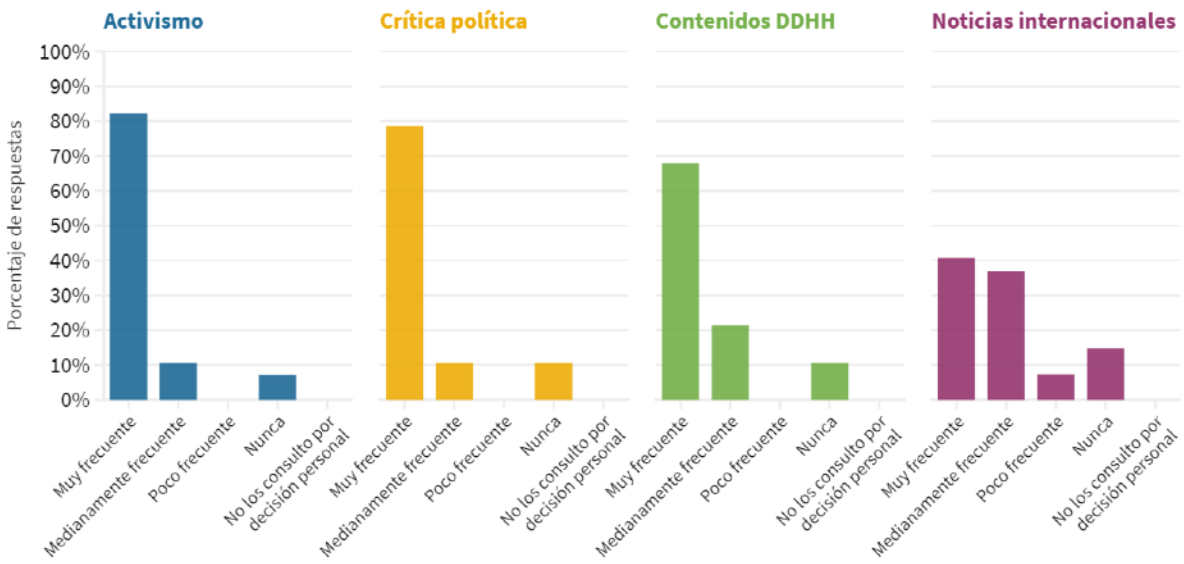
¿Cómo describiría la modalidad de los bloqueos en Internet, desde su experiencia de navegación, y cuál es su frecuencia?



https://public.flourish.studio/visualisation/4154085/

Otra de las preguntas estuvo relacionada con las restricciones de acceso. Se le preguntó a los encuestados con qué frecuencia tienen restricciones de acceso ciertos sitios web y se les dio un listado de categorías en los que se incluyeron: sitios web con información LGTBI, educación, salud, e-commerce, política, etc. Los sitios web que con más frecuencia sufren bloqueos, según los encuestados, son los relacionados al activismo, crítica política, con contenido u organismos de Derechos Humanos y noticias internacionales.

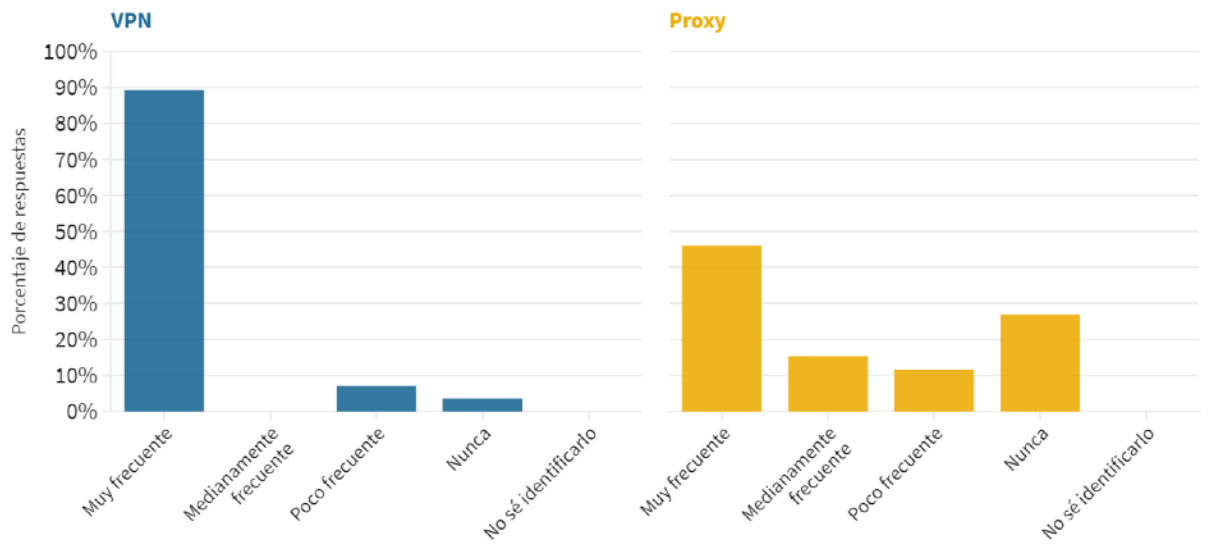
¿En cuáles de los siguientes tipos de sitios web tiene restricciones de acceso y con qué frecuencia?



https://public.flourish.studio/visualisation/4143126/

Los encuestados informan que la herramienta más frecuentemente utilizada para sortear los bloqueos es el VPN. Aunque también se hace uso del Proxy aunque en una medida considerablemente menor.

¿Utiliza algunas de las siguientes herramientas para sortear los bloqueos?



https://public.flourish.studio/visualisation/4154512/

Finalmente les pedimos que comentaran o describieran las condiciones generales de los servicios de Internet y la disponibilidad de contenidos desde el lugar donde vive. En su mayoría hablan de la mala conexión, la lentitud para la descarga de documentos o imágenes y los altos precios para acceder a Internet. También comentan sobre los bloqueos selectivos a páginas web y la necesidad del uso de VPN. A continuación citamos algunos de los comentarios más destacables:

-“En muchas ocasiones la señal es inestable o se ralentizan las conexiones. Hay muchos contenidos bloqueados por interés del monopolio estatal de las comunicaciones en Cuba. Mi acceso a Internet es susceptible de suspensión por parte del Gobierno y se me ha interrumpido el servicio en varias ocasiones.”

