GUÍA PARA TRABAJAR CON EVIDENCIAS DIGITALES POR LOS DERECHOS HUMANOS

TRABAJO CONJUNTO ENTRE:

TESTIGO EN LÍNEA

WITNESS SEE IT FILM IT CHANGE IT

OCTUBRE 2021

GRACIAS AL APOYO DE
DIGITAL DEFENDERS PARTNERSHIP

Este documento fue elaborado por Testigo En Línea y Witness Latinoamérica durante 2020 - 2021.

AUTORES

Indira Cornelio
WITNESS

Laura Salas
WITNESS

Danny Rayman
Testigo En Línea

Valentina Camilla
Testigo En Línea

EDICIÓN Y DIAGRAMACIÓN
Valentina Camilla

DISEÑO WEB
Quetzal Sáez

VIDEO SOBRE LA GUÍA
Joaquín Ríos

Para citar este documento puedes copiar y pegar lo siguiente:
"Camilla, V., Indira, C., Rayman, D. y Salas, L. (2021) "Guía para trabajar con evidencias digitales por los Derechos Humanos". Testigo en Línea/Witness Latinoamérica."

CONTENIDOS

GLOSARIO

A ——— ANONIMATO

Decisión de omitir elementos en el manejo de la evidencia digital que puedan volver identificable a una persona (por ejemplo: rostro, tatuajes, voz, marcas). También puede implicar la eliminación de metadata.

C ——— CÓDIGO ABIERTO

Característica de programas desarrollados con un código de fuente accesible al público para que este pueda ser visto, modificado, distribuido y auditado para acreditar su funcionamiento y confiabilidad.

E ——— EVIDENCIA DIGITAL

Archivos o registros de todo tipo que son capturados y trabajados desde distintos aparatos tecnológicos (teléfonos, cámaras, computadoras, etc).

M ——— METADATA

Se puede entender como “datos sobre los datos”. Es la información digital sobre un archivo creada automáticamente por un dispositivo electrónico o sistema. También puede agregarse manualmente luego de la creación de un archivo.

SOBRE LA GUÍA:

Cuando vivimos o presenciamos violaciones a nuestros derechos, nos encontramos con que el sistema judicial e instancias de opinión pública perpetúan estereotipos e injusticias, profundizando los daños que generan estas transgresiones y omisiones.

Contribuir a documentar estos abusos y velar por el resguardo de evidencias, nos recuerda que hay un camino para hacer justicia.

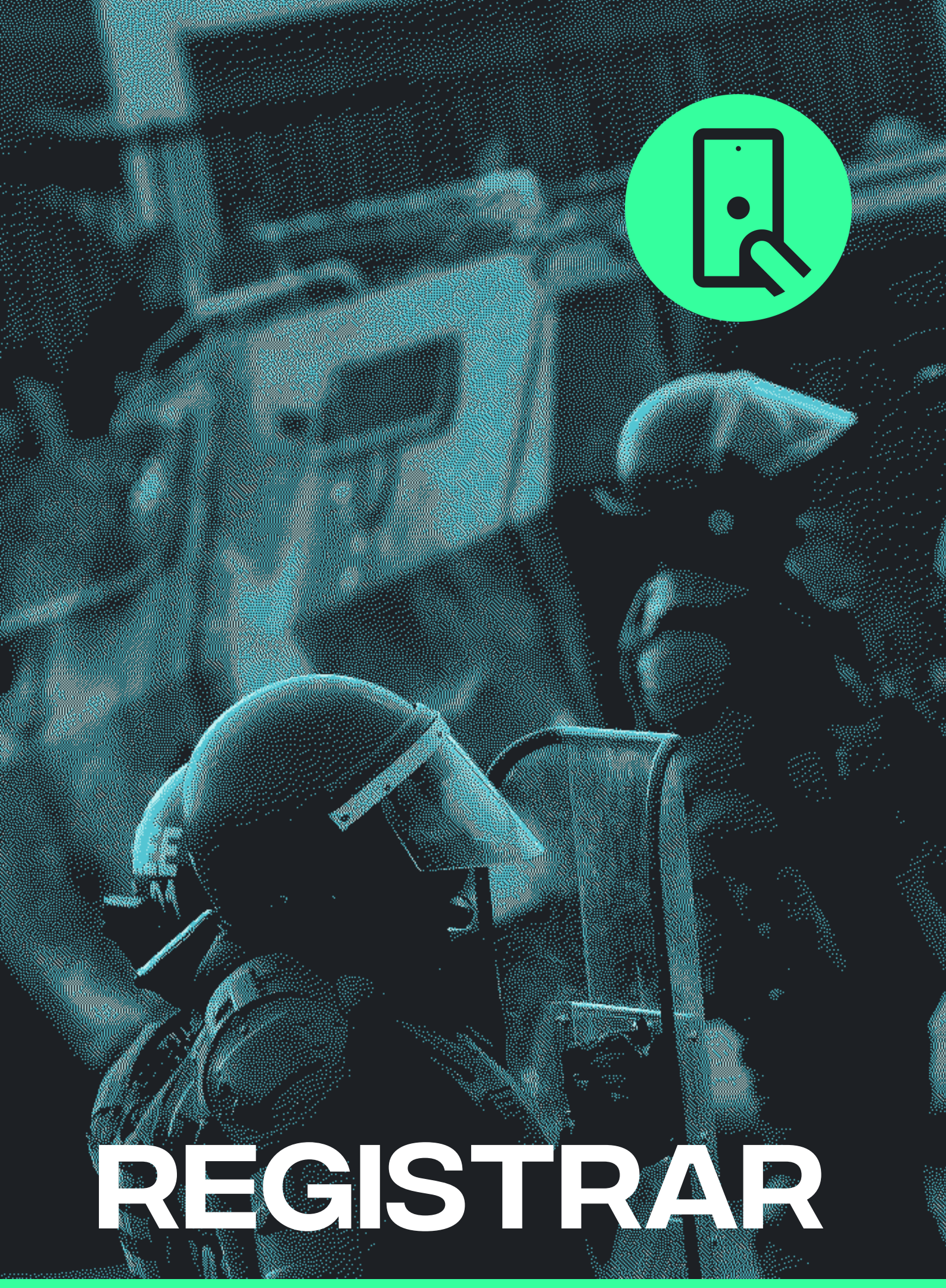
Trabajar para resguardar y recopilar material sobre violencia policial - vulneraciones a los derechos humanos, nos permite fortalecer estrategias de litigio; velar por el resguardo de evidencias; crear bases para la no-repetición y hacer justicia.

Ser parte de estos procesos nos brinda resiliencia gracias a una posibilidad y un objetivo para actuar, que tiene en consideración las versiones de los hechos desde las voces, testigos y habitantes de los movimientos sociales, alimentando consigo la memoria histórica.

Desde Testigo En Línea y Witness para Latinoamérica, creamos este insumo como una herramienta para las gestiones con evidencias digitales en miras de futuros procesos judiciales, trabajos de investigador@s, periodistas, abogad@s, comunicador@s, activistas y organizaciones sociales que luchan por la justicia y la protección de la integridad física, psicológica y emocional de las personas.

Nada de lo que está en esta guía es absoluto y varias de sus especificaciones pueden ser ajustadas a las necesidades de los contextos, territorios y herramientas disponibles.

Puedes encontrar este documento en línea aquí.


