MANUAL SOBRE APAGONES DE INTERNET Y ELECCIONES

Una guía para observadores electorales, embajadas, activistas y periodistas

#KeepItOn

#KeepItOn

Este manual explica cómo los apagones de internet socavan las elecciones democráticas, y proporciona consejos y recomendaciones para que actores clave naveguen por los apagones y comprendan y evalúen hasta qué punto una elección que tiene lugar durante un apagón es libre y justa. Está dirigido a quienes observan procesos electorales, personas en misiones diplomáticas, periodistas y activistas de derechos humanos en particular.

Actualizado: Julio 2021

Tabla de contenidos

I. Los hechos sobre los apagones de internet

Un apagón de internet es una interrupción intencional de **internet o de las comunicaciones electrónicas** que las vuelve inaccesibles o efectivamente inutilizables, para una población específica o dentro de una ubicación, a menudo para ejercer control sobre el flujo de información. Existen diferentes tipos de apagones (consulta el Glosario para obtener definiciones). Durante apagones generales o apagones totales de internet, el acceso a internet o a todos los servicios de telecomunicaciones se corta por completo, generalmente por parte de un actor del gobierno. En cambio los apagones parciales se dirigen a tipos específicos de redes (por ejemplo, redes móviles) o servicios como redes sociales y aplicaciones de mensajería. Un apagón de internet también puede tomar la forma de estrangulamiento, cuando las velocidades de internet se reducen intencionalmente con el fin de hacer más difícil, o incluso imposible, que las personas suban, descarguen o accedan a información. Una de las tácticas comúnmente utilizadas por los gobiernos es rebajar las velocidades de internet móvil de los niveles 4G y 3G a 2G.

Los apagones se pueden imponer en todo el país o pueden dirigirse a un vecindario, pueblo, región o provincia en específico. Los apagones selectivos pueden ser más difíciles de detectar y verificar, particularmente en regiones remotas y áreas aisladas del mundo exterior, como zonas de conflicto que pueden no ser accesibles para periodistas y personas que defienden los derechos humanos debido a razones de seguridad o restricciones impuestas por el gobierno.

Los gobiernos afirman que imponen apagones por una serie de razones, entre ellas, para proteger la seguridad nacional y restaurar el orden público, para evitar las trampas en los exámenes escolares y para obstaculizar la propagación de discursos de odio y desinformación. Sin embargo, las circunstancias en las que generalmente se ordenan los apagones revelan que los gobiernos realmente los despliegan como una táctica para restringir los derechos de la ciudadanía a la libertad de expresión e información, y para interferir con el derecho a la libertad de reunión y asociación, particularmente durante eventos como las elecciones, conflictos o manifestaciones masivas.

Entre 2018 y 2020, Access Now y la coalición #KeepItOn documentaron al menos **564 apagones en todo el mundo**. La mayoría de los apagones se produjeron en África, Asia-Pacífico, Oriente Medio y África del Norte. Sin embargo, estas cifras pueden no ser exhaustivas. Dada la metodología de Access Now para contar los apagones, que se basa en la medición técnica y en la información contextual, como informes de noticias o cuentas personales, puede haber casos de apagones de internet que hayan pasado desapercibidos o no se hayan informado.

II. Cómo los apagones de internet perjudican los derechos humanos

Interrumpir el acceso a internet obstaculiza el pleno disfrute de una amplia gama de derechos y libertades fundamentales, en particular el derecho a la libertad de expresión y opinión, el acceso a la información y la libertad de reunión y asociación. Por encima de todo, estas restricciones **afectan la vida cotidiana** al impedir que las personas se comuniquen, perjudican negocios e interrumpen la educación y el acceso a servicios y oportunidades en línea. En tiempos de crisis, como durante un conflicto armado o una pandemia mundial, los apagones ponen en peligro la salud y la seguridad públicas, pues las personas no pueden obtener información esencial sobre lo que sucede a su alrededor,

comunicarse con los servicios de emergencia o comunicarse con sus seres queridos y protegerlos. Los apagones de internet son medidas inherentemente desproporcionadas que no están justificadas por la normativa internacional de derechos humanos.

