

CONTENIDOS O TABLA DE CONTENIDOS

[DOCUMENTAR DURANTE APAGONES DE INTERNET: UNA SERIE DE BLOGS CON RECOMENDACIONES PRÁCTICAS](#)

[CONFIGURAR UN TELÉFONO PARA DOCUMENTAR CUANDO NO HAYA INTERNET](#)

[¿DEBO USAR ESTA APLICACIÓN DE DOCUMENTACIÓN?](#)

[MANTENER MULTIMEDIA VERIFICABLE DURANTE UN APAGÓN DE INTERNET](#)

[HACER UN RESPALDO DEL MULTIMEDIA DE UN TELÉFONO SIN INTERNET O UNA COMPUTADORA](#)

[INTERCAMBIAR DE ARCHIVOS Y COMUNICARSE DURANTE UN APAGÓN DE INTERNET](#)

DOCUMENTAR DURANTE APAGONES DE INTERNET: UNA SERIE DE BLOGS CON RECOMENDACIONES PRÁCTICAS

Escrito por con contribuciones de Arul Prakkash y Yvonne Ng.

Última revisión: 31 de enero de 2020.

Blog [original en inglés](#).

En junio de 2019, mientras continuaban los abusos contra los derechos humanos y una crisis humanitaria en Myanmar, el [Ministerio de Transporte y Comunicación](#) del país ordenó a las compañías de telecomunicaciones que cancelaran su servicio de internet móvil en partes del estado de Rakhine y el vecino estado de Chin. Alegando “disturbios a la paz” y “actividades ilegales”, el

gobierno de Myanmar afirma haber promulgado el cierre “en beneficio de la gente”. En realidad, el apagón impidió el acceso a información y comunicación esenciales a más de un millón de personas e interrumpió los esfuerzos humanitarios. Como Matthew Smith de Fortify Rights ha declarado: “Este cierre está ocurriendo en un contexto de genocidio en curso contra Rohingya y crímenes de guerra contra Rakhine, e incluso si estaba destinado a atacar a militantes, es atrocamente desproporcionado”.

El bloqueo se levantó parcialmente en cinco de los municipios en septiembre de 2019, pero continúa. Durante el mismo mes, en la vecina Bangladesh, donde muchos rohingya han huido, las autoridades ordenaron a los operadores de teléfonos móviles que bloqueen los servicios 3G y 4G en los campos de refugiados rohingya y que dejen de vender tarjetas SIM a los rohingya. A medida que entramos en 2020, cuatro municipios en Rakhine continúan separados del mundo, y Bangladesh continúa limitando el servicio en los campos de refugiados.

Documentar durante los apagones de Internet

A nivel mundial, los apagones de internet van en aumento. De acuerdo con la campaña #KeepItOn de AccessNow, hubo 128 apagones intencionales entre enero y julio de 2019, en comparación con 196 en todo 2018, y un aumento brusco de 106 en 2017 y 75 en 2016. En todo el mundo, gobiernos, con la cooperación de las empresas de telecomunicaciones están recurriendo cada vez más a los apagones de Internet como una estrategia para reprimir a las comunidades, evitar la movilización y evitar que se documente y comparta información sobre violaciones de derechos humanos.

“Internet shutdowns and human rights violations go hand in hand.”

– Berhan Taye, AccessNow

Los apagones pueden tomar varias formas, incluidos bloqueos específicos de plataformas que se dirigen a aplicaciones y sitios populares, apagones a los datos móviles, limitación de ancho de banda o apagones totales de Internet. Todos estos tipos de apagones tienen como objetivo interrumpir la capacidad de comunicar información y exponer violaciones en tiempo real. A menudo ocurren durante protestas, elecciones y períodos de inestabilidad política, y a menudo van acompañados de una mayor represión estatal, ofensivas militares y violencia. Si bien los gobiernos pueden tratar de justificar los bloqueos en nombre de la “seguridad pública” u otras razones, los bloqueos tienen lugar claramente en los momentos en que los estados represivos temen perder el control sobre su gente, información o narrativa política. Los apagones violan los derechos humanos, afectan gravemente la vida y los medios de vida de las personas y también tienen un impacto económico global.

Documentar las violaciones de los derechos humanos es tan importante como siempre durante un apagón de Internet. Incluso si la información no se puede compartir en el momento, la documentación puede ser una forma de preservar las voces que las autoridades están tratando de silenciar, y para asegurar evidencia de abusos que se pueden utilizar para exigir responsabilidad más adelante. Por supuesto, el contexto represivo y los impedimentos tecnológicos de un apagón de Internet hacen que documentar violaciones y mantener esa documentación de manera segura sea

mucho más desafiante y arriesgado. **¿Cómo pueden las personas activistas capturar y preservar sus videos durante un bloqueo, e incluso compartirlos sin conexión, y hacerlo de manera más segura?**

Esta serie

A través de nuestro trabajo con activistas que han experimentado apagones de Internet, hemos aprendido algunos consejos y enfoques útiles para capturar y preservar la documentación de video durante los apagones de Internet que compartimos en esta serie. Los escribimos teniendo en cuenta los dispositivos Android, pero los consejos también se pueden aplicar a los iPhone. Algunas de las estrategias requieren planificación anticipada (y, a menudo, acceso a Internet), por lo que es una buena idea revisarlas e implementar cualquier paso antes de encontrarse en una situación en la que no tiene Internet y necesita documentar. Guarda una copia de cualquiera de los tutoriales para que pueda consultarlos o compartirlos durante un apagón. Y finalmente, comienza a practicar las técnicas y métodos en tu trabajo diario para que se conviertan en una segunda naturaleza antes de que te encuentres en una situación de crisis.

Preparar

- **Configurar un teléfono para que puedas hacer la documentación cuando no haya internet**

Capturar

- **¿Debo usar esta aplicación de documentación?**

Mantener

- **Mantener multimedia verificable durante un apagón de Internet**
- **Hacer un respaldo del multimedia de un teléfono sin internet o una computadora**

Compartir y comunicar

- **Intercambiar archivos y comunicarse durante un apagón de Internet**

Una nota final: si bien estos consejos pueden ayudarte a continuar documentando frente a un apagón, queremos enfatizar que la solución final debe ser restaurar el acceso a Internet y defender con éxito el **derecho de las personas a grabar** y la libertad de expresión, información y reunión. Afortunadamente, hay un movimiento global liderado por organizaciones como **NetBlocks**, **AccessNow** y muchas otras que están monitoreando activamente y compartiendo información sobre apagones. Las personas defensoras a nivel mundial se están involucrando en litigios estratégicos contra apagones de Internet. Nos solidarizamos con su trabajo para defender los derechos humanos.