REGISTRAR

REGISTRAR

Conforme al derecho a la libertad de expresión, todas las personas tienen derecho a buscar, recibir y difundir información. Este derecho es reconocido como una garantía constitucional en Chile y como un derecho humano conforme a las obligaciones de derecho internacional de los Estados, incluido Chile.

ANTES DE REGISTRAR:

¿Realicé una evaluación de seguridad?

¿Conozco mis derechos en caso de ser detenid@?

¿Está bien configurada la fecha y hora de mi dispositivo?

¿Tengo suficiente memoria y batería en mi dispositivo?

¿Llevo baterías extra y memorias en caso de que necesite reemplazarlas?

¿Mi dispositivo cuenta con un PIN para ser desbloqueado?

¿El respaldo de mi dispositivo está sincronizado con la nube? ¿Es necesario?

¿Es conveniente activar mi GPS?

En caso de activar el GPS, ¿lo compartiré con personas de confianza?

¿Borré y/o dejé creado un respaldo seguro de la información sensible y de mis contactos en caso de ser requisado?

RECUERDA:

- Evalúa los riesgos de seguridad antes de decidir cómo configurar tu GPS de la forma que sea más seguro para ti. Si lo deseas, puedes mantenerlo encendido y disponible para personas que estén monitoreando tu recorrido por seguridad.

- También puedes optar por mantener tu dispositivo apagado en caso de que no quieras que tus llamadas y ubicación sean rastreables a través del proveedor de la red.

AL MOMENTO DE REGISTRAR:

1

Di en voz alta fecha, hora, lugar y descripción de los acontecimientos.

2

Si registras de forma anónima, puedes mostrar un papel con esta información, un reloj o la portada de un diario.

3

No realices insultos ni hables más de lo necesario mientras estás registrando. Esto puede poner en cuestión la veracidad y dificultar la comprensión de los acontecimientos.

4

Si lo estimas conveniente puedes narrar de forma descriptiva los acontecimientos.

5

Intenta recopilar los contactos de:

- Personas que se encontraban filmando
- Quienes fueron filmados
- Testigos que podrían aportar con información.

6

Si la agresión es cometida por policías, toma registro de:

- N° de oficiales
- Posiciones
- Uniformes
- Armas
- Vehículos / patentes

Al ser servidores públicos, su esfera de privacidad se encuentra limitada.

SOBRE LAS TOMAS:

Tiempo

Haz un registro de al menos 10 segundos de duración en cada toma.

Evita

Movimientos abruptos y agregar relatos o dichos que puedan anular la veracidad de tu registro.

Contexto

Realiza una toma en 360º para contextualizar el entorno y circunstancias de tu registro.

Formatos

Haz tus tomas de manera horizontal para recopilar mayor información sobre el espacio y contexto.

Tipos de tomas

Graba tomas amplias para facilitar el entendimiento de la escena y realiza tomas medias para el registro de la locación.

Detalles

Graba imágenes de cerca para mostrar detalles, elementos y personas claves en la escena.

- Considera que el ángulo desde donde grabas puede revelar donde estás ubicad@
- Intenta utilizar un trípode o alguna superficie para estabilizar tu cámara
- Aunque tengas que correr, no pares de grabar. El audio o las tomas que puedan recuperarse pueden ser útil en caso de que haya algún incidente durante tu movimiento.

RECOPILAR

RECOPILAR Y RESGUARDAR

Si vas a recopilar evidencias desde redes sociales o dispositivos, recuerda siempre conservar copias de respaldo del archivo original en dispositivos separados y en un lugar distinto de tu copia principal.

RECOPILACIÓN DESDE REDES SOCIALES

Puedes conectarte a redes sociales desde un navegador con algún VPN en tu dispositivo o desde un navegador privado.
Guarda una copia junto con el nombre del usuari@ que lo publicó, el título del vídeo y su descripción.
No alteres el archivo descargado.
Es importante que lo descargues porque puede desaparecer (sobretodo si contiene contenido explícito o controversial).
Puedes crear una cuenta anónima para realizar recolección de material sobre violaciones a los derechos humanos.
Configura la privacidad y visibilidad de tu perfil en redes sociales para resguardarte si lo consideras necesario.

RECOPILACIÓN DESDE DISPOSITIVOS

Mantén tus tarjetas de memoria a salvo de daño físico y confiscación reemplazando la tarjeta usada por una en blanco y escondiendo la usada.
Configura la protección de tu tarjeta de memoria antes de transferir el contenido.
Crea un respaldo en un servidor y dispositivo seguro.
Junto a tu respaldo, agrega una nota de texto con información sobre cada uno de los archivos.
No alteres el archivo original. Ni siquiera el nombre del archivo para crear la copia de resguardo.
Es importante que resguardes el material porque puede ser la única evidencia sobre lo ocurrido.

ARCHIVAR

ARCHIVAR

PASO A PASO

Organiza tu material una vez que puedas conectarte a un dispositivo seguro
No alteres el formato, nombres de archivo ni metadatos. Resguarda los originales.
Para no renombrar los archivos, crea carpetas y nombrarlas de manera estandarizada, tipo: **"AAAA_MM_DD_NOMBREAUTOR_DESCRIPCIÓNINCIDENTE".**
Incluye también el registro de las personas con las que has compartido el material, información de contacto o perfiles en redes sociales desde donde sacaste el material.
Crea un respaldo del material original en un disco duro externo o un servicio en línea.
Si el video te fue entregado por otras personas, acompaña el respaldo de los registros con una "cadena de custodia" donde indiques la forma en que obtuviste el material.

HERRAMIENTAS PARA RECOPILAR Y ARCHIVAR MATERIAL

Youtube-dl

Programa para descargar videos de plataformas como YouTube, Facebook, Twitter, entre otras.

Tella

App gratuita de Android para documentar evidencia de forma segura incluye cifrado y modo de recolección de metadatos para hacer archivos verificables.

ExifTool

Herramienta de línea de comandos que muestra metadatos incrustados en archivos de fotos y videos, y permite agregar metadatos.