Ya en 2011, el Relator Especial de las Naciones Unidas (ONU) sobre la libertad de opinión y expresión, la Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre la libertad de los medios de comunicación, la Relatora Especial de la Organización de los Estados Americanos (OEA) sobre libertad de expresión, y la Relatora Especial de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) sobre libertad de expresión y acceso a la información, ya condenaban los apagones. Emitieron una **declaración** conjunta en la que establecieron que cortar el acceso a internet es una acción que "no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional".

Una resolución de la ONU de 2016 sobre la **promoción, protección y disfrute de los derechos humanos** also condemns internet shutdowns, and urgen internet también condena los apagones de internet e insta a los estados a abstenerse de ordenarlos. Esta resolución fue mantenida en 2018. En 2016, la CADHP aprobó una resolución que condena los apagones ordenados por gobiernos durante elecciones o protestas. En un informe del Consejo de Derechos Humanos de 2019 sobre la libertad de reunión pacífica y asociación en la era digital, el Relator Especial sobre los derechos a la libertad de reunión pacífica y asociación dijo que "las interrupciones del servicio de las redes digitales contravienen claramente el derecho internacional y no se pueden justificar en ninguna circunstancia". Mientras que en su Observación general **núm. 37** (2020) sobre el derecho de reunión pacífica, el Comité de Derechos Humanos pidió a los Estados partes del Pacto Internacional de Derechos Civiles y Políticos que no deben "bloquear o dificultar la conexión a Internet en relación con las reuniones pacíficas".

III. Por qué los apagones de internet son una barrera para las elecciones democráticas

Los apagones de internet son un reflejo de una atmósfera general de represión política, censura, violaciones de derechos humanos, instituciones débiles o falta de estado de derecho. Durante los períodos electorales, el acceso a internet en sí mismo no aborda todos los factores institucionales y políticos más profundos que interfieren con la realización de elecciones libres y justas, pero su interrupción dificulta que los diferentes actores se involucren plenamente en el proceso electoral. Los apagones socavan la capacidad de las candidatas y los candidatos electorales, en particular la oposición, para hacer campaña e intercambiar ideas. También impiden que la población votante acceda a la información, debilitan la confianza en el proceso electoral y obstaculizan los esfuerzos de quienes documentan las irregularidades.

Los apagones violan los derechos humanos y las libertades democráticas

Los derechos humanos, incluidos los derechos a la libertad de expresión y al acceso a la información, así como la libertad de prensa, son esenciales para las elecciones democráticas.

Como se **señaló** en un Informe de 2014 del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, "establecer las condiciones necesarias para una comunicación política libre y limpia es esencial para garantizar procesos electorales justos y democráticos.". El mismo informe denunció las medidas que restringen la libertad de expresión en los procesos electorales en línea y fuera de línea como "especialmente perjudiciales".

Las personas que presenten su candidatura y los partidos políticos que compiten en las elecciones deberían poder organizarse, reunirse, expresar sus opiniones y comunicar libremente sus programas electorales. Las personas votantes, por otro lado, deberían poder acceder a la información, asistir y participar en mítines y campañas políticas, tomar decisiones informadas y participar libremente en el discurso democrático y el proceso electoral. El papel de los medios de comunicación es esencial para garantizar el acceso equitativo a todos los partidos políticos y candidaturas para presentar su plataforma política y sus puntos de vista sobre temas de suma importancia para las personas votantes, examinar a profundidad a quienes presentaron una candidatura y cualquier intento de interferir con el proceso electoral, y verificar la información errónea y la desinformación, que puede ser frecuente durante los períodos electorales.

Ya sea que tengan lugar antes, durante o después de una elección, los apagones de internet impiden que diferentes actores participen plenamente en el proceso electoral y dificultan que las personas votantes accedan a la información, participen en debates y expresen libremente sus afiliaciones políticas. Los apagones dificultan aún más que los medios reporten y mantengan informado al público, lo que socava la capacidad de los partidos políticos y candidatos y candidatas para hacer campaña y movilizar a quienes votan.