CONFIGURAR UN TELÉFONO PARA DOCUMENTAR CUANDO NO HAYA INTERNET

A pesar de estar en un bloqueo de Internet, quienes documentan aún pueden capturar evidencia importante en video que se puede compartir sin conexión o en cuanto puedan volver a conectarse. Aquí hay algunos consejos que hemos aprendido de activistas y otros profesionales sobre cómo configurar un teléfono para la documentación sin acceso a internet. Ten en cuenta que algunos pasos requieren acceso a Internet, por lo que debe hacerse antes de que ocurra un apagón o durante el período en que se restablezca. Además, no esperes hasta que te encuentres en una situación estresante para implementar estos pasos; hazlos ahora y tómate el tiempo para practicar el uso del teléfono antes de tener que usarlo en una crisis.

Los apagones a menudo coinciden con un mayor control de la información y restricciones a la libertad de expresión y reunión. Si eres unx documentalista, toma precauciones adicionales para protegerte y proteger tu información durante estos períodos. Si existe el riesgo de que las autoridades confisquen tu teléfono o te obliguen a desbloquearlo y revelar el contenido (durante un apagón o de otro modo), considera usar un teléfono diferente a tu teléfono personal principal para documentar. Esto puede ayudar a minimizar la información que llevas que pueda verse comprometida (por ejemplo, tus contactos, cuentas, mensajes, etc.). Si no puedes usar otro dispositivo, puedes seguir esta guía para reducir la cantidad de datos confidenciales y mejorar la seguridad en tu teléfono principal.

Si reutilizas un teléfono antiguo, límpialo primero

Para borrar tu teléfono, ejecuta un restablecimiento de fábrica.

Nota: Los [estudios](#) han demostrado que restaurar tu teléfono a la configuración de fábrica no borra necesariamente todos los datos. De hecho, la única forma 100% segura de borrar datos es destruir el teléfono, ¡pero ese método no es una opción si deseas reutilizar el teléfono! [En este artículo](#), un ingeniero de Android sugiere asegurarse de que el contenido de su dispositivo esté encriptado antes del restablecimiento de fábrica. El cifrado ya viene predeterminado en la mayoría de los teléfonos actuales, pero en caso contrario, ve a Configuración> Seguridad> Cifrar teléfono antes de reiniciar. De esta manera, cuando restablezcas el teléfono de fábrica, la clave de cifrado se pierde y los datos que no sean borrados serán ilegibles.

Practica la seguridad básica del teléfono

Existen prácticas generales de seguridad en el teléfono que son relevantes en cada situación, ya sea que estés documentando durante un apagón de Internet o no. [Aquí hay algunos recursos útiles](#)

de otras organizaciones. Si bien nada garantizará el 100% de seguridad, algunos consejos clave incluyen:

- Asegúrate de que tu teléfono está encriptado. Los teléfonos más nuevos tienen cifrado activado de forma predeterminada. Si no estás seguro acerca del tuyo, verifica la configuración de seguridad en tu teléfono.
- Ejecuta actualizaciones del sistema operativo (SO) regularmente, ya que a menudo corrigen vulnerabilidades de seguridad.
- Actualiza tus aplicaciones importantes (como las aplicaciones de mensajería) regularmente.
- Establece un código de acceso seguro para el teléfono que tenga al menos 6 dígitos y no se base en la huella digital/táctil o la identificación facial.
- Configura un bloqueo de pantalla y un tiempo de bloqueo.
- Desactiva los servicios de ubicación si no los necesitas (incluido el servicio de ubicación de emergencia, la precisión de la ubicación, el historial de ubicación y las funciones para compartir ubicación, y las opciones de escaneo de WiFi y Bluetooth). También verifica los permisos de ubicación para aplicaciones individuales.
- Desactiva el Bluetooth y WiFi cuando no los necesites, para evitar el seguimiento del dispositivo.
- Apaga el teléfono cuando no lo estés usando.

Instala aplicaciones útiles para la documentación

Para la documentación de fotos o videos, puedes usar la aplicación de cámara incorporada en tu teléfono, o puedes usar una aplicación de documentación más especializada, como **ProofMode** u otras, que permiten una captura y exportación de metadatos más robusta, identificación y autenticación, encriptación, galerías seguras u otras características.

Una aplicación útil para documentar un apagón en sí es **OONI Probe**, una aplicación de código abierto que ejecuta pruebas desde tu teléfono para medir si los sitios o plataformas están siendo bloqueados. Puede mostrarte cómo, cuándo, dónde y quién está bloqueando los sitios. Asegúrate de **comprender los riesgos potenciales** antes de usar esta aplicación.

¿No estás seguro de qué aplicaciones de documentación usar? Proporcionamos algunas preguntas orientadoras en nuestro tutorial, “¿**Debo usar esta aplicación de documentación?**”.

Instala algunas aplicaciones cotidianas

Tener muy poca información y solo unas pocas aplicaciones especializadas en tu teléfono puede despertar sospechas. Para que el dispositivo parezca un teléfono cotidiano, instala algunas aplicaciones que sean comunes en el área donde estás documentando (recuerda descargarlas de fuentes confiables) y toma algunas fotos para tu galería.

Para las aplicaciones de redes sociales, es posible que desees crear e iniciar sesión en cuentas alternativas, ten en consideración que las cuentas falsas violan los Términos de servicio para la mayoría de las plataformas, y los requisitos de verificación de identidad de algunas plataformas pueden dificultar la creación de cuentas falsas. Además, deberás pasar algún tiempo creando contenido y agregando amigos a estas, lo que puede ser laborioso.

Instala aplicaciones cuando no hay internet

Descargar e instalar aplicaciones sin acceso a Internet es obviamente un desafío. Debes anticipar la descarga de aplicaciones si anticipas un apagón de Internet.

Una estrategia que puede ayudarte a ti y a otros más adelante es descargar y guardar el archivo del paquete de Android (.apk) para la aplicación (**descargado de una fuente confiable**, por ejemplo, directamente del desarrollador) en el almacenamiento de tu teléfono o en una unidad. Tener estos APK ya descargados de internet te permite a ti u otras personas compartir aplicaciones cuando no haya acceso a internet.

Si bien no hemos tenido la oportunidad de probar esto, la **aplicación F-Droid** proporciona una interfaz para intercambiar estos APK fuera de internet. [Aquí está su tutorial](#).