OnionShare

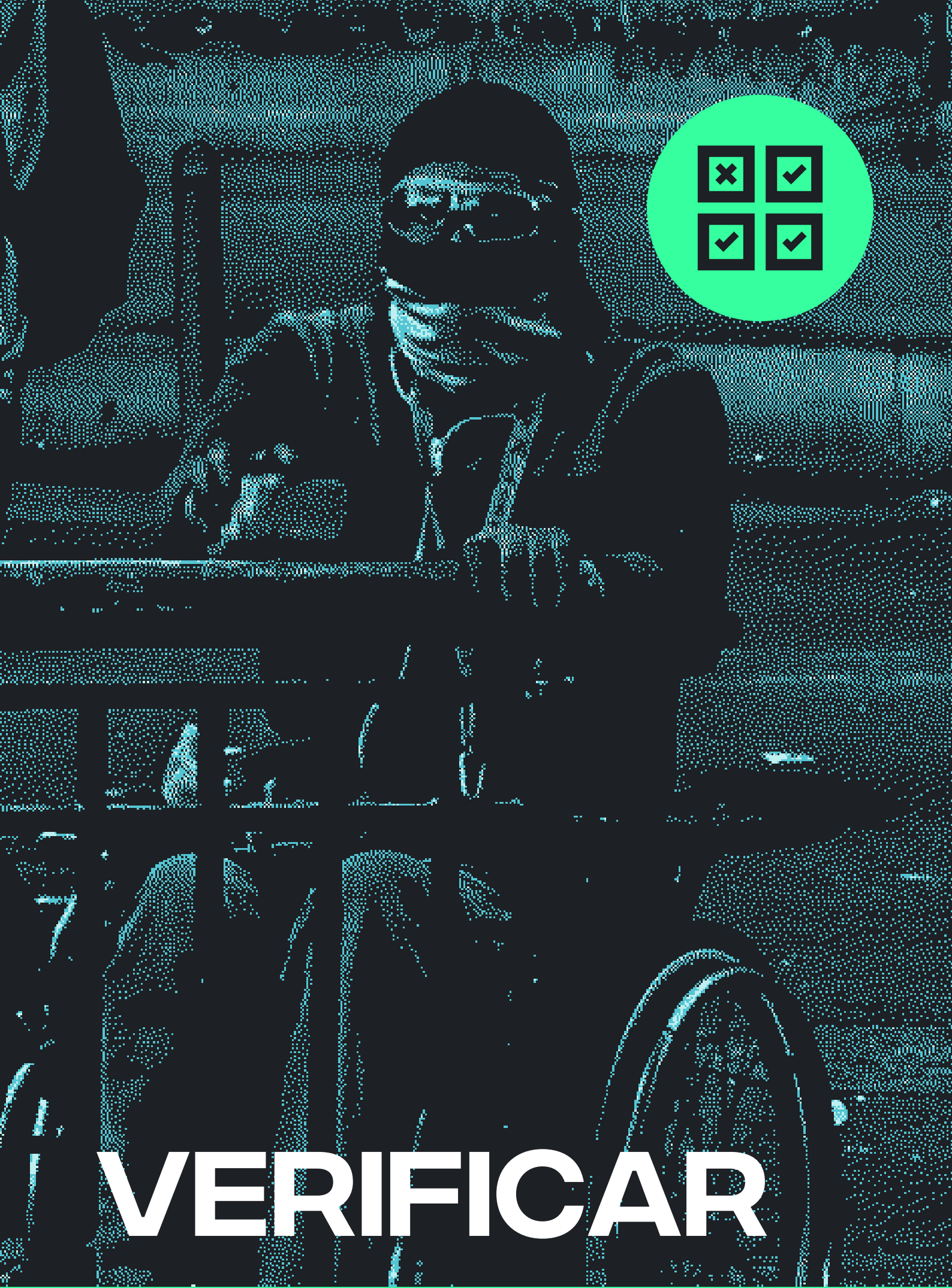
Transferencia de archivos pesados en línea desde computador.

MediaInfo

Muestra metadatos incrustados en archivos de video y audio.

Micro-tesauros

Terminología para categorizar diferentes aspectos de las violaciones de derechos humanos de manera consistente, para la compatibilidad y uniformidad en el registro.


VERIFICAR

VERIFICAR

El proceso de verificación es clave para el trabajo de periodistas; medios; observador@s de derechos humanos; investigador@s; analistas y abogad@s que requieren de la veracidad de la evidencia para utilizarla como herramienta a favor de: la reconstrucción de hechos; la visibilización de la violencia o ante la búsqueda de justicia.

AL MOMENTO DE VERIFICAR, RECUERDA:

No todos los materiales podrán ser verificados a pesar de ser auténticos.
Revisa los registros con escepticismo. Es común que personas suban contenido antiguo a plataformas con un nuevo título y descripción.
Mientras más te acerques al archivo original, más probable es que puedas confiar en que la descripción que contiene es correcta.
Recuerda que el material subido a una plataforma puede perder parte de los metadatos originales.
Los videos editados son más difíciles de verificar ya que pueden hacer falta detalles claves, esto porque registros de diferentes contextos pueden ser compilados juntos.
El agregar texto, música y gráficos puede poner en cuestión la autenticidad del material y/o poner en duda a sus espectador@s.
Si lo necesitas, puedes realizar un llamado público para recolectar material y así complementar la información recopilada.
Documenta y guarda junto con los archivos el proceso de cómo determinaste la veracidad del material.
Si el material no se recibe directamente de la fuente primaria quizás será imposible verificar dónde fue realizado el registro, es por esto que debes complementar la verificación con otros videos e imágenes de Internet.
La fecha y hora que se muestra puede no ser la misma de la zona horaria donde está ubicada la persona que comparte el material, sino la zona horaria donde se encuentran las oficinas de la plataforma a dónde se cargó el material.
En lo ideal trabaja con material sin editar.

ALGUNAS PREGUNTAS PARA LA VERIFICACIÓN:

- [ ] ¿El material aparece en artículos antiguos disponibles en línea?
- [ ] ¿Quién lo publicó tiene alguna buena razón para compartir el material original?
- [ ] ¿Hay otro material en línea que se refiera al mismo hecho?
- [ ] ¿Quién publica el material es un usuari@ nuev@? ¿o no?
- [ ] ¿Es posible saber desde cuando comenzó a publicar material en redes la persona que lo compartió?
- [ ] ¿La persona está afiliada a alguna causa o agenda política?
- [ ] Si la identidad de la persona que tiene el registro es pública, ¿corre algún riesgo su integridad?
- [ ] A simple vista ¿El material cuenta con efectos especiales?

Al utilizar contenidos de fuentes abiertas, recuerda analizar los impactos éticos y de privacidad que podrían producirse al publicar material que pueda perjudicar o generar riesgos para terceros o víctimas de violaciones a los derechos humanos.

HERRAMIENTAS PARA LA VERIFICACIÓN

Buscadores de imágenes en Internet

Búsqueda inversa de imágenes.

Google Imágenes

Yandex Imágenes

Tineye

Bing Imágenes

InVid / WeVerify

Búsqueda inversa en múltiples buscadores.

Google Earth

Para consultar el historial de imágenes en distintas fechas, meses o años. Se muestran imágenes satelitales desde diferentes ángulos y calidades.

Buscador de datos de Amnistía Internacional en YouTube

Extracción de previsualizaciones y búsquedas de imagen en Google.

Weather Underground

Clima de una determinada ubicación en una fecha y hora en específico.

Google Maps

Para revisión de mapas, fotos satelitales y vistas de calle para encontrar referencias.

SunCalc

Para la obtención de referencias horarias acorde a la luz, las sombras, la ubicación del sol o la luna.

A CONSIDERAR:

- Puedes revisar más herramientas para la verificación en esta guía práctica de la Red Internacional de Periodistas.
- Sé cautelos@ con un video de baja calidad o con baja iluminación, ya que la falta de claridad visual o de audio puede hacer más difícil que el espectador note la edición de un video manipulado.
- Un/@ espectador@ puede verificar la fecha, hora y ubicación de un video, pero puede ser casi imposible determinar si la acción que se muestra en el video fue actuada o auténtica.
- L@s espectador@s que están familiarizados con la región, problemáticas locales o el idioma pueden encontrar alertas si es que estás frente a un video manipulado.
- A medida que la tecnología avanza en torno a la manipulación de videos -como la generación de multimedia sintética a través de deep fakes- se necesita contar con mayor preparación para identificar falsificaciones de videos de formas más sofisticadas y personalizadas. Aprende más al respecto haciendo click aquí.
- Puedes utilizar contenido publicado en redes sociales para corroborar el acontecimiento que aparece documentado en los materiales disponibles. En ese caso, asegúrate de que los reportes sean independientes y no te confíes solamente de una fuente.
- Si varias personas fueron testig@s del incidente, es probable que con el transcurso de las horas haya más reportes disponibles en línea.
- Por último, recomendamos el curso Investigaciones de Derechos Humanos con fuentes abiertas producido por Amnistía Internacional y el el Protocolo de Berkeley para Investigaciones de Fuentes Abiertas de Archivos Digitales donde se entregan las primeras directrices globales sobre el uso de fuentes abiertas para ser usadas como pruebas en investigaciones internacionales en casos relacionados a violaciones de derechos humanos y derecho humanitario.