-”Las condiciones generales de los servicios de Internet que uso que son Nauta Hogar a una velocidad de 2 Mbps y Datos móviles 4G no son para nada las mejores. Dependiendo de la actividad que esté realizando y como esté la economía en ese momento uso una u otra. La conexión puede ser inestable y lenta. Aún así me siento privilegiada en comparación con muchos cubanos que no pueden conectarse fácilmente o que no lo han hecho nunca. El gobierno se toma la libertad de bloquear los sitios web de las diferentes voces alternativas en la Isla, así como diferentes contenidos en línea. También le han cortado el servicio de Internet a través de datos móviles a activistas y periodistas en momentos de protestas y actividades.”

-“Es bastante rápida la conectividad, lo más preocupante es el bloqueo de determinadas páginas web y la vigilancia y el espionaje desmedido por parte del régimen cubano hacia todos los ciudadanos. En otro orden también están las interrupciones del servicio en ocasiones por reparaciones técnicas y otras selectivas por cuestiones políticas.”

-“La conexión puede ser suspendida de modo selectivo si se conoce por las autoridades que participaré en un evento internacional vía Internet. Las tarifas son excesivas y no queda claro cuál es el consumo porque el crédito puede desaparecer de nuestros dispositivos.”

-“La conectividad se ha ido ampliando pero el servicio no es estable, hay momentos en que la red colapsa y no se puede navegar o se ralentiza. Sitios .informativos de interés están bloqueados y acceder con vpn comporta mayor consumo de datos y lentitud para cargar las páginas. Llama la atención que el número de sitios bloqueados ha ido en aumento. El servicio sigue siendo caro y el ministerio de informática y comunicaciones es el único proveedor del servicio.”

-“Decir que en Cuba la Internet es muy cara además de inestable. Muchos sitios sufren bloqueos selectivos y otros intermitentes lo que nos obliga en muchos casos a usar VPN o proxy anónimo. Además la única empresa que hay de telecomunicaciones es del Estado y responde a los intereses del gobierno, así que el día que la Seguridad del Estado lo ordena hacen corte selectivo del servicio de datos móviles a activistas y periodistas independientes.”

-“En los servidores nacionales de Cuba están bloqueados la mayoría de medios independientes con noticias de la Isla, los portales de organismos internacionales de DDHH y también plataformas de activismo como Change.org. Con un monopolio estatal de telecomunicaciones, el Gobierno aplica la censura ampliamente y mantiene altos precios de conexión a Internet. Además de existir leyes que restringen la libre expresión en las redes.”

-“Conectividad 4G de calidad aceptable, más veloz si se usa VPN. Bloqueo constante de la información relacionada con el acontecer político cubano desde una perspectiva no oficial y el activismo pro derechos humanos. Para acceder a esos contenidos y otros de mi interés, es necesario usar VPN o Proxy.”

7 | Rastrear la censura: construcción de protocolos de testeo e investigación

En este sección ofrecemos algunas sugerencias que pueden orientar a periodistas y defensores de derechos digitales a seguirle el rastro a la censura digital.

Para construir un protocolo de monitoreo y de investigación de largo aliento sobre los bloqueos digitales, primero hay que pensar en estructurar un proceso de consulta empírica con una periodicidad establecida para poder llegar a hallazgos sólidos, con evidencias suficientemente estructuradas que permitan contar historias o ser fuente de datos para reportes de investigación con buenos sustentos.

Esta exploración puede estar orientada a encontrar cambios o establecer patrones de censura digital y sus variantes que pueden responder a un comportamiento similar en varios países, pero que tiene unas condiciones locales particulares.

Por eso, sugerimos 13 elementos esenciales para establecer un protocolo de testeo e investigación sobre los bloqueos digitales. Estas fases no sólo están compuestas por la dimensión técnica, también se soportan en criterios de investigación y estadísticos que le dar mayor rigurosidad a los estudios en este campo:

Se debe tomar en cuenta una serie de elementos:

- Manejo de la aplicación móvil de OONI Probe
- Recolección de evidencias de bloqueos
- Configuración de la muestra para testear
- Preparación de una encuesta digital
- Ejecución de las mediciones en comunidad, gestión del equipo y el testeo colectivo
- Análisis estadístico y periodístico de las pruebas
- Contar historias basadas en datos y evidencias

Para este proceso también se deben tomar en cuenta varios criterios de medición e investigación que van orientados a cuidar varios aspectos multidimensionales

Dimensión	**Criterios**
Mercado de telecomunicaciones	Pensar en la representatividad de las operadoras de internet fijas y móviles de mayor consumo y que sean de fácil acceso para la investigación
Territorial	Distribución geográfica, según el alcance que se plantee la investigación

Tecnológica	Disponibilidad de los equipos móviles de medición con los que cuenta el equipo
Contenido	Selección de sitios web a analizar, según las interferencias más predominantes en el flujo de contenidos
Perido	Criterios de días, bloques horarios y extensión del tiempo en los que se pueden hacer las mediciones, según la disponibilidad del equipo
Contexto	Evaluación de las condiciones legales, políticas y sociales del entorno local
Conectividad	Análisis previo de las condiciones de navegación
Homogeneidad de las mediciones	Mediciones basadas en criterios de la comunidad internacional Construcción de base de datos propias
Difusión de evidencias e historias	Contar historias basadas en datos y evidencias, que tengan rigurosidad y que aporten insumos sustanciales para la discusión pública

A continuación desarrollamos un paso a paso que puede iluminar la construcción de un protocolo de medición e investigación.

0.- Análisis previo de los datos disponibles: podemos empezar analizando los datos disponibles en repositorios globales, según lo que se haya reportado y documentado. Se sugiere la construcción y actualización de una base de datos propias que nos permita tener un diagnóstico general y tener un mirada completa del problema.