Mantén la información personal o privada/confidencial fuera del dispositivo

Intenta reservar el dispositivo para hacer documentación. No lo uses para correo electrónico, llamadas telefónicas o mensajes con contactos personales o activistas que puedan estar en riesgo, y no conectes este dispositivo a ninguna de tus cuentas principales reales.

Usa funciones para ocultar contenido

En el caso de que se busque tu teléfono, puede ser útil hacer que tus intenciones sean menos obvias o que tu contenido sea más difícil de encontrar. En previsión de situaciones en las que tu teléfono solo será examinado superficial y rápidamente, puedes emplear tácticas simples como:

- Cambiar los nombres e íconos de los accesos directos de tus aplicaciones usando una aplicación Launcher (por ejemplo, **Nova Launcher**, pero hay muchas), hará que sea menos obvio para qué sirven realmente ciertas aplicaciones.
- Usar una función de privacidad incorporada como Modo privado (**Samsung**) o Bloqueo de contenido (**LG**), si su teléfono lo admite.

Coloca un archivo vacío llamado “.nomedia” dentro de cualquier carpeta para evitar que los archivos multimedia de una carpeta aparezcan en tu galería. Nota: Si aún aparecen los archivos multimedia, es posible que debas borrar el caché de la Galería. Puede que esto no funcione de manera consistente en todos los dispositivos.

- Crea carpetas ocultas (carpetas que comienzan con un “.”) utilizando una aplicación de administrador de archivos. Puedes mover archivos a la carpeta oculta manualmente, o si usas una aplicación de cámara como [Open Camera](#), puedes especificar dónde se almacenan los archivos multimedia que grabas. Asegúrate de desactivar la opción “Mostrar archivos ocultos” en tu Configuración para que los archivos ocultos no sean visibles.

- Algunas aplicaciones de documentación especializadas, como [Tella](#) o [Eyewitness to Atrocities](#), almacenan documentación en galerías encriptadas separadas cuyos contenidos solo son accesibles dentro de la aplicación, lo que puede hacer que sea menos obvio para alguien que busca en tu teléfono. La documentación en estas galerías seguras requiere un código de acceso de aplicación separado, por lo que permanece cifrado incluso cuando tu teléfono está desbloqueado.

Nota importante sobre ocultar su contenido

Es importante tener en cuenta que las técnicas anteriores pueden ser suficientes para detener a alguien que simplemente está deslizando rápidamente a través de su teléfono, pero **no ocultará efectivamente tu contenido ante alguien que realmente está mirando**.

También ten en cuenta que algunos países pueden tener leyes que restringen o penalizan el uso de aplicaciones de seguridad que cifran o borran tus datos. Usarlos para evitar que las autoridades accedan a tus datos puede verse como una destrucción de evidencia u obstrucción de una investigación, y puede ser punible como un delito. [Este mapa](#) (completo, pero de 2017) proporciona un buen punto de partida si tienes preguntas sobre las leyes de tu país.

Configurar el compartir sin conexión

En una situación en la que no tienes Internet después de haber capturado contenido, es posible que aún desees sacar la documentación de tu teléfono por razones de seguridad, para liberar espacio o para compartir con otras personas. Descargar regularmente la documentación de tu teléfono también ayudará a minimizar la información comprometida en caso de que tu teléfono sea confiscado y desbloqueado.

Incluso si no puedes conectarte a Internet, puedes conectarte a dispositivos habilitados para wifi o Bluetooth localmente, como otro teléfono o una unidad USB wifi. Por lo general, tu teléfono debe venir con una aplicación / interfaz para que pueda conectarse y transferir. Si tu teléfono lo admite,

también puedes conectar una unidad o conector USB On-The-Go (OTG) para descargar la documentación a la unidad OTG u otro dispositivo.

Estos métodos se analizan con más detalle en nuestro tutorial sobre [intercambio de archivos y comunicación durante un apagón de Internet](#) y nuestra hoja de recomendaciones de [Video como evidencia: Herramientas tecnológicas – Transferencia de archivos](#).

Practica antes de estar en una situación de crisis

Configura el teléfono ahora que tienes acceso a Internet. Comienza a practicar el uso de las aplicaciones en situaciones cotidianas (donde no hay problemas de seguridad) para que te familiarices y te sientas cómodo al usarlas. Haz que la seguridad básica del teléfono sea tu práctica predeterminada. De esta manera, los métodos serán de segunda naturaleza cuando te encuentres en una situación de crisis con otras cosas más de las que preocuparte.

Consulta la siguiente publicación de esta serie, “[¿Debo usar esta aplicación de documentación?](#)”

¿DEBO USAR ESTA APLICACIÓN DE DOCUMENTACIÓN?

Hay muchas aplicaciones que las personas que documentan pueden usar para capturar videos, desde la aplicación de [cámara nativa de tu teléfono](#) hasta aplicaciones de documentación más especializadas como [ProofMode](#), [Tella](#) o [Eyewitness to Atrocities](#). Algunas aplicaciones tienen características que dependen del acceso a Internet, así que ten en cuenta que esas características pueden no estar disponibles en caso de un apagón de Internet.

No podemos decirte qué aplicación específica es la más adecuada para ti, ya que eso depende de tu situación, necesidades y riesgos (consulta [esta publicación de blog](#) para obtener más información sobre cómo evaluar tus riesgos y amenazas). Con tu evaluación de riesgos en la mano, estas preguntas orientadoras a continuación pueden ayudarte a evaluar qué aplicación de documentación de video podría funcionar mejor para ti.

¿Quién hizo la aplicación y qué confianza tengo en ellxs?

Siempre debes pensar acerca de lxs desarrolladorxs de cualquier aplicación que descargues e instales en tu dispositivo, y preguntarte si puedes confiar en ellxs para no ponerte en riesgo, de forma intencional o no.

Algunas cosas a tener en cuenta son:

- ¿Quien desarrolla la aplicación tiene buena reputación? ¿Qué dicen las personas en su comunidad y la red más amplia sobre ellxs y sus herramientas?
- ¿El/la desarrolladora de la aplicación es vulnerable? Considera tu contexto y la probabilidad de que se vean obligadxs a entregar tus datos o crear una puerta trasera

para las autoridades (o si realmente lo han hecho en el pasado). ¿En qué país se almacenan los datos y cuáles son las leyes relativas a las órdenes judiciales en esa jurisdicción?