TRANSFERIR

TRANSFERIR

ALMACENAMIENTO

TRANSFERENCIA EN LÍNEA

El almacenamiento en la “nube” es sencillo de usar y se ha masificado debido a la transferencia de archivos vía Google Drive y Dropbox, pero estos medios poseen peligros potenciales y límites de almacenamiento restrictivos.

TRANSFERENCIA DIRECTA

La forma más común de almacenar y enviar un archivo directamente a alguien es vía correo electrónico, pero cuando se trata de video, ese método puede ser extremadamente lento y limitado por la cantidad y tamaño de los archivos.

TRANSFERENCIA FÍSICA

La forma más segura de almacenar y compartir tu video es ir en persona (o enviar un aliad@ de confianza) y transferir el video desde tu computadora o disco duro a la de tu contacto. También puedes entregar o enviar por correo una tarjeta SD, unidad flash o disco duro, siendo estas las formas más seguras y sencillas de transferir archivos entre distancias cortas.

SERVICIOS

TRANSFERENCIA EN LÍNEA

La mayoría de los servicios populares no cifran adecuadamente sus archivos. Cuando estos servicios tienen cifrado, a menudo almacenan las claves, por lo que pueden acceder a tus archivos y podrían llegar a entregarlos a alguna autoridad que lo solicite.

TRANSFERENCIA DIRECTA

Un servicio de transferencia práctico es BitTorrent Sync, basada en el protocolo BitTorrent, permitiendo una variedad de opciones para compartir información encriptada y privada, requiriendo que ambos dispositivos estén encendidos para hacer la transferencia. Sin embargo es importante considerar que no es de código abierto lo que implica que su código no puede ser auditado públicamente por fallas de seguridad.

Si quieres utilizar una herramienta de código abierto puedes recurrir a Sharedrop.io.

TRANSFERENCIA FÍSICA

Investiga en internet si el disco duro externo que tienes o vas a adquirir cuenta con opción para cifrar, la calidad del cifrado y de qué forma lo ofrece.

HERRAMIENTAS

TRANSFERENCIA EN LÍNEA

Para que compartir en la nube sea más seguro, intenta usar herramientas complementarias, cambia a proveedores de almacenamiento en la nube de "protocolo de conocimiento cero" que estén diseñados desde una perspectiva de privacidad.

TRANSFERENCIA DIRECTA

Para personas que trabajan a poca distancia, el uso de Bluetooth, WiFi Direct y otras tecnologías de comunicación de campo cercano (NFC) son opciones seguras y simples, pero funcionan mejor si solo está moviendo un número limitado de archivos más pequeños. Ten en cuenta desactivarlos cuando no estén en uso, o no utilizarlos en escenarios inseguros, por ejemplo cuando estés cerca de personas en quienes no confías.

TRANSFERENCIA FÍSICA

Si la persona u organización con la que estás compartiendo imágenes se encuentra cerca y es accesible, es factible entregar los archivos de manera física.

CONSIDERACIONES

TRANSFERENCIA EN LÍNEA

Puedes configurar un servidor autónomo donde los archivos estén resguardados y puedan ser subidos de forma anónima.

TRANSFERENCIA DIRECTA

La transferencia directa de archivos grandes de una persona a otra siempre ha sido difícil en la web y, a menos que tengas alojamiento web o puedas ejecutar tu propio servidor, sigue siendo un desafío.

TRANSFERENCIA FÍSICA

Una conectividad deficiente, el conocimiento técnico limitado entre l@s soci@s involucrad@s en una transferencia o las preocupaciones de seguridad pueden empujarte hacia la opción probada y verdadera de transferir archivos sin conexión.


PUBLICAR

PUBLICAR

- Antes de cualquier difusión o intercambio del material, la seguridad y la ética son lo primero.
- Publicar material sobre abusos, violencia explícita o violación de derechos humanos en línea puede hacer que tú o las personas/comunidad que registraste enfrenten represalias o se expongan a algún riesgo.
- Resulta clave considerar tu responsabilidad frente a las personas que fueron registradas, con quienes registraron y la audiencia que puede encontrarse con el material. Al momento de publicar cualquier contenido en línea pierdes el control sobre quién lo puede ver y cómo puede llegar a ser utilizado.

1

ÉTICA Y PRIVACIDAD

- Evalúa si la difusión del material podría dañar la privacidad, dignidad o retraumatizar a las personas afectadas.
- Si tienes el registro de una agresión, consulta con la víctima y sus familiares lo que consideran pertinente realizar con el material.
- Revisa tu configuración de privacidad y datos personales en redes sociales previo a la publicación de algún material para evitar exponerte a hostigamientos de cualquier tipo.

2

ANONIMATO

- No etiquetes en tus publicaciones a personas que identifiques en el registro a menos que cuentes con su autorización.
- Si estás realizando activismo anónimo, considera borrar los metadatos y anonimizar tu huella digital en Internet antes de publicar.
- Puedes compartir material de forma anónima a través de un/@ periodista, abogad@ u organización de confianza.

3

PLATAFORMAS

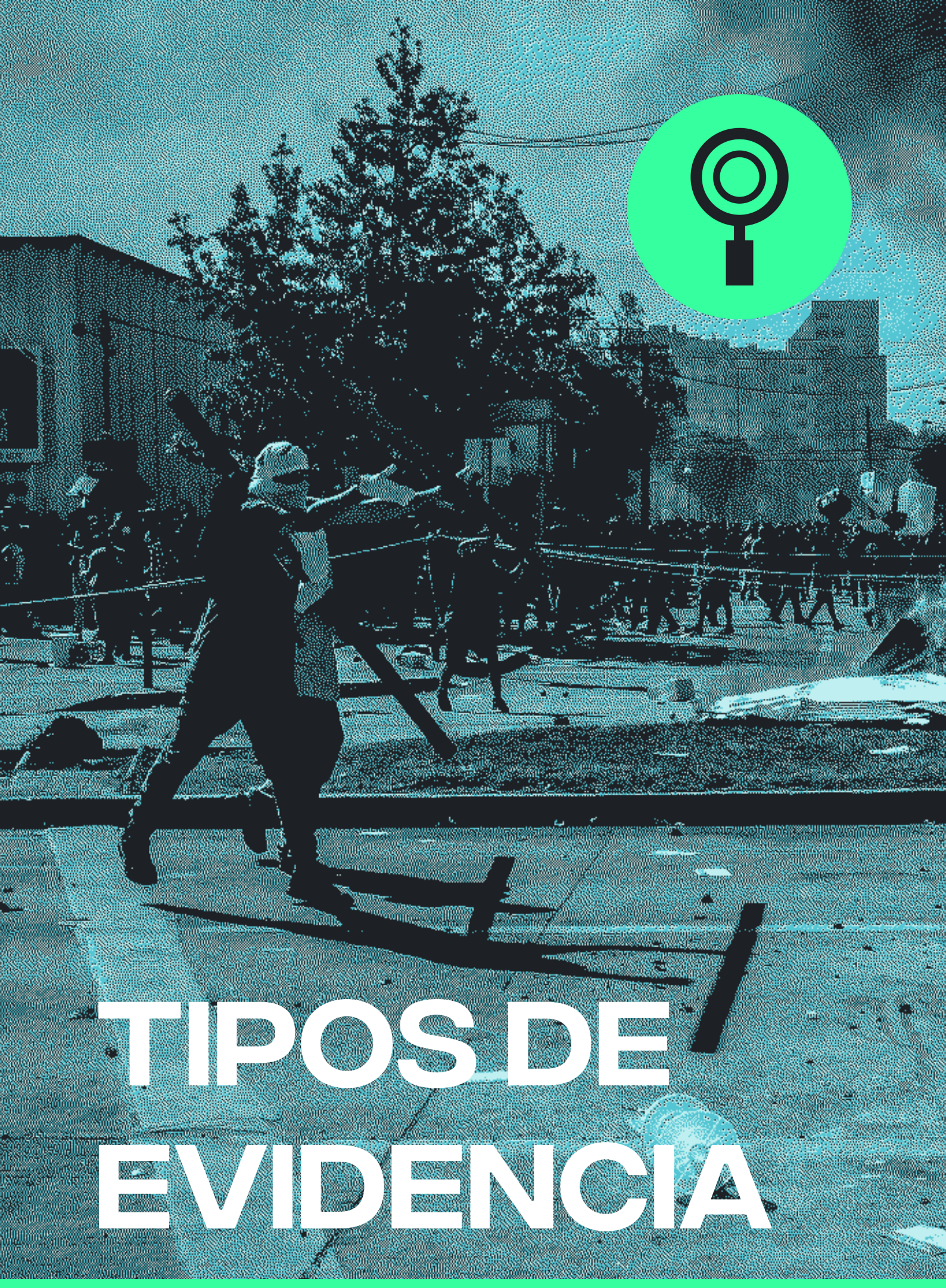
- Conserva el archivo original. Los sitios como YouTube mejoran los archivos de video para su transmisión en la web, lo que implica que el video es comprimido y se le despoja de información.
- Puedes usar herramientas como el blur de YouTube para proteger identidades. Si el riesgo es alto distorsiona el audio o cualquier característica que pueda identificar a las personas que necesitan del anonimato.
- Si editas tu video no incluyas música ya que puede ser censurado por incluir contenido con derechos de autor.