Los apagones socavan el acceso a los medios y la justicia electoral

En los períodos electorales, los gobiernos que imponen apagones de internet también despliegan otras tácticas para silenciar a sus oponentes políticos, como el control sobre los medios de comunicación y las restricciones a las campañas electorales y reuniones políticas. Esto le da a los partidos gobernantes y candidatos con vínculos estrechos con el gobierno una ventaja sobre sus competidores, particularmente quienes se presentan con candidaturas independientes y los partidos de oposición. Por ejemplo, en ausencia de un acceso confiable y sin trabas a internet, quienes hayan presentado una candidatura desde la oposición pueden quedarse con opciones limitadas para hacer campaña y atraer votantes y no pueden competir en igualdad de condiciones con los poderosos actores políticos que controlan los medios de comunicación. Esto es discriminatorio y una violación de la igualdad de acceso a los medios de comunicación, uno de los criterios clave para las elecciones democráticas.

Además, los apagones de internet impuestos después de una elección impugnada socavan las capacidades del partido perdedor, generalmente la oposición, de organizarse para desafiar los resultados. En contextos de represión política y censura de los medios de comunicación, la organización de protestas y campañas a través de internet es una de las pocas tácticas, si es que no la única, de la que dispone la oposición y las personas votantes para ejercer presión sobre las autoridades. Por lo tanto, interrumpir el acceso a internet solo inclina aún más la balanza a favor del partido ganador, lo que exacerba aún más la desconfianza y la sospecha de fraude y manipulación electoral.

Los apagones de internet interfieren con el rol de fiscalización de los medios

Los apagones de internet impiden que los medios de comunicación mantengan debidamente informada a la ciudadanía durante las distintas etapas del proceso electoral. El papel de los medios en las elecciones es esencial para informar sobre campañas políticas, candidatos y agendas políticas. Esto facilita que quienes votan puedan tomar decisiones informadas, verificar las declaraciones políticas, e investigar y exponer cualquier manipulación electoral.

Los apagones indican una atmósfera general de creciente represión política, censura y abusos contra los derechos humanos. Esto hace que el papel de los medios de comunicación sea aún más esencial. Sin embargo, las interrupciones de internet

dificultan que tanto periodistas como medios de comunicación hagan su trabajo cuando más se necesita información creíble. Sin un acceso irrestricto a internet, estos actores no pueden desempeñar adecuadamente el papel de fiscalización para garantizar la integridad y transparencia del proceso electoral.

Los y las periodistas no pueden presentar las noticias de última hora a tiempo, comunicarse con sus salas de redacción, acceder a la información y ponerse en contacto con las fuentes. Si bien los apagones totales de internet son la forma más extrema de interrupción del internet, las restricciones en el uso de las redes sociales y las aplicaciones de mensajería también presentan un gran obstáculo, pues constituyen herramientas que se han vuelto esenciales para que tanto periodistas como medios lleguen a las audiencias, difundan y promuevan su trabajo, y se comuniquen de forma segura con sus fuentes.

Los apagones debilitan la confianza del público en el proceso electoral

Según un **Informe del 2013** de 2013 del Secretario General de la ONU a la Asamblea General, "no basta con que el proceso electoral produzca un resultado exacto. Los ciudadanos también deben confiar en que ese resultado es el reflejo auténtico de su voluntad". El informe señaló además que "la credibilidad no surge del proceso electoral mismo, ni tampoco de un acontecimiento único. Las fuentes de la confianza y aceptación políticas son más profundas".

Construir la confianza electoral, por lo tanto, depende de una serie de factores que reflejan la atmósfera más amplia en la que se llevan a cabo las elecciones, como la igualdad de condiciones, la neutralidad de las autoridades electorales y el gobierno frente a todos los contendientes, el respeto de los derechos humanos y el estado de derecho, la inclusión y la transparencia.

Los apagones ponen en tela de juicio la legitimidad del proceso electoral. Obstruyen el libre flujo de información y expresión, que es necesario para generar confianza pública y facilitar elecciones transparentes y justas.

Además de esto, dado que los apagones impuestos por el gobierno se utilizan a menudo como una táctica para silenciar y privar a la oposición política de una herramienta esencial para hacer campaña y movilizar a las personas votantes, estas medidas erosionan aún más la confianza pública en la neutralidad de las instituciones estatales frente a todos los políticos contendientes.

Desafían la transparencia, la integridad y la responsabilidad de las elecciones

Los apagones de internet impiden que los actores independientes que trabajan para garantizar la transparencia, la integridad y la imparcialidad de las elecciones, como misiones de observación internacional, observadores nacionales no partidistas y activistas, monitoreen la realización de las elecciones y expongan cualquier irregularidad.