- ¿Quién desarrolló la aplicación la mantiene actualizada? Las herramientas sin mantenimiento son susceptibles a los hacks que explotan las vulnerabilidades descubiertas. Consulta el sitio web del desarrollador o la página de Google Play de la aplicación para conocer la fecha de “última actualización”.
- ¿Qué tan establecido está el desarrollador de la aplicación? ¿Parece que será capaz de mantener la aplicación con el tiempo?
- ¿La aplicación es de código abierto? Las aplicaciones que están abiertas al escrutinio tienen más probabilidades de abordar o al menos identificar sus problemas de seguridad. ¿El desarrollador es transparente sobre la eficacia y la seguridad de la aplicación?
- ¿Qué motivaciones o incentivos impulsan el trabajo del desarrollador de la aplicación y cómo podría influir eso en su confiabilidad? Por ejemplo, ¿están orientados por su misión? ¿Con fines de lucro? ¿Patrocinados por algún financiador particular?
- Si bien no es un indicador directo de confiabilidad o no, el costo de la aplicación puede ser una consideración importante. Algunas aplicaciones tienen una alta tarifa de suscripción mensual o tarifa por video.

Consulta la guía de la plataforma de Autodefensa de vigilancia [EFF](#) para [elegir aplicaciones](#) donde podrás obtener más información.

¿Desde dónde se puede descargar la aplicación?

Siempre debes descargar e instalar aplicaciones de tiendas o sitios web de buena reputación. Incluso si has realizado una investigación exhaustiva para determinar la confiabilidad de una aplicación, las tiendas de aplicaciones poco confiables pueden tergiversar sus productos y llevarte a descargar una aplicación ilegítima creada con fines nefastos. Por ejemplo, el año pasado, la organización de derechos digitales [SMEX](#) emitió una [advertencia](#) sobre varios sitios web que comercializan una aplicación llamada “WhatsApp Plus” (para ser claros, ¡este no es un producto de WhatsApp!), que podría estar almacenando y vendiendo datos de los usuarios, o permitiendo que los teléfonos que lo instalan sean hackeados.

Algunos desarrolladores conscientes de la seguridad incluso proporcionan claves criptográficas que te permiten verificar su autenticidad. Por lo general, proporcionarán una explicación sobre cómo verificar estas firmas.

¿Dónde se almacenarán los datos?

Algunas aplicaciones de documentación solo almacenan tus datos y documentación localmente en tu dispositivo, mientras que otras solo envían y almacenan tus datos en otro lugar. En muchos casos, esto es inherente al diseño y el propósito de la aplicación, como la aplicación Eyewitness to Atrocities, que envía una copia inalterada de tu documentación a una instancia de almacenamiento de Lexis Nexis para que Eyewitness pueda garantizar la cadena de custodia e integridad del

material. Solo puedes exportar tus multimedia fuera de la galería encriptada dentro de la aplicación Eyewitness después de que se haya enviado para su protección.

Depende de ti determinar si necesitas que tu documentación permanezca solo en tu dispositivo, si necesitas enviarla y almacenarla en una ubicación remota que controles (como una opción como [Tella](#)), o si necesitas enviarla a una organización/plataforma externa a la que permitirás acceder y utilizar tu documentación. Ten en cuenta que durante un apagón de Internet, no podrás transmitir tu documentación por Internet de inmediato, por lo que necesitarás una aplicación que al menos temporalmente te permita almacenar (e idealmente hacer una copia de seguridad) de tu documentación localmente (consulta [Hacer un respaldo del multimedia de un teléfono sin internet o una computadora](#)).

Si tus datos se enviarán a una ubicación remota, ten en cuenta en qué países residirán los datos. ¿Cuán vulnerables son los datos a la exposición en esos países, ya sea por órdenes judiciales u otros medios? ¿Qué riesgos enfrentas al tener tus datos expuestos allí?

¿La aplicación encripta mis archivos multimedia?

Algunas aplicaciones, como Tella y Eyewitness to Atrocities, proporcionan encriptación de archivos y/o almacenamiento encriptado para su documentación, aparte de la galería principal de tu teléfono y la encriptación de tu teléfono, de modo que tus archivos multimedia y metadatos nunca estén sin encriptar en tu dispositivo a menos que se acceda a través de la aplicación con un código de acceso. Esto significa que incluso si tu teléfono está desbloqueado, tu documentación permanece encriptada. Esto puede proporcionar un nivel adicional de protección para tu documentación. Si la aplicación envía y almacena tus archivos multimedia a una ubicación remota después de que se restablezca tu Internet, también considera si necesitas que tus archivos multimedia estén encriptados mientras está en tránsito y en la ubicación remota, como lo hace, por ejemplo, la aplicación EyeWitness.

Ten en cuenta que si bien el cifrado es legal en la mayoría de los lugares, algunos países pueden tener leyes que restringen o penalizan su uso. [Este mapa](#) (completo, pero de 2017) proporciona un buen punto de partida si tienes preguntas sobre las leyes de tu país.

¿La aplicación captura metadatos importantes (sin internet)?

[Los metadatos](#) son datos que describen tu video o foto, como la hora y la fecha o la ubicación. Esta información es valiosa para identificar, comprender, autenticar y verificar tu video o foto como documentación de un evento específico. En el contexto de un apagón de Internet, la capacidad de una aplicación para recopilar automáticamente ciertos metadatos y/o permitirte ingresar fácilmente información descriptiva útil en el acto es especialmente útil, ya que puede haber un largo período de tiempo antes de que puedas compartir la documentación con cualquier persona (tiempo durante el cual se pueden olvidar los detalles, las circunstancias pueden cambiar, etc., etc.).

La mayoría de las aplicaciones de documentación especializadas, como ProofMode, tienen características de metadatos mejoradas y recopilan más metadatos que las aplicaciones de cámara

integradas típicas. Los metadatos mejorados pueden incluir diversos datos del sensor, señales wifi o bluetooth cercanas, datos del dispositivo, hash criptográfico e información suministrada por el usuario, todo lo cual puede facilitar la autenticación y verificación de los archivos media más adelante.

Ten en cuenta que durante un apagón de Internet, necesitarás una aplicación que no requiera la transmisión de datos para generar o registrar los metadatos. Algunas aplicaciones pueden depender de Internet, en lugar de los sensores de hardware, para recopilar ciertos metadatos. Por ejemplo, si los datos de ubicación se capturan desde búsquedas en el dispositivo, los metadatos pueden reflejar la última ubicación donde el dispositivo tenía conexión de datos, en lugar de la posición real del hardware. Idealmente, la aplicación también debería permitirte almacenar los metadatos localmente sin internet, incluyendo guardar cualquier formulario que estés completando (por ejemplo, el “modo fuera de línea” de Tella).