Una de las alternativas para comenzar, es construir una base de datos a partir de los datos disponibles de OONI Explorer. El proyecto de este manual tuvo unos primeros avances en la construcción de una base de datos para llegar a una evidencias preliminares, que luego pueden ir alimentando y perfeccionando en el tiempo.

1.- Conformación de una mesa de trabajo multidisciplinaria: es necesario pensar el problema de los bloqueos desde diversas dimensiones, buscar todas las aristas que estén al frente y que contribuyan a construir el mapa o el árbol del problema. Esto es posible con un trabajo en equipo. En este caso en particular, un equipo diverso de periodistas, estadísticos, informáticos, sociólogos, y de otras áreas de la ciencia pueden trabajar de manera colaborativa para pensar cómo abordar la complejidad de las mutaciones y las manifestaciones de los bloqueos digitales; y poner manos a la obra en todas las fases de investigación

2.- Establecer un plan de acción: es necesario trazar la hoja de ruta que orientará el proceso de documentación y descripción del comportamiento de la censura digital. Un plan claro y preciso permitirá la formulación de preguntas y la búsqueda de respuestas adecuadas sobre este fenómeno. Permitirá ver con claridad cuestionamientos sobre la operatividad de diversos sitios web, la disponibilidad de

contenidos y el derecho de los ciudadanos a consultar contenidos e información en las plataformas digitales. Esta, también, puede ser una herramienta útil para centrar todas las acciones a levantar y producir información verificable y sólida con respecto a las modalidades de los bloqueos digitales.

3.- Hacer un diagnóstico previo: con el levantamiento de la información disponible de diversas fuentes periodísticas, de organizaciones civiles y organismos internacionales podemos obtener un diagnóstico detallado de las estrategias que las principales teleoperadoras aplican de manera directa e indirecta para censurar contenidos en la red.

4.- **Establecer alianzas:** el monitoreo técnico es indispensable. Por eso, la alianza con organizaciones que ya tienen capacidad instalada en materia de censura digital es fundamental. Una de ellas puede ser el Open Observatory Of Network Interference, una comunidad global que ha tenido experiencias en distintas partes del mundo. Se puede pensar en organizaciones de libertad de expresión y derechos digitales de la región que estén interesadas en colaborar y tengan una trayectoria previa en estos temas.

5.- Establecer una red de colaboradores: puede ayudar incorporar el activismo ciudadano. Los investigadores, los periodistas y los defensores de los derechos digitales a veces no pueden solos. Es importante pensar cómo podemos tener más alcance. Muchas veces, la colaboración ciudadana inteligente, coordinada y estructurada puede aportarnos muchos beneficios. La colaboración ciudadana puede, por ejemplo, contribuir a obtener evidencias que se pueden recabar a través de su aplicación móvil OONI Probe, que es un software libre y de código abierto diseñado para medir la censura de internet, disponible para sistemas operativos Android y IOS. Los ciudadanos aliados pueden correr la prueba de conectividad web de OONI que está diseñada para medir de manera automática si los sitios web seleccionados están bloqueados en sus diferentes modalidades: DNS, HTTP, TCP/IP.

La selección de los aliados pasa por determinar si las personas potenciales para colaborar cumplen varias condiciones:

a) están dispuestas a colaborar y entienden los riesgos a los que se podrían enfrentar y están dispuestos a asumirlos;

b) tienen la disposición de tiempo y en actitud para participar en jornadas colaborativas y estructuradas;

c) son personas comprometidas y responsables;

d) tienen acceso a internet para correr las pruebas;

e) tienen la capacidad tecnológica que se requiere: un teléfono celular o una computadora;

f) tiene los conocimientos digitales que se requieren para hacer las mediciones o tiene la actitud para aprenderlos rápidamente.

Es muy importante establecer un perfil específico de los colaboradores. En investigaciones de otros países se ha trabajado con un grupo de colaboradores cuyo perfil se ha delimitado a periodistas, tomando en cuenta varios criterios:

a) están acostumbrados a trabajar bajo presión;

b) entienden los riesgos

c) saben cómo dirimir conflictos; y

d) guardar y respetar el carácter de confidencialidad en la información que se está recogiendo.

6.- Hacer una gestión y estructuración estratégica del equipo: el activismo ciudadano debe ser acompañado por la estructuración del equipo. Se recomienda hacerlo de manera esquemática. Establecer un número de colaboradores representativos de acuerdo a las dimensiones del estudio que se quiere realizar. En otros países donde se han hecho mediciones de gran alcance, se ha contado con la colaboración de 50 y 60 personas. El primer paso es abrir una hoja de cálculo y registrar a cada personas con datos básicos, del estado, proveedor, tipo de dispositivo móvil, identificación personal (nombre, apellido, correo electrónico). Además de ello, con el acompañamiento estadístico, se ha hecho una codificación de los colaboradores, para asignarles una identificación que debe utilizar en todo el proceso de campo.

En otras investigaciones, se ha establecido un grupo de coordinación que se distribuye la tarea de coordinar, hacer seguimiento, responder a solicitudes y resolver inconvenientes por zonas geográficas y también por subgrupos de colaboradores. En resumen: una gestión estratégica del equipo.

6.- Establecer una muestra de sitios web a evaluar: por las diversas dimensiones de la censura digital, el equipo de investigación debe decidir qué sitios web va a estudiar portales. Una manera estratégica de hacerlo es segmentando los grupos de sitios web. Se puede empezar analizando cuáles son los sitios con contenidos más sensibles.

Por las evidencias sistematizadas en este experiencia, podemos sugerir la conformación de una muestra que evalúe a una o varias categorías de contenidos que sean específico, y evitar tener una mirada general y completa del problema de los bloqueos digitales. Por ejemplo, se puede evaluar la categoría de sitios de medios nacionales e internacionales más consultados en el país; o sitios relacionados con contenido de activismo o crítica política. Incluso, a modo de sugerencia: por la coyuntura global, se puede segmentar la selección y elegir las web relacionadas con información de la COVID-19.