Durante una elección, encontrar y comunicar información esencial, como informes de irregularidades, problemas con los sistemas de votación electrónica y violencia, se vuelve más difícil con un apagón. Los apagones obstaculizan la capacidad de los observadores para coordinarse con la sede de sus misiones, otros observadores y las autoridades electorales, además de impedirles verificar la exactitud de la información que reciben.

La interrupción del acceso a internet antes de una elección dificulta que los observadores accedan a información que pueda ayudarles a prepararse mejor, tomar precauciones de seguridad y monitorear diferentes aspectos de la fase preelectoral, como las campañas y el registro de votantes. Internet también ayuda a las personas votantes, periodistas y activistas a documentar y difundir informes e imágenes de manipulación, fraude y actos de violencia relacionados con las elecciones cuando ocurren.

El acceso sin trabas a internet es igualmente importante a medida que comienza el recuento de votos. Su interrupción impide que las misiones de observación y las que documenten irregularidades difundan amplia y oportunamente

sus declaraciones, informes, hallazgos y conclusiones al público.

En un período electoral, la diseminación oportuna de información que advierte irregularidades es importante para ayudar a garantizar que se aborde e investigue el fraude y que las impugnaciones legales se presenten dentro de los plazos establecidos por las leyes. Cuando las irregularidades no salen a la luz, hay menos posibilidades de abordarlas, aprender de ellas para mejorar los próximos ciclos electorales y, lo que es más importante, exigir cuentas a las personas responsables de las violaciones.

IV. Cómo navegar un apagón: consejos y recomendaciones

1. Comprender el contexto de los derechos digitales

Lee noticias y artículos sobre apagones de internet anteriores o en curso y su conexión con las elecciones.

Mantenerse informado o informada puede ayudarte a prepararte mejor en caso de que se produzca un apagón durante un período electoral. Comprender el papel que juegan la tecnología e internet en diferentes aspectos del proceso electoral, por ejemplo, en la campaña electoral, la votación y el registro de votantes, puede ayudarte a evaluar mejor cómo los apagones en un contexto y país en específico interfieren con el proceso electoral. También es esencial investigar el historial de apagones de internet y otras tácticas para limitar el flujo de información libre que se hayan utilizado en el país o la región afectada anteriormente. Por ejemplo, puedes comunicarte con grupos de derechos digitales y activistas que trabajan localmente para comprender mejor la situación de los derechos digitales, incluidos los grupos que forman parte de la coalición #KeepItOn. También puedes consultar organizaciones que documentan y monitorean los apagones de internet y la censura en todo el mundo, incluido Access Now, que mantiene el **Shutdown Tracker Optimization Project (STOP)**, (Proyecto de optimización de rastreo de apagones o STOP), y grupos de monitoreo de red como el **Open Observatory of Network Interference (OONI)**.

2. Prepárate antes de que ocurra un apagón

Instala y usa herramientas de elusión, como navegadores y herramientas basadas en tecnología Tor, redes privadas virtuales (VPN) y proxies que utilizan cifrado.

Las VPN crean su propia red que canaliza los datos a través de las redes existentes. Una VPN puede ayudarte a eludir el bloqueo de sitios web o plataformas en línea, incluyendo servicios específicos como plataformas de redes sociales y aplicaciones de mensajería instantánea. Para evitar que las personas accedan a sitios web y servicios bloqueados, los gobiernos a menudo recurren a bloquear el acceso a los proveedores de VPN durante un apagón, lo que dificulta la instalación de la herramienta una vez que el bloqueo ocurre. A veces también bloquean el tráfico de proveedores de VPN populares, lo que los hace ineficaces. Te recomendamos descargar varias VPN con anticipación si corres el riesgo de sufrir un apagón. No todas las VPN pueden garantizar tu privacidad u ofrecerte el mismo nivel de protección. Al elegir un proveedor de VPN, opta por herramientas de código abierto con códigos de acceso público y transparencia sobre cómo protegen tus datos. También debes asegurarte de que la VPN sea pública sobre su proceso de revisión de seguridad entre pares y que su seguridad haya sido revisada por auditores independientes. Si necesitas ayuda con recomendaciones de herramientas, puedes comunicarte con la Línea de **Ayuda de Seguridad Digital de Access Now**.