¿Puedes exportar datos desde la aplicación?

Dependiendo de tus intenciones para la documentación, puede ser esencial poder exportar la documentación de video y tus metadatos desde la aplicación, en un formato que no sea propiedad de la aplicación; es decir, para poder abrir, ver y usar los archivos multimedia y metadatos fuera de la aplicación. La capacidad de exportar significa que tu y otras personas no dependen de una sola aplicación o proveedor de servicios para acceder a tu documentación, y te da más libertad para trabajar con el contenido en el futuro. Ten en cuenta que algunos metadatos pueden no ser comprensibles si no tienes acceso a ciertas bases de datos o tablas de conversión para interpretar los números (por ejemplo, en el caso de ID de torre celular o redes Wi-Fi).

Ten en cuenta que algunas aplicaciones pueden tener una cadena de custodia cerrada deliberada y no permitir que los usuarios exporten, mientras que algunas aplicaciones simplemente no pueden diseñarse con un caso de uso de exportación en mente. También ten en cuenta que algunas aplicaciones, como Eyewitness to Atrocities, pueden no permitirte exportar hasta que hayas cargado los archivos multimedia en un servidor remoto (para lo cual necesitas acceso a Internet), y algunas aplicaciones pueden permitirte exportar los archivos multimedia, pero no los metadatos (que no sean metadatos que vivan en el archivo).

Si necesitas exportar, lo ideal es que tu aplicación te permita exportar una copia de los archivos multimedia sin ningún cambio o transformación, y una copia de los metadatos en un formato de texto legible estandarizado. Los metadatos de Tella, por ejemplo, se almacenan encriptados en la galería de Tella, pero se pueden exportar como CSV. Además, durante un apagón de Internet, es necesario tener opciones para exportar a aplicaciones fuera de Internet o servicios no dependientes de Internet. La mayoría de las aplicaciones que te permiten exportar tienen algún tipo de botón de “Compartir” que activa un menú para compartir, que Android completa con una lista de aplicaciones en tu teléfono que son capaces de manejar ese tipo de contenido. Lamentablemente, los desarrolladores de aplicaciones pueden personalizar sus menús compartidos y puede no haber coherencia entre las aplicaciones.

Para una mayor cantidad de archivos, puede ser más eficiente acceder a los archivos almacenados a través de una aplicación de administrador de archivos y copiar los archivos desde allí, aunque es posible que no puedas acceder a los metadatos almacenados en la base de datos de una aplicación

de esta manera. Esta opción tampoco está disponible para aplicaciones que proporcionan sus propias galerías seguras, ya que los archivos se cifrarán en el almacenamiento. Para estas aplicaciones, es necesario tener una función para compartir dentro de la aplicación. Consulta la siguiente publicación de esta serie, “[Mantener multimedia verificable durante un apagón de Internet](#)” y nuestra próxima tabla comparativa de aplicaciones de documentación.

MANTENER MULTIMEDIA VERIFICABLE DURANTE UN APAGÓN DE INTERNET

Las personas [defensoras de los derechos humanos](#), [investigadoras](#)[1] y [periodistas](#) a menudo confían en la documentación de primera mano filmada por testigos para monitorear, informar y abordar las violaciones de los derechos humanos. Para asegurarse de que están actuando sobre la información correcta, estas personas usuarias toman medidas para autenticar y verificar la documentación que reciben, un proceso que puede ser laborioso y lento. Como documentalista, hay cosas simples que puedes hacer para facilitar que otras personas verifiquen y corroboren su documentación, de modo que pueda usarse de manera oportuna y efectiva. Estos pocos pasos adicionales son aún más valiosos durante un apagón de Internet, considerando que:

- Si no puedes subir de inmediato, entonces la fecha de publicación y la información de ubicación proporcionada por las redes sociales no será tan útil para mostrar que tu video fue filmado en una fecha determinada o en una ubicación determinada o antes.
- Si otras personas tampoco han podido subir los contenidos, puede haber menos documentación disponible en general que pueda usarse para corroborar tu video.
- Si necesitas pasar tu video a través de muchas manos en físico, fuera de internet, para llevarlo a su destino, puede ser más difícil para otras personas también rastrear la fuente del video.
- Si necesitas eliminar el video original de tu teléfono para una mayor seguridad o por capacidad de almacenamiento limitada sin copia de seguridad en la nube, o si tienes que deshacerte del teléfono, puede ser más difícil confirmar la autenticidad del video.
- Si olvidas los detalles sobre un video en particular y la aplicación que estás utilizando no captura/graba metadatos sin acceso a Internet, es posible que otras personas no puedan identificarlo más tarde.

Los siguientes consejos pueden ayudarte a mantener tu video durante un apagón de Internet para maximizar su verificabilidad y usabilidad como documentación más adelante.

Filma o proporciona detalles de identificación en el video

Intenta incluir detalles en tu video que faciliten que un investigador o periodista identifique más tarde la hora y el lugar, como puntos de referencia únicos, el horizonte, letreros de calles, escaparates, placas, banderas, relojes, portadas de periódicos, etc. También puedes narrar información básica

como tu nombre e información de contacto (si es seguro hacerlo), la hora, la fecha y la ubicación/coordenadas GPS (o anota en un papel y filma el papel). Cuantos más detalles incluyas, más fácil será para otra persona investigar y verificar el video más tarde, incluso si no te conocen o no saben de dónde proviene el video. Consulta nuestros consejos sobre [Prácticas básicas para capturar, almacenar y compartir](#) para obtener más información.

Agrega descripción/metadatos

Aprovecha una de las muchas aplicaciones de documentación especializadas que extraen metadatos mejorados o información técnica de tu teléfono y te permiten ingresar manualmente información descriptiva adicional. Ten en cuenta que, durante un apagón, necesitas una aplicación que no dependa del acceso a Internet para registrar o almacenar estos metadatos. Consulta “[¿Debo usar esta aplicación de documentación?](#)” para obtener más información sobre cómo elegir una aplicación adecuada.