7.- Establecer mediciones previas: para llegar a un protocolo de medición acertado y efectivo, es útil incorporar una fase que permita realizar pruebas pilotos, que ayuden a corregir errores en el protocolo de medición y establecer parámetros adecuados, además que ayuda a que el equipo de colaboración y coordinación aprendan y se familiaricen con todos los procesos con antelación. Esto permite establecer el número de pruebas necesarias por proveedor, los días más convenientes de la semana, las franjas horarias en las que se puede ejecutar una medición simultánea de un grupo importante de colaboradores. Es importante lograr una ejecución simultánea de las mediciones, para darle mayor homogeneidad al estudio: todos haciendo la misma tarea en los mismos momentos.

8.- Determinar el plan de medición: para poder tener resultados de investigación sólidos que permitan determinar el comportamiento y la dimensión de los bloqueos, una prueba sola no basta. Es necesario tener representatividad y diversidad en las mediciones que permitan analizar un volumen importante de datos y encontrar patrones de comportamientos y discrepancias en cuanto a la dinámica de los bloqueos digitales. Las experiencias que se han desarrollado en otros países, han establecido cuatro días de

medición (que representen una semana), tres mediciones por día, distribuidos en los turnos de mañana, tarde y noche.

La disponibilidad de conectividad y de acceso a internet del país son determinantes en esta decisión, la cual, es recomendable consultarla con un equipo de estadístico, especialista en conformación de muestras y estudios de representatividad.

El protocolo de medición debe incluir las decisiones de los proveedores de internet a evaluar. Según esta decisión se debe establecer el número de colaboradores necesarios por cada proveedor, según las condiciones del mercado del país. Es importante pensar que los datos a obtener deben ser homogéneos y representativos.

9- Establecer un protocolo de coordinación: es indispensable crear unos estándares de entendimiento entre el equipo que lidera las mediciones y sus voluntarios. Esto implica la creación de manuales, términos de referencia, distribución de roles y responsabilidades, intercambio de información con conocimientos sobre el proceso y manejo de aplicaciones móviles para la captura de los datos, la creación de salas digitales de conversación para el seguimiento y el monitoreo de las jornadas de medición.

10.- Preparación de formularios digitales: cuando ya se ha conformado el equipo de voluntarios o colaboradores y se tiene claridad de la cobertura de las mediciones, los proveedores y los sitios web a evaluar, se establece un formulario digital que va a permitir recoger los datos de manera directa y en tiempo real. Esto va a facilitar el proceso del manejo de los datos. Se recomienda llenar un formulario por cada prueba corrida. El formulario debe tener una estructura sencilla, clara y corta. Es importante que tenga una usabilidad sencilla y se pueda llenar fácilmente y, sobre todo, que se pueda entender por sí solo y ser manejado de manera autoinstrucción. Las herramientas digitales gratuitas pueden servir para preparar el formulario.

Es importante que antes de las mediciones de campo, se pueda probar el formulario en una prueba piloto para hacer las correcciones que sean necesarias y que el equipo de investigación que se están recogiendo los datos necesarios de la manera correcta.

11.- Ejecutar el trabajo de campo y las mediciones: se puede pensar en jornadas de medición que se realicen en dos momentos. En la primera fase los colaboradores levantan simultáneamente pruebas a través de OONI Probe, desde sus dispositivos móviles. En la segunda fase, los colaboradores llevan los resultados obtenidos en las pruebas de OONI Probe a un formulario digital, el cual es recomendable que esté integrado a una base de datos. Este será el insumo principal para realizar el análisis de resultados. Cada miembro de la red de medición debe repetir la secuencia de la medición según se establezca en el diseño estadístico, pensando en tener unos datos robustos y con una amplia cobertura geográfica.

12.- Análisis de resultados: Durante la recolección de los datos y las mediciones de los colaboradores es necesario implementar un proceso de revisión, limpieza y organización de datos de las pruebas recibidas. Una vez que los datos estén bien estructurados se recomienda hacer un análisis estadístico,

que va a estructurar los resultados, e incluso encontrar la fortaleza y las limitaciones de los datos. Este intercambio es fundamental, para que los periodistas e investigadores interpretan correctamente los datos: saber qué decir, cómo decirlo y hasta dónde decirlo apeados a los criterios estadísticos y representativos.

Experiencias previas de otros países han permitido analizar estadísticamente más de 600 pruebas que han supuesto el análisis de 35 mil mediciones, entendiendo que cada sitio web de la lista corresponde a una medición.

El acompañamiento es fundamental incluso para pensar en establecer índices de bloqueos o una jerarquización de la gravedad de la dimensión de los bloqueos que se están encontrando.

El equipo estadístico va más allá: es muy útil en el proceso de revisión de las historias o el reporte final, para que certifiquen que lo que se diga ahí es lo que realmente reflejan los datos. Esto ayuda a corregir cualquier imprecisión antes de la publicación.

-**12: Entender el contexto y la delimitación de la investigación:** a la par de las mediciones y el avance del proceso de investigación, es fundamental documentar y analizar el contexto legal, político y social del país. Con ello, podemos encontrar similitudes con otros países o incluso rasgos muy propios del entorno local, que pueden hacer la diferencia en el comportamiento de la censura digital.

13-: Encontrar y contar las historias: luego que se tienen los datos, es necesario jerarquizar los hallazgos para saber cuáles son los realmente útiles para contar historias periodísticas e incluso para reportajes de investigación de largo o mediano aliento.

Este tipo de proyectos exigen la combinación de criterios periodísticos, criterios técnicos, una mirada multidisciplinario y estándares de derechos humanos y de derechos digitales, específicamente.

Es importante mostrar cómo afectan los bloqueos a los ciudadanos, soportado en un trabajo de reportería, y también incluir evidencias y declaraciones oficiales que muestren la versión tanto del Estado como de las operadoras.

De acuerdo con las fases previas, en las historias periodísticas sugerimos tomar en cuenta:

- Herramientas del periodismo y visualización de datos
- Gestión estratégica del equipo: tanto de investigación como de colaboración
- Involucrar a periodistas en el monitoreo técnico para encontrar evidencias
- Soporte metodológico y estadístico
- Análisis de la perspectiva de los derechos humanos en Internet

8 I Mapa de estrategias para sortear la censura digital

Antes de profundizar en las herramientas y estrategias para sortear la censura digital, se debe entender qué necesita una página web para funcionar. Las páginas web necesitan un dominio, que es el nombre único con el que la plataforma se muestra en Internet. http://ejemplo.com. En otros contextos se le conoce al nombre de dominio como URL, por el efecto localizador. Si vemos la página como una casa, el dominio es el nombre.