4

AL PUBLICAR

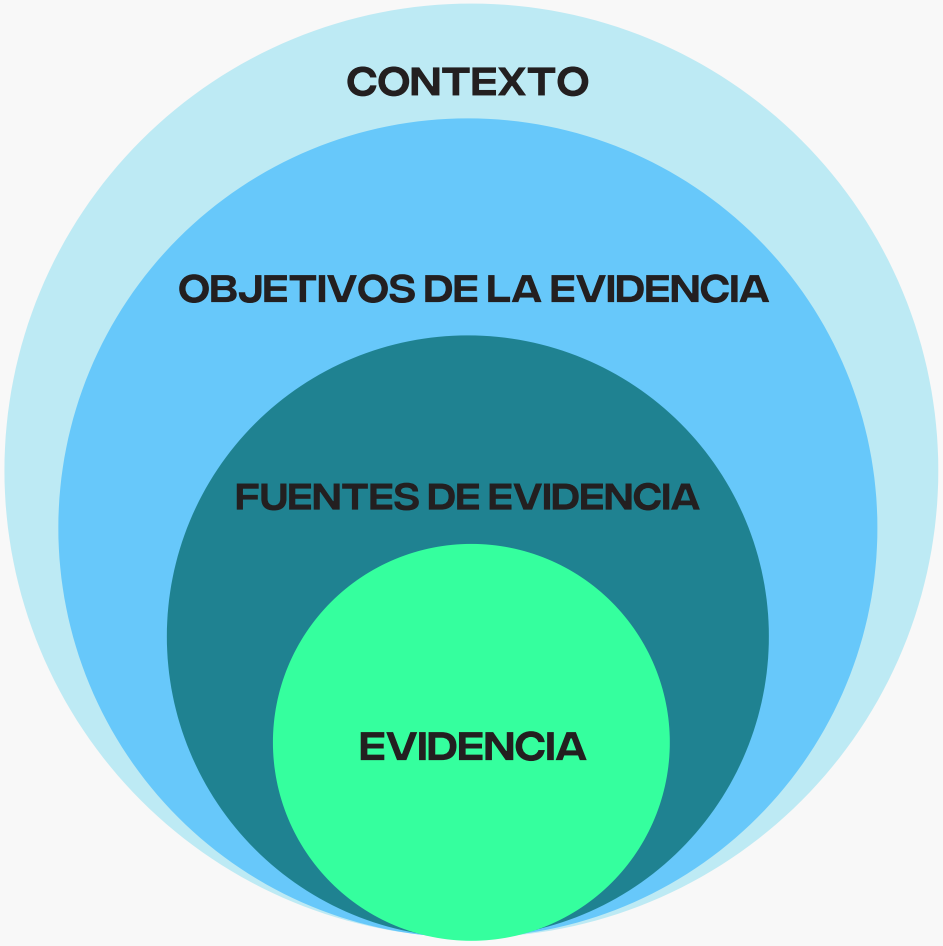
- Toma nota de correos electrónicos o contactos de las personas involucradas en los hechos para re-enviar el material.
- Indica en el título que el material es evidencia de violaciones a los derechos humanos. Esto ayuda a alertar a quienes vean el material y deja evidencia frente a la plataforma que es información valiosa para que no sea bajado de Internet.
- Al postear, debes incluir un título adecuado y claro junto con una descripción detallada de la fecha, hora, lugar y palabras descriptivas claves.

- Utiliza una hoja de cálculo o una base de datos para llevar un seguimiento de dónde almacenas los registros y con quien los compartes
- Para que tu material se utilice como parte de una investigación, deberás entregárselo a investigadore@s de derechos humanos.
- Si no tienes seguridad de quién es el agresor, no difundas información personal vinculando a alguien como autor de lo ocurrido.
- A modo de estrategia: Si vas a publicar el material, considera esperar a que las autoridades compartan su versión de los hechos antes de publicarlo. Esto ya que una vez publicado podría ser utilizado para rectificar las narrativas falsas presentadas por algún medio de comunicación o entidad de gobierno.



TIPOS DE EVIDENCIA

TIPOS DE EVIDENCIAS



01 EVIDENCIA	Información recopilada, guardada o difundida que puede ser utilizada como prueba en un proceso judicial.
02 FUENTES DE EVIDENCIA	Una prueba puede provenir de distintas instancias, como por ejemplo: Fuentes abiertas; Análisis técnico forenses; Documentos; Testimonios; Imágenes.
03 OBJETIVOS DE LA EVIDENCIA	Las pruebas pueden ser: Pruebas deductivas; Pruebas de carácter; Pruebas de aviso; Pruebas exculpatorias; Pruebas relacionadas con el delito; Pruebas de vinculación; Pruebas suficientes a primera vista; Pruebas corroborativas; Pruebas contextuales.
04 CONTEXTO	Para que las evidencias sean consideradas en su contexto, deben ser (1) RELEVANTES porque ayudan a probar un elemento en un presunto crimen; prueban o refutan un hecho; no son prejuciosas (2) FIABLES, caracterizándose por ser Auténticas, verificables; y tener una cadena de custodia comprobada.