Incluso si no estás utilizando una aplicación de documentación especializada, puedes crear información complementaria en forma de notas, mapas o fotos en tu teléfono. Puedes organizar tu video con esta información adicional utilizando tu aplicación de administrador de archivos favorita. La información complementaria clave que se debe incluir es la hora, la fecha, la ubicación del incidente registrado, así como la fuente de la grabación (es decir, tu nombre e información de contacto) si es seguro incluirla. Exporta los metadatos e inclúyelos con el video (puedes ponerlo todo en una carpeta y comprimirlo) cuando lo compartas.

Mantener una copia de seguridad

Realiza copias de seguridad de los archivos multimedia desde tu teléfono regularmente e idealmente en 2 dispositivos de almacenamiento separados. Puedes, por ejemplo, conectar On-the-Go (OTG) o memorias USB inalámbricas a su teléfono, incluso sin una computadora. Consulta nuestros consejos sobre “[Hacer un respaldo del multimedia de un teléfono sin internet o una computadora](#)” para obtener más detalles. Hacer una copia de seguridad o respaldo asegurará que conservas una copia de tu video en caso de que se pierda o rompa tu teléfono, o si necesitas eliminar videos de tu teléfono. Tener una copia segura de tu video original también le permite a un investigador o periodista que ve tu video a través de otros medios obtener el video directamente de ti más tarde (siempre que puedan rastrearte), creando una cadena de custodia completa y más corta.

Revisa la próxima publicación de esta serie, “[Hacer un respaldo del multimedia de un teléfono sin internet o una computadora](#)”.

HACER UN RESPALDO DEL MULTIMEDIA DE UN TELÉFONO SIN INTERNET O UNA COMPUTADORA

El **respaldo** es clave para garantizar que tus datos y documentación no se eliminen, corrompan o pierdan accidentalmente si tu dispositivo es confiscado. Durante un apagón o cuando limitan la velocidad del Internet, es posible que no puedas ejecutar tu copia de seguridad en la nube habitual o enviar tu documentación a una ubicación segura fuera del sitio. La descarga en una computadora de escritorio o portátil es una forma de hacer una copia de seguridad o respaldo, pero dado que las personas a menudo no tienen acceso a una, aquí hay algunas opciones y consejos para hacer una copia de seguridad de tus archivos multimedia desde tu teléfono durante un apagón de Internet sin una computadora.

Usa un OTG o unidad inalámbrica

Las unidades OTG, o on-the-go, son un tipo de unidad USB compatible con muchos (pero no todos) los teléfonos androids. Puedes conectar una memoria USB OTG directamente a tu teléfono o usar un adaptador OTG a USB para conectar tu teléfono con un disco duro USB normal. Con OTG, tu teléfono proporciona la potencia para la unidad.

Las marcas populares de unidades OTG incluyen SanDisk, Kingston y Samsung, aunque hay muchas otras. Por lo general, cuestan entre US \$8 y \$25 dólares, dependiendo de la capacidad de almacenamiento.

Las memorias USB/discos duros inalámbricos son similares a los discos duros normales, excepto que no requieren cables. Esto te permite conectar dispositivos que normalmente no se conectan a discos duros, como tu teléfono. Una ventaja de una unidad inalámbrica sobre una unidad OTG es que puedes conectar varios usuarios a la misma unidad inalámbrica a la vez. Esto puede ser útil, por ejemplo, en una situación de protesta cuando estás filmando como un equipo: las imágenes de todas las personas se pueden guardar en un disco duro que otra persona del equipo lleva. Ten en cuenta que debido a que no están obteniendo energía de un dispositivo, las unidades inalámbricas dependen de la energía de la batería y deben cargarse.

SanDisk es probablemente la marca más popular de memorias USB inalámbricas, aunque hay otras. Las memorias USB inalámbricas son generalmente más caras que las unidades OTG, y varían entre aproximadamente US \$25- \$100 dólares dependiendo de la capacidad de almacenamiento. Los discos duros externos inalámbricos más grandes comienzan en alrededor de US \$150 dólares dependiendo de la capacidad de almacenamiento.

Alternativa: usa un teléfono viejo sin usar

Si no tienes una unidad OTG o inalámbrica, pero tienes un teléfono antiguo que todavía funciona y que ya no usas, también puedes volver a utilizarlo para hacer una copia de seguridad. Mientras ambos teléfonos estén dentro del alcance físico, puedes conectar y copiar medios de uno a otro mediante Bluetooth, WiFi Direct o Near Field Communication (NFC)/Android Beam. Bluetooth y Wifi Direct son tecnologías inalámbricas que pueden “emparejar” dos dispositivos sin otro enrutador o punto de acceso intermedio. WiFi Direct proporciona un rango más amplio y una transferencia de datos más rápida que Bluetooth, pero consume mucha más energía. Mientras tanto, NFC tiene un alcance mucho más corto (~ 4 cm) y velocidades de transferencia mucho más lentas que Bluetooth

o WiFi Direct, pero se conecta más rápido y usa menos energía, por lo que puede ser útil para transferencias pequeñas y rápidas cuando tiene ambos dispositivos en la mano.

Es probable que tu teléfono tenga aplicaciones/funciones Bluetooth, WiFi Direct o NFC incorporadas que te permiten elegir dispositivos cercanos para compartir. Si ambos teléfonos tienen instalado Files de Google, también puedes compartir archivos sin conexión utilizando estas tecnologías dentro de la aplicación.

Importante: la desventaja de la facilidad de conexión proporcionada por estos servicios es que no son seguros. Los escáneres Bluetooth y wifi se pueden usar para rastrear tu ubicación o buscar información en tu dispositivo. Las personas infiltradas pueden intentar emparejarse con tu dispositivo, enviarte archivos no deseados o incluso obtener el control de tu dispositivo si es vulnerable. **Para estar más segurx, desactiva estos servicios cuando no los estés utilizando y solo actívalos cuando estés en lugares seguros, limita los permisos de la aplicación solo a lo que necesitas y a quién necesitas, y practica buenas medidas de seguridad en tu teléfono, como ejecutar actualizaciones y tener una buena contraseña de acceso.**

Incluye cualquier descripción/metadatos por separado

Al copiar archivos multimedia a una unidad OTG, unidad inalámbrica o un teléfono antiguo, es útil incluir cualquier información descriptiva o metadatos que puedan estar separados de los archivos multimedia. **Muchas aplicaciones de documentación**, por ejemplo, generan documentos de texto CSV o JSON que incluyen metadatos extraídos del dispositivo (por ejemplo, geolocalización, hora, fecha) y cualquier descripción ingresada manualmente por el usuario. Asegúrate de exportar e incluir estos documentos de metadatos en sus copias de seguridad también.