Lo siguiente es el hosting que es el espacio físico en el que se guardan los archivos de la página web. Suele venir asociado a especificaciones técnicas de una computadora junto con una tasa de transferencia. Esto es el tamaño y la dirección física de la casa. Luego necesita una programación backend, en este nivel se programan bases de datos y lógica de funcionamiento y finalmente la programación frontend, en este nivel se manejan todos los protocolos asociados a la interfaz de usuario

Existen tres ataques comunes que pueden recibir las páginas web. Uno de ellos es el SQL Inyection que se refiere a la inyección de código malicioso para saturar la recolección de datos de la página web. Otro puede ser el phishing que muestra un sitio web similar al nuestro o a la interfaz a la que se accede para manejar el contenido de nuestro sitio y un tercero es la denegación de servicio (DDOS) que consiste en saturar la tasa de transferencia del hosting

En cuanto a los bloqueos, pueden darse de diferentes tipos: basado en la plataforma (motores de búsqueda), basado en la inspección profunda de paquetes, basado en la URL, basado en los DNS, y basado en el protocolo y en la IP.

La data utilizada para la creación de este informe, se centró en el análisis de los últimos tres tipos de bloqueos mencionados. Bloqueos al HTTP, de DNS y en la IP.

Herramientas y estrategias para sortear la censura digital (Cómo aplicarlas y cómo obtenerlas)

Evadir la censura es el acto de sortear o burlar las prohibiciones que rigen el acceso a Internet. Hay muchas formas de hacer esto, pero casi todas las herramientas de evasión funcionan aproximadamente de la misma forma. Hacen que nuestro navegador Web tome un desvío a través de una computadora intermediaria, llamada proxy, que: está localizado en algún lugar que no está sujeto a la censura de Internet no ha sido bloqueado en nuestra localización sabe cómo buscar y devolver el contenido a usuarios como nosotros.[23]

Un proxy web es como un navegador incrustado dentro de una página web. Usualmente no es necesario instalar ningún programa en la computadora para utilizarlo. Entras a la URL del proxy web dentro de nuestro navegador, ingresas la URL que quieres chequear y listo.

Algunos proxys web gratuitos que pueden ser utilizados son PHProxy, Zelune, Glype y Picidae. Actualmente los navegadores, como Google Chrome, también permiten la configuración de proxys en sus opciones avanzadas.

Otra forma de sortear los bloqueos, sobre todo los de HTTP o IP, es con el uso de un VPN. El VPN cifra y envía todo el tráfico de Internet entre nuestra computadora y otra computadora, así que no solo hará que

[23] https://protege.la/wp-content/uploads/2018/05/0003_guia_bypassing-censorship-es.pdf

todo el tráfico de Internet parezca similar ante una “escucha” sino que el cifrado hará ilegible el tráfico del túnel a cualquiera que esté escuchando en el camino.

Mientras estamos conectados a una VPN el ISP no verá nuestro contenido, pero podrá ver que nos estamos conectando a una VPN. Como muchas compañías internacionales usan la tecnología VPN para conectar de forma segura sus oficinas remotas, es poco probable bloquear esta tecnología completamente.[24]

Algunos VPNs recomendados por expertos en seguridad digital son Psiphon, Pronton VPN o Lanthern. Además tienen versiones gratuitas descargables que funcionan bastante bien.

Otra manera de sortear la censura es el cambio del sistema de nombres de dominio. Los Proveedores de Servicio de Internet (ISP, por sus siglas en inglés), proporcionan una dirección IP que tramitan las solicitudes para acceder a las páginas web, básicamente ubicando las coordenadas numéricas que corresponden al nombre de la página a la cual se quiere acceder.

Cada Proveedor de Servicio de Internet, posee una librería de Direcciones IP, cuando se intenta ingresar a una página web, si la misma se encuentra dentro de esta librería podrás acceder, de lo contrario no te permitirá ingresar porque está bloqueada por este ISP.[25]

Cuando el DNS se cambia, la petición se envía al servidor que permite acceder a las páginas bloqueadas. Por ejemplo, si se utiliza como Proveedor de Servicio de la Empresa de Telecomunicaciones de Cuba, para poder acceder a algunos contenidos bloqueados por esta compañía, se puede cambiar el servidor de DNS del Proveedor de Internet por otro que no tenga bloqueado el contenido. Es importante resaltar que el cambio de DNS no garantiza el anonimato, es decir, el ISP podrá ver cuáles son las peticiones de acceso. El equipo de expertos digitales de Redes Ayuda recomienda utilizar servidores DNS de Google (8.8.8.8 y 8.8.8.4), Servidores de IBM (1.1.1.1) o Intra.

Para una seguridad más completa e impedir el rastreo de tu navegación online, se recomienda el uso de Tor Project. El Navegador Tor aísla cada sitio web que visitas de manera que rastreadores de terceros y publicidades no pueden seguirte. Las cookies se borran automáticamente cuando terminas la navegación. Como así también tu historial de navegación. Según informan en su página web, al usar Tor el tráfico es reenviado y cifrado tres veces. La red está comprendida por miles de servidores, ejecutados por voluntarios, conocidos como repetidores Tor. Por lo tanto, con este navegador eres libre de acceder a sitios que tu red local haya bloqueado.

Es importante decir que muchas de estas herramientas para sortear los bloqueos están también bloqueadas en Cuba. A continuación presentamos un listado de páginas web relacionadas con el anonimato en línea que han presentado al menos un bloqueo en los reportes de Ooni, durante el período del 1 de septiembre de 2019 al 1 de septiembre de 2020.