En algunos países, el uso de herramientas de elusión y VPN es ilegal o está sujeto a restricciones. Asegúrate de considerar cualquier riesgo legal y de seguridad personal que pueda surgir del uso de dichas herramientas. Si ciertas herramientas de elusión

están censuradas o criminalizadas en tu país, tal vez desees explorar la opción de configurar tu propio servidor VPN personal fuera del país, aunque esto también puede conllevar riesgos legales significativos en algunos contextos y está particularmente criminalizado en China.

Descarga y configura herramientas de comunicación seguras

Para una comunicación segura, te recomendamos que utilices aplicaciones y servicios que admitan el cifrado de extremo a extremo. Es importante elegir servicios y aplicaciones que sean de código abierto y se sometan a auditorías independientes de manera periódica. Por ejemplo, existen varias herramientas de mensajería instantánea de código abierto que utilizan el Protocolo Signal, un protocolo de cifrado de extremo a extremo para mensajes y llamadas de voz o video, incluyendo Signal y Wire. Lee atentamente la guía proporcionada por cada herramienta antes de usarlas, ya que algunos patrones de uso pueden ponerte en riesgo a ti o a tus contactos. Si tienes más preguntas sobre las herramientas de comunicación segura, pónte en contacto con la Línea de Ayuda de Seguridad Digital de Access Now.

Ten en cuenta que el uso de herramientas de comunicación seguras puede conllevar riesgos personales y legales. Algunos países han criminalizado el uso de herramientas específicas, y es probable que otros vigilen o monitoreen a las personas que buscan activamente mantener la privacidad de sus comunicaciones. Asegúrate de informarte y evaluar los riesgos antes de decidir qué herramientas son las mejores para ti.

Comprende y monitorea los apagones de internet en curso.

Si sospechas de un apagón de internet, puedes consultar herramientas de monitoreo como OONI Explorer, una base de datos mundial sobre censura de internet basada en millones de mediciones de red, Internet Outage and Detection Analysis (Análisis de interrupción y detección de internet o IODA) y el rastreador de tráfico e interrupciones de Google, que proporciona cerca de datos casi en tiempo real para identificar cortes de internet en varias redes. También hay rastreadores de apagones específicos de cada país, como killswitch.pk e internetshutdowns.in. Puedes medir los apagones de internet y la censura tú mismo utilizando la aplicación OONI Probe, que te permite ejecutar pruebas y documentar evidencia de diversas formas de interferencia de red. Los resultados de la prueba OONI Probe se publican abiertamente en el sitio de OONI Explorer en tiempo real. Antes de utilizar OONI Probe, asegúrate de conocer los riesgos potenciales.

Estos riesgos están asociados principalmente con las pruebas de censura, no con los apagones de internet. Ten en cuenta que en algunos países, las pruebas de censura pueden llevar a las autoridades a identificarte y señalarte por vigilancia o acoso. Ten en cuenta estos factores cuando busques información sobre si se está produciendo un apagón y cómo se está implementando. Aprender más al respecto no sólo te ayudará a comprender lo que está sucediendo, sino también a cómo responder de manera adecuada.

Después de que se lleve a cabo una elección, es importante seguir monitoreando la situación, ya que ha habido varios casos de apagones que inician después del día de las elecciones. Los gobiernos pueden imponer apagones después de una elección para evitar que la oposición y la ciudadanía se organice para desafiar los resultados y en un intento de encubrir el fraude electoral y la violencia. En algunos casos, un apagón puede haber sido difícil de detectar y puede haber más información disponible después de las elecciones, por ejemplo, cuando las empresas publican sus informes de transparencia.

Si te encuentras en un área afectada por un apagón total, no podrás consultar estos recursos en línea. Sin embargo, pueden ser útiles cuando un apagón afecta solo la velocidad de las redes o bloquea servicios, plataformas y sitios web específicos. Te recomendamos que guardes o imprimas este documento en caso de que pierdas acceso a internet.

3. Defiéndete a ti y a tu comunidad durante un apagón

Obtén la información bajo un apagón de internet.