Proteger con contraseña la unidad

Muchas unidades inalámbricas pueden protegerse con contraseña con una aplicación móvil que viene con la unidad. Ten en cuenta que la protección con contraseña no es lo mismo que el cifrado (ver más abajo). La mayoría de las unidades inalámbricas o OTG no permiten el cifrado de disco completo usando solo un teléfono móvil, aunque pueden cifrarse en disco completo usando una computadora.

Considera encriptar los archivos

Si necesitas almacenar tus archivos de manera más segura, puedes considerar cifrar tus copias de seguridad o respaldos. Si bien es posible que no puedas cifrar la mayoría de las unidades inalámbricas o OTG con un teléfono móvil, puedes cifrar los archivos antes de moverlos a la unidad. Algunas aplicaciones que pueden cifrar archivos en Android incluyen **ZArchiver** y **RAR**. Ten en

cuenta que debes recordar tus contraseñas de cifrado. No hay forma de recuperar archivos cifrados si pierdes la contraseña.

Ten en cuenta que algunos países pueden tener leyes que restringen o penalizan el uso del cifrado. Usarlos para evitar que las autoridades accedan a tus datos puede verse como una destrucción de evidencia u obstrucción de una investigación, y puede ser punible como un delito. Este [mapa de 2017](#) puede estar desactualizado pero proporciona un buen punto de partida si tiene preguntas sobre las leyes de su país.

Realiza 2 copias de seguridad en ubicaciones separadas

Una sola copia de seguridad no siempre es confiable. Por ejemplo, puedes perder el dispositivo de respaldo, dañarlo o puede que este simplemente fallar al azar. Las personas expertas en TI generalmente aconsejan a las personas que tengan 2 copias de seguridad (es decir, 3 copias en total), en dispositivos separados guardados en ubicaciones separadas. Esto ayuda a mitigar la variedad de riesgos para cualquier copia en particular.

Revisa la publicación final de esta serie, “[Intercambiar de archivos y comunicarse durante un apagón de Internet](#)”.

INTERCAMBIAR DE ARCHIVOS Y COMUNICARSE DURANTE UN APAGÓN DE INTERNET

El continuo bloqueo de internet y la represión en Cachemira, el apagón de internet más largo jamás impuesto en una democracia, ha tenido un [impacto catastrófico](#) en la vida de las personas en la región. Para agravar la situación, en diciembre de 2019, las [cuentas de WhatsApp de Cachemira comenzaron a revocarse](#) debido a los 120 días de inactividad de las personas usuarias según las políticas de WhatsApp.

Al momento de escribir este blog en enero de 2020, la Corte Suprema de la India dictaminó que el cierre indefinido en Cachemira es [ilegal y un abuso de poder](#). La banda ancha limitada y la Internet móvil se han restaurado en algunas áreas, pero solo para algunos sitios web “incluidos en la lista blanca”.

Los apagones de Internet están diseñados para impedir que las personas compartan información y se comuniquen (y también empujan a las personas a formas de comunicación menos seguras, como teléfonos móviles y SMS, que son más fáciles de interceptar y controlar por las autoridades). No siempre hay buenas soluciones durante los apagones completos. Durante los períodos más

estrictos del bloqueo en Cachemira, por ejemplo, las personas recurrieron al **uso de notas escritas a mano y correos** para enviar mensajes a sus seres queridos.

No tenemos formas seguras de eludir todos los bloqueos, pero a través de conversaciones con activistas y compañerxs, hemos aprendido algunos métodos y enfoques para compartir y comunicar sin conexión que pueden funcionar para ti, dependiendo de las circunstancias. Ten en cuenta que algunas de estas opciones requieren que Internet se configure inicialmente (por ejemplo, para descargar aplicaciones, etc.).

Comparte archivos directamente con Bluetooth, Wifi Direct o NFC

No necesitas tener una conexión a Internet para conectar tu teléfono con otro dispositivo cercano a través de Bluetooth, Wifi Direct o Near Field Communication (NFC) (a veces llamado Android Beam en dispositivos más antiguos). Bluetooth y Wifi Direct son tecnologías inalámbricas que pueden “emparejar” dos dispositivos sin otro enrutador o punto de acceso intermedio. WiFi Direct proporciona un rango más amplio y una transferencia de datos más rápida que Bluetooth, pero consume mucha más energía. Mientras tanto, NFC tiene un rango mucho más corto (~ 4 cm) y velocidades de transferencia mucho más lentas que Bluetooth o WiFi Direct, pero se conecta más rápido y usa menos energía, por lo que puede ser útil para transferencias pequeñas cuando tienes ambos dispositivos en tus manos.

Es probable que tengas funciones Bluetooth, WiFi Direct y NFC integradas en tu teléfono que se muestran en las opciones de uso compartido. Además, las aplicaciones con funciones para compartir archivos, como **Files By Google**, también integran estas tecnologías.

Importante: la desventaja de la facilidad de conexión proporcionada por estos servicios es que no son seguros. El bluetooth y los escaners de wifis se pueden usar para rastrear tu ubicación o buscar información en tu dispositivo. Los infiltrados pueden intentar emparejarse con tu dispositivo, enviarte archivos no deseados o incluso obtener el control de tu dispositivo si es vulnerable. **Para estar más segurx, desactiva estos servicios cuando no los estés utilizando y solo actívalos cuando estés en lugares seguros, limita los permisos de la aplicación solo a lo que necesitas y a quién necesitas, y practica una buena seguridad en tu teléfono, como ejecutar actualizaciones y tener una buena contraseña de acceso.**

Comparte archivos con una unidad inalámbrica o mediante una red de área local inalámbrica (WLAN)

Se puede utilizar un disco duro inalámbrico o una unidad flash para compartir archivos entre un equipo o varias personas a la vez. La unidad wifi generalmente viene con instrucciones y/o una aplicación para conectar tu teléfono a la unidad, y es relativamente fácil de usar. Recuerda establecer una contraseña en el disco por seguridad.

Si no tienes una unidad inalámbrica, también puedes compartir archivos en una unidad USB normal conectándola a un enrutador inalámbrico. Un enrutador de viaje con un puerto USB, por ejemplo, es

relativamente económico y muy portátil. Los usuarios pueden conectarse a la unidad USB a través de una red local (no se requiere internet). Para acceder a los archivos en la unidad USB conectada en tu teléfono, necesitarás usar una aplicación de administrador de archivos que pueda conectarse al almacenamiento en red, como [Solid Explorer](#). La dirección IP de tu enrutador generalmente se puede encontrar en la configuración avanzada de wifi de tu teléfono.