Afectado	**Dominio**
Jap	http://anon.inf.tu-dresden.de/

[24] https://protege.la/wp-content/uploads/2018/05/0003_guia_bypassing-censorship-es.pdf

[25] https://redesayuda.org/2019/06/13/ante-la-censura-del-regimen-herramientas-para-evadir-la-censura/

Anonymouse	http://anonymouse.org
The Proxy Authority	http://proxy.org
Trivia Security	http://triviasecurity.net
Mozilla	http://use-application-dns.net
Criptored	http://www.criptored.upm.es
1.1.1.1	https://1.1.1.1
Free DNS	https://freedns.afraid.org/
Dns Google	https://dns.google/
Ooni Tor Project	https://ooni.torproject.org
Tutanota	https://tutanota.com/es/
Pure VPN	https://www.purevpn.com/

9 I Glosario de la censura digital

Ofrecemos 28 conceptos y definiciones de la terminología indispensable que los periodistas y defensores de derechos digitales necesitan conocer para explorar, investigar y contar historias sobre la censura digital. Como toda lista es incompleta y puede considerarse como un compendio en construcción. Las definiciones provienen de aportes de organizaciones técnicas, de monitoreo y de estándares de libertad en la red.

A

1. **Acceso universal a Internet**: la Comisión Interamericana de Derechos Humanos, considera que esta "es una condición fundamental para la un Internet incluyente y para la libertad digital". Este organismo ha dicho que el entorno digital "requiere que los Estados garanticen la calidad e integridad del servicio de Internet protegiéndolo en todos los casos de bloqueos, interferencias o ralentizaciones arbitrarias". Para la CIDH, "la interrupción del acceso a Internet aplicada a poblaciones enteras o a segmentos de la población nunca está justificada, ni siquiera por razones de seguridad nacional.

B

2. **Bloqueos digitales**: son una forma de censura de contenidos en el entorno digital. Los bloqueos digitales pueden ser temporales o parciales. Según la CIDH, "afectan el ejercicio de los derechos humanos en línea". Se consideran una práctica basada en una política de control y regulación de la información, por parte de proveedores de Internet privados o estatales y, en algunos casos, con la actuación de instancias estatales. Organismos internacionales de derechos humanos, han considerado que los bloqueos digitales deben ser recursos extremos que sólo deben aplicarse en situaciones excepcionales, que deriven de decisiones judiciales dictadas por instancias legítimas y autónomas. En casos que se cumplan los principios de legalidad, necesidad y proporcionalidad, las decisiones de bloqueos excepcionales deben tomarse luego de un proceso riguroso, con una transparente evaluación y notificación del caso a los afectados. La CIDH considera que los bloqueos son suspensión de sitios web enteros o generalizados, plataformas, conductos, direcciones IP, extensiones de nombres de dominio, puertos, protocolos de red o cualquier tipo de aplicación, así como medidas encaminadas a eliminar enlaces (links), datos y sitios web del servidor en los que están alojados, constituyen una restricción que solo será excepcionalmente admisible en los estrictos términos establecidos en el artículo 13 de la Convención Americana. Las de bloqueos "deben, asimismo, ser autorizadas o impuestas atendiendo a las garantías procesales, según los términos de los artículos 8 y 25 de la Convención Americana".

3. **Bloqueo por DNS:** es el tipo de bloqueo a través del dominio de la página web. El Sistema de Nombres de Dominios (DNS, por sus siglas en inglés) puede entenderse como entre un **dominio** o nombre y la plataforma web que es un destino final. "Cuando la computadora de un usuario intenta utilizar un nombre bloqueado, el servidor especial devuelve información incorrecta, como la dirección IP de un servidor con un aviso que explica que el contenido se ha bloqueado. Otra posibilidad es que el servidor indique que el nombre no existe", según lo refiere un informe de Internet Society (ISOC).

4. **Bloqueo por HTTP / HTTPS**: este mecanismo interviene, restringe y redirige la ruta de navegación desde la propia ubicación en la web de la plataforma buscada. "Este control del tráfico en Internet es considerado más **efectivo** que el bloqueo de DNS, pero más costoso":

“porque el dispositivo de filtrado generalmente debe estar ubicado entre el usuario e Internet y, por lo tanto, requiere un elevado nivel de recursos para que su rendimiento sea aceptable”, dice ISOC.

5. **Bloqueo por IP:** representan prohibiciones para consultar páginas web, declarando como ilegal el IP o el TCP, que se entiende como la dirección de protocolo de Internet que se le asigna a cada conexión o dispositivo. El IP funciona como un número de localizador o un puerto asignado a cada usuario para su conexión a Internet.

6. **Bloqueo basado en la plataforma:** ISOC lo caracteriza como una restricción de contenido especialmente, en los motores de búsqueda. Esta organización ha dicho que forman parte del filtrado de información en medios sociales o buscadores web. Algunas empresas digitales y autoridades trabajan, de manera conjunta, para bloquear y evitar las descargas de aplicaciones específicas en algunos países.

C

7. **Censura digital:** es un mecanismo de interferencia de contenidos en plataformas y sitios de navegación en Internet. Investigaciones periodísticas han referido que puede entenderse como un una consecuencia que se deriva de los bloqueos que afectan la operatividad de diversos sitios web, la disponibilidad de contenidos y el derecho de los ciudadanos a consultar contenidos e información en las plataformas digitales. En muchos casos las restricciones de contenidos se aplican como medidas previas, o ex ante. La CIDH ha dicho que en ningún caso debe ser interrumpida “la circulación de cualquier contenido que tenga presunción de cobertura. Los sistemas de filtrado de contenidos impuestos por gobiernos o proveedores de servicios comerciales que no sean controlados por el usuario final constituyen una forma de censura previa y no representan una restricción justificada a la libertad de expresión”. La comisión también considera que las medidas de bloqueo de contenidos no se pueden utilizar para controlar o limitar la difusión de discursos especialmente protegidos o que tienen presunción de protección cuando dicha presunción no ha sido desvirtuada por una autoridad competente que ofrezca suficientes garantías de independencia, autonomía e imparcialidad. Los sistemas de bloqueo y filtrado de contenidos en Internet han generado con frecuencia el bloqueo de sitios de Internet y contenidos legítimos, y que algunos gobiernos han utilizado esta capacidad para impedir que la población pueda tener acceso a información fundamental de interés público que los gobiernos están interesados en oculta”.