La forma en que envíes información al mundo durante un apagón dependerá del tipo de interrupción que estés experimentando. El uso de una VPN puede ayudarte a evitar el bloqueo de servicios y sitios web específicos, como aplicaciones de mensajería, plataformas de redes sociales y servicios de correo electrónico. Cuando los gobiernos recurren a apagones totales de internet, son más difíciles de eludir. En una situación como ésta, considera tácticas como almacenar información, notas y trabajar en una memoria USB y enviársela a alguien que viaje fuera del área afectada por el apagón. Para mayor seguridad, puedes optar por cifrar la memoria o los archivos almacenados en ella mediante un software, como Veracrypt.

Si te preocupa que las autoridades espíen tus comunicaciones durante un apagón de internet, ten cuidado con el uso de una conexión satelital. Es fácil para las autoridades monitorear las comunicaciones por satélite y, en algunos países, incluso tener un teléfono por satélite está criminalizado. Además, el uso de una conexión satelital puede revelar tu ubicación, por lo que no querrás usarla si tu ubicación debe permanecer en secreto. Esto significa que si eliges utilizar una conexión satelital, debes considerar cuidadosamente el tipo y la sensibilidad de la información que estás compartiendo y las posibles implicaciones. Por ejemplo, una misión de observación electoral que utilice internet satelital para publicar y difundir una declaración pública y los hallazgos de la misión no enfrentarán el mismo nivel de riesgo que un periodista que se comunica con una fuente anónima que denuncia el fraude electoral. Puedes consultar esta guía que el Comité para la Protección de los Periodistas creó para las elecciones de 2021 en India para conocer los desafíos y los consejos de defensa relevantes más actualizados.

Comunícate de forma segura durante un apagón de internet.

Un apagón de internet, en particular un apagón total, puede obstaculizar tu acceso a herramientas de comunicación cifradas y ponerte a ti y a otras personas en riesgo. Antes de optar por utilizar una herramienta de comunicación insegura, asegúrate de evaluar los riesgos y las posibles consecuencias. Es importante considerar con quién te estás comunicando y los riesgos a los que te puedes exponer tú y las otras personas durante estas comunicaciones, pensar si está intercambiando información sensible y determinar si es mejor no comunicarse hasta que haya herramientas seguras disponibles. Por ejemplo, en el caso de un apagón total, un periodista que utiliza un teléfono fijo para entrevistar a un funcionario del gobierno puede correr menos riesgos que alguien de una organización de derechos humanos que utiliza las mismas redes telefónicas inseguras y no cifradas para discutir pruebas de fraude electoral o coordinar y comunicar internamente su respuesta a la violencia electoral. Amnistía Internacional publicó una guía en la que se describen los pasos que puedes seguir para comunicarte y documentar las violaciones de derechos humanos durante un apagón de internet.

Cada vez más, las personas afectadas por los apagones de internet, así como personas dedicadas a la investigación y a la ingeniería, han ideado formas creativas de acceder y compartir información durante los apagones totales. Estas soluciones incluyen sneakernet, comunicaciones en malla fuera de línea, módulo de identidad de suscriptor (SIM) en itinerancia de países vecinos, y comunicaciones no digitales como la radioafición. Todos conllevan riesgos diferentes, por lo que es importante evaluar adecuadamente qué opciones están disponibles y si es apropiado.

Documentar las violaciones de derechos durante un apagón de internet.

Cuando comunicar y hacer llegar información a otras personas durante un

apagón se vuelve difícil o imposible, es aún más importante documentar lo que está sucediendo en el terreno, ya sea evidencia de manipulación y fraude electoral o violaciones de derechos humanos y violencia. Incluso si no puedes compartir esta evidencia en tiempo real, más tarde se puede utilizar para informar al mundo de lo que sucedió durante el apagón y ayudar a las personas a exigir responsabilidades. La documentación puede tomar diferentes formatos, incluidos videos, testimonios, fotos y notas escritas. Asegurar y almacenar esta información es esencial para asegurarte de no perderla y evitar riesgos de seguridad personal. Si estás utilizando tu teléfono con fines de documentación, asegúrate de protegerlo con contraseña y de configurar el bloqueo de pantalla y el temporizador de bloqueo. Es posible que también desees utilizar un teléfono separado para la documentación, ya que esto minimiza la cantidad de información personal a la que las autoridades u otros actores pueden acceder si confiscan tu teléfono, como el contenido de tus mensajes, contactos, fotos personales, etc. También deberías considerar encriptar sus archivos y hacer una copia de seguridad de tus datos. Para obtener consejos prácticos y detallados, lee las guías de WITNESS sobre cómo documentar violaciones y abusos de derechos durante los apagones de internet, incluyendo cómo configurar un teléfono para la documentación sin conexión y mantener medios verificables durante un apagón de internet.