TIPOS DE EVIDENCIAS

Situaciones sobre las que recae la evidencia	Tipos de evidencias que grafican el "quién y cómo"
• Lesiones • Atropellos • Personas golpeadas por funcionarios • Personas rociadas con productos químicos por funcionarios • Daños a la propiedad civil • Daños a bienes culturales • Discursos de odio • Niñ@s portando armas • Torturas • Muertes	• Formaciones policiales en protestas ; tropas. • N° de placa y uniformes • Matrículas de vehículos oficiales • Equipo militar (incluido el serial de números) • Puntos de control • Documentos • Videos de documentos • Discursos • Pasaportes u otra identificación oficial • Instalaciones ocupadas y abandonadas • Equipo de comunicaciones; satélites; platos; radios; etc.

RECUERDA: Es importante proporcionar a tus contactos de confianza el video original que no ha sido modificado en ningún momento.

Para que la información pase a ser evidencia legal para ser utilizada en un juicio y sea aceptada por un tribunal, el material debe tener dos características clave: ser confiable y relevante para luego ser puesta en contexto.

¿DE QUÉ FORMAS PUEDE SER UTILIZADA LA EVIDENCIA?

Prueba principal

Información inicial que apunta a un delito y nos permite realizar una conjetura informada sobre lo que pudo haber sucedido en un determinado incidente.

Presunta evidencia

Información que permite establecer o presumir cierto hecho clave a menos que sea refutado.

Evidencia corroborativa

Información que respalda o verifica evidencia ya existente; también conocida como información de respaldo.

Prueba inferencial

Información que nos permite hacer una conjetura fundamentada sobre la intención del perpetrador, la cual debe ser corroborada.

Prueba de carácter

Información que da fe de la posición moral, la naturaleza general, los rasgos, las características y la reputación de un individuo en la comunidad.

Prueba exculpatoria

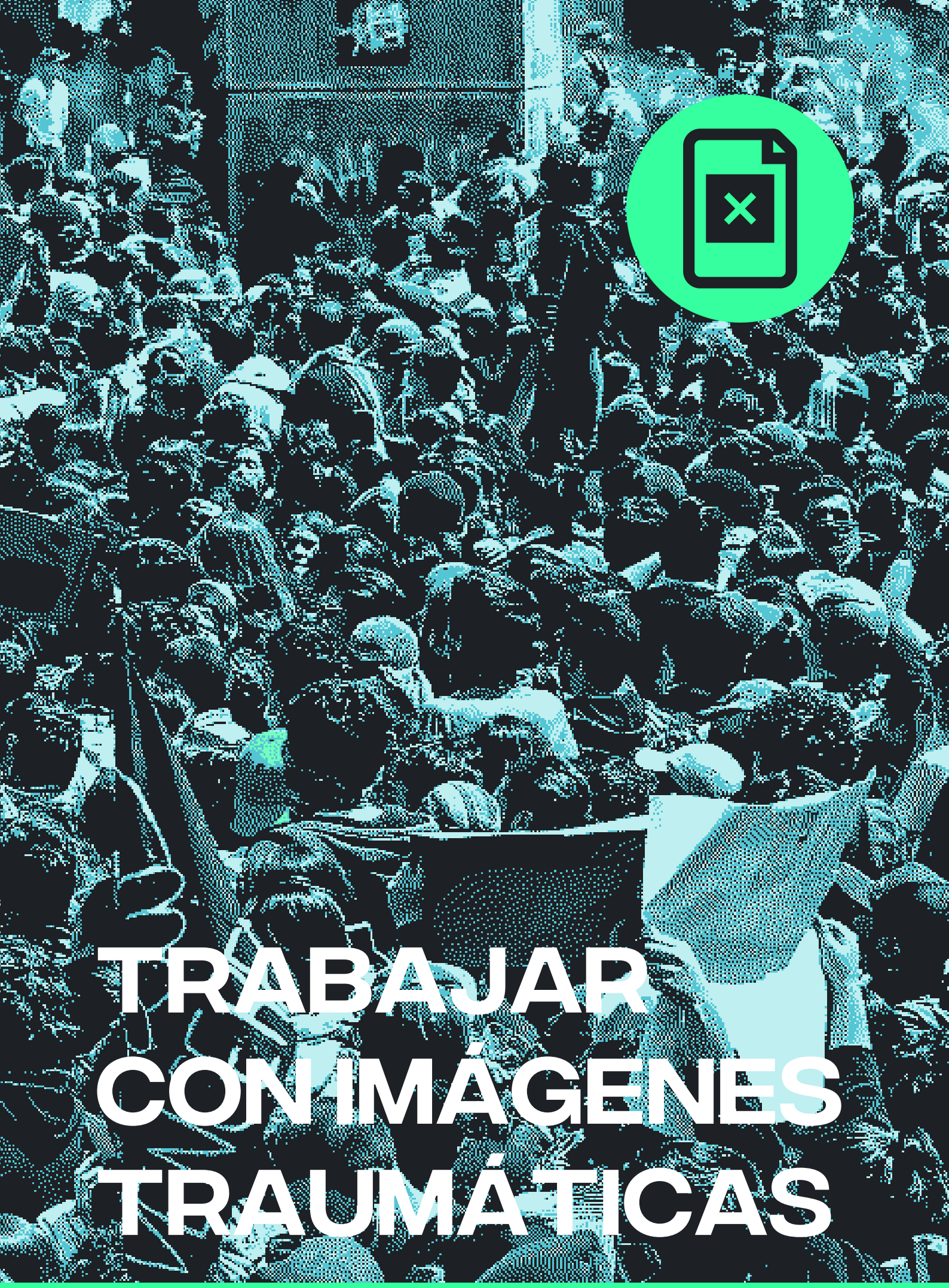
Información que ayuda a probar que un acusado es inocente o no tiene la intención de cometer un delito.

Evidencia sobre responsabilidad por el mando

Información que prueba que un comandante militar o un líder civil recibió información que aseguraba que sabían, o debían haber sabido, que las personas sobre las que tenían autoridad estaban cometiendo delitos.

Evidencia contextual

Información que permite a un juez o un jurado comprender mejor la atmósfera, la ubicación geográfica o el clima político en el que los hechos ocurrieron.



TRABAJAR CON IMÁGENES TRAUMÁTICAS

TRABAJAR CON IMÁGENES TRAUMÁTICAS

El trabajo con material asociado a violaciones a los derechos humanos implica una exposición a imágenes de contenido explícito, discriminación, discursos de odio y material pertubador.