8. **Conectividad web:** como lo ha definido OONI, este es un test de la metodología de OONI que examina distintos sitios web, algunos categorizados por el Citizen Lab de la Universidad de Toronto, o elegidos por el usuario de las pruebas de bloqueos en jornadas personalizadas de medición. Este test ofrece evidencias con respecto a la respuesta técnica para analizar si un sitio web o plataforma digital ha sido bloqueada o no. Los test de conectividad están diseñados para analizar diferentes problemas. Está diseñada para medir de manera automática si los sitios web seleccionados están bloqueados en sus diferentes modalidades: DNS, HTTP, TCP/IP.

9. **Consistencia de DNS:** es un test implementado por OONI que compara las solicitudes de los DNS (Sistema de nombre de dominio) con otra herramienta, que puede ser considerado una prueba de control. Su objetivo es detectar alteraciones.

D

10. **Derechos digitales:** son las garantías, en el plano individual y colectivo, para la defensa y la promoción de los derechos humanos en el entorno digital.

11. **Dirección IP**: corresponde a la abreviatura de dirección de Protocolo de Internet. Funciona como un identificador que tiene cada equipo o dispositivo que se conecta a Internet. Según ISOC, "se utiliza para ubicar e identificar un nodo en las comunicaciones con otros nodos de la red".

F

12. **Falso positivo:** de acuerdo con ISOC, un falso positivo corresponde al hecho cuando "se bloquea contenido que no se intentaba bloquear". Investigadores han determinado que, incluso, un falso positivo se da cuando la prueba de bloqueo arroja resultados imprecisos por errores de configuración o fallas en el dominio o link analizado.

H

13. **HTTP:** según OONI, es un protocolo de transferencia o intercambio de datos a través de Internet. Se ejecuta a partir de una solicitud de un usuario que desea conectarse a un servidor y recibe una respuesta del servidor. Contiene un encabezado del host que incluye información del dominio que desea visitar. Cada vez se hace más frecuente y recomendado el uso de HTTPS, que es un protocolo que tiene un mayor nivel de seguridad y de cifrado, para evitar que terceros puedan rastrear las solicitudes de los usuarios.

I

14. **Internet incluyente:** la CIDH ha dicho que Internet "debe tener una naturaleza multidireccional e interactiva, su velocidad y alcance global a un relativo bajo costo, y sus principios de diseño descentralizado y abierto, el acceso a Internet ha adquirido un potencial inédito para la realización efectiva del derecho a buscar, recibir y difundir información. A efectos de poder asegurar el disfrute efectivo y en forma universal del derecho a la libertad de expresión, los Estados deben adoptar las medidas para garantizar, de manera progresiva, el acceso de todas las personas a Internet, además de adoptar medidas para prohibir el bloqueo o la limitación al acceso a Internet o a parte de ésta. Internet tiene un impacto crítico en la dimensión social del derecho a la libertad de expresión".

15. **Inspección profunda de paquetes:** es conocida como DPI, por sus siglas en inglés: Deep Packet Inspection. Representa un mecanismo "filtrado de paquetes en redes informáticas que analiza los datos (y, posiblemente, también el encabezado) de un paquete al pasar por un punto de inspección, en busca incumplimiento del protocolo, virus, spam, intromisiones u otros criterios definidos para decidir si el paquete puede pasar o si es necesario darle otro tipo de tratamiento, que puede incluir su eliminación", según ISOC.

16. **Intermediario:** la CIDH ha dicho que "pueden ser definidos como cualquier entidad que permita la comunicación de información de una parte hacia otra". "La definición legal de intermediario puede ser distinta entre jurisdicciones o entre países. Son intermediarios desde los proveedores de servicios de Internet a los motores de búsqueda, y desde los servicios de blogs a las plataformas de comunidades en línea, las plataformas de comercio electrónico, servidores web, redes sociales, entre otros" La Declaración sobre Libertad de expresión en Internet, de la CIDH de 2011, establece: "Ninguna persona que ofrezca únicamente servicios técnicos de Internet como acceso, búsquedas o conservación de información en la memoria caché deberá ser responsable por contenidos generados por terceros y que se difundan a través de estos

servicios, siempre que no intervenga específicamente en dichos contenidos ni se niegue a cumplir una orden judicial que exija su eliminación cuando esté en condiciones de hacerlo ("principio de mera transmisión")".

17. **Internet Society:** conocida por sus siglas ISOC, es una organización no gubernamental cuya misión es el desarrollo mundial de Internet, concentrar sus esfuerzos y acciones con la colaboración multisectorial de Internet. Es una comunidad de individuos y se organiza por capítulos por países.

L

18. **Libertad en Internet**: se **considera** una condición indispensable para el ejercicio efectivo de los derechos humanos en el entorno digital. La CIDH la asocia al "ejercicio del derecho a la libertad de expresión" en entornos digitales, donde ha aumentado "la capacidad de las personas de recibir, buscar y difundir información. Esta instancia considera que la libertad digital "habilita y hace posible el ejercicio de otros" derechos humanos y las libertades fundamentales.

O

19. **Observatorio Abierto de Interferencia en Red:** conocida **como** OONI, es una red global que se dedica a rastrear las operaciones de censura, vigilancia y manipulación del tráfico en Internet en las distintas partes del mundo. Sus reportes están basados en criterios de transparencia y datos abiertos, incluyen estudios realizados en diferentes países como Sudán del Sur, Mali, Egipto, Etiopía, Nigeria, Pakistán, Sierra Leona, Irán, España, Cuba, Indonesia, Myanmar, Tailandia, Malasia, Gambia, Bielorrusia, Zambia, Uganda, entre otros. Está conformada por una comunidad de técnicos, investigadores y defensores de derechos digitales de distintos países del mundo.

20. **OONI Probe:** es **un** software libre y de código abierto diseñado y gestionado por OONI para medir la censura de Internet, disponible para sistemas operativos Android y IOS. Es una aplicación que puede analizar el bloqueo de sitios web, bloqueo de aplicaciones de mensajería instantánea, bloqueos de herramientas para sortear la censura en Internet, mide la velocidad de navegación de Internet, entre otras opciones. A través de OONI Probe, se pueden recoger datos con respuesta a potenciales hechos y evidencias de censura en Internet. Está disponible para dispositivos móviles y computadoras.