Recopilar y compartir evidencia de violaciones de derechos humanos bajo un apagón o censura a menudo es extremadamente difícil y te pone en gran riesgo. Las guías de WITNESS y Amnistía Internacional mencionadas anteriormente te ayudarán a crear un plan ejecutable para garantizar el éxito al hacerlo. Asegúrate de descargar y leer estas guías, preparar tu hardware, software y contactos antes de que ocurra un apagón, sigue los protocolos recomendados si ocurre un apagado y adquiere las herramientas o aplicaciones necesarias para apoyar tu plan.

V. Dónde aprender más y cómo actuar

➔ Si estás al tanto de un posible apagón de internet antes de una elección o durante el período electoral, puede comunicarte con la coalición #KeepItOn y Access Now en **shutdownalert@accessnow.org**. El Observatorio de Elecciones 2021 de **#KeepItOn tiene una lista** de elecciones que Access Now está observando en 2021 por posibles apagones.

➔ Si estás monitoreando apagones y buscando el historial de censura e interrupciones de internet de un país, **OONI Explorer** tiene datos sobre millones de mediciones de red recopiladas en más de 200 países. La base de datos STOP de Access Now también enumera algunos incidentes de apagones de internet por año y por país desde 2016.

➔ Para obtener más información sobre los daños causados por los apagones de internet, consulta el sitio web de la campaña **#KeepItOn**, su página de **preguntas frequentes** y el informe **informe #KeepItOn** sobre los apagones de internet registrados en 2020.

➔ Si eres periodista, miembro de la sociedad civil o defiendes los derechos humanos y necesitas asesoramiento técnico para volver a conectarte o proteger tus comunicaciones en línea durante un apagón, puedes comunicarte con la Línea de **Ayuda de Seguridad Digital de Access Now (Helpline)**. Brindamos asistencia 24 horas al día, 7 días a la semana sin cargo en nueve idiomas.

➔ Para obtener consejos y orientación sobre seguridad digital, consulta la guía **Anti-doxxing** de la Helpline y la **Guía para viajes** más seguros. La Electronic Frontier Foundation tiene una guía completa titulada **Surveillance-Self Defense** (Autodefensa para la Vigilancia). La guía incluye consejos sobre cómo **comunicarse de forma segura con otras personas**, preparar un **plan de seguridad**, **elefir la VPN** adecuada para ti y eludir la **censura de internet.**

Apéndice: El lenguaje de los apagones de internet: un glosario de términos

2G, 3G, 4G, 5G se refieren a las diferentes generaciones (de ahí la "G") de tecnologías de comunicación inalámbrica de banda ancha móvil en contraposición a los servicios móviles inalámbricos de primera generación (1G), que se basan en tecnologías de radio analógicas. Cada generación ofrece velocidades más rápidas y debe cumplir con estándares de calidad más altos. Por ejemplo, una velocidad de internet 2G ofrece una velocidad de 250 Kbps, mientras que las conexiones de internet móvil 3G y 4G normalmente generarían 3Mpbs y hasta 100Mpbs, respectivamente.

Un **apagón general** o un apagón total es una interrupción en la que el acceso a internet se corta por completo.

El cifrado es el **proceso** de codificar información o comunicaciones de una manera que solo puede ser leído por alguien que pueda descifrarlo o desencriptarlo de nuevo en un formato legible. La información se puede cifrar y descifrar utilizando una pieza de información llamada claves de cifrado. Una forma de cifrar las comunicaciones es a través de PGP, que significa Pretty Good Privacy (privacidad bastante buena), un sistema de cifrado de correo electrónico que permite a los usuarios intercambiar mensajes de correo electrónico cifrados. Los correos electrónicos enviados mediante PGP se convierten en texto cifrado en el dispositivo del usuario antes de enviarse a través de internet. Cuando están en tránsito, terceros como tu gobierno o tu proveedor de servicios de internet no pueden leer los mensajes. Solo el destinatario puede leerlos después de desencriptar el texto cifrado con su clave de cifrado.