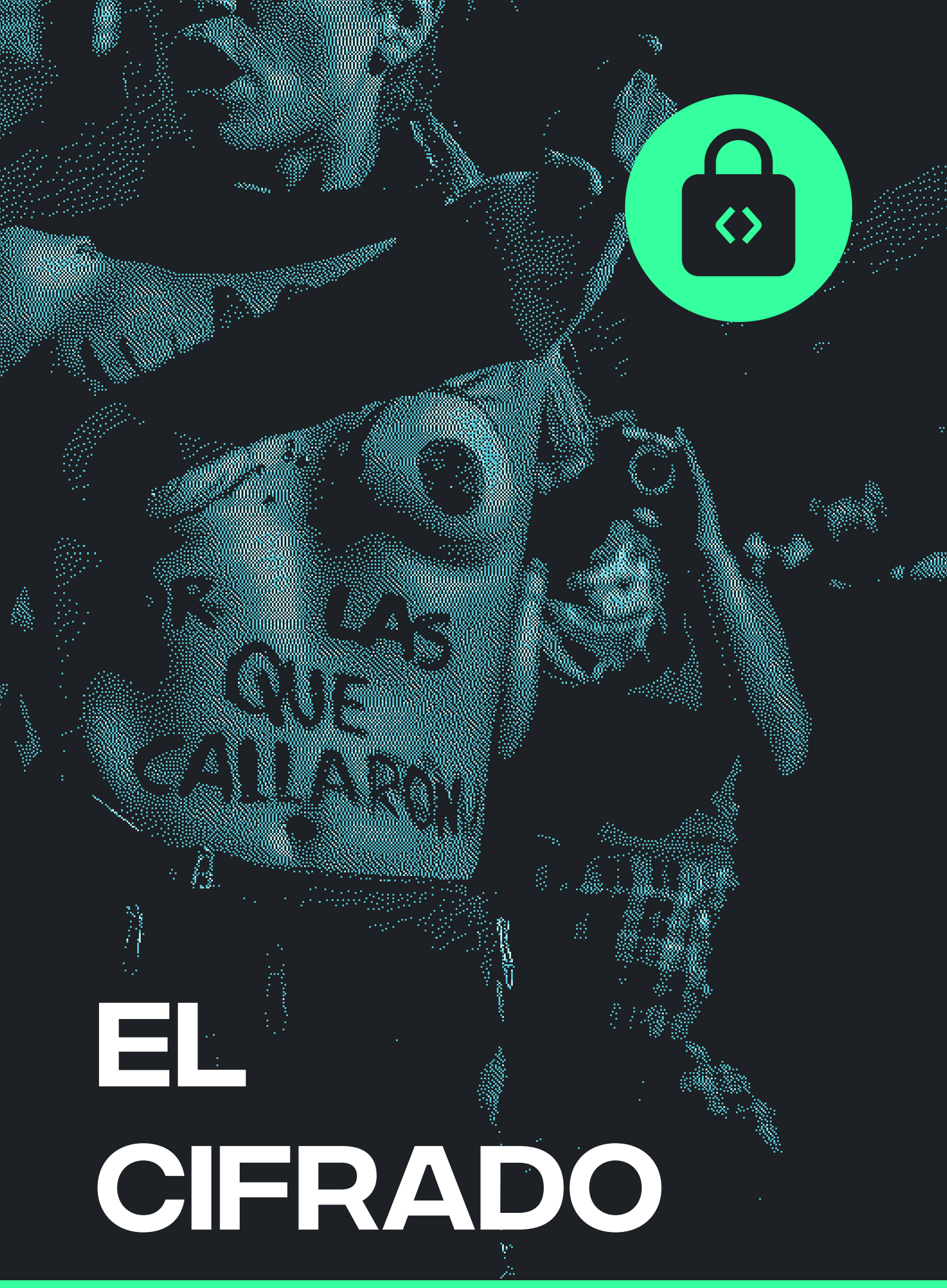
La frecuente exposición a este material puede traer consigo afectaciones a la salud mental y síntomas de trauma secundario el cual según las definiciones del Human Rights Center de la Universidad de Berkeley implica "una reacción adversa al residuo emocional de la exposición al dolor y sufrimiento de los sobrevivientes del trauma".

Entre los síntomas se puede observar: no dormir; dormir demasiado; no comer; comer demasiado; beber o consumir drogas en exceso; no realizar actividades frecuentes con amigos; irritabilidad y mal genio; incapacidad para disfrutar de las actividades normales de la vida.

Desde el Human Rights Center, indican que un trauma secundario no es solo una respuesta emocional esperada frente a algo desafiante, tampoco es un trauma o un síndrome de estrés postraumático.

En la misma línea de acción, es que el Centro DART para el Periodismo y el Trauma hace las siguientes recomendaciones para personas que trabajan con material traumático:

- [ ] Dimensionar el tipo de material con el que estás trabajando y los impactos que puede tener en tu bienestar.
- [ ] Asegurar tiempo de inactividad dentro de tu trabajo.
- [ ] Eliminar la exposición innecesaria.
- [ ] Establecer pautas claras sobre cómo se almacena y distribuye el material gráfico.
- [ ] Revisar los procedimientos de clasificación, organización y etiquetado de los archivos y carpetas digitales para reducir la visualización innecesaria.
- [ ] Experimentar con diferentes métodos para generar cierta distancia en la forma en que se revisa el material.
- [ ] Apagar el sonido cuando puedas, esto suele ser lo que más afecta del material revisado.
- [ ] Ajustar el entorno de visualización. Para esto puedes probar con reducir el tamaño de la ventana, ajustar la resolución de la pantalla o brillo para disminuir el impacto percibido.



EL CIFRADO

CIFRADO

El cifrado es un método que permite aumentar la seguridad de un mensaje o archivo mediante la codificación del contenido para que sólo pueda ser leído por quien tenga la clave para descifrarlo.

La seguridad siempre debe ser una prioridad cuando se trata de evidencias digitales. Por ello, intenta incluir el cifrado y el anonimato en tu flujo de trabajo.

Acá puedes consultar algunos tipos que pueden ser útiles para tu trabajo con evidencias digitales:

TIPOS DE CIFRADO

Cifrado de disco completo

Creación de volúmenes cifrados en tu dispositivo de almacenamiento externo.

Cifrado desde el sistema operativo

Compatibles para funcionar en PC, Mac, Linux, Android e iOS; sólo asegúrate de consultar las últimas actualizaciones de seguridad de los sistemas.

Cifrado en dispositivos móviles

Los dispositivos Android tienen una opción de cifrado en la configuración, aunque podría llegar a ralentizar el dispositivo (acorde a la cantidad de información que poseas). No hay una manera fácil -salvo un reinicio- de desactivar el cifrado en caso de perder la contraseña.

Cifrado de archivos individuales

Uso del estándar PGP desde tu correo electrónico pero requiere que todas las personas involucradas en la transferencia tengan las claves PGP configuradas y disponibles entre sí, por lo que se necesita un poco de preparación. Estas mismas llaves pueden utilizarse también para hacer el cifrado de los archivos dentro de tu propio equipo.

HERRAMIENTAS PARA EL CIFRADO

Gpg4win

Cifrado de mails y archivos para Windows

FileVault

Cifrado del disco duro de arranque de Mac

Bitlocker

Cifrado para Windows

GPGTools

Cifrado de mails y archivos para Mac

Android Privacy Guard (APG)

De las mejores opciones para usar PGP y cifrar archivos en Android.

LA SEGURIDAD DIGITAL

LA SEGURIDAD DIGITAL

La creación de una estrategia de seguridad digital -básica- es un proceso que requiere de:

1. Dimensionar el nivel de exposición en el que te encuentras, acorde a las labores que realizas.
2. Identificar la exposición a la que están sometidos tus dispositivos.
3. No olvidar lo delicada que puede llegar a ser la información que manejas en tus dispositivos.
4. Incorporar herramientas de seguridad digital proporcionales a tus usos.

En este apartado compartimos herramientas prácticas y consejos generales para comenzar a integrar aspectos de autocuidado digital en el contexto de defensa y observación de derechos humanos:

RECUERDA SIEMPRE:

- Revisar los términos y condiciones, junto con los permisos que le has otorgado a las aplicaciones para funcionar.

- Desinstalar aplicaciones que no utilizas ya que usan espacio en tu dispositivo y registran datos aunque no las utilices, intercambiando así información entre sí para ofrecer experiencias de anuncios y servicios más personalizada y no siempre bajo tu consentimiento.

- Utilizar contraseñas seguras distintas para cada cuenta, que incluyan al menos 8 caracteres, mezclados entre números, letras y símbolos. Estas no deben incluir información personal, ser predecibles, ni otra persona debe conocerlas.