21. **OONI Explorer:** es un explorador de OONI con datos abiertos de evidencias técnicas de censura en Internet y otras interferencias digitales que se han presentado alrededor del mundo. Desde 2012, OONI ha alcanzado millones de mediciones recolectadas en más de 200 países. Las pruebas de bloqueos responden a tres categorías: accesibles: así se clasifica a los contenidos que no tienen evidencias de interferencias; confirmados: son evidencias de bloqueos en países en los que se ha confirmado, con un régimen legal, la censura digital; anomalías: son evidencias de censura en países en los que la censura está en un estado no declarada, por lo cual la medición sugiere interferencias o bloqueos.

22. **OONI Run:** es la aplicación de OONI para configurar jornadas o campañas de medición públicas o privadas según los distintos tipos de pruebas que tiene disponible OONI**.** Permite configurar una prueba con una lista de URL que se puede someter a un proceso de análisis o mediciones individuales o colectivas desde OONI Probe. OONI Run genera un enlace que luego puede ser compartido para hacer mediciones desde diversos puntos o lugares.

P

23. **Principio de neutralidad de la red:** Los estándares de Internet incluyente de la CIDH han establecido que no debería existir discriminación, restricción, bloqueo o interferencia en la transmisión y en el manejo del tráfico en Internet. Esto indica que debe cumplirse el criterio de **igualdad** para la gestión de las condiciones de navegación de todos los actores de Internet.

24. **Proveedor de servicios de Internet:** También conocido como ISP, por sus siglas en inglés. Son actores estatales y privados encargados de dictar las políticas **de** telecomunicaciones, administrar, proveer Internet y manejar el acceso a los sitios web. La CIDH los define como actores que tienen la responsabilidad "de respetar los derechos humanos en línea, lo que incluye tanto la responsabilidad de no restringir los derechos como la obligación positiva de crear un entorno en el que se respeten los derechos".

25. **Proxy**: es un servicio digital que ofrece un servicio de puente o intermediario para vencer las interferencias de conexión.

S

26. **Sondas:** son los puntos de medición que se utilizan para correr las pruebas de censura digital. Se establecen utilizando criterios de distribución geográfica, del mercado de proveedores de Internet y de la tecnología disponible.

U

27. **URL:** La dirección del localizador uniforme de recursos (URL), llamada "dirección web" de manera informal, es una referencia a un recurso web que indica su ubicación en la red y un mecanismo para recuperarlo. Las URL por lo general se utilizan para hacer referencia a páginas web (https), pero también se utilizan para transferencia de archivos (ftp), correo electrónico (mailto), acceso a bases de datos (JDBC) y muchas otras aplicaciones. La mayoría de los navegadores web muestran la URL de una página web en una barra de direcciones situada arriba de la página. Una dirección URL típica puede tener el formato https://www.ejemplo.com/muestra.html, que indica un protocolo (https), un nombre de host

V

28. **VPN:** es una red privada virtual (VPN) que extiende una red privada sobre una red pública, como Internet. Como por una suerte de túnel, permite a los usuarios enviar y recibir datos a través de redes públicas o compartidas como si sus dispositivos estuvieran conectados directamente a la red privada, que puede ser de un servicio distinto desde el que se conecta o incluso desde servidores de países distintos desde donde se encuentra navegando el usuario.

10 I Lecciones aprendidas

Esta sistematización de conocimientos y experiencias nos dejan 10 lecciones que compartimos este apartado:

1. Como hemos visto en estos contenidos, los insumos técnicos deben complementarse con el conocimiento de los estándares de derechos humanos. Sugerimos contar historias con estas dos dimensiones.
2. Hay un gran potencial de trabajar los asuntos de bloqueos desde el periodismo de datos, esto ayudará a sistematizar las evidencias y aportar resultados sólidos y sistematizados. Recomendamos revisar la base de datos experimental y darle continuidad a la actualización.
3. Sugerimos pensar, diseñar, estructurar e implementar un protocolo de medición e investigación de largo aliento que permita tener hallazgos más detallados con respecto a la dinámica de los bloqueos digitales a escala local.
4. Es recomendable establecer alianzas estratégicas en dos niveles: 1) con organizaciones que tengan el Know-how sobre los bloqueos 2) con una red de colaboradores de confianza que puedan hacer mediciones en tiempo real y para investigaciones de largo aliento.
5. Es aconsejable pensar en la conformación de un equipo multidisciplinario para seguirle el rastro a la censura digital.
6. Gran parte de las herramientas para sortear los bloqueos están también bloqueadas en Cuba. Con esto nos referimos a páginas desde donde descargar VPNs, Proxies o con información sobre cómo cambiar DNS. Creemos que se debe proporcionar a los periodistas y activistas que trabajan en el terrero de otras maneras de acceso a estas herramientas.
7. Es importante destacar que la mayoría de los encuestados respondió que se conectaba con mayor frecuencia desde los teléfonos móviles. Ninguno de los encuestados destacó el uso de los puntos de wifi públicos con frecuencia. De realizarse pruebas de conectividad o presencia de bloqueos debería tomarse en cuenta el amplio uso del móvil.
8. Ooni solo muestra los bloqueos realizados por la Empresa de Telecomunicaciones de Cuba. De realizarse pruebas propias, se deberían agregar otras telefónicas que operan en la isla.
9. Aunque en el período analizado en este informe, no se encontró un número considerable de bloqueos a redes sociales o herramientas de mensajería instantánea. Durante el mes de octubre se presentó un bloqueo a Telegram que afectó a periodistas y activistas de la isla. Se debe mantener especial atención a este tipo de bloqueos. Así como también, a los bloqueos observados en las páginas relacionadas a información sobre el COVID-19 debido a que se está ocultando datos sobre salud pública que pueden afectar eventualmente a la población.
10. Detectamos una oportunidad en la documentación de la duración de los bloqueos para determinar qué tan prolongados pueden ser los bloqueos en el tiempo.