El cifrado de extremo a extremo es un **metodo** de comunicación en el que solo el remitente y el receptor pueden acceder y leer los mensajes o correos electrónicos transmitidos. El cifrado de extremo a extremo se considera más seguro que la Seguridad de la capa de transporte (Transport Layer Security o TLS), que solo cifra las comunicaciones en tránsito entre el dispositivo de un usuario y los servidores de una empresa o servicio. Con el cifrado de extremo a extremo, ningún tercero puede acceder o leer esas comunicaciones, ni siquiera la empresa.

Un **apagón de internet** o un cierre de internet es una interrupción intencional de internet o las comunicaciones electrónicas, que las vuelve inaccesibles o efectivamente inutilizables, para una población específica o dentro de una ubicación, a menudo para ejercer control sobre el flujo de información.

El **estrangulamiento de internet** es la práctica de ralentizar intencionalmente la velocidad de internet, lo que dificulta o imposibilita que los usuarios carguen o descarguen información. La limitación también puede apuntar a servicios, aplicaciones y plataformas específicos, dejándolos inutilizables.

Las **conexiones de línea fija** se refieren a las comunicaciones de voz y datos t **transmitidas** a través de cables físicos, a diferencia de las comunicaciones inalámbricas. Incluyen, por ejemplo, telefonía fija y servicios de datos por cable.

Metadata, Los metadatos, a menudo descritos como datos sobre datos, son información sobre las comunicaciones intercambiadas entre un remitente y un destinatario, pero no el contenido del mensaje. Incluye información como con quién se está comunicando, las fechas y horas de las comunicaciones, su ubicación al realizar la comunicación, la duración de las conversaciones y el asunto de un correo electrónico. Los metadatos son **importantes** porque, si bien es posible que no revelen el contenido de sus conversaciones, aún pueden revelar mucho sobre ti y tu vida.

Una red móvil o una red celular es una **red de radio** que permite a los usuarios de dispositivos móviles enviar y recibir comunicaciones inalámbricas de voz y datos. Las **interrupciones de la red** se dirigen a

todas las redes de telecomunicaciones o a algunas en específico, en contraposición a servicios particulares. Por ejemplo, pueden afectar a las redes móviles 3G o 4G.

El **código abierto** es un tipo de código de software de computadora mediante el cual sus autores lo ponen a disposición de otras personas para que lo usen, estudien, redistribuyan y modifiquen. Esto hace que el código esté disponible para todas las personas que tengan las habilidades para inspeccionar, incluso para detectar cualquier vulnerabilidad, lo que puede ayudar a mejorar la seguridad de una herramienta o aplicación.

Los **apagones parciales** son interrupciones que se dirigen a servicios específicos como plataformas de redes sociales y aplicaciones de mensajería o redes como las redes móviles.

El **internet satelital** es un acceso a internet **proporcionado** por proveedores de servicios de internet (Internet Service Providers o ISP) mediante satélites de comunicación. Funciona cuando un ISP envía señales a un satélite en el espacio, que luego se envían de regreso a la Tierra y son capturadas por la antena parabólica del usuario.

Sneakernet es un término informal para la transferencia de información electrónica mediante el movimiento físico de medios, como una cinta magnética, disquetes, discos ópticos, unidades flash USB o discos duros externos entre computadoras, en lugar de transmitirla a través de una red informática.

Acerca de la coalición #KeepItOn

Este manual es una publicación de Access Now para la coalición #KeepItOn y fue escrito por Afef Abrougui en colaboración con el equipo de Access Now.

La campaña **#KeepItOn** coordinada por **Access Now**, une y organiza el esfuerzo global para poner fin a los apagones de internet. La coalición está compuesta por más de 240 organizaciones miembro de más de 100 países de todo el mundo, incluidos centros de investigación, grupos de derechos humanos, organizaciones de libertad de prensa y medios de comunicación y grupos de monitoreo de internet. Desde 2016, la coalición ha hecho uso de una variedad de tácticas para combatir los apagones, incluyendo la promoción de base, participación directa con quienes formulan políticas, apoyo técnico e intervención legal.

Para obtener más información, comuníquese con Melody Patry en **melody@accessnow.org**.

MANUAL SOBRE APAGONES DE INTERNET Y ELECCIONES

Una guía para observadores electorales, embajadas, activistas y periodistas

#KeepItOn