- Revisar los permisos que les has otorgado a las aplicaciones. Puedes (1) desactivar los permisos que no son necesarios para que la aplicación tenga para funcionar (2) activar la opción para que funcionen solo mientras la App esté en uso.

HERRAMIENTAS DE SEGURIDAD DIGITAL

Terms of service: Didn't read

Análisis de medidas de seguridad y tratamiento de datos

Protonmail

Mail cifrado y seguro

GPGTools

Cifrado de mails y archivos para Mac

Open PGP

Cifrado de mails

Tor

Navegación segura

DuckDuckGo

Buscador privado

Jitsi

Videoconferencias seguras

Sync

Nube de almacenamiento seguro y cifrado

OnionShare

Transferencia de archivos pesados en línea desde computador

Tutanota

Mail cifrado y seguro.

NetxCloud

Alternativa a Google Drive

Mailvelope

Cifrado de mails

HERRAMIENTAS DE SEGURIDAD DIGITAL

RiseUpVPN

Ocultamiento de nuestro número IP al navegar.

OpenVPN Connect

Ocultamiento de nuestro número IP al navegar

KeePass

Almacenamiento y generador de contraseñas

Strongbox

Almacenamiento y generador de contraseñas para iOS y MacOS

Tresorit

Nube de almacenamiento seguro y cifrado

Etherpad

Alternativa a Google Docs

Orbot

Ocultamiento de nuestro número IP al navegar para Android

Authy

Creación de contraseñas dinámicas para procesos de autenticación en dos pasos

Have I Been Pwned?

Plataforma para chequear filtraciones de datos desde cuentas personales

How Secure Is My Password?

Verificar la seguridad de tus contraseñas acorde al tiempo que podría tardar alguien en descifrarla

EN CASO DE VIVIR ALGÚN TIPO DE HOSTIGAMIENTO EN LÍNEA :

- Construye una minuta o bitácora en donde registres: URL de la cuentas, registros disponibles, plataforma en que ocurrieron los hechos, fecha y hora.
- No borres los mensajes recibidos.
- Reporta las cuentas y bloquéalas.
- Toma nota del número del reporte que realizas a la plataforma. Esta información es entregada por algunas de las plataformas.
- En TWITTER puedes bloquear la cuenta o denunciarla por ser una cuenta abusiva; en FACEBOOK puedes denunciar un perfil por discursos de odio o por ser abusivo; en INSTAGRAM puedes reportar otra cuenta por spam o por ser inapropiada; en WHATSAPP bloquea el número desde la App y luego desde tu teléfono.
- Revisa con regularidad las normas comunitarias de las plataformas para más información respecto a sus condiciones y protocolos.
- Recuerda que proveer información sobre el contexto de lo ocurrido dentro de los formularios también puede ayudar a que se atienda de mejor forma tu solicitud.

Puedes utilizar de referencia la guía de sursiendo.org sobre Registro de Incidentes como práctica de mitigación del riesgo.

Si una persona que conoces vive hostigamiento en línea puedes revisar Take Back The Tech, Acoso.online.

¿TE PARECIÓ ÚTIL ESTA GUÍA?

¿TE GUSTARÍA COLABORAR CON TUS SABERES PARA PODER OPTIMIZARLA?

¡CONTÁCTANOS!

TESTIGO ENLINEA

@testigoenlinea

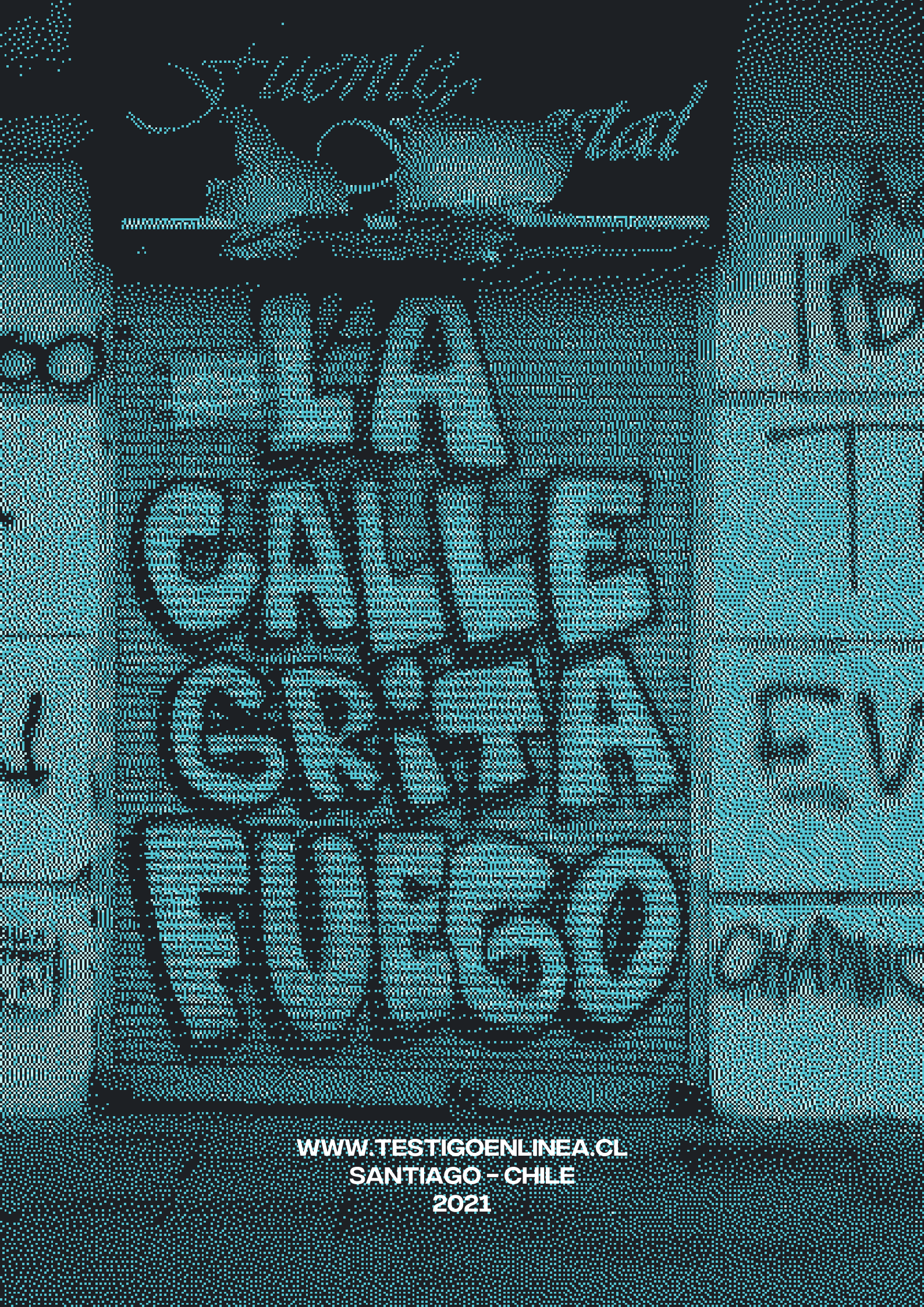
@testigoenlinea

WITNESS
SEE IT FILM IT CHANGE IT

@witness_es

@witness_es

facebook.com/witnessespanol


Stanley Kubrick
WWW.TESTIGOENLINEA.CL
SANTIAGO - CHILE
2021