Mientras tanto, otra opción es [PirateBox](#), un proyecto de hágalo usted mismx que proporciona software con licencia gratuita. Los usuarios pueden compartir archivos como se indicó anteriormente, pero Piratebox les permite hacerlo de forma anónima, y también incluye funciones de chat y mensajería. Configurar un Piratebox requiere descargar, instalar y configurar algunas piezas de software. Las [instrucciones](#) están en el sitio web de Piratebox.

Actualización: el proyecto [Pirate Box](#) se está cerrando lentamente. El sitio web y el repositorio de Github todavía están en línea, pero la principal persona desarrolladora del proyecto ya no está dando mantenimiento activo.

Comunicarte a través del chat de peer to peer

Dos nuevas aplicaciones de mensajería entre pares que conocemos a través de redes activistas son [Briar](#) y [Bridgefy](#). Todavía no los hemos probado, pero conocemos a otrxs que los están probando.

[Briar](#) es una aplicación de mensajería cifrada de código abierto de extremo a extremo que no se basa en un servidor central, sino que sincroniza los mensajes entre los dispositivos de los usuarios (por lo que el contenido reside en el dispositivo de cada usuario). Se puede sincronizar incluso cuando no hay internet usando Bluetooth o WiFi (cuando hay internet, la aplicación sincroniza dispositivos a través de la red Tor). Briar también presenta grupos privados, foros públicos y blogs. Cuando se usa sin conexión, su alcance está limitado por su alcance Bluetooth o WiFi (máximo ~ 100 metros).

Mientras tanto, [Bridgefy](#) es una aplicación de mensajería cifrada de extremo a extremo (excepto cuando se usa la función de “transmisión”) que utiliza Bluetooth para enviar mensajes. A diferencia de Briar, los mensajes pueden viajar distancias más largas saltando a lo largo de una red mesh de otras personas usuarias de Bridgefy (solo el destinatarix puede leer el mensaje). Bridgefy carece de los grupos privados, foros y funciones de blog de Briar, pero tiene un modo de transmisión a través del cual puedes enviar un mensaje a hasta 7 usuarios de Bridgefy dentro del alcance, que no necesitan ser tus contactos (los mensajes de transmisión no están encriptados).

Comunicarte a través de SMS cifrados

Los mensajes de texto SMS se envían a través de redes celulares y no dependen de Internet, por lo que aún pueden funcionar durante los apagones de Internet. Sin embargo, los SMS se consideran muy inseguros. A diferencia de las aplicaciones dependientes de Internet como WhatsApp o Signal, los SMS no están encriptados de extremo a extremo. Esto significa que los mensajes de texto (y sus metadatos) pueden ser leídos por gobiernos y operadores de telefonía móvil, o interceptados

por piratas informáticos. Los SMS también pueden ser “falsificados”, lo que significa que un remitente puede manipular la información de su dirección para hacerse pasar por otro usuario.

Si necesitas usar SMS, [Silence](#) es una aplicación que encripta los mensajes SMS de extremo a extremo. Es de código abierto y utiliza el protocolo de cifrado de Signal. Si bien no lo hemos probado nosotros mismos, hemos escuchado que otros lo han usado. Tanto el remitente como el destinatario deben tenerlo instalado e intercambiar claves entre ellos. Dado que los mensajes SMS pasan necesariamente por los servidores de sus telecomunicaciones, incluso con Silence el hecho de que estás enviando un mensaje cifrado y los metadatos sobre su mensaje serán accesibles para la compañía de telecomunicaciones.

Bloqueo parcial de Internet: acceder a sitios bloqueados

Un “apagón de Internet” a menudo no significa un apagón total de Internet, sino que bloquea el acceso a sitios web específicos o plataformas de redes sociales. Los gobiernos, a través de los proveedores de servicios de Internet (ISP), pueden bloquear sitios en función de la dirección IP, el contenido o las búsquedas de DNS. ¿No estás seguro si un sitio está siendo bloqueado?

Organizaciones como [Open Observatory of Network Interference](#) y [Netblocks](#) monitorean y miden las interrupciones de internet y la censura en todo el mundo.

Afortunadamente, siempre que tengas acceso a Internet, hay algunas maneras de tratar de sortear los bloqueos parciales. Al igual que con el cifrado, ten en cuenta que eludir los sitios bloqueados puede estar criminalizado en tu país.

VPN

Una forma de evitar el bloqueo basado en IP y en contenido es utilizar una red privada virtual o VPN, como [ProtonVPN](#) o [TunnelBear](#). Cuando te conectas a través de una VPN, tu tráfico de Internet se cifra y se enruta a través de un servidor VPN en otra ubicación, como en otro país, ocultando así el verdadero destino y el contenido de tu tráfico a tu ISP.

Ten en cuenta que algunos gobiernos prohíben el uso de VPN o pueden intentar detectar y bloquear las conexiones VPN. También es importante utilizar un proveedor de VPN confiable, y preferiblemente uno que no almacene datos o registros, ya que el proveedor podrá ver tu actividad en Internet. Ten en cuenta en qué país se basa el proveedor de VPN y a qué procesos legales pueden estar sujetos según su jurisdicción. También considera que las VPN aprobadas por el gobierno pueden permitir la vigilancia e inspección de sus datos.

Servidores DNS

Los servidores DNS (“sistema de nombres de dominio”) funcionan traduciendo los nombres de dominio o URL que un usuario escribe en un navegador en las direcciones IP numéricas que Internet utiliza para identificar páginas web. Un ISP puede modificar los servidores DNS que controla para bloquear ciertas consultas o devolver una página incorrecta que dice que el sitio web

no existe. En 2014, el primer ministro turco, Recep Tayyip Erdogan, [intentó bloquear Twitter](#) durante las elecciones turcas utilizando esta técnica. [La prohibición fue frustrada](#) rápidamente por activistas que compartieron consejos paso a paso sobre cómo usar las VPN y cambiar los servidores DNS.

Puedes cambiar el servidor DNS predeterminado en la configuración de red o wifi de tu teléfono. En lugar del servidor DNS predeterminado, puedes usar servidores DNS alternativos como [Google Public DNS](#).

Estas son solo dos formas de eludir las técnicas de bloqueo más comunes. Consulta las guías de [Internet Society](#), [Access Now](#), [Security-in-a-Box](#), y [EFF](#) para obtener información más detallada.